Odessa I.I. Mechnikov National University, Odessa

3d International Conference on Computer Algebra and Information Technologies

August 20 – 25, 2018
Odessa, Ukraine

PROCEEDINGS

Одеський національний університет імені І.І. Мечникова, Одеса

ІІІ Міжнародна Конференція "Комп'ютерна Алгебра та Інформаційні Технології" CAIT-Odessa-2018

20-25 серпня 2018р.

Одеса, Україна

ПРАЦІ

Одеса
Видавець М. О. Бондаренко
2018

ББК 36.973.2-018.431

УДК 004.4:519.61(061)

3d International Conference on Computer Algebra
К 637 and Information Technologies.
August 20 – 25, 2018, Odessa, Ukraine. Abstracts. − Odessa:
Bondarenko M., 2018. − 198 p.

III Міжнародна Конференція"Комп'ютерна алгебра
К 637 та інформаційні технології".
20-25 серпня 2018 року, Одеса, Україна. Праці конференції. - Одеса:
Бондаренко М.О., 2018. - 198 с.

ISBN 978-617-7613-18-2

C O N T E N T S
З М І С Т

The ***Odessa Competence Center for Artificial intelligence and Machine learning*** (***OCCAM***) is a private non-profit research laboratory, whose mission is to advance both fundamental research and practical application in the fields of artificial intelligence and machine learning. The fundamental research is focused on so-called Artificial General Intelligence (AGI), which refers humanity's long term dream of constructing thinking machines that can solve a wide range of tasks without being specifically programmed for any of them.

Specifically, our research is focused on general approaches to inductive reasoning, which is related to data compression. We use the language of algorithmic information theory in order to derive efficient induction algorithms, which can then be used to guide intelligent action. We also develop new ways of grounded reasoning about data without the usage of formal logic. On the practical side, we develop a Python-based system for data compression that implements and tests the theoretical insights.

OCCAM is a small and dynamic team that welcomes both young and advanced researchers in the fields of information theory, Kolmogorov complexity, artificial intelligence as well as competent software engineers.

Provectus — это IT-компания, которая занимается разработкой ПО для корпоративного сегмента, мобильных платформ и WEB по всему миру. Среди клиентов, известных в Украине, можно выделить Uber, Looksery, Sony etc. Сейчас в компании уже более 400 сотрудников. Кроме этого, 4 офиса в разных странах мира.

Помимо основной деятельности, ***Provectus*** регулярно поддерживает социальные проекты Одессы. В этом году совместно с IT2School, они открыли Atom Space — пространство в центре Одессы, где талантливые подростки возрастом от 14 до 18 лет могут бесплатно обучаться и создавать свои IT-проекты. Кроме того, в августе этого года сотрудники компании приняли участие в акции «Шкільний портфелик» и помогли собрать в школу 200 ребят из семей, которые оказались в сложных жизненных обстоятельствах.

Provectus is a team of proactive experts in software development, design, QA, Big Data & Analytics, DevOps, and Business Consulting that works efficiently together as a team.

Основанная в 2013 году, компания ***KeepSolid*** сегодня является продуктовой ИТ-компанией, предоставляющей клиентам во всем мире инновационные он-лайн решения, обеспечивающие защищенность и продуктивность.

Наши сотрудники – это профессионалы, ежедневно работающие для того, чтобы обеспечить безопасность и защищенность, а также сделать проще ведение бизнеса и выполнение ежедневных рутин. Наша миссия – обеспечение высококачественных решений по продуктивности и надежности для наших клиентов.

Мы заботимся о каждом этапе производственного процесса – от зарождения идеи сервиса или решения до их реализации и эксплуатации, обеспечивая этим возможность заниматься своим бизнесом, не отвлекаясь на посторонние решения, для своих клиентов.

Controller design for second order systems to track sinusoidal signals with zero steady state error and prescribed transient response

Alon Kuperman
Ariel University
Beer-Sheva, Israel
alonku@ariel.ac.il

***Abstract*—In this paper, resonant controller structure is derived according to prescribed tracking behavior of general second order systems, excited by sinusoidal input. It is shown that while the typically employed proportional-integrative-derivative (PID) control structure is incapable of tracking/rejecting such signals with zero steady state error, the proposed controller guarantees both near-ideal tracking and disturbance rejection while following a prescribed transient response. The validity of presented theoretical analysis is validated by simulations applied to a three-level single-phase pulse-width-modulated (PWM) inverter, and supported by experimental results of its low-power equivalent circuit.**

***Keywords*— Second-order systems, sinusoidal excitation, transient performance, resonant controller.**

I. INTRODUCTION

In order to achieve zero steady state current tracking error in DC and AC systems, PID control in stationary or synchronous frame is the conventionally utilized technique [1], [2]. Stationary frame resonant compensators, capable of achieving zero steady state error at AC frequency became popular in the last decade [3] – [7]. The use of resonant controllers in AC systems is based on internal model principle [8], [9] utilizing integrative controllers in DC systems and resonant controllers in AC systems [10]. Derivation of PR converters is mostly performed either from equivalent synchronous frame PI controllers [6], [11] or using conventional Bode diagram tools, since the resonant term of conventional PR controller has little contribution outside the resonant frequency [5], [6]. Consequently, the proportional gain is mainly used to shape the frequency response.

Recently, a method for deriving proportional-resonant controller structure and coefficients according to desired transient behavior of AC signal amplitude, applied to typical power converter current loop was presented in [12], where AC signal envelope was treated as DC signal and its transient behavior was shaped utilizing well-known approach employed in DC systems loop shaping.

Unfortunately, proportional-resonant controllers proposed by far are usually designed mainly for first-order systems. Nevertheless, it is well-known that many typical plants in power electronics and motion control are represented by second order transfer functions. Consequently, this paper suggests a method of designing resonant controllers for second order systems based on desired time-domain tracking performance. It is revealed that the resulting structure contains proportional, derivative and resonant terms and the controller is hence referred to as proportional-derivative-resonant. The validity of the presented analysis is confirmed by simulation and experimental results.

II. PROBLEM FORMULATION

Consider an uncertain generalized second-order system with disturbance, described by the following differential equation,

$$a\ddot{y}(t) + b\dot{y}(t) + cy(t) = hu(t) + f(t) \quad (1)$$

where the coefficients may be split into nominal (known) and uncertain pars as

$$a = a_n + \Delta a,\ b = b_n + \Delta b,\ c = c_n + \Delta c,\ h = h_n + \Delta h \quad (2)$$

with subscript "n" denoting nominal terms. In (1), $y(t)$, $u(t)$ and $f(t)$ denote system output, control input and disturbance input, respectively. Substituting (2) into (1) and rearranging, there is

$$\ddot{y} + a_n^{-1}b_n\dot{y} + a_n^{-1}c_n y = a_n^{-1}h_n(u + d), \quad (3)$$

with

$$d = h_n^{-1}(f - \Delta a\ddot{y} - \Delta b\dot{y} - \Delta cy + \Delta hu) \quad (4)$$

denoting lumped uncertainty and disturbance. Applying Laplace transform, there is

$$Y(s) = P(s)(U(s) + D(s)), \quad (5)$$

where $Y(s) = L\{y(t)\}$, $U(s) = L\{u(t)\}$ and $D(s) = L\{d(t)\}$ with $L\{\cdot\}$ symbolizing the Laplace transform operator and

$$P(s) = \frac{G_P}{s^2 + 2\xi_P\omega_P s + \omega_P^2} \quad (6)$$

with

$$G_P = a_n^{-1}h_n,\quad \omega_P^2 = a_n^{-1}c_n,\quad 2\xi_P\omega_P = a_n^{-1}b_n. \quad (7)$$

Closed-loop block diagram of the system is shown in Fig. 1. The goal of the controller $C(s)$ is forcing the system output to track a reference given by

$$y^*(t) = R\sin(\omega_0 t) \quad (8)$$

while rejecting the following disturbance,

$$f(t) = F\sin(\omega_0 t + \theta). \quad (9)$$

Therefore following (4), the steady state lumped uncertainty and disturbance is also given by

$$d(t) = W\sin(\omega_0 t + \theta). \quad (10)$$

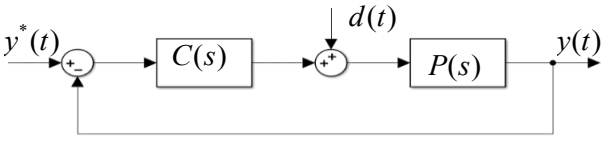


Fig. 1. Closed-loop block diagram of the system.

In DC systems, the plant (6) is usually stabilized by a PID controller given by e.g.

$$C(s)=\frac{\omega_{CL}}{s}\frac{s^2+2\xi_P\omega_P s+\omega_P^2}{G_P} \tag{11}$$

in order to create the following closed-loop tracking and disturbance rejection behaviors,

$$H_T(s)=\frac{Y(s)}{Y^*(s)}=\frac{\omega_{CL}}{s+\omega_{CL}} \tag{12}$$

and

$$H_D(s)=\frac{Y(s)}{D(s)}=\frac{sG_P}{\left(s+\omega_{CL}\right)\left(s^2+2\xi_P\omega_P s+\omega_P^2\right)}, \tag{13}$$

especively, with $Y^*(s) = L\{y^*(t)\}$. Nevertheless, as shown in [12], (12) possesses both non-unity gain and non-zero phase for any $\omega_0 > 0$. Likewise, it may be easily shown that the gain of (13) is larger than zero for any $\omega_0 > 0$. Consequently, employing (11) would result in both amplitude and phase steady state errors.

III. Proposed Solution

Following [12], it is proposed to define the prescribed transient response by

$$y(t)=A\left(1-e^{-\omega_{CL}t}\right)\sin\left(\omega_0 t\right), \tag{14}$$

reflecting amplitude transient time constant of ω_{CL}^{-1} and zero steady state amplitude and phase error. Taking the Laplace transforms of (8) and (14), there is

$$Y(s)=\frac{A\omega_0}{s^2+\omega_0^2}\cdot\frac{2\omega_{CL}s+\omega_{CL}^2}{(s+\omega_{CL})^2+\omega_0^2}=Y^*(s)\cdot H_T(s) \tag{15}$$

with

$$H_T(s)=\frac{C(s)P(s)}{1+C(s)P(s)}=\frac{2\omega_{CL}s+\omega_{CL}^2}{(s+\omega_{CL})^2+\omega_0^2}. \tag{16}$$

The loop gain is then obtained as

$$C(s)P(s)=\frac{2\omega_{CL}s+\omega_{CL}^2}{s^2+\omega_0^2}, \tag{17}$$

leading to a resonant proportional-derivative-resonant (PDR) controller given by

$$\begin{aligned}C(s)&=\frac{2\omega_{CL}s+\omega_{CL}^2}{s^2+\omega_0^2}\cdot\frac{s^2+2\xi_P\omega_P s+\omega_P^2}{G_P}\\&=K_P+K_D s+\frac{K_{R1}s+K_{R2}}{s^2+\omega_0^2}\end{aligned} \tag{18}$$

with

$$\left.\begin{aligned}K_P=\omega_{CL}^2+4\xi_P\omega_P\omega_{CL},\quad K_D=2\omega_{CL},\\K_{R1}=2\xi_P\omega_P\omega_{CL}^2+2\omega_{CL}\omega_P^2-\omega_0^2K_D,\\K_{R2}=\omega_{CL}^2\omega_P^2-K_P\omega_0^2.\end{aligned}\right\} \tag{19}$$

Employing (18), disturbance rejection capability is governed by

$$H_D(s)=\frac{P(s)}{1+P(s)C(s)}=\frac{G_P\left(s^2+\omega_0^2\right)}{\left(s^2+2\xi_P\omega_P s+\omega_P^2\right)\left((s+\omega_{CL})^2+\omega_0^2\right)}, \tag{20}$$

obviously possessing zero gain at $\omega = \omega_0$ and thus any disturbance described by (10) will be completely rejected in steady state.

IV. Verification

A. Simulation framework

Consider a single-phase three-level PWM inverter, shown in Fig. 2. The converter is fed by an equally split DC source and feeds linear loads. The power stage consists of switching circuitry and an LC filter, as shown. The PWM circuitry used to operate the inverter is shown in Fig. 3. It receives the control signal $-1 < d < 1$ from the controller and generates appropriate switching signals fed to power transistors.

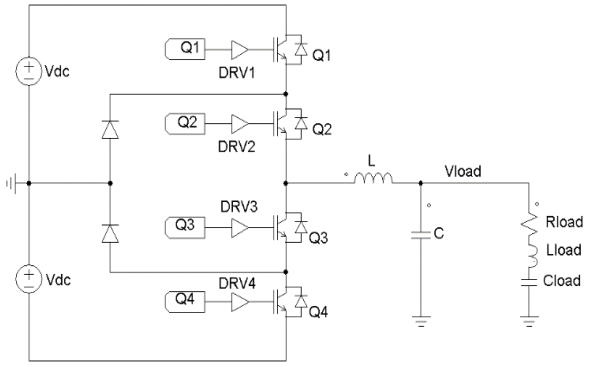


Fig. 2. Power stage of a three-level single-phase inverter.

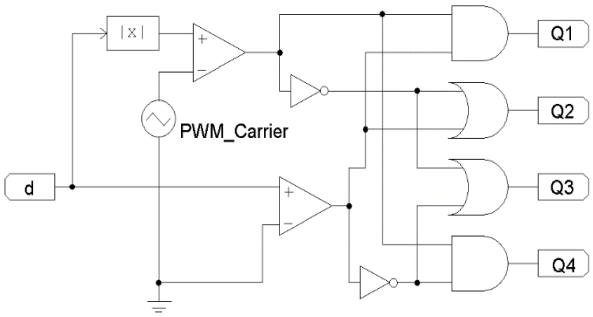


Fig. 3. PWM circuitry.

Consequently, the plant is governed by the following transfer function,

$$P(s)=\frac{V_{load}(s)}{d(s)}=V_{dc}\frac{{}^{1}\!/_{sC}\,\|\,Z_{load}}{sL+{}^{1}\!/_{sC}\,\|\,Z_{load}} \tag{21}$$

with $Z_{load}=R_{load}+sL_{load}+{}^{1}\!/_{sC_{load}}$. In case of pure resistive load, the plant is given by

$$P(s)=\frac{{}^{V_{dc}}\!/_{LC}}{s^2+{}^{s}\!/_{R_{load}C}+{}^{1}\!/_{LC}}, \tag{22}$$

i.e. matches (6) with

$$G_P=\frac{V_{dc}}{LC},\quad \omega_P^2=\frac{V_{dc}}{LC},\quad 2\xi_P\omega_P=\frac{1}{R_{load}C}. \tag{23}$$

The controller is then designed following (18) with a small modification as follows: an additional pole at half switching frequency $\omega_S/2$ is added in order to make the

controller transform function proper, i.e.

$$C(s)=\frac{K_P+K_D s+\dfrac{K_{R1}s+K_{R2}}{s^2+\omega_0^2}}{1+\dfrac{s}{0.5\omega_s}}. \qquad (24)$$

Taking into account simulation data, given in Table I, bode diagrams of $H_T(s)$ and $H_D(s)$ magnitudes are shown in Fig. 4. Unity gain of the former and zero gain of the latter at $\omega = \omega_0$ are evident.

TABLE I. SIMULATION DATA.

Parameter	Value	Units
DC voltage, V_{dc}	400	V
Switching frequency, ω_S	40000π	rad/s
Filter inductance, L	1	mH
Filter capacitance, C	4.7	μF
Nominal resistive load, R_{load}	16	Ω
Excitation frequency, ω_0	100π	rad/s
Transient time constant, ω_{CL}	400π	rad/s
Reference amplitude, A	$230\sqrt{2}$	V

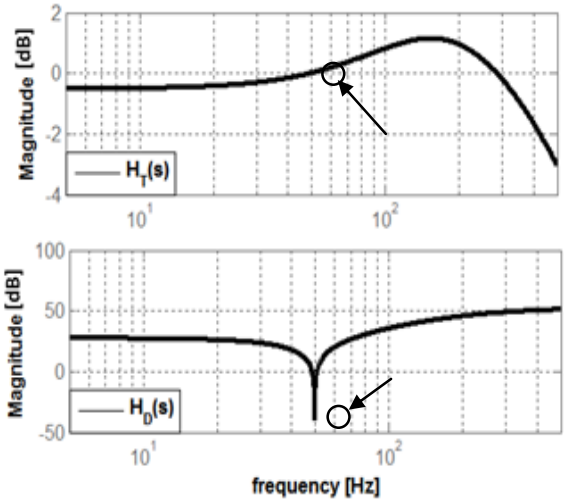


Fig. 4. Closed-loop tracking (top) and disturbance rejection (bottom) capabilities.

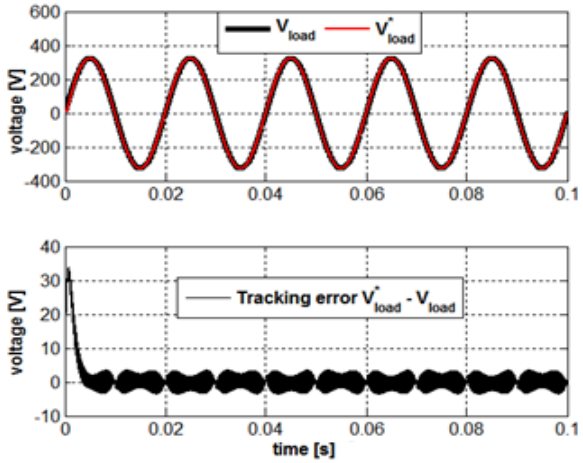


Fig. 5. Simulation results – nominal system.

Time-domain simulation results of the system with nominal parameters and rated load are shown in Fig. 5. It may be concluded that the system reaches zero steady state error after a short transient. Frequency content of tracking error is shown in Fig. 6, revealing that the error contains mainly switching ripple components.

In the second simulation, the controller was designed according to nominal parameters while the inverter was modified as follows: DC link voltages were reduced to 350V each (12.5% uncertainty), filter inductance was reduced to 0.5mH (50% uncertainty) and filter capacitance was reduced to 2.35μF (50% uncertainty).

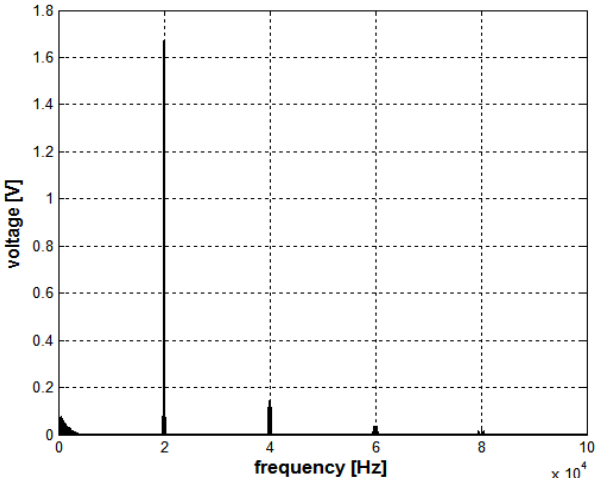


Fig. 6. Tracking error frequency content.

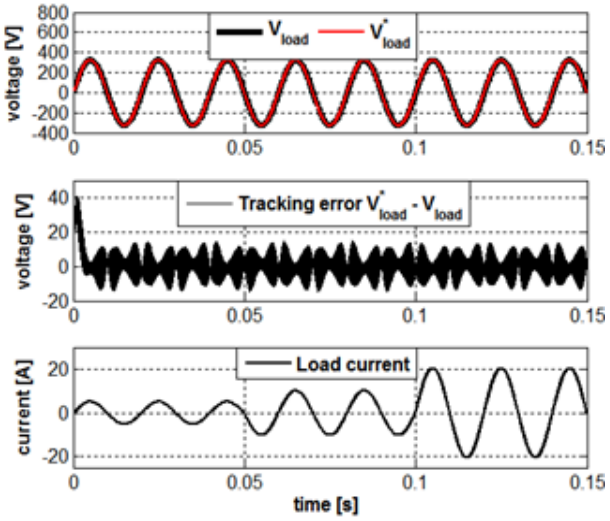


Fig. 7. Simulation results – uncertain system with disturbances.

Moreover, the following load variations were applied,

$$R_{load}=\begin{cases}64\Omega, & 0<t\le 50ms\\ 32\Omega, & 50ms<t\le 100ms\\ 16\Omega, & 100ms<t\le 150ms\end{cases}. \qquad (25)$$

The results are shown in Fig. 7. It may be concluded that the system is able to reach zero-steady state error despite parameter uncertainties and disturbances.

B. Experiments

In order to verify the proposed method experimentally, a low-power equivalent of (22) was realized using analogue circuitry with *Vdc* = 12V and the controller (24) was implemented in digital form using a TMS320F28332 Texas Instruments Digital Signal Processor (DSP). Experimental setup is pictured in Fig. 8.

During the experiments, the amplitude of the reference signal was varied according to

$$A = \begin{cases} 10V, & 0 < t \le 500ms \\ 5V, & 500ms < t \le 1000ms \\ 10V, & 1000ms < t \le 1500ms \end{cases} . \quad (26)$$

Experimental results are shown in Fig. 9 (for better visibility, zoomed and shifted results are given in Fig. 10). As expected,

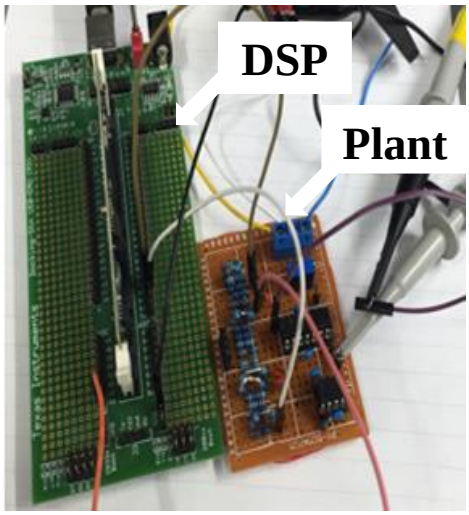


Fig. 8. Experimental setup.

tracking error is kept near zero both during transients and in steady state.

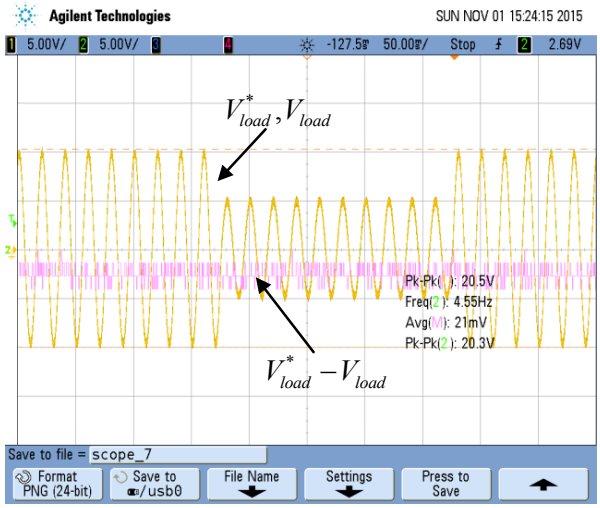


Fig. 9. Experimental results.

V. Conclusions

A method for deriving proportional-derivative-resonant controller structure and according to desired transient behavior of second order systems, excited by sinusoidal signals, was proposed in the paper. The controller allows obtaining zero steady state tracking error even if parameter uncertainty is present. The presented findings were validated by both simulation and experimental results.

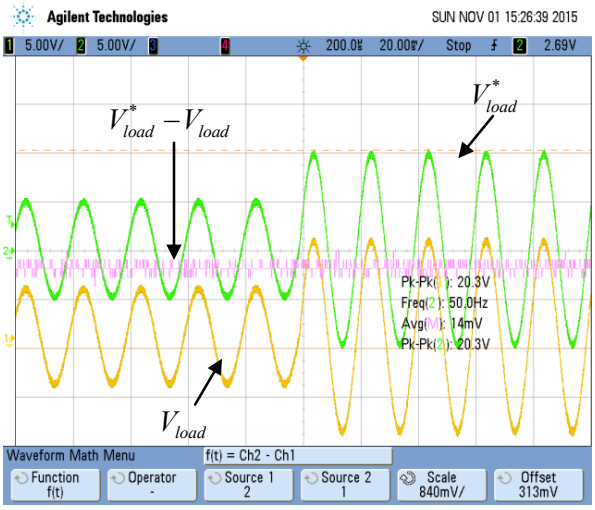


Fig. 10. Experimental results (zoomed and shifted).

References

[1] M. Kazmierkowski and L. Malesani, "Current control techniques for three-phase voltage-source PWM converters: A survey," *IEEE Trans. Ind. Electron*., vol. 45, no. 5, pp. 691 – 703, Oct. 1998.

[2] X. Bao, F. Zhuo, Y. Tian and P. Tan, "Simplified feedback linearization control of three phase photovoltaic inverter with an LCL filter," *IEEE Trans. Power Electron*., vol. 28, no. 6, pp. 2739 – 2752, Jun. 2013.

[3] Y. Sato, T. Ishizuka, K. Nezu and T. Kataoka, "A new control strategy for voltage-type PWM rectifiers to realize zero steady-state control error to input current," *IEEE Trans. Ind. Appl*., vol. 34, no. 3, pp. 480 – 486, May 1998.

[4] D. Zmood, D. Holmes and G. Bode, "Frequency domain analysis of three-phase linear current regulators," *IEEE Trans. Ind. Appl*., vol. 37, no. 2, pp. 601 – 610, Mar. 2001.

[5] D. Zmood and G. Holmes, "Stationary frame current regulation of PWM inverters with zero steady-state error," *IEEE Trans. Power Electron*., vol. 18, no. 3, pp. 814 – 822, May 2003.

[6] R. Teodorescu, F. Blaabjerg, M. Liserre and P. Loh, "Proportional-resonant controllers and filters for grid connected voltage-source converters," *IEE Proc. Electr. Power Appl*., vol. 153, no. 5, pp. 750 – 762, Sep. 2006.

[7] D. Holmes, T. Lipo, B. McGrath and W. Kong, "Optimized design of stationary frame three phase AC current regulators," *IEEE Trans. Power Electron*., vol. 24, no. 22, pp. 2417 – 2426, Nov. 2009.

[8] B. Francis and W. Wonham, "The internal model principle for linear multivariable regulators," *Appl. Math. Optim*., vol. 2, no. 2, pp. 170 – 194, 1975.

[9] C. Garcia and M. Morari, "Internal model control: A unifying review and some new results," *Ind. Eng. Chem. Process Des. Dev*., vol. 21, pp. 308 – 323, 1982.

[10] S. Fukuda and T. Yoda, "A novel current-tracking method for active filters based on a sinusoidal internal model," *IEEE Trans. Ind. Appl*., vol. 37, no. 3, pp. 888 – 895, May 2001.

[11] A. Kuperman, "Synchronous frame current controllers design based on desired stationary frame transient performance," *Electron. Lett.*, vol. 51, no. 22, pp. 1769 – 1770, 2015.

[12] A. Kuperman, "Proportional-resonant current controllers design based on desired transient performance," *IEEE Trans. Power Electron.*, vol. 30, no. 10, pp. 5341 – 5345, Oct. 2015.

A multicriteria industrial site selection methodology using MCDA, fuzzy set theory and GIS

Svitlana Kuznichenko
dept. of Information Technologies
Odessa State Environmental University
Odessa, Ukraine
skuznichenko@gmail.com

Iryna Buchynska
dept. of Information Technologies
Odessa State Environmental University
Odessa, Ukraine
buchinskayaira@gmail.com

***Abstract*—In the paper, the GIS-based multi-criterial model of decision-making support for industrial site selection is proposed. The formalized description of spatial decision-making process is based on the use of multi-criterial decision analysis in a spatial context, where alternatives, criteria, and other elements of solution to the problem have spatial dimensions. The method of decomposition of the set of source objects influencing the decision making on the thematic layers of criteria, is described. The sampling procedure for vector layers for criteria is described in a raster model, which allows a set of cells, attributes of which contain information about the value of function of the effect of layer objects as well as method of determining the set of possible alternatives, taking into account constraints that may be imposed on attribute values. The method of standardization of criteria based on fuzzy logic methods, which allows using expert knowledge in spatial analysis, is proposed. It is shown that phasing of criteria, that is, the transformation of their values of attributes into a fuzzy set on the basis of the expert estimation of a fuzzy membership function allows further combining of criteria with the help of fuzzy rules of output. Fuzzy logic operations such as intersection or union may be used for this purpose. Different methods for determining the standardized weighting criteria and aggregation operators that can be used in the GIS environment, are described. It is noted that it is more reasonable to use the OWA operator, which allows to formalize expert information about the acceptable form of compromise between values according to different individual criteria with the help of a fuzzy quantifier. It is shown that the use of fuzzy logic in the decision making model allows to take into account the uncertainty of the source information and to obtain a more informative combined suitability map by determining the rank of suitability of alternatives, that is, to perform ranking of territories according to the degree of suitability for industrial site selection.**

Keywords—geographic information system; decision support system; multiple-criteria decision analysis; fuzzy logic; site selection analysis.

I. INTRODUCTION

Modern geographic information systems (GIS) are an important component of decision support systems (DSS) thanks to advanced functions of preservation, processing and analysis of spatial data, simulation tools and availability of visualization tools. Spatial solutions by their nature are always multi-criteria [1], so DSSs that are designed to support spatial decision-making are often used in cases where a large number of alternatives should be evaluated based on several criteria.

In the last 20 years, GIS actively integrates various methods of multi-criteria decision analysis (MCDA) [2-4]. Separate attempts to fully integrate MCDA and GIS tools in the general interface revealed problems with the lack of flexibility and interactivity of similar systems that can not provide the necessary freedom of action for analysts [5]. Therefore, the choice of procedure and appropriate methods of MCDA, which can provide a better solution to a specific problem, is an urgent task for developers. In addition, preferences of the decision maker (DM), which are often vague, are unimportant, play an unclear role in the MCDA procedure. To take into account subjective fuzzy DM judgments, it is expedient to improve methods of MCDA with the help of the apparatus of "soft" computing, the fuzzy sets theory [6].

II. FORMALIZATION OF THE PROCESS OF MULTI-CRITERIA DECISION ANALYSIS IN GIS

Consider the use of multi-criteria decision analysis to support the adoption of managerial decisions on finding the best location of an industrial object. The general process diagram is shown in Fig. 1. In solving such a task it is important to take into account multiple factors that influence the decision making: the geographical location of the site and its physical characteristics, resource supply of production, transport and social infrastructure, the condition of natural environment and possible negative impact on it, regulatory and legal constraints, etc. There is a complex structure of interaction of various objects and factors of different physical and socio-economic nature. The more precise these factors will be determined at the preliminary stage of study of the problem, the more adequate the model will be. For example, in [7] authors developed a multi-criteria model for making decisions on placement of landfills for solid household waste in the south of the Odessa Region, which took into account physical, environmental and socio-economic factors. In general, 14 criteria were formulated, which were presented in the geo database in the form of vector and raster layers.

We describe the method of decomposing a plurality of objects belonging to the investigated territory and influencing decision-making in the thematic layer of criteria.

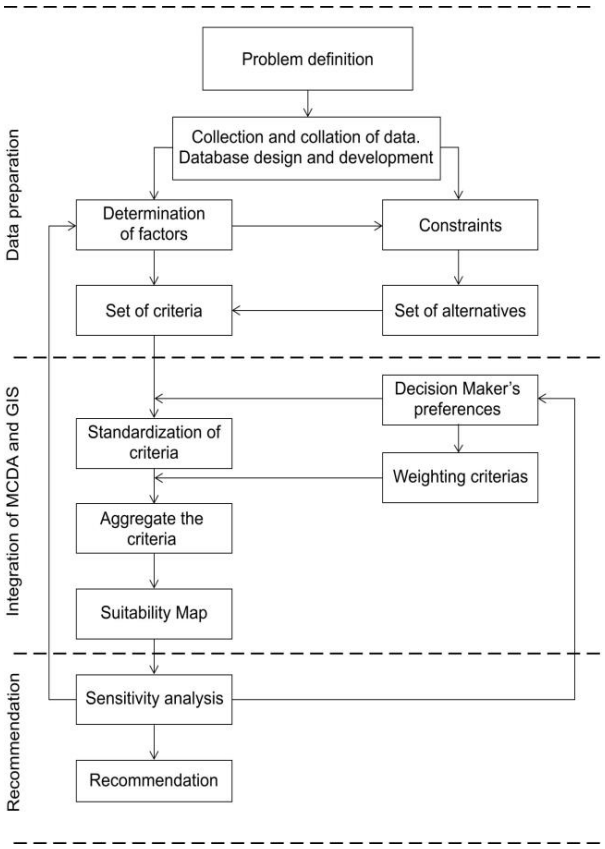


Fig. 1. General diagram of the process of multicriterial decision analysis in GIS

Let us imagine some finite set of objects that influence the solution be given:

$$O = \{o_i\} = \left\{\left(G, \{I_j\}\right)_i\right\}, i = \overline{1,n},\ j = \overline{1,m}, \qquad (1)$$

where G is information on the spatial position of the object; I is attributive information about the object; n is the total number of objects belonging to the investigated area and affect the decision; m is the number of attributes of the object.

It is necessary to select a set of O_j subsets that influence the decision on any factor (availability of transport infrastructure, type of soil, ecological safety, etc.) from a set of objects O and combine them into separate vector layers of criteria.

$$O = \bigcup_{j=1}^{t} O_j, O_j \in O. \qquad (2)$$

The method of decomposing objects involves performing an analysis of their spatial and attributive information. Decomposition is usually performed according to following features:

- the set of geometric properties $G' = \{g_1, g_2, g_3\}$, where g_1 is point objects; g_2 is linear objects; g_3 is polygon objects;
- the set of attributive properties $I' = \{Q, N\}$, where Q is a set of qualitative properties that determines belonging of an object to a certain thematic group (transport infrastructure, water objects, settlements, etc.); N is the set of quantitative characteristics of the properties of the object (for example, for entities belonging to the "Settlements" thematic group, one can make a decomposition according to the population size).

Thus, belonging of objects to a certain layer of criteria can be determined by following set of properties:

$$S = \langle G', I' \rangle. \qquad (3)$$

Schematically, the process of decomposition of the set of objects O on thematic layers of criteria is shown in Fig. 2.

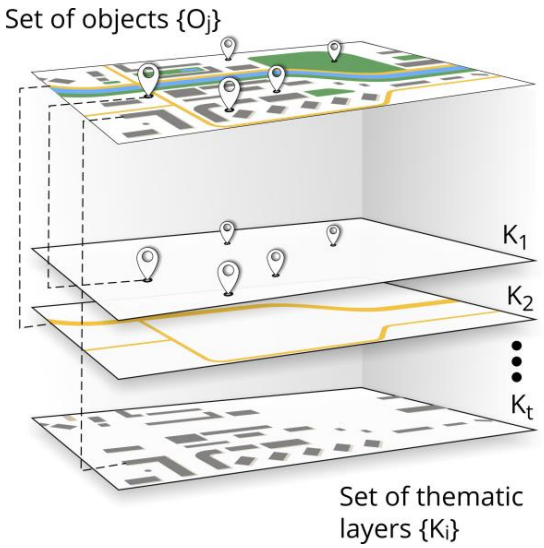


Fig. 2. Scheme of decomposition of objects in thematic layers

After the process of decomposing objects and structuring the problem, we obtain a vector map K representing a set of thematic vector criteria layers K_i (Fig. 2):

$$K = \{K_i\}, i = \overline{1,t}, \qquad (4)$$

$$K_i = \{O_j^i\}, j = \overline{1,l}, \qquad (5)$$

where i is a number of map layer K, j is an object number in the i-th layer.

For conducting a spatial modeling, it is convenient to use a raster data model. Therefore, it is advisable to represent the received vector layers of objects as a set of cells (pixels) in a GIS raster model, which has the form of a two-dimensional discrete rectangular grid of nxm cells, where $\Delta x = \Delta y = \Delta r$ is a cell size:

$$A = \{a_i \mid a_i = n\Delta r, m\Delta r\} \qquad (6)$$

The set A is a set of alternatives. To reduce the equation (5), it can be written as follows:

$$A = \{a_i \mid i = \overline{1, n \cdot m}\} \qquad (7)$$

It is important to choose such a sampling procedure for vector layers of the criteria in the raster, which will receive a set of cells whose attributes contain content

information about the value of impact function of objects of the layer. For example, attributes can be derived from vector maps that contain point objects of observation points by the value of some factor using different methods of interpolation.

Often, the distance measurement is used to study the relationship between objects and their interaction, for example, using the Euclidean metric, the value of which between two point objects O_1 (x_1, y_1) and O_2 (x_2, y_2) is calculated by equation:

$$ED(O_1, O_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}. \quad (8)$$

In the case of a raster data model, the distance from any cell of the raster to the object O_i will be equal to the minimum distance from this cell to each cell that covers the object being investigated.

After completing the sampling procedure, since attributes are variable solutions, you can represent the result of the solution as x_{ij}, that is, the value of the j-th attribute according to the i-th alternative:

$$X = \left\{ x_{ij} \mid i = \overline{1, n \cdot m}, \;\; j = \overline{1, t} \right\} \quad (9)$$

There may be restrictions imposed on the set of alternatives A: onto attribute values (non-spatial constraints) or onto placements (spatial constraints). For example, in [7], taking into account the State Building Regulations of Ukraine, vector layers of restrictive zones around reserves, airfields, forests and forest plantations, agricultural lands were created with the help of the buffering procedure.

The general restrictive vector layer K^{constr} was constructed using an overlay union operation:

$$K^{constr} = \bigcup_{r=1}^{R} K_r, \;\; R \subset T, \quad (10)$$

where K_r is a thematic vector boundary layer; R is the set of thematic vector layers on which the general boundary layer is constructed; T is a total number of thematic vector layers.

After performing the rasterization and reclassification operations of the K^{constr} layer C, a raster, cells of which are invalid alternatives, have a value of 0, cells that are possible alternatives – value 1, can be obtained.

$$C = \left\{ c_i \mid c_i \in \{0,1\} \right\}, \; i = \overline{1, n \cdot m}. \quad (11)$$

To determine the set of possible alternatives A' from the set of alternatives A, we must remove the set of bounding cells by conjunction operation.

III. Use of fuzzy logic apparatus to standardize criteria

Layer criteria typically have different ranges or scale values of attributes. The normalization procedure allows you to transfer output values of attributes from the unprocessed scale to the [0, 1] scale.

The description of spatial information based on methods of fuzzy logic is based on transformation of values of attributes of the i-th layer in the sense of degree of belonging to the fuzzy set a_i:

$$a_i = \left\{ (x, \mu_a{}^i(x)) \mid x \in U \right\}, \;\; \mu_a{}^i(x) : x \to [0,1], \quad (12)$$

where x is the value of the attribute, and U is a continuous set of attribute values.

The membership function $\mu_a(x)$ indicates the degree of membership of the attribute x to to the fuzzy set a_i. Typically, the membership function is built under participation of an expert (expert group), so that the degree of membership is approximately equal to the intensity of manifestation of some factor. In practice, following types of membership functions are applied: linear, triangular and trapezoidal (linear-lump); nonlinear (Gaussian function, sigmoid function, spline).

Fuzzification of criteria, that is, conversion of their attribute values to a fuzzy set, based on expert assessment of the fuzzy membership function, allows further combining the criteria with the help of fuzzy rules of output. Fuzzy logic operations such as intersection or merge may be used for this purpose.

The standard fuzzy intersection of sets $a_1, a_2, \ldots, a_t$ for all $x \in U$ is defined as follows:

$$\bigcap_{i=1}^{t} \mu_a{}^i(x) = \min\left[\mu_a{}^1(x), \mu_a{}^2(x), \ldots, \mu_a{}^t(x) \right]. \quad (13)$$

The standard fuzzy union of sets $a_1, a_2, \ldots, a_t$ for all $x \in U$ is defined as follows:

$$\bigcup_{i=1}^{t} \mu_a{}^i(x) = \max\left[\mu_a{}^1(x), \mu_a{}^2(x), \ldots, \mu_a{}^t(x) \right]. \quad (14)$$

The use of a fuzzy intersection operation (13) leads to alternative ranking based on only the lowest rank, that is, it is a pessimistic approach to decision making. Fuzzy union operation (14) takes into account only best evaluations of all criteria.

IV. Methods for determining the normalized weight of criteria

Using multi-criteria decision analysis involves assigning weight criteria to specify their relative importance. In the case of t criteria, the set of weights is defined as follows:

$$W = \left\{ w_i \mid \sum w = 1, \; i = \overline{1, t} \right\}. \quad (15)$$

The easiest way to evaluate the importance of criteria is to rank, that is, to streamline criteria by an expert in order of importance. Once the rating is set, we can calculate weights according to the equation:

$$w_i = \frac{t - r_i + 1}{\sum (t - r_j + 1)}, \quad (16)$$

where w_i is the normalized weight for the i-th criterion, t is the number of criteria considered $(j = 1, 2, \ldots, t)$, and r_i is the rank position of a criterion.

Weights of criteria can be found directly by experts on the basis of a given scale, for example, from 0 to 100. In

this case, the normalized weight of a criterion is calculated as follows:

$$w_i = \frac{w'_i}{\sum w'}, \quad (17)$$

where w_i is the normalized weight for the i-th criterion, and w'_i is the score for the i-th criterion.

The normalized weights of criteria can be calculated by the Analytical Hierarchy Process (AHP) [8], which is based on a pair comparison of criteria using the 9-point fundamental Saaty scale of absolute numbers. According to the results of the pair comparison of t criteria, we can construct a matrix $(t \times t)$ in which each element a_{ij}, $i, j = 1, 2, ..., t$ is the estimation of a pair comparison of the i-th criterion with the j-th criterion. For the matrix, own numbers and their own vectors are calculated, and a vector of local priorities is formed.

In order to control the consistency of expert assessments, two related characteristics, the Consistency Index, C.I. and the Consistency Ratio, C.R., are introduced. The reasonable level of consistency in paired comparisons is $C.R.<0.10$, while $C.R.\geq 0.10$ indicates conflicting expert judgments.

V. Methods of Aggregation

Aggregation of attributes according to different criteria can be accomplished using various methods of MCDA, which are implemented in GIS. The easiest method is the weighted linear combination (WLC) method, which is based on finding of the average value. The alternative membership function is calculated as follows:

$$\mu_a^{WLC}(x_i) = \sum_{j=1}^{T} w_j \mu_a{}^j(x_i). \quad (18)$$

where $\mu_a^j(x_i)$ is the function of the membership of the alternative to the i-th criterion, and w_j is the normalized weight of the i-th criterion and $\sum_{j=1}^{T} w_j = 1$.

The weighted product method (WPM) uses the multiplication operation:

$$\mu_a^{WPM}(x_i) = \prod_{j=1}^{T} \left(\mu_a{}^j(x_i) \right)^{w_j}. \quad (19)$$

An alternative to the GIS aggregation operators considered is the OWA operator, which was developed in the context of the theory of fuzzy sets [9]. It includes a weighted averaging for specific cases, and maximum and minimum operators – as extremums. The method has two sets of scales: the importance of the criterion and order one. By changing weighting rates of order, you can create maps for different decision making strategies. The OWA operator is flexible and allows to formalize expert information on the permissible form of compromise between values according to different individual criteria with the help of a fuzzy quantifier.

Finally, we note the importance of analyzing the sensitivity of evaluation results to the change in parameters of the model of multicriterial task before formation of final recommendations of DMs, which usually involves analyzing sensitivity of results of ranking alternatives to change in weight rates of criteria.

VI. Conclusion

Based on the proposed GIS-based multi-criteria decision support model, a composite map of suitability can be constructed and ranking of territories according to the degree of suitability for placement of industrial objects can be completed. Application of fuzzy logic in the model of apparatus allows to take into account expert knowledge and judgment, which partially compensates for the lack of information through the use of experts' experience.

References

[1] S. Chakhar and V. Mousseau, "Spatial multicriteria decision making" // Shehkar S. and H. Xiong (Eds.), Encyclopedia of GIS, Springer-Verlag, New York, 2008, pp.747–753.

[2] S. Chakhar and J.M. Martel, "Enhancing geographical information systems capabilities with multicriteria evaluation functions", Journal of Geographic Information and Decision Analysis, Vol. 7, No. 2, 2003, pp. 65–71.

[3] J. Malczewski, "GIS–based multicriteria decision analysis: a survey of the literature", International Journal of Geographical Information Science, 20 (7), 2006, pp. 703–726.

[4] J. Malczewski, "Review Article on the Use of Weighted Linear Combination Method in GIS: Common and Best Practice Approaches", Transaction in GIS 4(1), 2000, pp. 5–22.

[5] K. Lidouh, "On themotivation behind MCDA and GIS integration", Int. J. Multicriteria Decision Making, Vol. 3, Nos. 2/3, 2013, pp. 101–113.

[6] L. A. Zadeh, "Fuzzy sets", Information and Control, 8 (3), 1965, pp. 338–353.

[7] S. Kuznichenko, L. Kovalenko, I. Buchynska and Y. Gunchenko, "Development of a multi-criteria model for making decisions on the location of solid waste landfills", Eastern-European Journal of Eenterprise Technologies, №2/3(92), 2018, pp. 21–31.

[8] T. Saaty, "Decision making with the analytic hierarchy process", Scientia Iranica, 9(3), 2002, pp. 215–229.

[9] R. R. Yager, "On ordered weighted averaging aggregation operators in multicriteria decision making", IEEE Transactions on System, Man, and Cybernetics, 18, 1988, pp.183–190.

Integrated fault tolerant consensus algorithm

Yevhen Leonchyk
department of Mathematical Analysis
Odessa I.I.Mechnikov National University
Odessa, Ukraine
leonchyk@ukr.net

Igor Mazurok
Chair of optimal control and economical cybernetics
Odessa I.I.Mechnikov National University
Odessa, Ukraine
igor@mazurok.com

Valerii Pienko
department of Mathematical Support of Computer Systems
Odessa I.I.Mechnikov National University
Odessa, Ukraine
vpenko@onu.edu.ua

***Abstract* — The work is devoted to research and development of an integrated parallel fault-tolerant consensus algorithm for distributed processing and storage systems with low latency. An essential feature of this algorithm is the economic model which embedded into algorithm structure. This economic model ensures sustainable development of the system in accordance with the objectives of the usage. The proposed algorithm allows for one pass of the protocol to obtain coordinated decisions on the following issues: what information will be put into storage, in which place of the synchronized repository it will be written and; what will be the reward for correct functioning. The algorithm is based on the ideas of the algorithms SBFT and Raft. It involves resistance to two types of errors - Byzantine errors and crush equipment failures.**

Keywords—Blockchain, consensus algorithm, distributed system, fault tolerance.

I. INTRODUCTION

There is a fairly wide range of tasks, which requires the formation of trusted relations between participants. A practically useful option for organizing such relations is the PKI infrastructure, based on the use of asymmetric cryptography.

The characteristic trend of modern information systems is the transition to a distributive architecture. In this case it is important to provide the following requirements:

- performance;
- scalability;
- tolerance relative to various types of attack;
- immutable and tampering safety;
- logic consistency.

To support such a set of characteristics recently used technology, which is commonly called BlockChain. Due to the distributed nature of these systems, the consensus mechanism (the ability to make concerted decisions) plays a key role. In traditional systems based on BlockChain technology, a proof-of-work consensus (Bitcoin, Ethereum) is used. However, for many applications this type of consensus is not acceptable due to low system performance (low throughput).

The aim of this paper is to develop a version of the consensus protocol that will meet the following requirements:

- the scale of the system that is typical for corporate tasks (that is, the system presents a high entry threshold to new nodes and as a result, the number of network nodes is limited to several hundreds);
- the system should provide high speed response to the client request;
- processing nodes of the system are functionally equal, ensuring its decentralization;
- the usefulness of the system's functionality for network clients is to obtain signed certificates;
- customer requests in the system are handled separately, without uniting the blocks (this reduces client waiting time by increasing the overall system performance);
- the system should be economically motivated (this factor is intended for its sustainable functioning).

II. THE PROTOCOL FOR ISSUING A CERTIFICATE

The system consists of nodes communicating over a peer-to-peer protocol. At different stages of the communication protocol, the nodes perform different roles:

- ordinary node which signs and stores certificates;
- receptionNode which receives a client CSR (Certificate Signing Request). It also receives a client payment and performs remuneration for nodes;
- leader which coordinates message exchange between the other nodes.

To maintain the necessary level of synchronization, the protocol introduces two supplementary notions:

- term (t) - the number of the epoch from the moment the network starts functioning, within which the next leader operates. The number of the term is increased by one when the leader changes;
- beat is the sequence of protocol steps performed from the CSR receiving to the certificate recording in the system blockchain.

All node's messages transmit information in a cryptographically signed form, in order to avoid its distortion during the transmission by the communication channel.

In order to provide sustainable functionality the system has to satisfy the next requirement: the total node number n must be greater than 2f+c where

- f - the maximum number of faulty (byzantine) nodes;
- c - the maximum number of crashed nodes (at least within established period of time).

At every communication stage the current leader gets not less than 2f+1 uncorrupted messages with no more than f faulty messages among them. Thus there are always at least f+1 identical messages which is sufficient for the majority considerations.

If the node receives a message that is valid at this stage of the protocol within a certain time, it generates a subsequent message. Otherwise, there is a so-called timeout and this node initiates the re-election of the leader. In fact, a new leader is determined by the implementation of a special Raft protocol [2].

Let's consider the information flows that arise when the certificate is issued using the modified SBFT based scheme [3] (Fig.1).

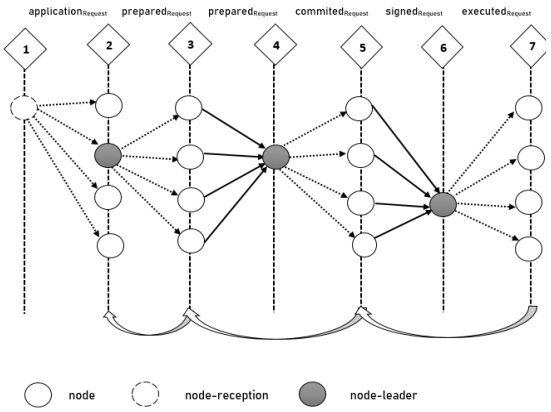


Fig. 1. Data flow during issuing certificate

1) receptionNode sends to all nodes the applicationRequest message (a request to receive a certificate with payment confirmation) with a client public key.

2) After receiving the applicationRequest message the current leader sends the prepreparedRequest message with its First Free Ledger Number to all nodes:

3) Every node sends to the current leader the preparedRequest message with just received prepreparedRequest message. Thus, the leader collects the data from all nodes. In case the node's ledger is incomplete compared to the leader's ledger, the node starts the process of updating its ledger.

4) After receiving the 2f+1 messages (it will be enough for majority rule) the leader sends them inside the commitedRequest message as an array to all nodes.

5) At this stage of the protocol, the certificate is issued based on the received message array by the rule of majority and sent to the leader in the signedRequest message. Note that in diagram on Fig.1 the change of the current leader as a result of re-elections is reflected as an example in step 4.

6) Leader (Executor) accumulates 2f + 1 signedRequest messages and passes them in executionRequest message as an array.

7) If there are f + 1 identical records in the message, the information is considered valid and persists in the ledger by all nodes, and the signed certificate is sent to the client (receptionNode).

III. FAULT TOLERANT ELECTION PROTOCOL

Information flows of the fault tolerant election protocol are shown on Fig. 2

Each node maintains in its state an integer value, called a term (t). At the beginning of each leader election procedure, node-candidate increases the value of its term by 1. Thus, the term used as the conventional discrete time of a distributed system for synchronizing nodes activity. It expresses the number of attempts (not necessarily successful) to re-elect a new leader.

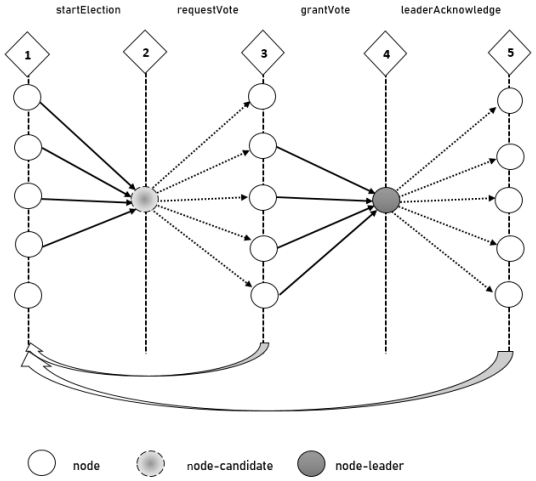


Fig. 2. Data flow during leader election

The protocol consists of five steps.

1) A timeOut event occurs, if for a certain period of time the node does not receive messages from other nodes or receives incorrect data from them. As a result, this node increases its term by 1 and initiates the re-election of the new leader, sending the node with the number t mod n inside the message startElection.

2) If the node has received a sufficient (2f+1) number of checked startElection messages with the same t it becomes the node-candidate for the term t. As a result, it sends a requestVote message to all nodes. This message contains the value of term, the last element of its ledger and 2f+1 startElection requests:

3) node that receives the requestVote message checks the following condition

$$(t_{requestVote} >= t_{node})$$
and
(requestVote has 2f+1 checked startElection messages)
and
$$(lastLogEntry_{requestVote} \text{ corresponds } lastLogEntry_{node})$$

If all checks are successful, node gives its vote to the node-candidate by sending it a grantVote message.

If the above check fails, the node tries to initiate the re-election procedure (step 1-2)

4) If the node-candidate receives 2f+1 valid grantVote messages, it becomes the node-leader and sends to the rest nodes the leaderAcknowledge message certifying the fact

of its leadership. This message contains the leader's term and information about the nodes that voted for the leader.

5) The node that receives the message leaderAcknowledge, checks it, taking into account the value of term (the term in the message is greater than the term of the node), increases its term and becomes a node-follower (usual node) using this leader.

If this check fails, the node tries to initiate the re-election procedure (step 1-2)

IV. TOKENOMICA: COMMON DESCRIPTION AND AGREEMENTS

Tokenomica is an arrangement between elements of a distributed system which is based on the application of crypto currency (tokens). In our system the tokenomica is aimed at ensuring high performance of individual components (fault tolerance, integrity and performance). Such performance of individual components should ensure the stability of the system as a whole.

The system is operated by the transmission and processing of asynchronous messages between nodes.

To find the optimal parameters for the functioning of the system and its components, we define an information model containing information about the chronology of the actions performed by participants in the action system.

Such a model can be formulated in a natural way on the basis of a representation of the functioning of the system in the form of an oriented loaded graph whose nodes are the servers of the system (more precisely, their participation in a certain stage of interaction in a certain role protocol); communications are messages or queries marked with information accompanying these communications.

A route in such graph describes the sequence of stage executions of the communication protocol which leads to the achievement of the result. At this point you can determine the share of the participant's remuneration based on the effectiveness of his participation in the protocol.

The proposed tocenomic system is functioning under the following agreements:

1. The certificate and all transactions for the transfer of funds for its issuing and maintenance are stored together in blockchain, forming a separate unit.

2. When the request for work appears, the nodes make stakes, which guarantees their honest and reliable functioning. The amount of these stakes and the payment of the certificate by the Client form the overall budget of the certificate.

3. When the protocols are executed, information about the contribution of each node to the overall work is transmitted.

4. The remuneration (budget) of each measure is distributed in accordance with the stake and the share of each bona fide node within its current clock cycle.

5. When charging remuneration for the issuing and maintenance of certificates, the commission is not charged.

V. BUDGET FORMATION

For the issuance and maintenance of the life cycle of each certificate system gets from the client (via receptionNode) a certain token amount S_{client}. It is called the internal price of the certificate in system tokens. Then by s_i we denote the stake of the i-th node, which is lost if the node was among f (faulty) or c (crashed) nodes in the current beat. The purpose of the stakes is to stimulate reliable functioning. Then the budget of the certificate can be calculated using the following formula:

$$B_{CSR} = S_{client} + \sum s_i$$

There are four staking models:

1) Free Stake Fixed Model: All nodes of the network can either play at a fixed stake σ, or not play at all;

2) Free Stake Gambling Model: A model that provides the freedom to choose a stake in a certain range, or not play at all;

3) Force Stake Fixed Model: Participants play only at a fixed rate σ;

4) Force Stake Gambling Model: The model that is obliged to play, however, allows you to independently determine the value of the stake in the range.

Forced stakes make it economically unsuitable for node downtime. Multiple downtime jeopardizes the functioning of the quorum in the certificate issuance system. Gambling Model allows nodes to build their reputation, reliable nodes can afford to make stakes of a larger size. Thus, the Force Stake Gambling Model is the preferred option for efficient and stable network operation.

Note that the proposed scheme of tokenomics provides economic motivation for all processes implemented by the proposed protocol: issuing a certificate, writing to the ledger and maintaining its integrity.

VI. CONCLUSIONS.

A consensus protocol is proposed for use in the system of issuing certificates. The protocol provides a trusting relationship and, as a consequence, maintaining the coordinated state of the ledger between the participants, despite the presence of an acceptable number of Byzantine errors in the system.

The search for specific parameters of the tokenomics for the effective operation of the system is the subject of further research. Due to the fact that the tokenomics parameters in the proposed scheme are expressed in the protocol messages, it is possible to build a multifactor simulation model for the optimal configuration of the model.

REFERENCES

[1] M. Jakobsson, ; A. Juels, "Proofs of Work and Bread Pudding Protocols". Communications and Multimedia Security. Kluwer Academic Publishers: 258–272, 1999.

[2] G. G. Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M.K. Reiter, D-A. Seredinschi,O. Tamir, and A.Tomescu, “SBFT: a Scalable Decentralized Trust Infrastructure for Blockchains,” Cornell University Library, April 2018.

[3] D. Ongaro, and J. Ousterhout, “In search of an understandable consensus algorithm,” In Proc ATC'14, USEN1X Annual Technical Conference, 2014.

Symmetry in dermatology versus in science

Piotr Milczarski
Faculty of Physics and Applied Informatics
University of Lodz
Lodz, Poland
piotr.milczarski@uni.lodz.pl

Zofia Stawska
Faculty of Physics and Applied Informatics
University of Lodz
Lodz, Poland
zofia.stawska@uni.lodz.pl

***Abstract*—In the paper, definitions of object symmetry have been discussed. Dermatological asymmetry measure in shape (*DASMShape*) and its two implementations are also presented. Then, the results of (a)symmetry classification using several methods have been compared: kNN, NN, C4.5, Random Forrest and SVM. They have been applied to the skin lesion asymmetry assessment. Comparing the results of DASMShape measures and a lesion asymmetry given by the experts in PH2 dataset we achieved the best accuracy (83.2%) using SVM with RBF kernel function for the DASMShape. Although the NN results are lower by 9.5% it is always overestimating the asymmetry.**

Keywords—dermatological asymmetry of skin lesion, classification of dermatological features, support vector machine, kNN, neural network.

I. INTRODUCTION

Symmetry of the object is an important feature in many different areas. Symmetry is usually associated with the mathematical concept, but it is equally important, for example in psychology or medicine. It plays a significant role in the field of computer vision. It can be useful both for detecting objects in an image and for classifying them. Symmetry of objects has been studied by many authors. They have suggested a great variety of methods of defining it. The first works of the symmetry as an computer science instance appeared with the rise of the computers epoch in 40's and 50's of 20 century. The most important ones are summarized below:

- Shape description using weighted symmetric axis features. The symmetry axial transform (SAT). SAT has an ability to retrieve only maximal axes of symmetry [15].
- SURF is a patented local feature detector and descriptor, applied in object recognition, image registration, classification or 3D reconstruction. SURF was conceptually based on scale-invariant feature transform (SIFT) descriptor [3].
- Retrieving of a global symmetry (if it exists) from the local curvature of contours, through the locus of mid-edge-point pairs [16].
- A vector potential is constructed from the gradient field extracted from filtered images. Edge and symmetry lines are extracted through a topographical analysis of the vector field [17].
- Symmetries are based on the evaluation of the axial moment around its center of gravity. Gray levels are considered the point masses. The descriptor has been applied at a local level to define DST. Object symmetries are studied with axial moments of regions previously selected [6].
- The scale-invariant feature transform (SIFT) is an algorithm in computer vision to detect and describe local features in images [13][19].
- A "measure" of symmetry and an axis orientation are provided at each point. It is computed in convolving with the first and second derivative of Gaussians [18].
- The symmetry descriptor of a given object is based on a cross correlation operator evaluated on the gray levels [9].
- Axial symmetry of pigmentation refers to pattern symmetry around any axis through the center of the lesion. This does not require the lesion to have symmetry of shape [10].
- Complex moments - Fourier or Gabor transforms of the images [14][20].
- A measure is built of two terms: symmetric and asymmetric energy. Minimizing the asymmetric term of the energy over an image [21].
- The automatic extraction of skin lesion's boundary to measure symmetry applying minimal boundary box [29].
- The axial symmetry of pigmentation refers to pattern symmetry around any axis through the center of the lesion [31]
- Axial symmetry of pigmentation refers to shape, hue/color and structure distributed on symmetry around any axis through the center of the lesion or two perpendicular axes [32].
- The lesion is bisected by two lines that are placed 90° to each other. The first line attempts to bisect the lesion at the division of most symmetry and the other one is placed 90° to it [33]
- Based on selection of equidistant points along contours or equiangular edge points around the patterns centre-of-mass (centroid). From these n points the nearest Cn-symmetric pattern is built in rotating the average of the counter rotation version of the points by $2i\pi/n$, $[0 \leq i \leq n-1]$ [7]
- Given any symmetry transform S, SK of a pattern P is the maximal included symmetric sub-set of P for all directions and shifts. The associated symmetry

measure is a modified difference between the respective surfaces of a pattern and its kernel [22].

Symmetry in Dermatological/Dermoscopic Images

In many areas, the notion of symmetry deviates slightly from its mathematical definition. For example, in dermatology, symmetry is an significant element in the diagnosis of skin lesions. It should be noted, however, that this concept includes not only the symmetry of shape, but also the symmetry of color and structure of skin lesion, which are understood as a kind of differentiation in the lesion area. Diagnosis of the lesions requires an algorithms detecting disease changes [30]. There are several known methods used by dermatologists in the case of disease changes detecting: ABCD or ABCDE rule, three-point or seven-point checklist [2]. The expanded version of 3-point checklist are CASH algorithm[11] and extended 3PCLD (x3PCLD) [12]. Each of these methods takes into account symmetry of the lesions. They are defined as follows:

- 3-point checklist [2][32] – symmetry is treated as symmetry of shape, color/hue and/or structure in one or two perpendicular axes;
- 7-point checklist [8] – this method doesn't take into account symmetry directly but takes into account irregularity of some parameters as shape and distribution of pigment network, dots, globules or streaks;
- ABCD and ABCDE rule [8] – first point of both rules is **A**symmetry - the two halves of the area may differ in shape. This rules also takes into account irregularity of the lesion border;
- CASH algorithm [11] – one of four criteria taking into account in this method is symmetry;
- Menzies method [10] – this method uses so called "negative" and "positive" features. Symmetry is in the group of negative ones and it means symmetry of all pattern structures, including color along any axis through the center (of gravity) of a lesion.

The examples of the methods of symmetry applied for the images can base on textures rotation invariance like in [23]. For the melanoma asymmetry there are several approaches like in Hernandez [24] and Milczarski [25].

The skin lesion asymmetry measure methods can be divided into two groups. The first approach is based on a description of several regions in reference to a set of axes e.g. in [26], [27]. The second approach use is to region convexity from which asymmetry is inferred [28].

In the paper, we will check which classification method SVM, kNN, Random Forrest, NN and C4.5 is the best in dermatological asymmetry assessment.

The paper is organized as follows. Section II shows dermoscopic asymmetry measure as a function of a shape, hue/color and structure. In addition, results and observations of different asymmetry of shape functions are shown in Section III as well as the conclusions.

II. Dermatological Asymmetry Measure in Shape

Dermatological asymmetry (DAS) was defined by the dermatologists [2] and in our previous works [4] and [5]. The method of calculation of the asymmetry values and DASMShape measure consists of six steps.

In the first step the geometrical center of the lesion (or binary mask of the lesion) is calculated.

In the second step the axis is put through the geometrical center. The resemblance in the shape of two obtained, partial images is calculated and compared to the size of the lesion. If the result is higher than the threshold ti, then the axis is regarded as the symmetry axis for that shape with a threshold ti. The number of symmetry axes for that threshold n(ti) is raised by 1. To speed out the method the resemblance in shape and number of symmetry thresholds are calculated at the same time for a chosen set of thresholds { t1, … , tn}, where n>1.

Then the axis is rotated by the defined earlier angle e.g. 5°. The second step calculations are done again and n(ti) are increased by 1 if they fulfill the conditions described in step 2. The method is continued until the axis is rotated 180° around the geometrical center.

The number of symmetry axes n(ti) has maximum that depends on the initial rotation angle e.g. for 5° we achieve 180°/5°=36. To avoid regarding 2 symmetry axes as the one we regard 2 axes as one if they differ less than 10°. Hence, we can result in the maximum number of 18 symmetry axes.

In the third step the vector of the shape symmetry W for the given image is calculated. It is defined as

$$\mathbf{W} = [n(t_1), n(t_2),\ldots, n(t_k)] \quad (1)$$

In the paper, the vector **W** is calculated using 5 thresholds:

$$n(t)=\{0.9, 0.93, 0.94, 0.95, 0.97\} \quad (2)$$

In the fourth step, the DASMShape function is designed as the one depending on the vector W. We propose to build the DASMShape function as an exponential or a rational one.

Dermatological Asymmetry Measure in Shape was presented as exponential and rational ones normalized in values to the interval (0,2>. The first, exponential type function is described by the formula:

$$DASMShape(W) = 2e\hat{}(-f(W)) \quad (3)$$

where f: Rk → R+ ∪ {0} and can be regarded as a polynomial function of the n(ti). In the paper, the exponential function is labelled as DASMShape2 with the coefficients of the inner f(W) function given like in [5].

The second example of the DASMShape function, a rational one is given as function of W:

$$DASMShape(W) = \frac{2}{f(W)} \quad (4)$$

where inner function $f: R^k \rightarrow <1, \infty)$ and it is also a polynomial function of $n(t_i)$. In the paper, the exponential function is labelled as DASMShape1 with the coefficients of the inner $f(W)$ function given like in [5].

Both functions are used in the procedure in asymmetry/symmetry of the lesion asymmetry derivation.

In the **fifth** step, for each of the DASMShape functions a set of two crisp shape thresholds (ST): ST={*lst, ust*} (see Diagram 1) is introduced. The values of *lst* and *ust* are from the interval (0,2) and might be related to the type of the function given in equations. (2) and (3) as well as the formula of the function *f(W)* [4][5].

The final choice of the coefficients *lst* and *ust* is derived using optimization procedure that takes into account maximum accuracy and minimum number of underestimated cases. From the dermatological point of view it is better to overestimate the result of non-invasive diagnosis. That is why the second optimization criterion has been used.

In the **last** step, using the formulas that are in the last position of the Diagram 1, the DASMShape value is achieved.

Dermoscopic datasets

There are a few publicly available databases of dermoscopy images. PH2 [34] and EDRA [35] image databases are most commonly used by the research communities. The other example is the ISIC Archive for the Melanoma project which is a large public database of dermoscopy images **[1]** created by International Skin Imaging Collaboration (ISIC).

In the paper, PH2 is used as the reference dataset in our research. The examples of the skin lesions with binary masks are given in Fig. 1. The coefficients of the vector of shape symmetry **W** are provided in the left part of Tab. I for the images from PH2 with ids IMD075, IMD211, IMD404, IMD406.

After optimization of the thresholds values for the coefficients $\mathbf{a_x}$,$\mathbf{a_y}$, $\mathbf{a_z}$, for the exponential version of the DASMShape function are used [5]. The coefficients $\mathbf{a_m}$ and $\mathbf{a_k}$ are used for the polynomial one [5].

The values of the DASMShape function for that images are provided in the right part of Tab. I. The column with the coefficient $\boldsymbol{a_m}$ is the one used in DASMShape1 and the column $\boldsymbol{a_z}$ is the one used in DASMShape2. The other vectors $\boldsymbol{a}$ are shown to present the values of the dermatological symmetry function.

III. Results and Conclusions

In the research, several versions of function *f (***W***)* in (2) and (3) with different coefficients and for a different subset of thresholds but for the same symmetry thresholds given in (1).

In the DASMShape1 and DASMShape2 cases the vectors of shape symmetry **W** have been constructed using the same values , see Tab. I.

TABLE I. The Examples Of Shape Symmetry Vectors W From The Training Set

No.	Number of symmetry axes					DASM Shape
	n(0.9)	n(0.93)	n(0.94)	n(0.95)	n(0.97)	
1	16	16	16	16	16	0
2	4	4	4	4	4	0
3	2	2	2	2	2	0
4	8	6	4	4	2	0
5	8	6	4	2	1	0
6	4	4	3	3	2	0
7	1	0	0	0	0	2
8	1	1	0	0	0	2
9	3	1	0	0	0	2
10	5	0	0	0	0	2
11	5	1	0	0	0	2
12	2	1	1	0	0	2
13	5	3	2	1	1	1
14	3	3	2	1	1	1
15	2	1	1	1	1	1
16	8	5	3	3	3	1
17	5	3	3	3	3	1
18	7	3	1	1	1	1

In our experiments we have tested three versions of kNN (1NN, 3NN, 5NN), 2 versions of SVM (RBF and linear function), C4.5, Random Forrest and NN classifiers with different set of properties. We have prepared the training set containing 38 cases of shape symmetry vector

W. Some example are presented in Tab. I.

In the first step the training set was cross-validated to check the baseline accuracy. The cross-validation accuracy was 86.8% for 3NN, 97.4% for NN and 100% for SVM, C4.5 and Random Forrest.

TABLE II. The Vectors Of Shape Symmetry **W** For The Example Images From the PH2 Dataset

Image ID from PH2	VoSS vector W coefficient values					*DAS* (PH2)	DASMShape values for f(W) and coefficients a				
	n(0.9)	*n*(0.93)	*n*(0.94)	*n*(0.95)	*n*(0.97)		$\mathbf{a_x}$	$\mathbf{a_y}$	$\mathbf{a_z}$	$\mathbf{a_k}$	$\mathbf{a_m}$
IMD152	10	2	2	0	0	**0**	0.50991	0.57888	0.66131	1.60	0.66667
IMD211	2	1	1	1	0	**1**	1.25627	1.48164	1.18193	1.31406	0.90909
IMD242	3	0	0	0	0	**2**	1.82786	1.82786	1.92928	1.99401	1.53846

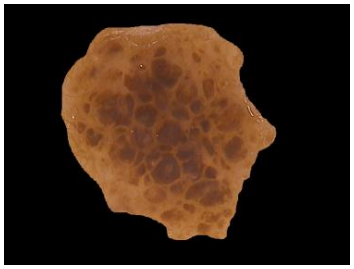
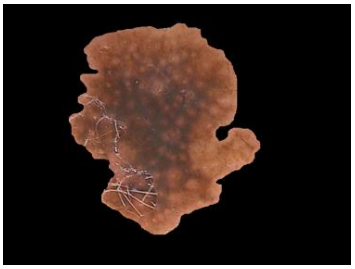
a)  b)  c) 

Fig **1**. The masks of the selected lesions from PH2 dataset [13] with dermatological asymmetry DAS:
a) IMD152 (Common Nevus) DAS=0; b) IMD211 (Nodular Melanoma) DAS=1; c) IMD242 (Lentigo Maligna) DAS= 2

TABLE III. SKIN LESION ASYMMETRY CLASSIFICATION RATE USING THE BEST CLASSIFIERS

Classifier	Type of DAS/ DASMShape	Number of Corr. Classified Instances	Number of Incorr. Classified Instances	Class. ratio	TP rate for a class			FP rate for a class		
					0	1	2	0	1	2
3NN	DAS(PH2)	57	110	34.1	18.7	61.3	62.1	10.0	55.9	20.3
	DASMShape1	97	70	58.1	30.2	100	82.1	0.0	49.3	0.0
	DASMShape2	100	67	59.9	28.9	96.7	95.7	0.0	48.2	0.8
SVM (RBF)	DAS(PH2)	83	84	49.7	48.6	41.9	62.1	23.3	31.6	19.6
	DASMShape1	134	33	80.2	75.6	96.0	80.4	1.2	22.5	0.0
	DASMShape2	139	28	83.2	71.1	100	95.7	2.6	19.0	0.0
NN	DAS(PH2)	76	91	45.5	40.2	45.2	65.5	16.7	33.8	25.4
	DASMShape1	107	60	64.1	53.5	60.0	82.1	8.6	31.7	7.2
	DASMShape2	123	44	73.7	58.9	76.7	100	0.0	27.0	5.8
C 4.5	DAS(PH2)	71	96	45.5	40.2	29.0	65.5	18.3	28.7	33.3
	DASMShape1	122	45	73.1	62.8	80.0	85.7	0.0	19.7	15.3
	DASMShape2	123	44	73.7	60.0	73.3	100	0.0	19.0	15.0
RF	DAS(PH2)	67	100	40.1	34.6	35.5	65.5	15.0	33.1	33.3
	DASMShape1	114	53	68.3	53.5	80	85.7	0.0	25.4	15.3
	DASMShape2	115	52	68.9	51.1	73.3	100	0.0	24.8	15

In the Tab. III, the best classification ratios as well as true positive and false positive classification ones are presented. We achieved the best results for 3NN, SVM with radial basis kernel function (RBF) and neural network with one hidden layer with 10 nodes. Although for the DASMShape2 measure, the SVM with RBF is achieving the best results (83.2% accuracy), the NN classifier (73.7%) always overestimated the asymmetry of the lesion while SVM was underestimating the classification results in two asymmetric cases (DASM=2) and gave them the asymmetry equal 0. The 3NN classifier is achieving almost 60% accuracy but taking into account that using the training set we achieved inner accuracy 86.8%, we can assume that its overall accuracy is around 70%.

In the case of dermatological asymmetry measure that is provided in PH2 dataset [34] the vectors of shape symmetry W have been constructed using the same values as in the DASMShape1 and DASMShape2 cases. DAS measure from PH2 is giving the lowest results but that measure takes also into account asymmetry in color/hue and structures distribution.

It can be concluded that the mathematical definition of the symmetry summarized in the first section generally differs from the dermatological one. The results shown in the row for DAS(PH2) confirm that.

REFERENCES

[1] ACS – American Cancer Society - https://www.cancer.org/research/cancer-facts-statistics.html.

[2] G. Argenziano, H. P. Soyer, S. Chimenti, R. Talamini, R. Corona, F. Sera, M. Binder, L. Cerroni, G. De Rosa, G. Ferrara and R. Hofmann-Wellenhof, "Dermoscopy of pigmented skin lesions: results of a consensus meeting via the Internet," Journal of the American Academy of Dermatology, vol. 48, no. 9, pp. 679-693, 2003.

[3] H. Bay, A. Ess, T. Tuytelaars, L. Van Gool, "SURF: Speeded Up Robust Features," Computer Vision and Image Understanding (CVIU), 110(3), pp. 346-359, 2008.

[4] P. Milczarski, Z. Stawska, L. Was, S. Wiak, M. Kot., "New Dermatological Asymmetry Measure of Skin Lesions," Int. Journal of Neural Networks and Advanced Applications, Vol.4, pp. 32-38, 2017.

[5] P. Milczarski, Z. Stawska and P. Maslanka, "Skin Lesions Dermatological Shape Asymmetry Measures," In: Proceedings of the IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, pp. 1056-1062, 2017.

[6] V. Di Gesù, C. Valenti, "Symmetry operators in computer vision," Vistas Astronom. 40(4), 461-68, 1996.

[7] H. Zabrodsky, S. Peleg, D. Avnir, "Symmetry as a continuous feature," IEEE Pattern Anal. Mach. Intell. 17(12), 1995.

[8] G. Argenziano, G. Fabbrocini, P. Carli, V. De Giorgi, E. Sammarco, M. Delfino, "Epiluminescence microscopy for the diagnosis of doubtful melanocytic skin lesions. Comparison of the ABCD rule of dermatoscopy and a new 7-point checklist based on pattern analysis," Arch. Dermatol. 134, pp. 1563-1570, 1998.

[9] G. Marola, "On the detection of the axes of symmetry of symmetric and almost symmetric planar images," IEEE Trans. Pattern Anal. Mach. Intell. 11, 104–108, 1989.

[10] S.W. Menzies, K.A. Crotty, C. Ingvar, W.H. McCarthy, "An atlas of surface microscopy of pigmented skin lesions: Dermoscopy," 2nd edn. Roseville McGrawHill, 2003.

[11] J.S. Henning et al, "The CASH (color, architecture, symmetry, and homogeneity) algorithm for dermoscopy," J Am Acad Dermatol. 56(1), 45-52, 2007.

[12] L. Was., P. Milczarski, Z. Stawska et al., "Analysis of skin diseases using segmentation and color hue in reference to melanocytic lesions," in LNCS 10245, Springer, pp. 677-689, 2017.

[13] D.G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," Int. J. of Computer Vision. 60 (2), pp. 91-110, 2004.

[14] J. Bigun, J.M.H. DuBuf, "N-folded symmetries by complex moments in Gabor space and their application to unsupervized texture segmentation," IEEE Pattern Anal. Mach. Intell. 16(1), 1994.

[15] H. Blum, R.N. Nagel, "Shape description using weighted symmetric axis features," Pattern Recognition 10, pp. 167-180, 1978.

[16] M. Brady, H. Asada, "Smoothed local symmetries and their implementation," Int. J. Robot. Res. 3(3), pp. 36–61, 1984.

[17] A.D.J. Cross, E.R. Hancock, "Scale space vector fields for symmetry detection," Image Vision Comput. 17(5-6), pp. 337–345, 1999.

[18] R. Manmatha, H. Sawhney, "Finding symmetry in intensity images," Technical Report, 1997.

[19] D.G. Lowe, "Object recognition from local scale-invariant features," In: Proc. of Int. Conf. on Computer Vision, 2, pp. 1150-1157, 1999.

[20] D. Shen, H. Ip, K.T. Cheung, E.K. Teoh, "Symmetry detection by generalized complex moments: a close-form solution," IEEE Pattern Anal. Mach. Intell. 21(5), 1999.

[21] D. Shen, H. Ip, E.K. Teoh, "An energy of assymmetry for accurate detection of global reflexion axes," Image Vis. Comput. 19, pp. 283-297, 2001.

[22] B. Zavidovique, V. Di Gesù, "The S-kernel:Ameasure of symmetry of objects," Pattern Recognition 40, pp. 839-852, 2007.

[23] P. Milczarski, Z. Stawska, L. Was, S. Wiak and M. Kot, “New Dermatological Asymmetry Measure of Skin Lesions,” Int. Journal of Neural Networks and Advanced Applications, Prague, pp. 32-38, 2017.

[24] D.A.G. Hernández, R. Santiago-Montero, „Border and Asymmetry measuring of skin lesion for diagnostic of melanoma using a perimeter ratio,” Asian Journal of Computer Science and Information Technology, vol. 6, no. 2, pp. 7-13, 2016.

[25] P. Milczarski, „Symmetry of Hue Distribution in the Images,” Artificial Intelligence and Soft Computing ICAISC'18, pp. 48-61, 2018.

[26] S.M. Rajpara, A.P. Botello, J. Townend, A.D. Ormerod, “Systematic review of dermoscopy and digital dermoscopy/artificial intelligence for the diagnosis of melanoma,” British Journal of Dermatology, 161(3), pp. 591-604, 2009.

[27] T.D. Satheesha, D. Sathya-Narayana, M. Giriprasad, “Review on early detection of melanoma,” In: Proccedings of International Journal of Advanced Technology and Engineering Research, 2(4), pp. 80-90, 2012.

[28] Z. Liu, J. Sun, L. Smith, M. Smith, R. Warr, “Distribution quantification on dermoscopy images for computer-assisted diagnosis of cutaneous melanomas,” Medical and biological engineering and computing, 50(5), pp. 503-513, 2012.

[29] N.M. Sirakov, M. Mete, and N.S. Chakrader, “Automatic boundary detection and symmetry calculation in dermoscopy images of skin lesions,” In: 18th IEEE International Conference on Image Processing, Brussels, pp. 1605-1608, 2011.

[30] C. Rosendahl, A. Cameron, I. McColl, D. Wilkinson, “Dermatoscopy in routine practice: ‘Chaos and Clues’,” Aust Fam Physician. 41(7), pp. 482-487, 2012.

[31] H.P. Soyer, G. Argenziano, R. Hofmann-Wellenhof, I. Zalaudek, “Dermoscopy: The Essentials,” 2nd ed. Saunders Ltd., 2011.

[32] H.P. Soyer, G. Argenziano, I. Zalaudek, R. Corona, F. Sera, R. Talamini et al., “Three-point checklist of dermoscopy. A new screening method for early detection of melanoma,” Dermatology 208(1), pp. 27- 31, 2004.

[33] W. Stolz, A. Riemann, A.B. Cognetta, L. Pillet, W. Abmayr, D. Hölzel, et al., “ABCD rule of dermatoscopy: a new practical method for early recognition of malignant melanoma,” Eur J. Dermatol. 4, pp. 521-527, 1994.

[34] T. Mendoncca, P.M. Ferreira, J.S. Marques, A.R.S. Marcal, J. Rozeira, “PH2 – A dermoscopic image database for research and benchmarking,” In: 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Osaka, pp. 5437-5440, 2013.

[35] G. Argenziano, H. P. Soyer, V. D. Giorgio, D. Piccolo, P. Carli, M. Delfino, A. Ferrari, R. Hofmann-Wellenhof, D. Massi, G. Mazzocchetti, M. Scalvenzi and I. H. Wolf, “Interactive atlas of dermoscopy,” Milan: Edra Medical Publishing & New Media, 2000.

Decision support system for set-up of investment portfolio as a part of company development program

Valentina Moskalenko
Department of Software Engineering and Management Information Technologies
National Technical University «Kharkiv Polytechnic Institute»
Kharkiv, Ukraine
valentinamosk17@gmail.com

Svitlana Kachanova
Department of Software Engineering and Management Information Technologies
National Technical University «Kharkiv Polytechnic Institute»
Kharkiv, Ukraine
ksvetlana13.96@gmail.com

***Abstract*—The analysis carried out in this paper describes the functionality of existing investment decision support systems. A business process for the formation of an investment portfolio as part of the company development program was proposed. The portfolio consists of three parts: a portfolio of development projects of the company, a portfolio of projects of other companies and a portfolio of securities. The architectural solution for the software implementation of the decision support system in the field of portfolio investment is presented. It is proposed to present the DSS for the formation of an investment portfolio in the form of five containers, in which the corresponding tasks are performed: evaluation of investment projects; evaluation of securities; Assessment of the importance of investments for the development of the company; allocation of the company investment funds between portfolios; formation of the company investment portfolio. This decision support system is associated with Enterprise Performance Management systems which are designed for information and analytical support of strategic company management processes. Implementing of DSS that the user can solve package investment problems for making certain investment decisions and solve them in package for implementing the company development program during the strategic period.**

Keywords—investment, decision support system, software architecture, service-oriented architecture.

I. INTRODUCTION

The investment program is the mean of the company's strategic plan implementation. The investment program is the whole of investment projects and amounts of their financing within the strategic period. The plan for implementing a set of investment projects is determined by the company investment policy, which, in turn, depends on the strategic objectives of the company. The investment program of the company also covers the determination of the size and structure of the capital necessary for its implementation. Since the formation and implementation of the investment program involves the collection and analysis of a large number of heterogeneous information, with the solution of a multitude of tasks, decision support systems are being introduced into the investment management system. The software market offers various systems that support the processes of managing companies' investments in information and analytics. However, in the conditions of a dynamic investment market, with the advent of new mechanisms and sources of financing for the activities of various companies, there is a need to use new information technologies and to revise the structure of such systems. In this paper, an architectural solution for a decision support system is proposed. It will allow implementing of DSS in the form of a software package in such a way that the user can solve package investment problems for making certain investment decisions and solve them in package for implementing the company development program during the strategic period..

II. LITERATURE REVIEW

Not only advanced information technologies in the field of collection, storage and analysis of data on investment objects are used in modern DSS, but also new models, methods for solving investment problems, for example, investment valuation, investment portfolio set-up, etc. This is due to the fact that the objects of investment, the nature of the factors affecting the investment attractiveness of these facilities, etc. change. In the conditions of the modern investment market functioning some questions arise with regard to attracting investments for social projects For example, the decision-making model for participation in social venture capital (SVC) was proposed in [1]. The evaluation is carried out using this model for various aspects related to investment decisions. The investment attractiveness of a company that needs investments is assessed in terms of the following aspects: previous experience of the investor with the company (past); financial condition of the company and its intangible assets (present); a proposed project for investment, which is assessed on the basis of financial and social criteria (future). As a result, the investment object is estimated using 26 criteria and 160 indicators, their priorities are determined by the process of the variant analysis method (AHP). This, on the one hand, makes it possible to simplify the difficult task of assessment through hierarchical analysis, but, on the other hand, subjective judgments of experts are used, which cannot always reflect the real situation. The models of mathematical programming are most often used for the investment portfolio forming. The task of forming project investment portfolios is traditionally considered as the multi-criteria problem. For example, the DSS proposed in [2] is based on single-criterion and multi-criteria optimization models with the possibility for an investor to choose different criteria for profitability and risk for project selection. Methods of mathematical programming

are also widely used to form a portfolio of securities [3, 4]. Multi-criteria decision-making technology is used in [5]. The choice of an investment object is simplified if you use the AHP method. As a result, the system allows you to create a rating of criteria for selecting securities by the user, and then evaluate them and make investment decisions. This approach is appropriate only for making decisions on the purchase of a individual securities, it will be difficult to form an investment portfolio for a long period with the help of this system. Many scientific references pay great attention to the analysis of information about the object of investment. The three-layer structure of DSS is proposed in [6] and consists of Analysis, Synthesis and Investment Decision Support System. The multidimensional dynamics of the investment market is determined at the first level. Multidimensional dynamics is synthesized to reflect real and potential market situations at the second level. The support for making investment decisions is based on traditional methods of solving investment problems at the third level. Conclusions can be made on the basis of analysis of structures and analytical-algorithmic support of investment decision-making processes. The systems that were offered are mainly intended for analysis and decision making on one type of investment object - either securities or investment projects, in some cases - real estate objects [7]. A number of studies most often contemplate an investment object on the basis of indicators of profitability and risk. Investments invested in projects or securities are not analyzed from the perspective of the development of an investor company which makes it difficult to use such systems for making long-term decisions, for the formation of a development program for the company.

III. Purpose and Objectives of the Research

A. Business process of investment portfolio formation

We will assume that all projects, that are included in the investment program, relate to the activities of the enterprise in the field of external and internal investment. By internal investment we will understand the investment of the company funds for its own development, for example, modernization and expansion of production capacities, introduction of new technologies, etc. External investment involves investing in the company securities and projects that are implemented by other organizations, companies, etc. The goal of external investment can be not only obtaining investment profit, but also, for example, merging enterprises within the strategy against competitors, the strategy of horizontal or vertical integration of related enterprises, etc. The strategy, investment policy and investment portfolios are developed for each type of investment activity. Thus, within the framework of the investment policy it is necessary to form:

- investment projects portfolio of company development;
- real and financial investment portfolios within the framework of external investment activities.

Then the business process of forming an investment portfolio is proposed to be presented in the form of the following basic procedures (Fig. 1).

A1. Allocation of investment resources to the types of investment portfolios. For this, an algorithm is used that implements the mechanism of proportional allocation of a homogeneous resource. The utility function is proposed as the allocation criterion. The utility function includes the criteria of profitability and risk, as well as a criterion for estimating investments in an object in terms of the importance of such an investment for the company development prospects.

A2. Formation of an investment projects portfolio which will be implemented in this company as a part of the enterprise development program. The general process of the formation of this program is presented in [8]. This process is built on the concept of strategic alignment [9, 10]. The plans of the divisions are formed over the years of the strategic period. Based on the decomposition of strategic objectives and cascading key performance indicators. The key indicators that characterize the company investment activity are also determined. Investment projects are evaluated in terms of their significance for the development of the enterprise. This portfolio is a set of projects for the years of the strategic period.

A3. Portfolio of external investment is formed by a preliminary analysis of investment projects that will be implemented by other companies. The portfolio of projects is formed on the basis of this analysis, and the formation of portfolios is carried out over the years of the strategic period according to the model of multi-criteria optimization. The following criteria are considered as criteria: maximizing the profitability of investments, minimizing risks, and maximizing the importance of investing investment funds in a project for the development of an investor company.

A4. Preliminary selection is carried out during the implementation of the procedure for forming a portfolio of securities which are important for the company from the perspective of its development prospects. Then, models of financial portfolio formation are used, which use the criteria for maximizing the profitability of investments and minimizing their risks.

A5. The company total investment portfolio is formed as a combination of three portfolios. Here, the overall yield of the portfolio, the risks and the significance of future investments for development are analyzed. Key indicators of investment activity were determined during the development program, they will form the basis for deciding whether to approve or revise the portfolio of investments [8].

Therefore, it is possible that it will be necessary to reconsider the importance of selection criteria for investment objects – securities and projects, after analyzing the formed portfolios. Next, it will be necessary to implement this process again, beginning with procedure A 1.

Thus, as a result of the iterative process, the portfolio of investments will be formed; such a portfolio will be implemented by the company within the framework of investment activities in the strategic period.

B. The software package architecture that implements the DSS for investment portfolio formation

Software packages that have different architectures: monolithic; modular; component; client-server; service-oriented, are used to solve investment problems [11]. Applications of monolithic architecture are applicable for solving individual investment problems, for example, assessing the effectiveness of investment projects, forming a portfolio of securities. This limits the use of such architecture for the implementation of DSS in the field of investment management of the company.

Software products with a modular or component architecture assume the decomposition of the application into several parts that can be used multiple times. Such architecture makes it possible to build multifunctional software packages, so it is often used for DSS development. However, the modules must be universal and all together represent a localized softwarepackage.

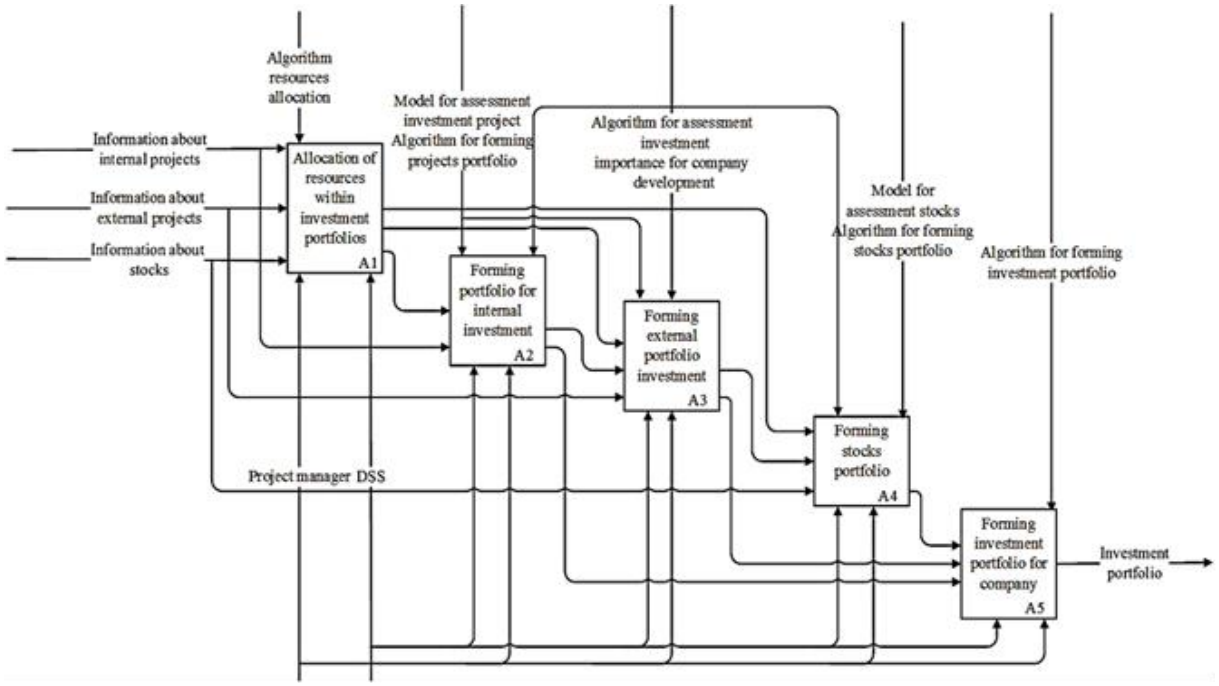


Fig. 1. Business process for the formation of the company investment portfolio

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

Client-server architecture implements the logic of clients' autonomous work with a certain business application that interacts with the server part - the DBMS or the file server. Here, heterogeneous modules interact through information and communication networks. DSS for the formation of an investment project portfolio is built with this architecture according to investment estimates, etc. In service-oriented architecture (Service Oriented Architecture), the interaction of two or more allocated software modules is most fully realized. SOA is used to build package allocated information systems based on the integration of Web services. Since the specifics of large companies, that are engaged in different types of investment, involves the use of different data servers, standalone applications that solve individual investment problems and must be combined together logically into one system for supporting investment decision-making. Therefore, based on the analysis of architectural solutions of software products in the field of investment, it was concluded that SOA is the most acceptable solution for building DSS for investment within the company development management system [12]. SOA allows you to establish links with micro-services, which are focused on solving individual business problems. It is proposed to present the DSS for the formation of an investment portfolio in the form of five containers, in which the corresponding tasks are performed (Fig. 2): evaluation of investment projects; evaluation of securities; Assessment of the importance of investments for the development of the company; allocation of the company investment funds between portfolios; formation of the company investment portfolio. This decision support system is associated with Enterprise Performance Management (EPM) systems which are designed for information and analytical support of strategic company management processes [12]. EPM is a process and software system designed to help companies link their strategies to their plans and their implementation. The objective of EPM is to ensure that strategic goals and objectives are clearly communicated and understood by managers, and are reflected in their budgets and plans. Getting all of the various departments of an organization aligned around goals and objectives is a critical starting point.

IV. CONCLUSIONS

1) The analysis of the existing investment decision support systems functionality was conducted.

2) The business process for an investment portfolio formation as part of the company's development program was proposed. The portfolio consists of three parts: a portfolio of the company's development projects, a portfolio of other companies' projects of and a portfolio of securities.

3) The architecture for software that implements a decision support system in the field of investment portfolio was proposed.

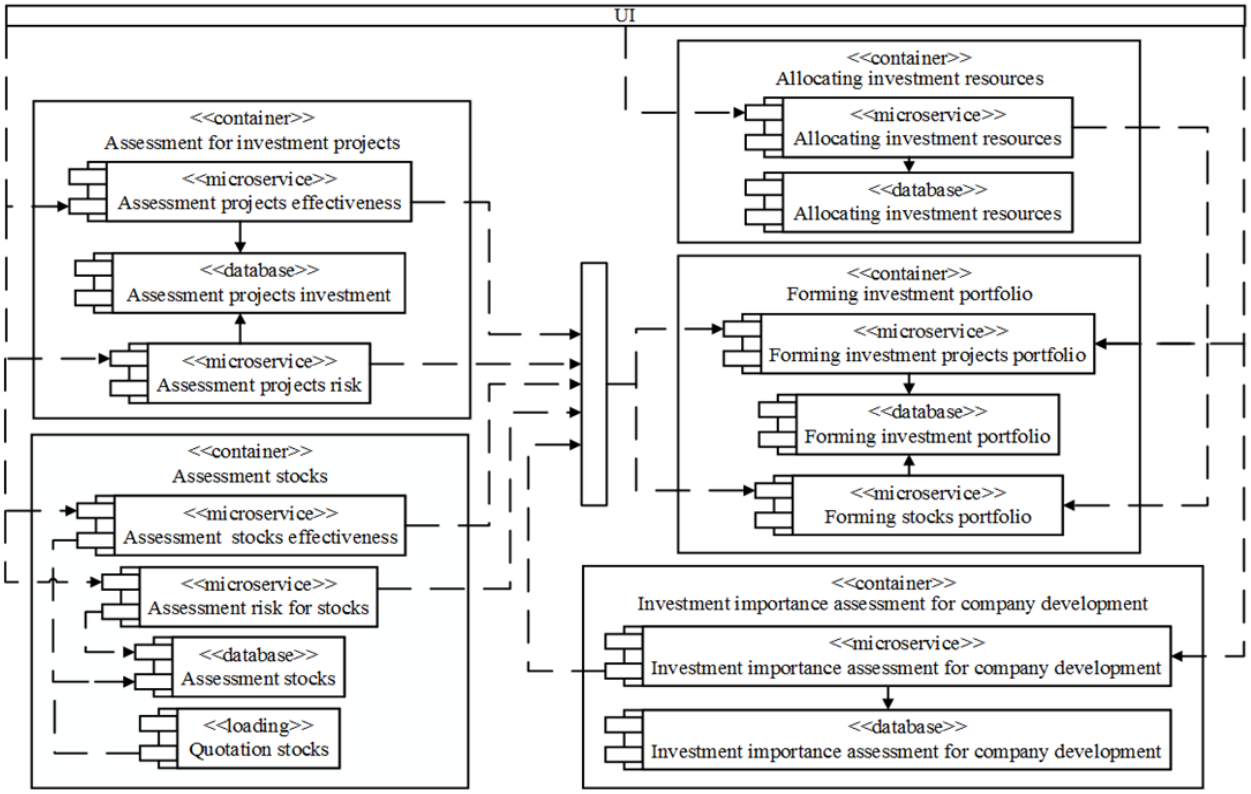


Fig. 2. The software package structure that implements DSS for formation investment portfolio

REFERENCES

[1] C. Serrano-Cinca, and B. Gutiérrez-Nieto, "A decision support system for financial and social investment", in Applied Economics, Taylor & Francis Journals, vol. 45(28), 2013, pp. 4060-4070.

[2] H. C. Caballero, and Schmidt, E. K., "Decision support system for portfolio components selection and prioritizing", Paper presented at PMI® Global Congress 2014 – North America, Phoenix, AZ. Newtown Square, PA: Project Management Institute.

[3] M. Mansoury, B. Mansoury, and S. A. H. Golpayegani, "Enhanced decision support system for portfolio management using financial indicators", in International Journal of Business Information Systems Strategies (IJBISS), 2012, vol. 1, pp. 1–9.

[4] Keerti. S.Mahajan, R .V. Kulkarni, "Stock Market Prediction and Investment Portfolio Selection Using Computational Approach", in Journal of Computer Engineering, V. 17, Issue 3, Ver. VII (May – Jun. 2015), pp. 53–62.

[5] P. Songsangyos, "The Decision Support System for Hierarchical Portfolio Management", in International Journal of Information and Education Technology, vol. 4, No. 4, August 2014, doi: 10.7763/IJIET.2014.V4.423.

[6] W. Chen, L. Cao , and Z. Qin, "An Investment Decision Support System (IDSS) for Identifying Positive, Neutral and Negative Investment Opportunity Ranges with Risk Control in Stock Markets", in International Journal of Intelligent Systems Technologies and Applications, vol. 4, May 2008, pp. 239–253.

[7] R. Valverde, "An adaptive decision support station for real estate portfolio management", in Journal of Theoretical and Applied Information Technology, 2009, pp. 84–86.

[8] V. V. Moskalenko, T.V. Zakharova, and N.G. Fonta, "Technology of formation of development program as a system of company's annual plans based on key performance indicators", in European cooperation Scientific Approaches and Applied Technologies, Vol. 2(2), 2015, pp. 108–124.

[9] H. L. Wang, and A. Ghose, "On the foundations of strategic alignment", The Proceedings of the 2006 Australia and New Zealand Academy of Management Conference. Dunedin, New Zealand, December 2006.

[10] J.Walter, F. W. Kellermanns, S. W.Floyd, J. F. Veiga, and C. Matherne, "Strategic alignment: A missing link in the relationship between strategic consensus and organizational performance", in Strategic Organization, 11(3), 2013, pp.304–328.

[11] B. J. Sovetov, A. I. Vodjaho, V. A. Dubeneckij, and V. V. Cehanovskij, "Architecture of information systems", Izdatel'skij centr "Akademija", Moscow, 2012, 288 p. (In Russ.)

[12] V. V. Moskalenko, and Y. S. Berezenko, "The concept of an architectural solution for the service intended to build an enterprise strategy map", in Bulletin of NTU "KhPI", Series: System analysis, control and information technology, vol 55 (1276), 2017, pp. 45–50.

Module of selecting the company development strategic goals in the Enterprise Performance Management System

Valentina Moskalenko
Department of Software Engineering and Management Information Technologies National Technical University «Kharkiv Polytechnic Institute»
Kharkiv, Ukraine
valentinamosk17@gmail.com

Abstract – The procedure for the strategic goals setting has been considered as a part of the business process for creation of the enterprise development program. For goals selection it is proposed to use the Analytic Hierarchy Process. In consequence of application of direct and reverse analytic hierarchy process, are determined the estimates of changes in the enterprise performance when the goals are reached. Realizing the Analytic Hierarchy Process is carried the comparison of the estimates of changes in the company performance indicators when achieving the goals in question. By analyzing these estimates the potential goals and achievement strategies are selected. Strategies are defined by the aspects of the company development: production, finance, personnel, marketing. The result of this procedure is desired strategic goals selected from among all of such goals which would be less risky, i.e. would be to a lesser extent subject to external impacts. The business process of the development program forming is the basis of the strategic planning module of the Enterprise Performance Management system. Implementation of such a process will permit to realize the strategic alignment and to increase the company efficiency by setting adequate strategic goals.

Keywords – strategic alignment, strategic goal, development strategy, development program, analytic hierarchy process

I. INTRODUCTION

Present-day businesses face multiple challenges with regard to strategic management. One of the major challenges is setting the proper strategic goals and development of strategies to achieve these goals. On a practical level the SMART tool (specific, measurable, achievable, relevant, time-based) is widely used to formulate the goal. Its advantage is the elegancy, it allows the company to move beyond the fuzzy goal and to set the specific result to be achieved. However, the goal statement does not allow assessing its feasibility. Therefore, the issue of setting goals achievable in the conditions of the functioning company continues to be relevant. Also the task is not only to set a strategic goal, but to select effective achievement strategies as well. Therewith, the company must pay due regard to the factors of the external and internal environment influencing the effectiveness of the strategy implementation and the goals feasibility [1]. Such strategic level tasks are solved within the scope of information systems of the company performance management: EPM – Enterprise Performance Management (alternative names: CPM – Corporate Performance Management, BPM – Business Performance Management. At the IT market such systems are offered both by major companies like Oracle EPM, IBM Cognos Disclosure Management, SAP EPM, SAS Strategy Management and small enterprises like Host Analytics, Infor, Longview Solutions, etc. However, these systems do not pay enough attention to verification of the strategic goals feasibility and justification of the choice of the company development goals.

II. LITERATURE REVIEW

Presently, to solve the problems of strategic plans implementation, the strategic alignment process is used. Strategic alignment is seen as a tool to achieve the intended goals [2]. By applying the strategic alignment process the company identifies the processes required for strategies implementation.[3].

Paper [4] deals with the resolution of resource conflicts between the strategies, the conclusion is that it is essential to make allowance for changes in resource needs during the strategies implementation. However, no attention is paid to the procedure for these strategies development, the way of the strategies selection depending on the company's desired goals is not given due regard either.

For successful strategy implementation, some approaches for aligning the company's business processes with the strategic plan are proposed [5]. For instance, the proposed methodology for aligning the processes with the ongoing planning [6] allows for strategic alignment in the company. It is based on generation of system charts for all business processes executors. Such charts permit to increase the organizational understanding of processes. The processes are assessed prospectively; the processes strategic significance is determined by linking each process with the strategic goal directly. Such an approach will unambiguously allow all processes to be linked to the company's goals. However, the paper does not show the mechanisms of the company's goals forming depending on the internal organizational changes that can occur during a long period of the goals achieving.

The widespread use got the concept of cascading the company strategy by management levels down to the individual doers. For instance, paper [7] focuses on

building effective communications, which are necessary to convey the strategy to the lowest management level.

Paper [8] proposes to maintain consistency between the strategy and its operative implementation by establishing a direct link between strategic goals, success factors and project performance indicators. Practical application of such cascading mechanisms permits to improve the efficiency of the company's plans in progress; however, their realizeability will depend on the extent to which the goals themselves are adequate with regard to both the external environment and the internal company status. And such issues are practically not touched upon in these studies.

Information technology (IT) is widely used for implementation of strategic management processes. A lot of studies are devoted to the issues of strategic IT alignment. Paper [9] proposes a model for studying the interrelationships between IT capabilities and business strategies; it also considers the IT strategies alignment in the context of the company development. However, these studies contemplate the issues of organization of the analysis forming processes and the development goals revising simultaneously with setting of IT goals mainly on the "proclamatory" (declarative) level.

Thus, reviewing the existing studies in the field of strategic alignment, it can be concluded that the researchers put main emphasis on creating a link between strategies and their implementation, strategies and business processes, projects and operational plans. However, the issues of checking the adequacy of the strategic goals actually formed as a result of strategic analysis are almost neglected. Still remains the unresolved problem of selecting of all the goals those that not only would be achieved, but also would allow the company to stay effective. Therefore, still remain urgent the issues of developing effective mechanisms and technologies for formation of potential strategic goals that would be adequate with respect to changing conditions of the company's operation. These technologies should be implemented within the EPM system of the company.

III. PURPOSE AND OBJECTIVES OF THE RESEARCH

A. Study of the process of formation of the company development program

Papers [10, 11] propose the process of forming the company development program that realizes the concept of the strategic alignment. From the goals development to the formation of the company plans system the strategic goals as well as relevant indicators are decomposed down to the budget indicators. Fig. 1 presents the business process of development program forming. Implementation of each procedure results in formation of performance indicators, the company plans and plans of its subdivisions. The effectiveness of this process depends largely on the goals selected. Therefore, the procedure (A2) for forming the company potential goals is highlighted.

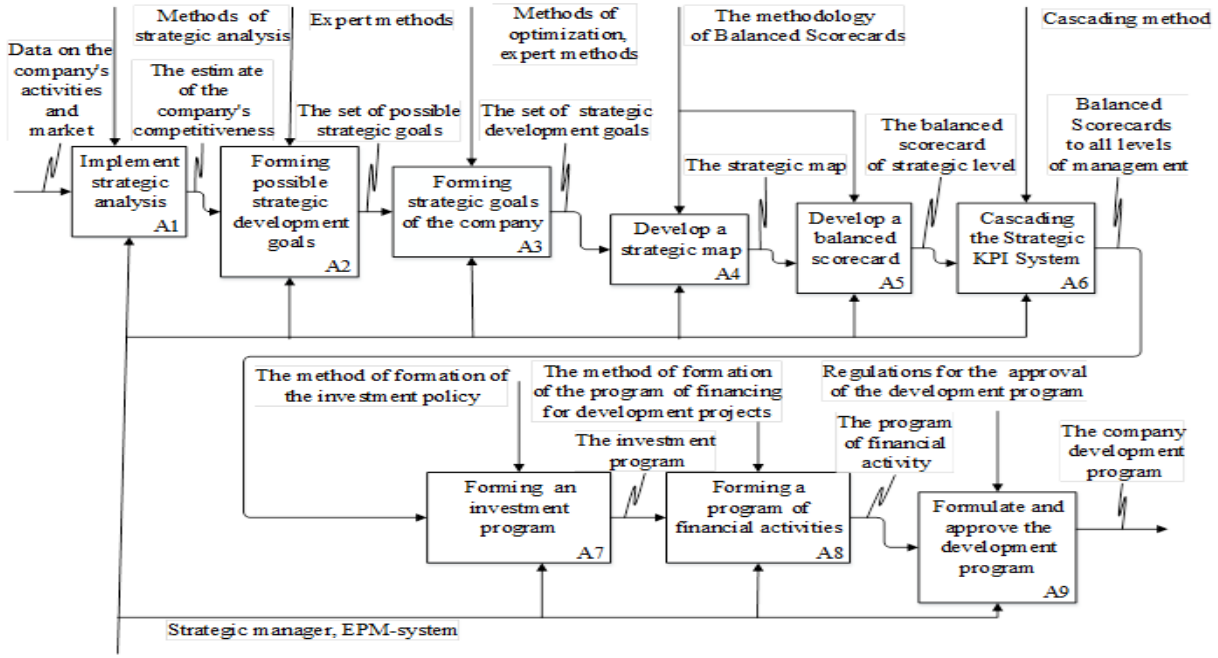


Fig. 1. Business process of the company development program formation

The company management forms the goals based on the on the market situation analysis and the desired prospects of the company development. However, it is necessary to analyze the consequences for the company of achieving these goals in terms of business performance. Also these goals should be checked for feasibility in terms of the company resource capabilities. And with that done, the selected goals are taken as planned ones and become the basis for the company plans.

Implementation of such a process within the scope of the EPM system will permit to realize the strategic

alignment and to increase the company efficiency by setting adequate strategic goals.

B. Business process of potential strategic goals formation

The business process of forming of the company potential strategic goals is presented in graphical notation IDEF0 (Fig. 2). The company's performance and its market perspective are assessed based on results of the strategic analysis. Previously, the market situation is predicted for the strategic period and the company's competitiveness is assessed Based on results obtained the company management and the owners form the desired goals for the strategic period. However, the success of such goals implementation will heavily depend on the degree of impact of various factors, as well as the selected achievement strategies.

Therefore, before accepting these goals as the planned ones it is proposed to conduct procedures for verifying them for realizability. The first procedure involves analyzing the impact of various factors on the effectiveness and the risk of a failure to achieve the goals, the second procedure is the a verification of their feasibility in terms of the company resource capabilities. Let's have a closer look at the first procedure which in the business process in Figure 1 is presented as A2.

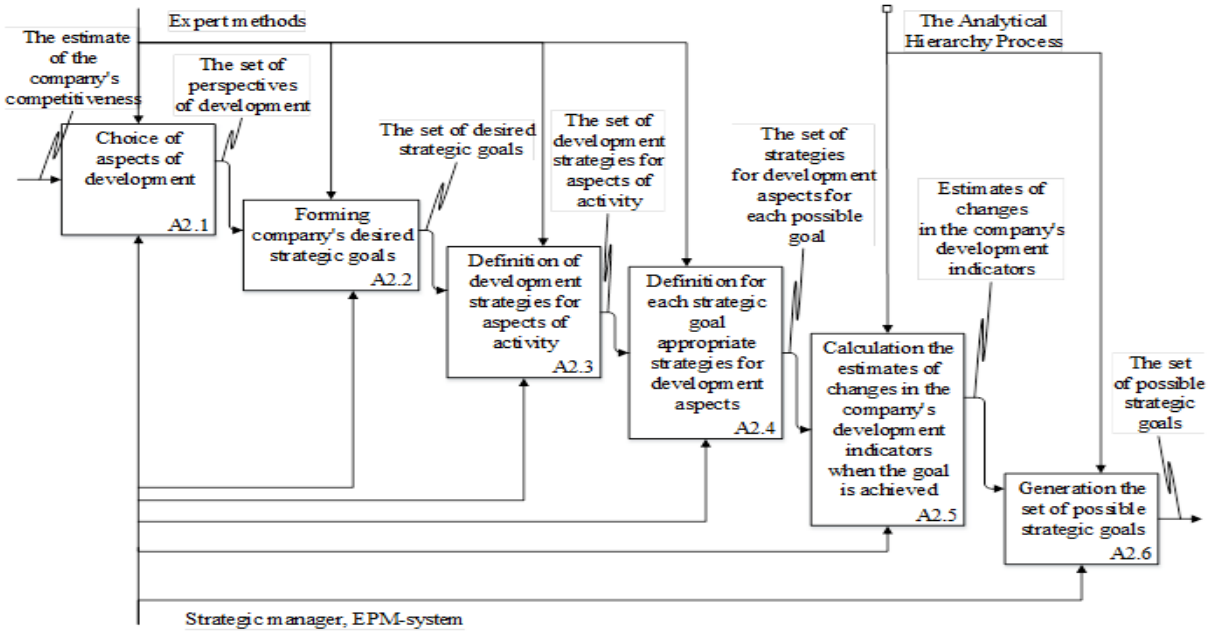


Fig. 2. Business process of potential strategic goals formation

The result of this procedure is desired strategic goals selected from among all of such goals which would be less risky, i.e. would be to a lesser extent subject to external impacts. For these goals potential achievement strategies are identified. Strategies are defined by the aspects of the company development: production, finance, personnel, marketing. For goals selection it is proposed to use the Analytic Hierarchy Process (AHP) [12]. Realizing the direct and reverse process is carried the comparison of the estimates of changes in the company performance indicators when achieving the goals in question. The proposed business process for goals formation has been implemented for the Ukrainian agricultural company. Three strategic goals were considered: 1) to increase the market value of the business; 2) to enter the top ten market leaders; 3) to fulfill business diversification (Fig. 3). For each goal development scenarios by the aspects of activity were elaborated. Iterative procedures have been implemented in accordance with the AHP for all goals. Priority strategies by the aspects of the company development were identified for achieving each goal.

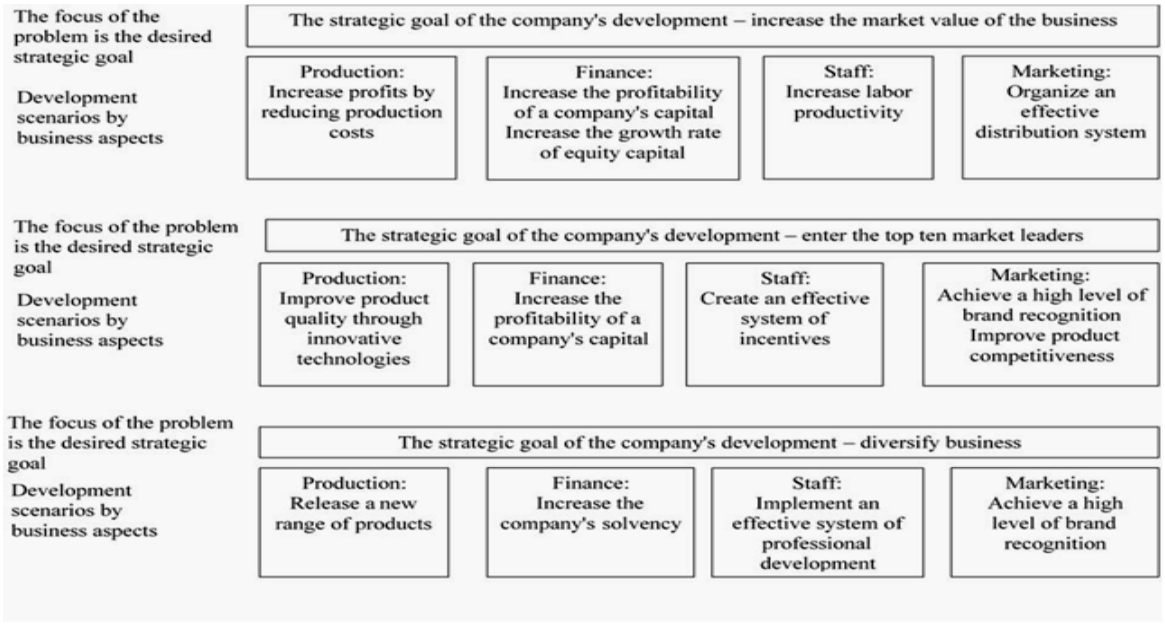


Fig. 3. Examples of development strategies for strategic goals for the Ukrainian agricultural company

IV. CONCLUSIONS

1. The business process of the company development program formation and the business process of forming of the company potential strategic goals are presented.

2. The business process for the strategic goals setting was proposed. For goals selection it is proposed to use the Analytic Hierarchy Process. The result of this procedure is desired strategic goals selected from among all of such goals which would be less risky.

3. The proposed business process for goals formation has been implemented for the Ukrainian agricultural company. Priority strategies by the aspects of the company development were identified for achieving select goals.

4. Mathematical and algorithmic support for other procedures for the development program forming is considered in other works of the author.

5. The business process of the development program forming is the basis of the strategic planning module of the EPM system.

REFERENCES

[1] L. Á. Guerras-Martín, A.Madhok, and Á. Montoro-Sánchezc, "The evolution of strategic management research: Recent trends and current directions", in Business Research Quarterly, vol. 17(2), 2014, pp. 69–76.

[2] B.Heesen, "Effective Strategy Execution, Management for Professionals", Springer-Verlag Berlin Heidelberg, 2012.

[3] M. Lederer, P. Schott, S.nHuber, and M. Kurz, "Strategic business process analysis: a procedure model to align business strategy with business process analysis methods", in S-BPM ONE-Running Processes, Springer Berlin Heidelberg, 2013, pp. 247–263.

[4] H.Wang, "Dynamic re-alignment: Understanding organizational response to changing business contexts using a conceptual framework for strategic alignment", the Proceedings of the 2008 Australia and New Zealand Academy of Management Conference, Auckland, New Zealand, December 2008.

[5] D. Morrison, A. K. Ghose, H. K. Dam, K. G. Hinge, and K.Hoesch-Klohe, "Strategic Alignment of Business Processes", International Conference on Service-Oriented Computing – ICSOC 2011, Workshops, pp. 9–21.

[6] B.McIlrath, and T. Kotnour, "Process alignment for strategic implementation" in Industrial Engineering and Management Systems, University of Central Florida, 2002.

[7] M. Dean, "How To Effectively Communicate Strategy to Employees", 2015, Available at: https: peakon.com/resources/guides/how-to-effectively-communicate-strategy-to-employees.

[8] T. Rahschulte, "Aligning execution and strategy through program management", Paper presented at PMI® Global Congress 2014, North America, Phoenix, AZ. Newtown Square, PA: Project Management Institute, 2014.

[9] F. K. Y. Chou, E. T.G.Wang, and F.W. Yang, "Realizing IT Strategic Alignment and Business Performance", An Integration of Three Perspectives, PACIS 2015 Proceedings.

[10] V. V. Moskalenko, T. V. Zakharova, N. G. and Fonta, "Technology of formation of development program as a system of company's annual plans based on key performance indicators", in European cooperation Scientific Approaches and Applied Technologies, Vol. 2(2), 2015, pp. 108–124.

[11] V. V. Moskalenko, Y. S. Berezenko, "The concept of an architectural solution for the service of building a strategic enterprise map", in Bulletin of NTU "KhPI", Series "System analysis, control and information technology", Vol. 55 (1276), 2017, pp. 45–50.

[12] T. Saaty, "Decision making with the analytic hierarchy process". in International journal of services sciences, Vol. 1, 2008, pp. 83–98.

Quality indicators for reproducing fine details of digital images with threshold limiting of spectral components

Olena Osharovska
Department of Television and Sound Broadcasting
O.S. Popov Odessa National Academy of Telecommunications
Odessa, Ukraine
osharovskaya@gmail.com

Mikola Patlayenko
Department of Television and Sound Broadcasting
O.S. Popov Odessa National Academy of Telecommunications
Odessa, Ukraine
nick_msa@ukr.net

Natalia Samus
Department of Television and Sound Broadcasting
O.S. Popov Odessa National Academy of Telecommunications
Odessa, Ukraine
natalia_samus@ukr.net

***Abstract*—The article considers the effect of compression of the information stream on high-definition image quality image parameters on the receiving side. In order to assess objectively the quality of the reconstructed images, two parameters are selected: the peak-to-noise ratio and the ratio of the peak signal-to-noise value at the boundaries of the image objects. The boundaries of objects are proposed to be selected by the gradient method, after that to make a binary matrix whose area will depend on the set threshold of significant signal values. With the use of spectral transformations and the rejection of small spectral components, the compression of the digital stream is carried out with losses. Several quantization matrices of frequency components are considered and it is shown that, in some cases, image textures that have low contrast are distorted or disappeared. Compression coefficients and corresponding signal-to-noise ratios for frequency-dependent quantization matrices are calculated. In this work, we have also resulted in the dependence of the decoded image quality parameters depending on the length of words that define the brightness and color difference signals.**

Keywords—image, compression, frequency-dependent quantization, quality indicators

I. INTRODUCTION

Advances in digital image processing and image processing technologies have revolutionized our way of life. The acquisition of images, storage, transmission, viewing, and processing technologies have undergone incredible achievements in recent years.

In our daily life, we use a number of applications for image processing with or without our knowledge. For example, when someone captures a scene using a mobile phone, the image captured by the sensor after appropriate correction is compressed in JPEG format and stored in memory. The image can then be transferred to the social media network via the communication channel. [1-7]. The user on the computer screen may later view the image; the pixel size is smaller than the actual image size. In this case, the image must be changed in order to fit on the display screen.

During these operations, the original image undergoes changes that may affect image quality. Therefore, it is necessary to evaluate the suitability of the received (extracted) image for use for its intended purpose. Since most images are ultimately intended for viewing by observers, the only reliable test for evaluating image quality is a subjective examination that allows you to visually evaluate an image by a group of observers and derive a statistically reliable quality assessment [4-6]. Subjective image estimation not only takes a long time, but also a very expensive. The procedure is not practical in real-time applications. In addition, there may be individual factors that can affect perceived image quality. Therefore, it is necessary to evaluate the image quality objectively, taking into account the properties of the human visual system (HVS) as the basis for such an assessment. Any objective algorithm for assessing the quality of IQA images must meet the following requirements: (1) it must have a close connection with visual perception; (2) it must work in a wide range of types of distortion; (3) it must be computationally simple and efficient, and (4) it can be embedded in imaging systems or allow real-time evaluation.

II. ALGORITHM FOR ASSESSING THE QUALITY

Accordingly, IQA algorithms can be broadly classified into three categories, namely, without comparison with a reference image, without reference IQA (No-Reference IQA), algorithms using partial references to the reference image (Reduced Reference IQA), and algorithms determining image quality by a full comparison with the standard, called the Full Reference IQA.

The method for predicting image quality using the Full-Reference IQA (FR-IQA) algorithm uses a reference image to estimate the quality of the distorted image. Since this method has complete information about the reference image, the FR-IQA results must be higher than other prediction algorithms IQA: Some approaches to FR-IQA are based on the accuracy of image representation, accumulated errors, RGB or HVS color characteristics, image structure, content, image statistics and machine capabilities etc.

A. Mean Squared Error

This algorithm calculates the root-mean-square error between the examined image and the original image pixel-by-pixel. Usually the MSE is calculated according to formula (1):

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[B_r(x,y) - B_d(x,y)\right]^2 \quad (1)$$

$B_r(x,y)$ the reference image;

$B_d(x,y)$ the distorted image;

$M \times N$ the image dimension.

The advantage of this metric is its simplicity, but the MSE has a poor correlation with the subjective test results.

B. The Ratio of the Peak Value of the Signal to the Average Value of the Noise

The ratio of the peak value of the signal to the average noise (PSNR). This method also compares the reference image and the distorted image for each pixel and calculates the PSNR [9-11] as follows (2):

$$PSNR = 10\log_{10}\frac{2^P - 1}{MSE}, dB \quad (2)$$

Parameter P is the bit depth of the image representation of the pixel brightness. The main disadvantage of PSNR is a weak correlation with HVS.

Expression (2) can be represented in the form (3):

$$PSNR = 20\log_{10}\left(\frac{B_{pic}(x,y)}{\sqrt{MSE}}\right), dB \quad (3)$$

where $B_{pic}(x,y)$ is the maximum value of image signal.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality.

Typical values for the PSNR in loss image and video compression are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better. For 16-bit data, typical values for the PSNR are between 60 and 80 dB, [9, 10]. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB, [11, 12].

C. The PSNR of the edge areas

The PSNR of the edge areas (EPNSR) is computed as follows:

$$EPSNR = 10\log_{10}\left(\frac{P^2}{MSE_{edge}}\right), dB \quad (4)$$

where:

P : peak pixel value;

MSE_{edge} average noise near bounders.

In the model, this EPSNR is used as a basic objective video quality score.

In the model, an edge detection operator is first applied, producing edge images. It is noted that this edge detection algorithm is applied to the source image (fig.1). Then, a mask image (binary edge image) is produced by applying thresholding to the edge image. In other words, pixels of the edge image whose value is smaller than threshold, t_e, are set to zero and pixels whose value is equal to or larger than the threshold are set to a non-zero value. Fig. 2 and fig. 3 show examples of mask images. Although one may apply the edge detection algorithm to processed images, it is more accurate to apply it to the source images. Next, differences between the source image and processed image, corresponding to non-zero pixels of the mask image are computed. In other words, the squared error of edge areas of the frame is computed as follows to (1).

To estimate EPSNR for separation boundaries and their surroundings, the gradient of the image brightness distribution function is used as the sum of the gradient projection modules $\text{grad}_{\text{horizontal}}(x,y)$ and $\text{grad}_{\text{vertical}}(x,y)$ on horizontal and vertical axes (4):

$$\text{grad}(x,y) = \left|\text{grad}_{\text{horizontal}}(x,y)\right| + \left|\text{grad}_{\text{vertical}}(x,y)\right|, \quad (5)$$

where x and y are the image coordinates horizontally and vertically.

Fig. 1. Example of a image “Vehicles truck”

Fig. 2. Example of an edge image “Vehicles truck”

Fig. 3. Example of a mask image “Vehicles truck”

The resulting mask is multiply per pixel by the brightness component of the image, highlighting the values on the contours. In some cases, it is advisable to subject the luminance signal to low-frequency filtering.

III. FREQUENCY-DEPENDENT QUANTIZATION OF SPECTRAL COMPONENTS

The progress of compression methods for still images and intra-frame compression of video sequences is a key element in the construction of broadband image transmission systems for various purposes. In this respect, the main criterion for the degree of compression is the estimates obtained by measuring distortions of the sharp image boundaries arising as a result of nonlinear processing of the spectral components.

In this work, the main attention is paid to the problem of choosing a threshold level on the basis of a compromise between the achievable compression ratio and the possible preservation of the image texture and the corresponding estimates are given. This compromise can be of great importance both for broadcast applications and for a wide range of video applications, in which a large number of stages of production, processing, storage, transmission and reproduction of video information where texture transmission can play a significant role are realized.

When you try to save a digital image in a smaller volume, you often have to decide what "quality settings" (compression level) to use. The JPEG file format allows you to choose the appropriate trade-off between file size and image quality. It is important to understand that JPEG (and almost all lossy file formats) are not suitable for intermediate editing because repetitive saving usually reduce the quality of the working file. In addition to the cumulative introduction of visual artifacts, repeated decompression also leads to destructive color changes. It is for these reasons that the preferred choice for intermediate processing is lossless compression of file formats (such as TIFF, PSD, BMP, etc.). JPEG should only be used to store the final image.

Suppose that there is a color image with dimensions N × N = 2048 × 2048 pixels, each element is represented by m = 10-bit code in each of the three components. In this case, the required amount of memory V needed to store one still image RGB or Y Cb Cr is (5):

$$M=3 \times N \times N \times m = \quad (6)$$

$$M= 3 \times 2048 \times 2048 \times 10 = 120 \text{ Mbit.}$$

To reduce the required amount of memory, lossy compression is used based on spectral transformations. The most common is the Fourier transform. Compression of information about color images consists of several stages, including both lossless compression based on statistical properties, and lossy compression based on the generalized discrete Fourier transform $F(\nu_H, \nu_V)$. T(Tabhe spectrum of the two-dimensional image signal consists of horizontal ν_H, vertical ν_V and diagonal ν_D spatial frequencies (7):

$$F(\nu_H, \nu_V) = \sum_{x=0}^{N_x-1} \sum_{y=0}^{N_y-1} B(x,y) e^{-j2\pi\left(\frac{x\nu_H}{N_x}+\frac{y\nu_V}{N_y}\right)}, \quad (7)$$

Thanks to the numerous algorithms for fast Fourier transforms, it is possible to obtain the spectrum of the entire image in an acceptable time. The main energy of the spectrum is concentrated at low frequencies, and the high-frequency components are usually very small in amplitude and. in a number of cases, they can be neglected, equating them to zero. The greater the number of high-frequency components will be equated to zero, the greater the compression ratio can be obtained. However, from the point of view of storage and transmission of the image spectrum obtained by the formula (6), a significant drawback is the need to work with two arrays representing the real and imaginary part of the complex numbers of the spectrum.

In practice, special cases of Fourier transforms are used, such as discrete cosine transform (DCT) or discrete sine transformation (DSP). The JPEG and MPEG-2 standards use DCT. A feature is segmentation in blocks - raw image data is divided into blocks of 8 × 8 pixels (these blocks are the minimum coded block). This means that the JPEG compression algorithm largely depends on the position and alignment of the boundaries of these blocks. In MPEG-4, the block sizes vary from 4 × 4 to 16 × 16 pixels.

Taking into account the obtained values of the spectral coefficients at the DCT step, they are sorted in order of increasing numbers from the low-frequency components (changes that occur at a greater distance from the image block) to high-frequency components (changes that can occur with each pixel). It is widely known that people are more critical of errors in low-frequency information than high-frequency information. The JPEG algorithm discards many of these high-frequency (noise-like) details and saves slowly changing information about the image. This is done by dividing all the spectral coefficients by the corresponding value in the quantization table and rounding the result to the nearest integer. Components that either had a small coefficient or a large divisor in the quantization table are likely to be rounded to zero. The lower the quality setting, the greater the divisor, which gives a greater chance of getting a zero result. On the other hand, the setting for the highest quality would have the values of the quantization table of all frequencies equal to one, which means that all the original data of the discrete cosine transform (or sinus) is stored.

If the quantization tables correspond to the standard trend of limited compression in low-frequency components that increase to moderate compression in high-frequency components, then the approximate quality factor can really give an idea of how the overall quality can be displayed.

IV. RESULTS OF COMPUTATIONAL EXPERIMENTS

At the first stage, the values of the spectral components were limited, depending on the peak value of the luminance signal in the selected area with a low-contrast texture. Limit thresholds were 0.5%: 1%; 2% and 5%. The results are given in Table I for test images Tab II.

TABLE I. QUALITY INDICATORS FOR FOURIER TRANSFORMATION

Test Image	Threshold of restriction			
	0.5%	1 %	2 %	5 %
	EPSNR, dB			
Vehicles truck	25.1	22	19.8	18.4
Flowers	28.3	26	24.6	21.9
Sea	22.4	21	19.2	18.6
Music Box	23.7	21	20.2	18.7

TABLE II. TEST IMAGES

IMAGE NAME	TEST IMAGE
Flowers	
SEA	
MUSIC BOX	

Subjective evaluation of reconstructed images corresponds to a satisfactory estimate, there is blurring of boundaries and fading of details of low-contrast textures.

In the next step, we calculated signal-to-noise ratios PSNR, EPSNRS and the DCT compression ratio (CR) for the four signal-word lengths. (Table III).

TABLE III. DEPENDENCE OF EPSNR AND CR ON THE WORD LENGTHS

Bit	EPSNR	PSNR	CR	EPSNR	PSNR	CR
	Flowersr			***Sea***		
6	30.5	39.2	27	33.5	42.8	29
8	31.3	40.1	24	34.5	44.1	27
10	31.9	40.9	22	35.3	45.1	26
12	32.5	41.7	18	36.1	46.0	23
	Music Box			***Vehicles truck***		
6	36.2	46.1	27	36.5	46.5	33
8	36.2	46.2	31	37.1	47.2	29
10	36.4	46.3	22	37.5	47.8	30
12	36.7	46.0	18	37.9	48.3	24

We carried out frequency-dependent quantization using the quantization matrices Q of the cameras of known manufacturers. The results of calculating the PSNR EPSNR, CR are summarized in Table IV for one of the test images "Sea"

TABLE IV. DEPENDENCE OF EPSNR ON THE Q-MATRIX

Quantization Table Q-matrix	Sea	
	DCT EPSNR, dB	***DST EPSNR, dB***
SONY - DSC-N2 (fine)	45.1	44.8
NIKON - E8800 (EXTRA)	45.5	46.3
Canon EOS 10D (fine)	46.1	45.2
NIKON - COOLPIX S10 (FINE)	46.8	46.5
NIKON D80 (FINE)	47.4	46.6
Canon PowerShot A700 (superfine)	48.2	49.1
JPEG standard	48.4	45.8

Analysis of the results shows that all these frequency-dependent quantization matrices of the spectral coefficients give an acceptable quality of the reconstructed image, but not a very high compression ratio. Conclusion

CONCLUSION

The use of such quality indicators of recovered images as PSNR, or even better, EPSNR allows you to objectively predict the reproduction of boundaries and textures.

REFERENCES

[1] Recommendation ITU-R BT.1683:2004, “Objective perceptual video quality measurement techniques for standard definition digital broadcast television in the presence of a full reference”.

[2] Recommendation ITU-R BT.1867-0:2010, “Objective perceptual visual quality measurement techniques for broadcasting applications using low definition television in the presence of a reduced bandwidth reference”.

[3] Recommendation ITU-R BT.1908:2012, Objective video quality measurement techniques for broadcasting applications using HDTV in the presence of a reduced reference signal.

[4] Recommendation ITU-T J.144:2004, Recommendation BT,1908:2012, “Objective perceptual video quality measurement techniques for digital cable television in the presence of a full reference”.

[5] Recommendation ITU-T J.246:2008, Perceptual visual quality measurement techniques for multimedia services over digital cable television networks in the presence of a reduced bandwidth reference.

[6] Recommendation ITU-T J.247: 2008, Objective perceptual multimedia video quality measurement in the presence of a full reference.

[7] Oleg Gofaizen, Olena Osharovska, Mikola Patlayenko, Volodymyr Pyliavskyi, “Test signals for assessment image quality in HD and UHD TV video path”, 2016 8th International Conference on Ultrawideband and Ultrashort Impulse Signals (UWBUSIS), pp. 42–46, 5–11 Sept., 2016, DOI: 10.1109/UWBUSIS.2016.7724147

[8] N. Thomos, N. V. Boulgouris, M. G. Strintzis. “Optimized Transmission of JPEG2000 Streams Over Wireless Channels.” IEEE Transactions on Image Processing, 15 (1) January, 2006.

[9] L. Xiangjun, C. Jianfei, “Robust transmission of JPEG2000 encoded images over packet loss channels.” ICME 2007 (pp. 947-950). School of Computer Engineering, Nanyang Technological University.

[10] David Salomon, Data Compression: The Complete Reference (4 ed.). Springer. p. 281. ISBN 978-1846286025. 2007.

[11] Huynh-Thu, Q.; Ghanbari, M. "Scope of validity of PSNR in image/video quality assessment". Electronics Letters. 44 (13): 800. 2008. doi:10.1049/el:20080522.

A proposal to make Odessa the pilot city to build the5G network in the Black sea area

Andrzej Rychlik
Institute of Information Technology, Lodz University of Technology
Łódź, Poland
andrzej.rychlik@p.lodz.pl

***Abstract*—The concept of designing and building networks for digital data transmission, including the 5G network, includes the choice of a small area where we test solutions in real conditions. The basis for the selection of such area is the presence of the phenomena characteristic for the entire area, on which we build the network. The agreement for the Strategy "5G for Poland" for the pilot 5G network chose the city of Łódź for the territory of Poland. Using the same selection criteria to choose the author proposes the city of Odessa as a pilot area for the coast of the Black Sea. 5G technology is characterized by the fact that the frequency of the signal and the size of the cell vary depending on the subscriber's density. For the highest density of subscribers we have the highest carrier frequency and the smallest cell. Signal strength may not exceed the permissible PEM values for areas inhabited by people. The data transmission between base stations is implemented in fiber optics and between the mobile subscriber stations over the air. Odessa and Łódź will cooperate to reduce the costs of pilotage and accelerate the receipt of test results.**

Keywords—5G, a pilot city, mobile network, Internet of Things, a smart city

I. INTRODUCTION

The idea of designing large systems includes the element that first a fragment of such system is built in a small area and only in the case of receiving positive effects; it is expanded throughout the planned area. In Poland concluded on 28 June 2017 Agreement for the Strategy "5G for Poland" by and between Minister of Digital Affairs, hereinafter referred to as the "Leader" and President of the Office of Electronic Communication, hereinafter referred to as the "Partner" and National Institute of Telecommunication hereinafter referred to as the "Organizer" and other Parties in number 50. This agreement was chosen by the city of Łódź as a pilot area for the construction of a 5G network for the Polish area. Using the same criteria, we choose the city of Odessa as a pilot area for building a 5G network for the Black Sea area. The city of Łódź is a partner city for Odessa, which will undoubtedly facilitate the transfer of experiences from the pilotage of Łódź to Odessa.

II. THE ESSENCE OF 5G TECHNOLOGY

The 5G network in its assumption will use many techniques and solutions that are necessary to provide functionalities previously unachievable in existing mobile and cellular networks. It is difficult to talk about the details of many of these solutions, due to the fact that full technical specifications for the 5G system have not yet been developed. The analysis of the current state of knowledge, however, allows us to formulate some observations and predictions in this respect. In order to meet IMT-2020 requirements for medium and peak gigabit data rates for a wide range of users and devices, as well as low signal delays, it is assumed that 5G network transmitters should be connected with optical fiber lines. This applies to both macro cells (range up to several or a dozen kilometers) in rural and suburban areas, and for microcells (range up to 2km) in city centers. In addition, small cells (pico and femto cells), for which the range will be from a dozen to several dozen meters, will be used as local access points in places such as stadiums or public space. To achieve the planned technical parameters of the 5G network will be necessary in particular:

- The use of multi-antenna MIMO technology (Multiple Input Multiple Output) in the massive variant with a large number of antennas, thanks to which it will be possible to transmit signals in the range of high frequency bands and simultaneously transmit signals for a large number of users. The main assumption of MIMO massive is the use of large antenna arrays in base stations in the physical layer for simultaneous operation of many autonomous terminals.
- The use of dense networks (the size of the cell adapts to the number of subscribers working in a given area) will significantly increase the spectral efficiency of data transmission channels.
- The use of full duplex, information can be sent in both directions simultaneously in both directions without a decrease in spectral efficiency.
- The use of various multi-access techniques: OFDMA (Orthogonal Frequency-Division Multiple Access), PDMA (Pattern Division Multiple Access), MUSA (Multi-User Shared Access), IMDA (Interleave Division Multiple Access). The use of non-orthogonal methods of multiple accesses is also envisaged, including SCMA (Sparse Code Multiple Access) and NOMA (Non-orthogonal Multiple Access). Orthogonality generally helps to eliminate the problem of interference and provides a large capacity, but at the price of complex signaling and longer delays.
- Use of Multi-RAT (Multi-Radio Access Technology), which is a kind of 5G network integration with other solutions: Wi-Fi, 4G, 3G. Users will be able to automatically connect using the optimal interface at the moment (depending on their requirements or network load).

The use of a number of new technologies: SDN (Software Defined Networking), NFV (Network Functions Virtualization, MEC (Mobile Edge Computing), C-RAN (Cloud-RAN), UDN (Ultra Dense Network), SON (Self-Organizing Network).

In the 5G network system, it is assumed to use in the first order 3 frequency bands: the 700 MHz band, channel width 5 MHz, 3.4-3.8 GHz band, channel width 50 MHz, 24.25-27.5 GHz band, channel width 100 MHz. Three scenarios of using digital data transmission channels were also defined: eMBB (enhanced Mobile Broad Band), mMTC (massive Machine Type Communication), cMTC/URLLC (critical MTC/Ultra Reliable Low Latency Communication). The 700 MHz band enables good propagation as well as signal penetration through damping materials, and thus can be used to build the cover layer for services of the mMTC type. The 3.4-3.8 GHz band allows the use of MIMO massive and at the same time is a compromise between propagation and the capacity resulting from spectral resources. The 26 GHz band is limited as to the area of use, especially due to the requirements for uplink transmission. It can only be used for eMBB hot spots and cMTC / URLLC picocells. As part of the 3GPP (3rd Generation Partnership Project), i.e. a joint project of several standardization organizations aiming at the development of 3G mobile telephony systems, technical aspects of the physical layer for 5G mobile communication - NR (New Radio) are developed. However, it should be borne in mind that work on the specification of the 5G network has not yet been finalized and will finally be published in the next document dedicated to 5G networks [1].

III. Selection of a pilot city for the implementation of the 5G commercial network

When choosing a pilot city for 5G technology, pay attention to its existing potential:

- Many cities in Poland have been preparing for the implementation of Smart City services for several years: the necessary market analyzes have already been carried out, specific services have been designed, and now further solutions are being slowly implemented. The 5G pilot in such a place is the opportunity to use ready-made applications, check their functionality in the real world technology, without the need to build an application-service layer from scratch.
- The city to implement the 5G network should enable testing of intelligent transport scenarios, in particular in a highly urbanized environment and in motorway conditions.
- To start the installation of the 5G network should be selected locations in such places where the current value of the electrical component E of the PEM electromagnetic field strength is at a level ensuring adequate reserve in relation to the limit value of 7V / m. (Value of the standard in force in Poland). The supply is necessary to run the pilot plant network 5G limit value 7V / m is not exceeded.
- The city selected for the implementation of the 5G network should have an attractive location - it should be located in the vicinity of an important transport hub, sea port, motorway, airport, where trade routes work - these elements will allow for testing in the field of modern smart logistics solutions and intelligent transport.
- It is advisable that there is a developed industry in the selected city (factories, production companies), with a strongly developed business base (banks, corporation offices, fairs, state offices, market halls, where important events are organized).
- Of great importance is the readiness of the city to carry out efficient piloting and implementation of new technology, we have in mind the openness of the city authorities on technological innovations, technological maturity of the municipal office, the existence of a development strategy taking into account technological development.
- Scientific potential is the opportunity to engage universities, especially those conducting research in the 5G domain and wireless systems, in 5G pilot tests and prototype solutions.
- It is desirable that commercial companies active in the city, also at the international level, develop standards in the development of standards and new technologies used in 5G networks.

The city of Łódź for the territory of Poland and the city of Odessa for the Black Sea area meet the above criteria, therefore they can be recommended as cities for piloting and implementing the 5G network. The city of Łódź can provide Odessa with experience in the implementation of certain applications such as Smart building, innovative lighting system, and local applications supporting residents, Electronic Urban Traffic Control System, air quality map in real time. The city of Lodz, because of its location near the intersection of the main communication routes (A1, A2, S8, S14) is one of the largest hubs in Poland, the city of Odessa is a hub for-transport sea, air and land are good places for the implementation of pilot services in the area of intelligent transport, in particular for testing and implementing the services of autonomy and automated vehicles, for which 5G connectivity is the basis of existence and functioning. There are strong academic centers located in the city of Łódź (Lodz University of Technology, University of Lodz, and Medical University of Lodz) and the city of Odessa (Odessa I. I. Mechnikov National University, Odessa National Polytechnic University, Odessa National Medical University, Odessa National Maritime University).

IV. Potential possibilities of Smart City solutions based on the 5G network for the city of Odessa

Two basic applications of the network built in 5G technology are mobile television and smart city. The use of 5G network for the construction of mobile television has been described in [2]. Of course, the prelude of 5G is the elimination of congestions in telephone conversations in areas with very high density of subscribers who are talking, for example, after sports competitions, concerts, devotions.

The basic assumptions of choosing Smart City solutions in the city of Odessa are as follows:

- Take into account the specificity of Odessa, which is as follows:
  - large urban agglomeration,

- located by the sea,
- an important tourist and sanatorium center,
- developed industry and academic center.

- Benefit cost analysis takes into account the widespread use of services provided.
- Solutions are comprehensive and integrated under the Smart Cities model: services, applications, communication platform, ICT networks, and sensors.
- The data collected by the systems should be standardized so that they can be used (real value not only bring individual services, but also implement them together in the whole ecosystem).

It should be emphasized that only the submission of individual services will constitute the environment and potential of the entire city or agglomeration. It follows that the service is made as a combination of information coming from other services, and thus the information can be reused by various services. This will be, for example, obtaining information for the development of investment plans, activities related to public safety, rescue operations, crisis management, integrated transport systems, energy and water management in the city. For example: a car accident can include a large number of services and entities, detection and control of traffic, police activities, fire brigades, telemedicine and consultation at the scene of the accident, control of lights to give preference to the ambulance, informing the event on the Internet. Additionally, you can also link data related to traffic, emission, lighting and video data, which can be simultaneously used by traffic management in the city, law enforcement, and parking management. An another example, services for tourist service can be implemented by mobile applications providing information on available parking lots, weather conditions, traffic in cities and on roads, air cleanliness and information on weather hazards or other natural disasters. It follows from the above that data must be downloaded from parking applications, weather and monitoring of the environment and work of central and local services. For critical systems from the point of view of the functioning of the city, we provide a high level of security and always conduct a risk analysis [3].

V. Methodology of choosing the Smart City application

There are two options for work on the selection of Smart City applications and telecommunications solutions:

1. Analytical variant - analysis of current Smart City services and telecommunications resources and their modification in order to obtain a target solution.

2. Synthetic variant - creating a target model to which Smart City solutions will be adapted (ideal model).

As far as the work is concerned, these can be direction variants of works:

- Technical - taking into account the possibilities of technical implementation resulting from the resources and organizational capabilities.
- Social - determined by social needs and benefits.

The socio-economic analysis for the implementation needs includes: description of the area specification, identification of the scope of services that can be implemented using Smart City, social benefits from the provision of services, list of stakeholders. At the initial pilot stage in the city of Odessa, the author proposes to implement: remote reading and electronic invoices for utility services, gas, electricity, water, heat, intelligent tourist guide, intelligent parking lots, intelligent lighting, intelligent security and intelligent transport systems. Of course, for all these systems we are building a common, large database and knowledge as a cognitive dynamic system. For example, the intelligent tourist guide will be available as a personalized mobile application, which in addition to information functions will enable the purchase of services and connection with the social media environment. The tourist will receive a presentation of the place of being on the map, also in the rooms (location not only with GPS but also 5G), information about events with the possibility of making a mobile payment for participation, access to knowledge base about tourist and cultural attractions, information on vacancies and opportunities and remote purchase, information on transport services, information and weather forecast, warning about danger, placing your own comments and photos using social media. The information system for remote reading and electronic invoices for utility services has been described in [4].

VI. Conclusion

5G technology is not a specific technical solution for digital data transmission, but a slogan requiring standardization to be implemented around the world. Currently, ITU (International Telecommunication Union) works under the WRC-19 (World Radiocommunication Conference 2019) standards to enroll these standards in the Radiocommunication Regulations [5]. The role of pilot cities is huge in this process because the services run there confirm or not, in practice, the results of laboratory tests. The author proposes far-reaching cooperation between Łódź and Odessa cities, based on the exchange of test results, so that they do not carry out identical implementation work twice. This cooperation will contribute to lowering the pilotage costs of both partners. State governments do not plan to finance pilotage from central budgets, but only create legal and organizational facilitations, so that test network installations in 5G technology arise in the mode of public-private ventures, where local governments are to be on the public side.

References

[1] Strategia 5G dla Polski, https://www.gov.pl/documents/31305/436699/Strategia+5G+dla+Polski.pdf/0cd08029-2074-be13-21c8-fc1cf09629b0

[2] Rychlik A.: Мобильное телевидение в сетях 5G, Proceedings of the International Scientific-Practical Conference «Information Control Systems and Technologies» (ICST-ODESSA-2018)

[3] Inteligentne miasta (Smart Cities) na progu technologii 5G https://mc.bip.gov.pl/.../inteligentne-miasta-smart-cities-na-progu-technologii-5g-pdf.html

[4] Rychlik A.: The Information System for Remote Control and Calculation of the Use of Utilities, proceedings of 18-th International scientific-practical conference «MODERN INFORMATION AND ELECTRONIC TECHNOLOGIES» Odessa, Ukraine, 2017

[5] Rychlik A.: Strategy of implementation of 5G technology, proceedings of 19-th International scientific-practical conference «MODERN INFORMATION AND ELECTRONIC TECHNOLOGIES» Odessa, Ukraine, 2018

Hybrid neural network based on Kohonen networks and the perceptron

V. M. Sineglazov
Aviation Computer-Integrated Complexes Department, Educational & Research Institute of Information and Diagnostic Systems,
National Aviation University
Kyiv, Ukraine
svm@nau.ua

O. I. Chumachenko
Technical cybernetics department, Faculty of informatics and computer science
NTUU "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
chumachenko@tk.kpi.ua

***Abstract*—It is considered basic approaches for hybrid neuron network creation. As an example the counter propagation neural network is analyzed. It is effectively used for image processing. Two modes of this neuron network functioning is considered. They are: accreditation and interpolation. Interpolation approach permits to reveal more complex features and can supply more precise results. Based on this analysis it is developed a new hybrid structure that includes Kohonnen neural network and perceptron. It is proposed a learning algorithm of this hybrid neuron network.**

Keywords—hybrid neural networks; Kohonnen neural network; perceptron; learning algorithm.

I. INTRODUCTION

The problem of combining different types of neural structures in a single architecture, which leads to properties that they do not have separately is often discussed [1] – [6]. The example of such combining is counter propagation network. In this article, it is developed a system architecture based on the counter-distribution network, but instead of the Grossberg network, it is taken a single-layer perceptron. Such hybrid neural network, consisting of Kohonen layer and single-layer perceptron has much better characteristics than the network with one hidden layer of neurons. Figure 1 shows a simplified version of a direct action hybrid.

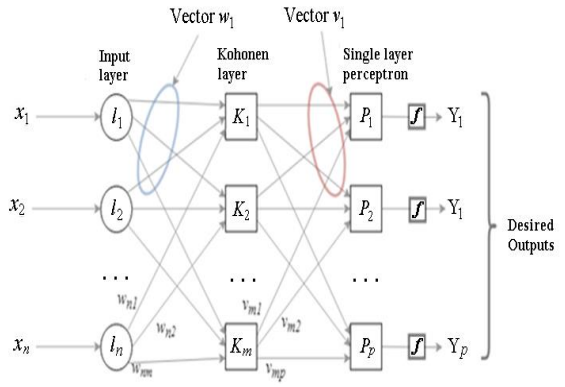


Fig. 1. Simplified structure of hybrid neural network.

The ability to generalize, which allows to obtain the correct output at an incomplete input vector is one of the main characteristics of hybrid neural networks. It allows you to effectively use this network for pattern recognition.

II. SOLUTION OF THE PROBLEM OF STRUCTURAL SYNTHESIS OF HYBRID NETWORK

To determine the problem of structural synthesis of a hybrid neural network based on Kohonen and the perceptron, it is necessary to analyze three mechanisms necessary for the operation of this network. The first mechanism is the criterion for selecting "winner" neurons and the frequency of selecting the same neuron as the "winner". This is quite an important question, because there may be a situation when one neuron several times becomes a "winner" and gradually increases its weight, which will lead to the appearance of "dead" neurons that will no longer participate in the training of the network. One of the methods of this problem solution is the method of "justice".

The next mechanism is the strategy of neurons – "winners" choosing. This is done through the interpolation mode in which the Kohonen network operates. Let us consider in more detail the principle of this mode.

The main difference between the accreditation mode and the interpolation mode is the ability to choose not one "winner", but several. The problem is how many" winners " to choose for the pattern recognition problem, in this case – numbers.

The third mechanism is the connection of the Kohonen layer neurons with the layer of the perceptron. The peculiarity of the single-layer perceptron is the absence of "hidden" layers. This means that the input vector immediately forms the output vector depending on the weight on the neuron. The single-layer perceptron does not use the back propagation method because this learning algorithm works for multi-layer networks. Therefore, when training the network, it is used the correction method. Nonlinear activation functions are also used by multilayer networks, so in our case it is more reasonable to use the threshold activation function, which results in 0 or 1.

III. PERCEPTRON. FEATURES AND STRUCTURE

The perceptron is the simplest network and consists of a single layer of artificial neurons connected by weight coefficients with multiple inputs (Fig. 2)

The perceptron is trained by feeding a set of images one at a time to the input and adjust its weight until all the elements have reached the desired output.

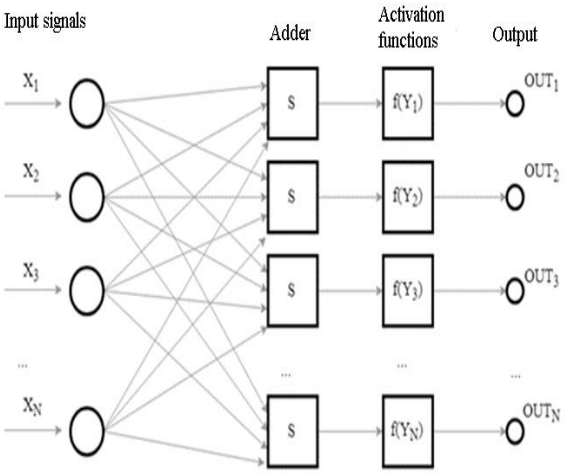


Fig. 2. Structural diagram of the perceptron.

During training, the so-called Delta rule is used to change the weight.

It is necessary to remark some features:

- single-layer perceptron is represented as a mesh size *a* on *b*. As a result, it gives us *a*·*b* neurons in the perceptron layer.
- as a result, the output from the networks is compared to the expected value. If the network is wrong, change the weights of those neurons that were part of the neurons with incorrect classified figure.

Let's start with the Kohonen network. The work of this network takes place according to the standard scheme. The only difference is that in combination with the perceptron the network can operate in the interpolation mode, not accreditation. Let us examine this mode in more detail.

In the interpolation mode, several neurons can become "winners". Their number depends on the task.

Algorithm for selecting neurons – "winners" has the following form:

1) Set a certain value C (count), which will be equal to the required number of neurons – "winners" for the task.

2) Calculate the values of the Kohonen layer neurons outputs

$$\delta = T - OUT. \quad (1)$$

3) *After receiving the values of all output signals, select C maximum values by format* $\max(OUT_k), k = 1...M$, *choosing one neuron-"winner" –* $OUT_k = 1, C = C - 1,$ *then repeat the search for the next maximum*.

4) *Choosing C neurons-"winners", the output signals of other neurons is equal to 0.*

5) We are sending output signals to the neuron-"winners" to the input of the perceptron layer.

We will analyze how many neurons are needed for the most optimal network operation for the pattern recognition problem if we use a single-layer perceptron.

If *C* = 2, which is the minimum for the interpolation mode, the network will select two neurons with the highest result value according to the equation (1). Their output will be 1 and the others 0. That is, these are the two figures that are closest to each other. An example is a pair of numbers 0 and 8, 3 and 8, 2 and 7, 7 and 1 and so on. As a result, if the image was not clear enough, there is a possibility of ignoring the required number and not defining its class as a neuron-"winner", which will lead to low accuracy.

If *C* = 3, the network will select three neurons with the highest result value according to the equation (1). Their output will be 1 and the others 0. That is, these are the three figures that are closest to each other. An example is the three digits 3, 8, and 0, and 2, 7, and 1. As a result, if the image was not clear enough, the probability of including the required number and determining its class as a winner neuron is higher than in the case when *C* = 2. But for our case, there is a problem, because the training immediately image of three digits may not lead to a correct change in the weights of neurons. If it is necessary to choose 3 or more neurons-"winners", it is more expedient to use a multilayer perceptron.

If *C* = 4 and 5, the network will select four or five neurons with the highest result value. Since the similarity of numbers as a whole consists of three elements (given in the example C=3), such a choice is the most optimal.

Since the optimal number of neurons - "winners" is not determined and depends on the task, we can assume that the optimal value is found – *C*= 2 and 3. In our case, we will use 2, because it is necessary to check the quality of the network. In the future, the network can be developed by replacing the single-layer perceptron on the multi-layer.

Let's move on to the key feature and at the same time the problem of the Kohonen network – the probability of choosing the same neuron for the "winner" neuron, which will lead to a primitive ignoring of the training of other neurons. The method of solving this problem is the method of "justice". In this case, it is optimal because of the simplicity of its implementation and, as a result, the homogeneous training of all the neurons of the Kohonen layer. It is determined as:

$$pass = \frac{1}{M}, \quad (2)$$

where *M* is the number of iterations for which a neuron can be only once a "winner"; *pass* is the value of the neural network weight change.

The rule of use of this method is: "for a neuron that has received the status of "winner" more than once in *M* iterations, the weight decreases, but the activation of the neuron is not canceled." Thus, for the neuron that the second time becomes the winner for a certain number of iterations, the weight decreases, thereby reducing its "rank", which makes it possible to teach other neurons.

$$w_{k(i+1)} = w_{k(i)} - pass, \quad (3)$$

where $w_{k(i+1)}$ is the new weight of neuron-"winner"; $w_{k(i)}$ the old weight of the neuron-"winner", and is the iteration number. With this method, other neurons on the background of such a neuron-"winner" "rise" in its "rank".

From equation 2, we see that it is not advisable to use a low value of M, since then the weight of the neuron will be severely cut, which dramatically reduces its potential to become a neuron-"winner" in the further training of the network.

Analyze the result of the network at various values of *M*: At *M* = 1, in fact, the network does not have any criterion for lowering the rank, since each subsequent iteration will be new for the entire network and the previous neuron-"winner" will be able to become it again. It is also inappropriate to use this value, since the weight will decrease to a critical value.

At *M* = 2, the network has some control over the situation, but only if two consecutive times one and the same neuron claims to be the "winner". This number of iterations makes sense, but is not very effective. It is also inappropriate to use this value, since the weight will decrease to a critical value.

At *M* = 3, the network more actively analyzes the "winners", but there are still situations where certain neurons will become winners every fourth or fifth iteration, thereby not falling under the method of "justice" and at the same time preventing the training of other neurons. In this case, the weight is reduced to not too large, but still sufficiently large.

At *M* = 7...10 the network maximally controls the moment of determining the neuron-"winner", which negatively affects the learning of the network. If you take the maximum value in 10 iterations, it actually means that for ten iterations, none of the neurons can not be selected as a "winner" twice, because it will lead to weight reduction.

Given this analysis, we can conclude that the optimal value of M is 4.5 or 6. The value of the number of iterations for the "equity" method It's best to test software programmatically and choose one of the three best options that will give the network the highest accuracy.

CONCLUSION

The network of counter propagation is analyzed. Thanks to the results of this analysis, the architecture of the hybrid neural network based on the Kohonen network and the perceptron, focused on the task of recognizing handwritten digits, was designed.

In order to maximize the accuracy of the work of the network, two basic mechanisms, the method of "justice" for the ability to teach all neurons of the Kohonen network and the approach to choosing neurons-"winners" in interpolation mode, are analyzed.

As a result of the conducted research, an algorithm for the operation of the hybrid neural network was obtained, allowing to recognize handwritten digits with an accuracy of more than 90%. The developed model can be used for recognition of automobile license plates, or a more global task – *X*-ray detection and diagnosis.

REFERENCES

[1] V. V. Borisov, V. V. Kruglov, and A. S. Fedulov, Fuzzy models and networks. 2 nd ed., The stereotype. 2012. (in Russian)

[2] Khaykin Saymon. Neural networks: full course, 2nd edition. 2006. (in Russian)

[3] A. P. Rotshteyn, Intelligent identification technologies: fuzzy sets, neural networks, genetic algorithms. Monograph. Vinnitsa: "Universum-Vinnitsya," 1999, 295 p. (in Russian)

[4] J.-S. R. Jang, ANFIS: Adaptive-Network-Based Fuzzy Inference Systems, IEEE Trans. Systems, Man & Cybernetics 23 (1993).

[5] Y. Bengio, A. Courville, and P. Vincent, Representation Learning: A Review and New Perspectives. Department of computer science and operations research, U. Montreal. 2014.

[6] X. Glorot and Y. Bengio, Understanding the difficulty of training deep feedforward neural networks. 2010.

An emulation approach to testing on distributed denial of service in web applications

Berk Arslan
National Technical University "Kharkiv Polytechnic Institute"
Kharkiv, Ukraine
berk.arslan93@gmail.com

Mykola Tkachuk
V.N. Karazin National University, National Technical University "Kharkiv Polytechnic Institute"
Kharkiv, Ukraine
tka.mobile@gmail.com

Rustam Gamzayev
National Technical University "Kharkiv Polytechnic Institute"
Kharkiv, Ukraine
rustam.gamzaev@gmail.com

***Abstract*— Increasing popularity of web platform, in order to make applications easily accessible, brings the need of information security, where an availability principle ensures that the information is readily accessible to authorized individuals when it is needed. One of the most dangerous threats to availability principle is Distributed Denial of Service (DDoS) attack and there are protection techniques against such attacks. In the article, an emulation approach to testing on Distributed Denial of Service in web applications is described. It supposes to develop a software emulator of DDoS attacks, which provides experimental testing results for a real web application to be evaluated. It can be used for both to detect DDoS vulnerability and to test an effectiveness of DDoS protection. To formalize this approach the operating model of a SE is proposed, which includes structured data, algorithms and some metrics needed to perform DDoS vulnerability testing. The obtained test results and their analysis are presented and discussed.**

Keywords— information, security, web application, software emulator, CIA triad, distributed denial of service, operating model

I. INTRODUCTION

The fundamental security model [1] (a.k.a. CIA triad) is designed to provide a baseline standard for evaluating and implementing information security regardless of the underlying system. CIA triad has three main principles: (1) confidentiality principle is protecting information from unauthorized access, (2) integrity principle is maintaining trustworthiness of the information over its entire life-cycle, and (3) availability principle ensures that the information is readily accessible to authorized individuals when it is needed. The most important principle for organizations is availability principle. Because, if the information is not accessible, then it cannot be manipulated. That is why, when the availability principle is violated, it is nonsense to consider confidentiality and integrity principles. Moreover, violation of availability principle can damage financially (e.g. violation of availability principle in banking systems). Therefore, it is important to use DDoS protection systems that can be easily found online, such as; Intrusion Detection System (IDS), load balancers or other DDoS protection systems.

However, these solutions do not visually represent a web server's behavior under different DDoS attacks on different protocols. Thus, organizations may not know how the protection systems works. On the other hand, if an organization has just decided to use a DDoS protection system, it is important to find out which type of DDoS attacks can successfully violate the availability principle in the current system.

The article explains how DDoS attacks work and an algorithm for detecting DDoS vulnerabilities. This algorithm is based on emulation of real DDoS attack against a target server and simultaneously checking the availability of the server. It is to mention that exactly an emulation approach [2] is to replicate a real DDoS attack with real servers by sending real packets over a network while a simulation approach supposes to evaluate a DDoS attack without having real servers sending packets over network.

Result of these DDoS tests can help organizations properly assess and prioritize their vulnerability management process or test existing DDoS protection systems' effectiveness.

II. DISTRIBUTED DENIAL OF SERVICE ATTACK

In computing, a Denial of Service (DoS) attack is a cyber-attack in which adversary seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disruption services of a host connected to internet. DoS is typically accomplished by flooding the target machine in an attempt to overload systems and prevent some or all legitimate requests from being processed. Therefore, DoS attack is targeting availability principle of the CIA triad. However, DoS attack from one adversary is mostly insufficient to overload a system. That is why, a group of adversaries attacks simultaneously to flood the target machine, or they can use botnets to achieve the same effect. If more than one DoS attack targets the same machine, then this attack is called as Distributed Denial of Service (DDoS) attack.

There are several different DDoS attack techniques [3], but in the article, TCP SYN flood and ping of death attacks are explained to have better understanding on DDoS attack types and how to prepare malicious packet that is used in DDoS emulation.

A. TCP SYN Flood Attack

The TCP three-way handshake in Transmission Control Protocol (TCP) is the method used by TCP to set up a TCP/IP connection over an Internet Protocol (IP) based network. This method has three steps: (1) client requests to connect to the server and sends a synchronize (SYN) message, (2) server acknowledges the SYN message and sends back a synchronize – acknowledge

(SYN-ACK) message, and (3) client responds back with an acknowledge (ACK) message.

The main goal in TCP SYN flood attack is to send numerous SYN messages to the server as a first step of three-way handshake, and do not complete the sequence by sending ACK messages to the server. As a result, the target server creates an entry in its connection table for each received SYN message, responds to each with SYN-ACK message and waits for ACK message from the client. But, client never sends ACK message to the server. As the client continues to send SYN messages, the server's connection table becomes full and it can no longer respond to any more connection request. That is why, availability principle is being violated. In order to understand how to perform such attacks programmatically, it is important to understand Internet Header [4] (IH).

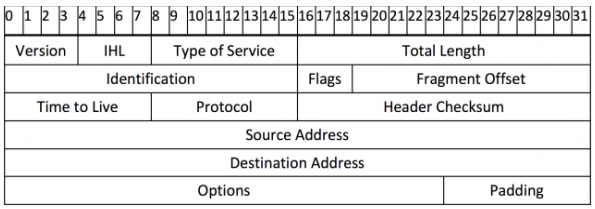


Fig. 1. Internet header.

Fig. 1 shows IH with all components. Numbers in Fig. 1 show the data size, such as; version is 4-bits, type of service is 8-bits, and source address is 32-bits.

In order to perform a TCP SYN flood attack, it is needed to prepare and send an IH with spoofed source address. Because of the fact that source address contains the address of the client that wants to establish a connection, sending an IH with a fake source address results in the server sending SYN-ACK message to the spoofed source address. Even if there is a machine in the spoofed source address, and since that machine did not request any connection, the server never receives an ACK message to establish a connection.

B. Ping of Death Attack

The main goal of Ping of Death (PoD) attack is to send numerous echo-reply messages to the target server larger than the maximum allowable size to freeze or crash the target server.

Internet Control Message Protocol (ICMP), echo-reply message or ping is a network utility used to test a network connection. While some ICMP packets are very small, IPv4 ICMP packets can be much larger and can be as large as the maximum allowable size of 65,535 bytes. This size comes from the 16-bit Total Length data of IH which is represented in Fig. 1. Total Length data holds the length of the datagram, measured in octets (bytes), including IH and data.

All servers must be prepared to accept datagrams of up to 576 octets whether they arrive whole or in fragments. It is recommended that servers only send datagrams larger than 576 octets if and only if they have assurance that the destination is prepared to accept larger datagrams.

In order to execute a successful PoD attack, it is needed to prepare an ICMP packet which is larger than 65,535 octets and send the packet to the target server. When maliciously large packet is transmitted from client to server, the packet becomes fragmented into segments, each of which is below the maximum size limit. When the server attempts to put pieces together, the total size exceeds the maximum allowable size and a buffer overflow can occur. As a result, it causes the server to freeze, crash or reboot. Thus, it violates the availability principle of the CIA triad.

C. Related Work

Our approach aims to detect DDoS vulnerability before the real attack happens. That is why, this approach must be used to find out how would the server behave under DDoS attack. However, there is also a way [5] to simulate DoS attack and detect the attack manually while the attack is being executed.

On the other hand, there is a research [6] on simulation and analysis of DDoS attack by specialized simulator using virtualization. The goal in this research is to create a virtual network using VirtualBox 4.2.6 and simulate DDoS attacks on the virtually created network.

III. Our Approach

To develop a DDoS attacks Emulator in a systematic way an operating model techniques (OM) can be used [7]. Such an OM in our case can be represented a tuple

$$OM\ (DDoS) = \langle InfoBase,\ Algorithms,\ Metrics \rangle \quad (1)$$

where: InfoBase is set structured data, which is needed for DDoS emulation, e.g. Internet headers, protocols (see below), etc., Algorithms is a collection of algorithms to be implemented in Emulator, and Metrics includes quantitative in estimate some operating parameters of a real web applications under DDoS attacks. These OM components are described in more details below.

In order to emulate real DDoS attacks it is necessary to use a distributed software system that is why the DDoS scanner has to be designed exactly in this way. Deployment diagram of the proposed DDoS Scanner is represented in Fig. 2.

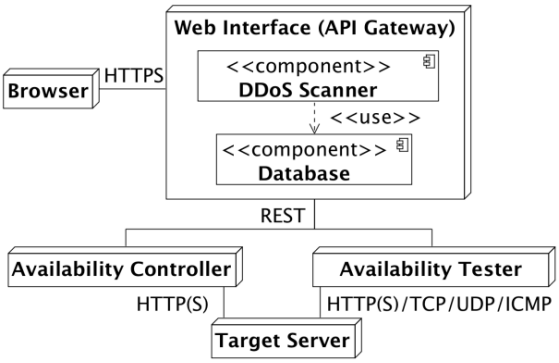


Fig. 2. Deployment diagram of proposed DDoS scanner.

DDoS scanner has three main modules: (1) web interface that is accessible for users to start new tests and to see test results represented as chart, (2) availability controller that is sending HTTP(S) requests to the target server in a short period of time and log the target server's response time under DDoS attack, and (3) availability

tester that is emulating the DDoS attack by sending malicious packets explained in the previous section via TCP, UDP, ICMP protocols. If it is required to perform load tests, then it can also send requests over HTTP(S). Availability tester and controller nodes are controlled by web interface with the help of REST API calls.

Availability controller and availability tester nodes must be deployed on different servers not to use a shared computing resource and to work in maximum performance. Ideally, it is better to deploy them on servers that are using different Internet Service Providers (ISP), not to flood DDoS scanner's own network.

On the other hand, depending on the target server's performance, it is possible to add more availability tester nodes to increase the power of the DDoS attack. In this way, DDoS scanner is able to emulate a DDoS attack with all availability tester nodes to find out existing vulnerabilities, and also able to repeat DDoS attacks with different amount of availability tester (e.g. with only one availability tester node and with two, three or more availability tester nodes) to find out the limits of the target server against DDoS attacks.

Advantage of using more availability tester nodes instead of only one more powerful availability tester node is being safe from flooding scanner's own network causing a slow network due to large number of malicious packets in the network. Therefore, it is better to have several availability tester nodes instead of only one more powerful node. If DDoS scanner floods its own network, this means it attacks itself and gets affected from DDoS attack. In this case, test results may not be illustrating the real test results.

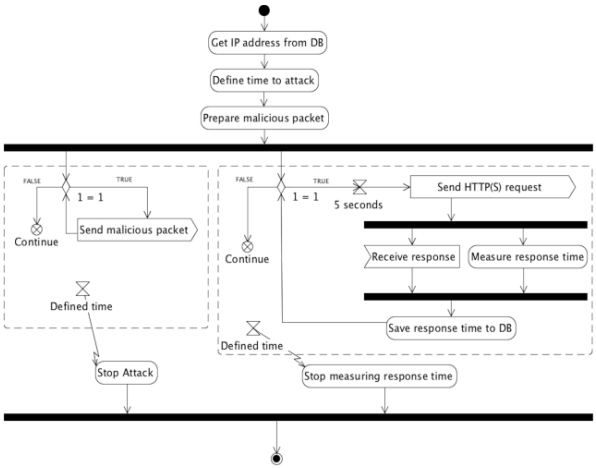


Fig. 3. DDoS vulnerability detection algorithm.

Fig. 3 explains the proposed DDoS vulnerability detection algorithm, which is a part of OM defined in formula (1). In order to start a new DDoS test, a user should provide at least an IP address to be stored in database (DB). When availability tester node starts emulating a DDoS attack, it reads the IP address of the target server from DB. Next, it defines the attack time that is used to end infinite loops to send malicious packets to server and to check server's response time. Depending on the DDoS attack type, it must prepare the needed malicious packet explained in the previous section. When these preparations are completed, DDoS scanner must create two simultaneous processes; one for availability tester nodes and one for availability controller node. This means, availability tester and controller nodes must work together at the same time. Availability tester node sends the malicious packet to the target server in an infinite loop while availability controller node sends HTTP(S) GET request to the home page of the target server in a time interval which is 5 seconds in Fig. 3 and measures the server's response time. Server response time must be stored in DB to create a chart as a result of this test. These two loops work till the defined attack time is over. When the defined attack time is over, both of availability tester and controller nodes must stop sending packets and request to the target server. It is also possible to add another condition to end the test on DDoS vulnerability detection. For example; DDoS scanner can stop the test if server response time is increasing over time under DDoS attack or if response time is getting longer than a pre-defined response time.

According to the introduced OM with formula (1), we have to define some metrics or conditions to be used for DDoS attack's evaluation. In the proposed approach, the condition to successfully detect a DDoS vulnerability can be explained with the help of Packet per Second (PPS) which means the maximum number of packets that a client can send, or a server can handle in a second. Let's assume P_{tester} is availability tester node's PPS, N_{tester} is number of availability tester nodes, and P_{server} is the target server's PPS. Then the appropriate condition can be defined as follows

$$N_{tester} \text{ x } P_{tester} > P_{server} \quad (2)$$

Equation (2) describes the condition when DDoS scanner can detect a DDoS vulnerability, such as: overall PPS limit that DDoS scanner has, must be greater than target server's PPS limit.

By the end of test, DDoS scanner must visually illustrate test results based on the target server's stored response times. These results will help users to understand the target server's behavior under DDoS attack, and to make a conclusion. Analyzing test results and conclusions are explained in the next sections.

IV. Test Results

When tests are completed, DDoS scanner must create charts based on server's response time over DDoS attack duration. These charts explain the server's behavior under DDoS attack.

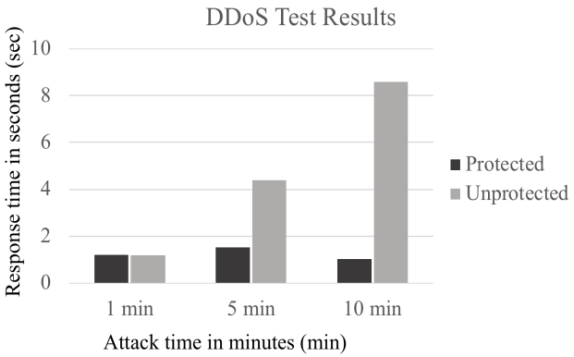


Fig. 4. DDoS test result comparison of protected and unprotected servers.

Fig. 4 simply shows comparison of protected and unprotected servers' behavior under DDoS attack. Protected server represents a server that has a DDoS protection and unprotected server represents a server that has no DDoS protection.

Protected server must be able to resist the attack and server's response time must stay in the same range during the attack. If server's response time is increasing under the attack, then it is a sign of DDoS vulnerability. In the example test result that is represented in Fig. 4, it is clear that protected server's response time stays in the same range while unprotected server's response time increases over attack time.

V. CONCLUSION

Proposed emulation approach for DDoS tests helps us to execute DDoS attacks without flooding our own network. It provides realistic test results to help organizations to assess and prioritize their vulnerability management process. Moreover, it can also help organizations to see effectiveness of the used DDoS protection systems.

As a possible way to improve the proposed approach, we propose to consider including response time limit. Sometimes defined attack time may be much longer than attack time that a target server can handle. In this case, it will cause target server to crash. In order to eliminate such side-effects, it is possible to include a condition to the algorithm which is shown in Fig. 3, such as: if response time is greater than a pre-defined response time limit, than it must end all simultaneously running DDoS attacks controlled by availability tester nodes that is explained in Fig.2. Therefore, it is possible to check DDoS vulnerability without violating the availability principle of CIA triad.

On the other hand, it can also be improved by using other DDoS attack techniques [8] to have a complete DDoS scan to find a vulnerability. Besides that, it is a special task to investigate some advantages and disadvantages for DDoS protection which can be achieved with usage of such advanced solutions as e.g. KEMP LoadMaster product line [9], and to compare them with the proposed approach.

REFERENCES

[1] Mark Rhodes-Ousley, Information security: the complete reference, 2nd ed., 2013, pp. 85 – 87.

[2] Ian McGregor, "The relationship between simulation and emulation", Proceedings of the 2002 Winter Simulation Conference, December 8-11, 2002, USA, pp.1683-1688.

[3] Subramani Rao Sridhar Rao, "Denial of service attacks and mitigation techniques: real time implementation with detailed analysis", SANS Institute InfoSec Reading Room, pp. 8 – 9, 2011.

[4] IETF, Internet protocol – RFC 791, September 1981, pp. 11 – 23.

[5] Aditi Srivastava, Deepak Chaudhary, "Simulation of dos, ddos attacks & design test its countermeasures", IJSER, vol. 5, issue 1, pp. 1801 – 1807, 2014.

[6] Sonal Sinha, Madhulika Sharma, "Simulation and analysis of ddos attacks by specialized simulator using virtualization", IJETTCS, vol. 3, issue 2, pp. 271 – 273, 2014.

[7] De Vries, M. et al. "A Method for Identifying Process Reuse Opportunities to Enhance the Operating Model", IEEE International Conference on Industrial Engineering and Engineering Management, pp. 1005 – 1009, 2011.

[8] Keyur Chauhan, Vivek Prasad, "Distributed denial of service (ddos) attack techniques and prevention on cloud environment", IJIACS, vol. 4, special issue, pp. 210 – 215, September 2015.

[9] Alex Barclay, Ravi Kumar, "Protecting Applications from Denial of Service Attacks with the KEMP LoadMaster", The Technical Note, Version 1, KEMP Technologies, May 2016.

On the application of cyber physical production systems

How a digital twin of physical Systems can be created, updated and utilised in manufacturing automation

Michael Weyrich
Institute of Industrial Automation and Software Engineering
University of Stuttgart
Stuttgart, Germany
michael.weyrich@ias.uni-stuttgart.de

***Abstract*—This paper presents latest research approaches in manufacturing automation based on cyber-physical systems. Three industrial examples are given to sketch how cyber physical systems particularly Digital Twin, change the engineering, commissioning and operation of manufacturing. This paper introduces the concept of the digital twin and discusses how it can be created and kept up-to-date throughout that lifecycle. Methodologies are presented on how engineering data can be interconnected, how a digital twin can be kept updated in operation and data can be used to learn and steer operation.**

Keywords—cyber physical production systems, digital twin, information management, learning control and cognition

I. INTRODUCTION

Cyber physical systems are a novelty in the field of automation technology since they have been conceived around the year 2006 by [Lee]. Cyber physical systems are by definition a combination of the physical assets of a real plant and the world of data, information and software, which form the cyber aspect.

As depicted in Fig.1 physical manufacturing systems consist of machinery, robots, gages and logistical units. These physical assets of the plant are connected using information technology and comprise of multiple data which regard the engineering and the operation.

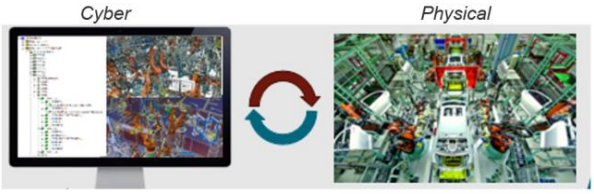


Fig. 1: Example of a cyber physical systems in Automtive Body and White production [4]

In today's manufacturing systems a very large diversity of e.g. hundreds of subsystems exists as there are multiple manufactures who integrate their systems with the subsystems of others. This results in an ongoing complexity of such systems making it very difficult to manage. The operation of such large scale systems demands for standardization, be it classification schemas for components and their grouping, information models etc. This is very much required as the linkage of components in Hard- and Software is extended. A change or update in one instance of a domain, e.g. a mechanical hardware device, may trigger multiple updates in other areas, such as in the electronics or software.

As a result, the automated manufacturing systems as of today and even more in the future are going to be a composition of software, data, which form a digital twin along with the electronics and mechanical hardware of the physical systems.

II. STATE OF THE ART

It was evident in research in the early 2000 (see for instance [3]) that the networking of physical assets results in a large diversity of data. A swarm of sensor systems capturing all types of information, stored in a cloud infrastructure accessible by mobile devices anywhere has become a reality today. Machine to machine communication systems, the "cloud" or internet-of-things (IoT) operating systems are available in terms of commercial products. Furthermore the product lifecycle of management activities have resulted in large Engineering backbone systems.

Due to the availability of these products, research questions evolve from a plain technical feasibility to the question of how to master the tremendous complexity of software systems and their data. Obviously the question is how the step toward cyber physical systems can be made, which assists a hybrid of "cyber" e.g. the information world and the "physical" world of hardware. [3, 4]

A physical system and its cyber part are being created which means in unison on a digital twin. As depicted in Fig. 2 the characteristics and functionalities of physical assets are pictured by a digital twin along the life cycle.

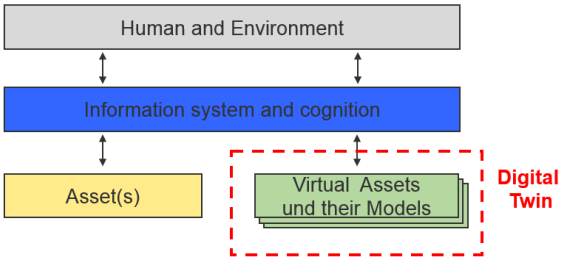


Fig. 2: A Digital Twin is a part of a cyber physical system

A full integration of cyber physical systems and availability of a digital twin, i.e. a cyber representation which could be managed in a cyber or physical way, is still a future vision [1, 2] as a number of frontiers of the automation technology as of today need to be overcome.

As it becomes evident from the interaction with experts in the field [6] the following issues have been raised and need attention:

- Improved techniques are required for establishing the communication between the components of the cyber physical systems in order to reduce the effort for interoperability.
- New types of standards, e.g. for the semantic processing of information, are required but are difficult to conceive.
- Means to manage the complexity of very large automation systems a yet to be invented.
- The topics of analytics, machine learning and artificial Intelligence need to be deployed to enable Self-X functionalities and present limitation in automatic adjustment of systems.

The outcome of the fulfilment of these aspects, a new way of how assets of the physical world are working with the digital twin, being the cyber part, would result in a new engineering and operation process for automation systems [7].

As Fig. 3 illustrates the present engineering process as of to date, which is rather sequential and runs through the phase of engineering, commissioning and test until the operation and runtime of production starts. In some cases a retrofit might be an eventual stage in which the manufacturing is being rebuilt, before a new operation phase would start.

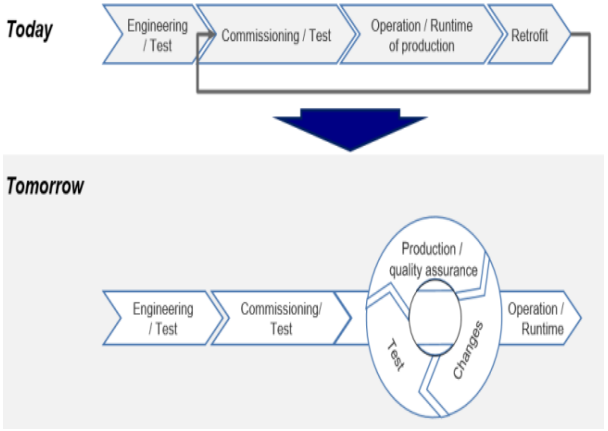


Fig. 3: Design moves to runtime in which changes are omnipresent

This means that once the production has commenced, a change of the system might be normal leading to a situation in which new products could easily be manufactured as the manufacturing would change that way.

Consequently, this implies an enormous paradigm shift as a continuous change is the normal mode of operation. This also means that traditional concepts of quality assurance become obsolete and dissolve with system testing [8].

III. Examples of Cyber-physical Systems for Application in Manufacturing

An illustration of the usage of Cyber-physical systems based on examples of research work with major manufacturing and automation supplier companies; their perspectives are be highlighted:

1. The Engineering for Change and the modular configuration of systems
2. The maintenance of a digital twin once automatic changes in manufacturing are taking place
3. The utilization of big data for quality control during operation

All three provide an overview on present research challenges which are due to the extended availability of data and information which form the cyber part respectively utilize that information as a digital twin of the physical system.

A. Example 1: How to seamlessly integrate the multiple sub disciplines in digital twin in engineering?

To date automated manufacturing systems are designed by means of computer aided design systems (so called CAD or CAx-Systems). For many years these systems have been utilized during the engineering phase in order to design the mechanics, electrical wiring or the sequential control.

By doing so, different views of the design data are supported in the Engineering phase. As a result various computer-based models of a manufacturing system exists such as a description of the 3D appearance of the parts, the layout of the machinery in the plant, electronics, and models of the control software or administrative data of the various components. A large variety of these components can be administrated in commercial tools)* which interconnect the information in an extended database.

However many question arise on the seamless integration of the information in a digital twin. Product lifecycle databases)* entail the above mentioned data of mechatronic components from multiple domain but the data is very often not very well connected between each other. Once a change in the design happens all the different sources might be affected. For instance if a sensor is replaced by another model it is required to update the mechanics, the wiring as well as the software. Despite the fact that all data might be stored in a database, different CAx-tools need to be deployed to update the data. In practical application such updates lead to a significant amount of manual work which has to be done by human operators.

This problem leads to the research question of how a Digital twin can automatically be synchronized or at least how a computer aided assistance function can help update the data sets which from the digital twin of the manufacturing installation.

The Fig. 4 illustrates the information architecture of such an assistance system. A manufacturing cell is made up of data in the domain of mechanical design, electrical / electronic design and software. Each of the assets which are represented in the digital twin has three types of data which are stored in a repository or come from a library

which is reused. Additionally the system entails information, e.g. on how the components are interconnected by means of a product structure.

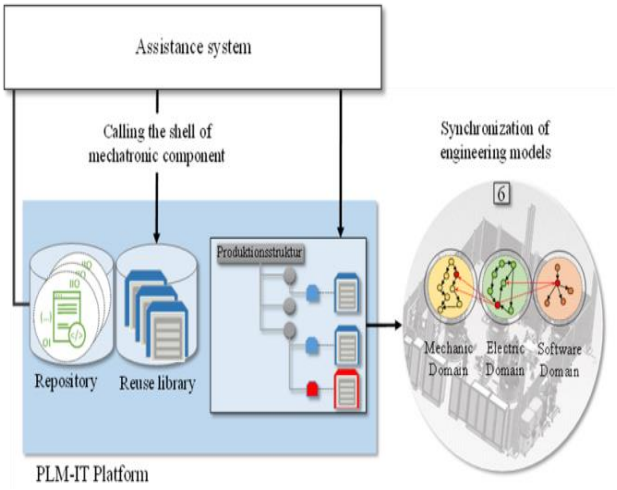


Fig. 4 Concept of an assistance system which keeps the digital twin of a mechatronic manufacturing up-to-date

A method for automatic detection of changes is researched based on the industrial setup on. In [5] we explain how so-called anchor points can be utilized to interconnect information models of the multiple domains.

The research work conducted has a strong empirical aspect and requires physical installations of manufacturing which should be typical machinery utilized in practice. In this work, the research campus Arena 2036 is the testbed for experiments which provides the required installation of "real life" machinery and a full set of state-of-the-art PLM/CAx tools.

We are very fortunate to have the installation of th Arena 2036 available for empirical research in order to understand how the cyber physical systems evolve in practice.

B. Example 2: How to manage the vast variety of information of manufacturing facilities in automotive?

In automated manufacturing in the automotive industry a huge variety of data is being created describing the manufacturing facilities. These data need to be systematically administrated over the course of time as product changes and updates happen during the operation phase.

Automotive manufacturing for instance in body-and-white has invented an elaborated set of methods and tools in order to obtain and administrate their data. Today, the manufacturing planning is based on Standards and De-factor Standards of the automotive manufacturing company and their equipment suppliers.

In Fig. 5 an outline of today's data is provided and the means on how to structure them. Many ideas on standard and schemas are already implemented in automotive, basically aiming towards the structuring of information. Be it by means of markup languages such as Automation-ML or specially released standards which are agreed upon by the stakeholders in the automotive community.

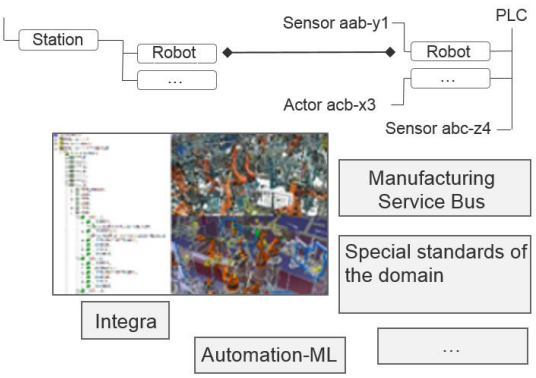


Fig. 5: Schemas for structuring engineering data in Automotive Body and White [4]

However, despite all efforts a central question on how to create transparency remains, e.g. by automatically interconnecting fragmented information. With the appearance of cyber physical systems and the digital twin this question becomes even more relevant as data is required for retrofits or a contours update of the cyber-physical equipment.

Should a new vehicle require adjustments in the manufacturing systems, all the planning data needs to be up-to-date. The work which is described in [4] analyses how planning data can be updated. This means it investigates on an automatic data update of planning objects based on multiple methods and aims to interconnect them.

In order to update the digital twin the following sources of information are engaged:

- Existing planning data which are stored in CAx-databases as per example 1
- IT Network Scan of all fieldbus systems in the shop floor can be utilized in order to capture all components which are utilized in the system
- 3D Scans of the shopfloor are undertaken to obtain volumetric data on all the physical installation
- High-resolution pictures of all installed systems with high resolution panoramic cameras which document all types of detail in the manufacturing

The research work on how to connect these pieces of information is ongoing, but will be very much required to create an up-to-date digital twin of the manufacturing line in operation.

C. Example 3: How to engage data driven qulity control during operation?

Sensor data entail information about the plant and process and can be analyzed to improve process quality. The control can be based on the process data obtained during operation and can be used for Prediction and optimization of product quality for automatic control or as recommendation of action for the operator.

In this setting the digital twin captures operational data which help to identify patterns which can thereafter be used for action proposals.

The ultimate goal for this research is that systems learn about dynamics and disturbances based on real process data.

As per Fig. 6 a special learning approach needs to be conceived in order to adjust the various quality loops which are responsible for the quality of the manufacturing operation.

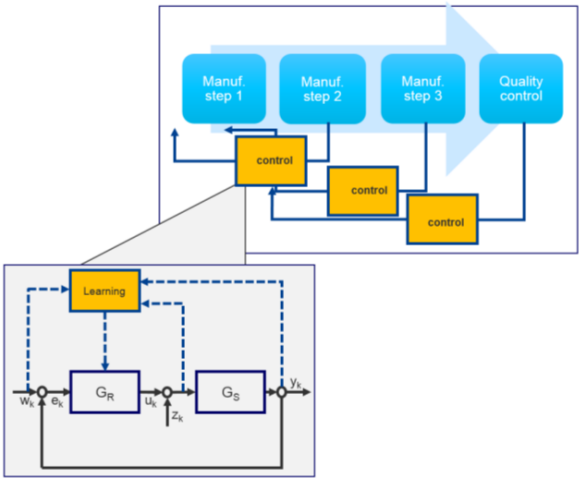


Fig. 6: Cascaded quality loops for learning control of manufacturing operation.

The research of [9] is based on terabyte of real factory data of machinery and all types of sensors to obtain that quality control. Results can be achieved by deploying learning algorithms. The challenge is however twofold: First: The structure of the model, the manufacturing and its quality control needs to be adequate. Second: known correlations and relationships in the process need to be available. Both aspects support the convergence of the algorithms. So far, anomalies in the manufacturing systems can be detected or even predicted which results in an adjustment of the control loops.

CONCLUSION

This paper presents a model for the digital twin as a core element of cyber physical production systems and provides scenarios on how the digital twin can be utilized in industrial application.

It is evident that the digital twin concept is very straight forward and clearly supports the engineering, commissioning and later operation. However, the work also illustrates the diversity of the various data sources which feed the digital twin. From the examples presented it becomes obvious that the synchronization of the digital twin with the physical world is albeit challenging, can provide an enormous potential as it enables a new way of work with a reconfiguration and optimization of manufacturing operation.

ACKNOWLEDGMENT

The author is appreciative of the ARENA2036 (Active Research Environment for the Next Generation of Automobiles) on Campus of University of Stuttgart)[1].

The sponsors of this work which are the Siemens AG and Daimler AG which support the Graduate School of manufacturing Engineering of University of Stuttgart in which two graduate students are working on the topics. Further the Federal ministry of Economic affairs and Energy (BmWi) Provides funding for the Research project Emudig)[2].

REFERENCES

[1] Schuh, G.; Anderl, R.; Gausemeier, J. ten Hompel, M. Wohlster, W. (Hrsg.): Industrie 4.0 Maturity Index. Die Digitale Transformation von Unternehmen Gestalten (Acatech Studie). München, 2017

[2] Weyrich, M.;Klein, M.; Schmidt, J.; Jazdi, N.; Bettenhausen, K.; Buschmann, F.; Rubner, C.; Pirker, M.; Wurm, K.: "Evaluation Model for Assessment of Cyber-Physical Production Systems," in Industrial Internet of Things: Cybermanufacturing Systems, S. Jeschke, C. Brecher, H. Song, and D. B. Rawat, Eds. Cham: Springer International Publishing, 2017, pp. 169–199

[3] Rabaey, J., Pederson , D.: A Brand New Wireless Day. What does it mean for design technology? ASPDAC 2008, Seoul, Keynote presentation. http://www.aspdac.com/aspdac2008/Keynote-Address-I.pdf (abgerufen am 01.04.2018)

[4] Biesinger, F.; Meike, D.; Kraß, B.; Weyrich, M.: A Case Study for a Digital Twin of Body-in-White Production Systems. IEEE Conference on Emerging Technologies And Factory Automation (ETFA), Turin, Sept. 2018 (submitted)

[5] Ashtari, B.;Jazdi, N., Schloegl, W., Weyrich, M.: Consistency check to synchronize the Digital Twin of manufacturing automation based on anchor points. 51st CIRP Conference on Manufacturing Systems, Stockholm, May 2018 (accepted)

[6] Klein, M.; Weyrich, M.: "Institut für Automatisierungstechnik und Softwaresysteme," Industrie 4.0 Management, 4/2016 Sonderausgabe, no. 4, 2016.

[7] Faul, A.; Beyer, T.; Klein, M.; Vögeli, D.; Körner, R.; Weyrich, M.: Eine agentenbasierte Produktionsanlage am Beispiel eines Montageprozesses. In: Vogel-Heuser, B. (Herausgeber): Softwareagenten in der Industrie 4.0, De Gruyter Verlag; Erscheint Juni 2018

[8] Klein, M.; Löcklin, A.; Jazdi, N.; Weyrich, M.: A negotiation based approach for agent based production scheduling. 28th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2018), June, 2018, Columbus, USA (accepted)

[9] Lindemann, B.; Karadogan; C.; Jazdi, N.; Weyrich, M.; Liewald, M.: Data driven quality control in discrete manufacturing using a self-learning approach - CIRP Conference on Intelligent Computation in Manufacturing Engineering, Italy, 18 - 20 July 2018 (accepted)

)[1] see: www.arean2036.de
)[2] see: www.massivumformung.de/forschung/emudig-40/

Time series prediction based on evolving neural network CMAC

Oleg G. Rudenko
Information system department
Kharkiv National University of Economics
Kharkiv, Ukraine
oleg.rudenko@hneu.net

Oleksandr O. Bezsonov
I*nformation system department*
Kharkiv National University of Economics
Kharkiv, Ukraine
oleksandr.bezsonov@hneu.net

Oleksandr S. Romanyk
Electronic computer department Kharkiv National University of Radioelectronics
Kharkiv, Ukraine
romanyk@gmail.com

***Abstract*— Artificial neural networks (ANN) have found increasing consideration in forecasting theory, leading to successful applications in time series and explanatory sales forecasting. The conventional neural network CMAC (Cerebellar Model Articulation Controller) can be applied in many real-world applications thanks to its high learning speed and good generalization capability. In this paper it is proposed to utilize a neuro-evolutional approach to adjust CMAC parameters. The general structure of the evolving NN CMAC (ECMAC) is considered. The paper demonstrates that the evolving NN CMAC can be used effectively for the solving of time series prediction task. The simulation of the proposed approach for various time series is performed. The results proved the effectiveness of the developed methods.**

Keywords—neural network, training, time series, evolution, chromosome

I. INTRODUCTION

Using a mathematical model of the cerebellar cortex developed by D. Marr [1] in 1975 J. Albus proposed a model describing the motion control processes that occur in the cerebellum, which was subsequently implemented in the neural network controller for controlling the robot - arm, which he called CMAC - Cerebellar Model Articulation Controller [2, 3]. Ease of implementation and good network of approximating properties have ensured its wide usage not only in the tasks of controlling the robotic arm in real time, but also to solve many other practical problems [4, 5].

However, it should be noted that in designing a network CMAC a number of difficulties in the selection of parameters such as the number of levels and the quantization levels, the shape of the receptive field, the type of applied information hashing algorithm and training. These parameters have a significant impact on the accuracy and speed of CMAC network, and therefore, the determination of the optimal values of these parameters is an important practical problem. In this article, for eliminating the drawbacks of traditional methods of synthesis and functioning ANN CMAC we provide the use of a new class of networks - evolving ANN (EANN) in which, in addition to traditional learning it is used another fundamental form of adaptation - evolution, realized by applying the evolutionary computation [6, 7].

The main advantage of using evolutionary algorithms (EA) as learning algorithms is that many ANN parameters can be encoded in the genome and determined in parallel. Moreover, unlike most optimization algorithms designed to solve a problem, EA operate with a multitude of solutions - the population, which allows reaching a global minimum, without getting stuck in the local ones. In this case, information about each individual of the population is encoded in a chromosome (genotype), and the solution (phenotype) is obtained after evolution (selection, crossing, mutation) by decoding.

Among EAs that are stochastic and include evolutionary programming, evolutionary strategies, genetic algorithms, genetic programming, in particular, programming with gene expression, genetic algorithms (GA) are the most common [8, 9]. GA abstract the fundamental processes of Darwinian evolution: natural selection and genetic changes due to recombination and mutation.

II. NEURAL NETWORK CMAC

ANN offer great flexibility in modelling quantitative forecasting methods. This work is focused on time-series point predictions with neural network ECMAC. A variable $\hat{y}_{t+h}$ is predicted using only observations of the same variable y_t ,interpreting the time t as the only independent variable [10]. At a point in time *t (t=1,...,T)*, a one-step ahead forecast $\hat{y}_{t+1}$ is computed using observations y_t, y_{t-1}, …, y_{t-n} from *n* preceding points in time *t, t*–1*, t*–2*, ..., t*–*n*–1, with *n (n*=1,...,*N)* denoting the number of input units. This models a time-series prediction in analogy to an non-linear autoregressive AR(*n*) model [10] of the form $\hat{y}_{t+1} = f(y_t, y_{t-1},..., y_{t-n})$.

The modification of the network proposed by Albus for solving this problem is shown in Fig. 1. The network consists of the input, hidden and output layers, labeled L1, L2, L3, respectively, and uses two basic conversions: S: $X \Rightarrow A$, P: $A \Rightarrow y$, where X - N-dimensional space of continuous input signals; A - n-dimensional space associations; y - a one-dimensional output.

Converting $S \Rightarrow A$ in turn consists of two transformations: $X \Rightarrow M$, $M \Rightarrow A$, where M - the space of binary variables.

The principle of the network operation as an associative memory is as follows. Approximated function $y = f(x)$ is given to a limited number of points (argument values) **x** constituting N-dimensional space of the input signals. This space is divided into subspaces M formed the

input signals **x**(i) ($i = \overline{1,M}$). Number of subspaces M impacts the accuracy of the network and number of utilized memory cells. Therefore, on the one hand side it should be big enough to ensure good approximation capabilities of the network and on the other hand side it should be not too big to save some memory. In constructing the cerebellum model Albus proceeded from the fact that the appearance of the excitation signal activates its a certain area of the cerebellum, or receptive field, characterized by a parameter ρ.

Therefore, storage of values of **y**(i) (network output signal) corresponding to **x**(i) ($i = \overline{1,M}$), used ρ memory cells, the number of which is constant for all vectors of the input signals on the network. At receipt of the input signal **x**(i) a signal **y**(i) appears at network output, which is the sum of ρ addressable cells content.

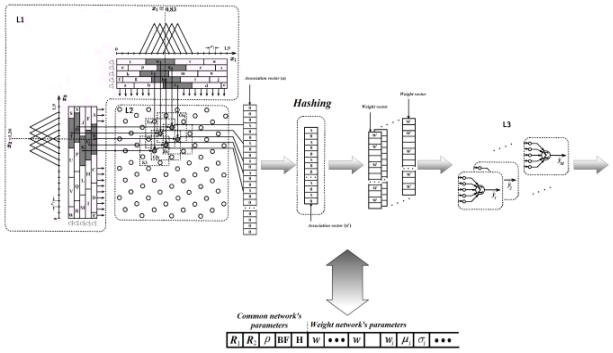


Fig. 1. Albus network

Associative CMAC properties manifest themselves in the form of used addressing, which is based on a special coding input information and called hash coding or hashing [11].

III. Encoding Information in CMAC

Information coding in the network means that to each *N*-dimensional input vector **x**(*i*) a n-dimensional association vector **a**(*i*), is assigned and stored in virtual memory.

Elements of **a**(*i*) can take the values from the interval [0, 1] (in the papers cited above it is assumed that these elements take the values 0 or 1). Thus only ρ << n elements of the vector have non-zero values, i.e. only ρ memory elements are active.

Continuous plurality of input signals by sampling (at the level of quantization) is converted into discrete. Thus to represent the *i*-th input signal components R_i quantization levels used with the appropriate quantization step r_i ($i = \overline{1,N}$). It should be noted that the accuracy of the system identification depends substantially on the size of the quantization step, and loss of stability is possible in digital automated control systems with an incorrect choice of this parameter.

Each stage is characterized by a corresponding association matrix A_i ($i = \overline{1,\rho}$), only one element of which is different from zero.

Construction associations vector as follows. For a given total number of input signals association matrix A_i of each quantization stage ($i = \overline{1,\rho}$) are formed. The columns of these matrixes form association vectors $\boldsymbol{a}_i$ ($i = \overline{1,\rho}$).

The dimension of these vectors, *n*, equal to the sum of all elements of the matrices A_i ($i = \overline{1,\rho}$) and can be calculated by the formula:

$$n = \left\rceil \rho \left(\frac{R-1}{\rho} + 1 \right)^N \right\lceil ,$$

where *R* - the number of used levels for quantizing input signals; *N* - the dimension of the input vector; ⌉•⌈ - means rounded to the nearest whole number.

Since all ρ matrices A_i ($i = \overline{1,\rho}$) have only one non-zero element, from the *n* components of the vector $\boldsymbol{a}(i)$ only ρ are non-zero.

The quantization region are arranged in a such way, that any of them relating to the adjacent stages, have not more than (ρ - 1)-th connection. This corresponds to a restriction on the maximum total number of cells equal to (ρ - 1) used for storing two different vectors of the input signals in which their recognition is still possible.

IV. Evolving ANN CMAC

During switching from ANN to EANN for all types of networks the common evolutionary procedure (initialization population, an estimation of the population, selection, cross-breeding, mutations) is used. Differences are only in the method of encoding the structure and parameters of a particular form of ANN in the chromosome.

At the beginning of EA functioning, population P_0 that consisting of N individuals (ANN): $P_0 = \{H_1, H_2, .., H_N\}$ is randomly initialized. The proper choice of the N's value is very important as this parameter significantly affects the speed of the algorithm and its selection is critical for real-time systems. Each individual in the population at the same time gets its own unique description, encoded in the chromosome $H_j = \{h_{1j}, h_{2j}, ...h_{Lj}\}$, which consists of L gene, wherein $h_{ij} \in [w_{\min} w_{\max}]$ - *i*-th value of *j*-gene chromosome ($w_{\min}$ - the minimum and $w_{\max}$ - maximum allowable values, respectively).

Figure 1 shows an example ECMAC chromosome's format and the correspondence between genes and network parameters stored in the chromosome. It should be noted that chromosome length depends on the dimensionality of the problem and the maximum amount of memory.

As seen from the drawing, it consists of a chromosome gene in which information about corresponding network parameters is stored. At the beginning of the chromosome there are genes that contain information about the parameters of the noise and they are active only in case of the noisy measurements. Next gene's block encodes the number of levels and the quantization steps, the shape of the receptive field of neurons and type of algorithm that is used for hashing information.

Due to the large amount of the BF that can be used in CMAC, there is a special gene in its chromosome BF, that is responsible for coding the type of the used functions. There is also a gene H in the chromosome, that encodes a type of the hashing algorithm (If its value is set to 0, than hashing is not used).

Then, in the chromosome there is a group of genes encoding weighting parameters directly relevant to the associative neurons. During the initialization phase initial values are assigned to all these parameters by using a random number generator.

Since during evolution mutation may occur in the parameters affecting the amount of used associative neurons, the length of the chromosome can vary. The use of variable length chromosomes occur individuals with specific genetic code segments (introns) which are not used for coding characteristics [12].

Typically, introns are used in the EA:

1) As noncoding bits that are uniformly added to the genetic code (in this case introns only fill the space between the active genes of the chromosome).
2) As the nonfunctional parts of the genetic code, i.e., parts of the decision which do not actually do anything, thus not affect the fitness of the chromosome (this usually occurs in the genetic programming and in the chromosomes, which are subject to the cycle of development after birth).
3) As posteriori useless part of the chromosome, which do not participate in the calculation of its fitness (usually it manifests itself in some types of competitive-trained neural networks, in which only neurons-winners in contrast to other neurons that are a posteriori useless affect network performance results).

Once the initial population is formed, the fitness of each individual part in it evaluates by some defined fitness function.

Conventionally, as such a function the quadratic one is used:

$$F(x) = \frac{1}{M}\sum_{i=1}^{M}\left(y^*(x_i) - \hat{y}(x_i)\right)^2,$$

where $y^*(k)$ - the desired network response; $\hat{y}(k)$ - real output signal; M – sample size.

The next step is the selection of individuals, the chromosomes of which are involved in the formation of the new generation, and subsequent hybridization.

The task of crossing operator (crossover) is the transfer of genetic information from the parent individuals to their offspring. After completion of the operator's work, any gene of any individual in the new population may mutate, i.e. change its value.

Since chromosome uses hybrid coding, during the mutations various operations must be performed for different encoding methods.

For example, in case of the gene that is responsible for neuron's activation and uses binary encoding, inverse mutation should be used. For coding the BF and weighting parameters, that uses real values, different types of mutations may be used.

Thus ECMAC algorithm can be represented as follows.

1) Create an initial population.
   a. Initialization of each individual chromosome.
   b. Estimation of the initial population.
2) The stages of evolution - the construction of a new generation.
   a. Selection of candidates for mating (breeding).
   b. 2.2 Hybridization, i.e. causing by each pair of selected candidates some new individuals.
   c. Mutation.
   d. Evaluation of the new population.
3) Check the completion criterion, if not satisfied - go to 2.

V. Conclusions

The results showed that the evolving neural network CMAC is quite effective and convenient in solving practical problems of time series prediction.

Some experimental results in forecasting a stationary time series using ECMAC are computed, evaluating the performance in competition to basic forecast methods using various error measures.

An additional advantage of the evolutionary approach to CMAC network training is the solution of the problem of choice the associative neurons receptive field form that is affecting the method and the prediction accuracy of the studied time series. In the case ECMAC this problem is solved automatically.

References

[1] Marr, D.: A Theory of Cerebellar Cortex. Journal Physiology, Vol. 202, 437-470. (1969)

[2] Albus, J.: A new approach to manipulator control: the cerebellar model articulation controller (CMAC). ASME Trans., J. Dynamic Systems, Measurement and Control, Vol. 97, №3, 220-227. (1975)

[3] Albus, J.: Data storage in cerebellar model articulation controller (CMAC). ASME Trans. J. Dynamic Systems, Measurement and Control, Vol. 97, №3, 228–233. (1975)

[4] Miller, W., Glanz, F., Kraft, L.: CMAC: An associative neural network alternative to backpropagation. Proc. of the IEEE, Vol. 78, №10, 1561–1567. (1990)

[5] Miller, T., Hewes, R., Glanz, F., Kraft, L.: Real-time dynamic control of an industrial manipulator using a neural-network-based

[6] learning controller. IEEE Trans. Robot. Automat., Vol. 6, 1-9. (1990)

[7] Yao, X.: A Review of Evolutionary Artificial Neural Networks. Int. J. Intell. Syst., №8 (4), 539-567. (1993)

[8] Yao, X.: Evolving Artificial Neural Networks. Proc. of the IEEE, Vol. 87, №9,1423-1447. (1999)

[9] Holland, J.: Adaptation in Natural and Artificial Systems. An Introductory Analysis With Application to Biology, Control and Artificial Intelligence. University of Michigan (1975)

[10] Goldberg, D.: Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley, MA. (1989)

[11] S.Makridakis, S.C.Wheelwright, R.J.Hyndman, Forecasting Methods and Applications, Wiley, New York, 1998

[12] Rudenko, O., Bessonov, O.: Hashing information in a neural network CMAC. Control Systems and Machines, №5, 67-73. (2004)

[13] Castellano, J.: Scrapping or Recycling: the Role of Chromosome Length-Altering Operators in Genetic Algorithms. Technical Report. GeNeura Group, Department of Architecture and Computer Technology, University of Granada. (2001)

Візуалізаційне моделювання процесів секторної кооперації в розподілених системах управління

Любомир Петришин
кафедра управління
Науково-Технологічний Університет AGH
Краків, Польща
l.b.petryshyn@gmail.com

Марцін Капера
кафедра інформатики
Науково-Технологічний Університет AGH
Краків, Польща
m.kapera@gmail.com

Володимир Глущенко
кафедра комп'ютерних систем та мереж
Східноукраїнський національний університет
ім. В.Даля
Сєвєродонецьк, Україна
2847@i.ua

Михайло Петришин
кафедра інформатики
ДВНЗ Прикарпатський національний університет
ім. В.Стефаника
Івано-Франківськ, Україна
m.l.petryshyn@gmail.com

Visualization modeling of sectoral cooperation processes in distributed management systems

Lubomyr Petryshyn
dept. of Enterprise Management
AGH University of Science and Technology
Cracow, Poland
l.b.petryshyn@gmail.com

Marcin Kapera
dept. of Computer Science
AGH University of Science and Technology
Cracow, Poland
m.kapera@gmail.com

Volodymyr Glushchenko
dept. of Cybernetics and Computer Systems
Volodymyr Dahl East Ukrainian National University
Severodonetsk, Ukraine
2847@i.ua

Mykhailo Petryshyn
dept. of Computer Science
Vasyl Stefanyk Precarpathian National University
Ivano-Frankivsk, Ukraine
m.l.petryshyn@gmail.com

***Анотація*—Моделювання процесів управління секторною кооперацією в розподілених інформаційних системах дозволяє зредукувати кошти впровадження та експлуатації таких складних систем. Запропонований метод візуалізації інформаційних моделей відображає в графічній формі складові процеси та спрощує порозуміння на стадії аналізу і проектування між замовником та розробником системи. Наведено основи візуалізаційного моделювання та спрощений приклад розробки моделей двосекторної системи керування паркуванням.**

***Abstract*—Simulation of the processes of sectoral cooperation management in distributed information systems allows to reduce the means of introduction and operation of such complex systems. The proposed method of visualization of information models reflects graphically the constituent processes and simplifies the understanding at the stage of analysis and design between the customer and the system developer. The basics of visualization modeling and simplified example of development of models of two-sectoral parking management system are presented.**

Ключові слова—візуалізаційне моделювання, інформаційні процеси, секторна кооперація, розподілені системи, управління

Keywords—visualization modeling, information processes, sectoral cooperation, distributed systems, management

I. Вступ

Управління складними ситеми в умовах секторної кооперації вимагає застосування інформаційних технологій, що забезпечують відображення стану та уможливлюють управління системою в режимі реального часу. Візуалізація процесів управління дозволяє зняти психологічний барєр та уникнути взаємного непорозуміння між замовником та розробником інформаційних систем, а також зредукувати кошти розроблення, впровадження та експлуатації таких систем.

Метою опрацювання є представлення візуальних методів моделювання процесів управління складними

системами в умовах секторної кооперації, а також розробка спрощеного прикладу двосекторної системи управління мережею паркінгів.

Новизна роботи полягає у впровадженні графічних методів моделювання, що забезпечують візуалізацію процесів управління та спрощення розуміння їх перебігу.

Практична значимість полягає у можливості відображення структури та перебігу процесів управління, в уникненні непорозуміння при постановці завдання та забезпеченні вимог замовника, а також зниженні коштів розробки та експлуатації систем.

Основи візуалізаційного моделювання опубліковано в [1]. Нижче проаналізуємо спрощений приклад моделювання інформаційної системи управління двома вибраними секторами об’єкту інформатизації.

Компанія «Parkstop» спеціалізується на управлінні міським простором з метою створення паркувальних місць, виконує зовнішні замовлення на вимогу міст або приватних установ. Динамічний розвиток компанії забезпечено створенням автостоянок P & R у великих містах і численних модифікаціях існуючих автостоянок у міських центрах, що призвело до необхідності розробки IT-системи, яка могла б покращити діяльність компанії.

Представлений приклад проекту інфосистеми допоможе оптимізувати процес потоку даних в компанії та забезпечить ефективну комп'ютеризацію компанії при скороченні експлуатаційних коштів. На рис. 1 зображено ієрархічну організаційну структуру компанії «Parkstop».

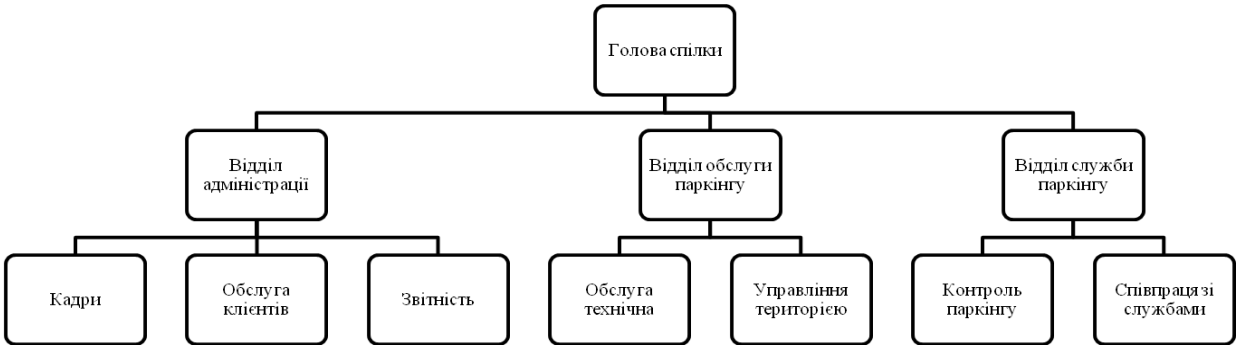


Рис. 1. Ієрархічна організаційна структура компанії «Parkstop»

II. Аналіз організаційних підрозділів компанії

Голова правління спілки координує діяльність компанії та очолює роботу всіх підрозділів. Його представник на ділових зустрічах відповідає за прийняття замовлень та поточний напрям розвитку компанії.

Відділ адміністрації:

- підрозділ кадрів відповідає за поточне управління та набір працівників; відповідає за підготовку та розвиток робочої сили; координує заробітну плату компанії та здійснює програми стимулювання,
- підрозділ закупівлі та технічного обслуговування клієнтів відповідає за підготовку пропозицій компанії до тендерів на розробку земельних ділянок для паркувальних місць, веде спілкування та переговори з клієнтом, переглядає існуючі угоди та керує маркетинговим дослідженням з метою знаходження нових клієнтів,
- підрозділ звітності та розрахунків займається обчисленням заробітної плати та рахунків у компанії, а також підготовкою аналізів для клієнта, які представляють прибуток від експлуатації автомобільних паркінгів.

Відділ обслуговування паркінгів:

- підрозділ технічного обслуговування займається ремонтом та встановленням паркоматів, а також наданням технічних послуг,
- підрозділ територіального управління підготовлює майданчики для паркування, визначає місця паркоматів, розмітку ліній паркування, вирізку дерев, підготовку можливих торгових приміщень та налагодження паркування відповідно до стандарту, розробленого в договорі.

Відділ персоналу обслуговування паркінгів:

- підрозділ контролю за паркуванням здійснює координування працівників, залучених до продаж та перевірки квитанцій,
- підрозділ співпраці з спецслужбами забезпечує накладання за необхідності штрафів, або евакуацію неправильно припаркованих транспортних засобів шляхом повідомлення відповідних служб, передає звіти та статистику чинностей до відділу звітів та розрахунків.

Інформаційна система управління компанією «Parkstop» дозволяє забезпечити інфообмін між підрозділами, спільне використання та зберіганням даних і, як наслідок, оптимізацію співпраці підрозділів.

III. Приклади процесів системи, які може здійснити користувач системи

В табл. I здійснено аналіз системних операцій процесу по розмітці паркувальних місць, натомісць в табл. II проаналізовано системні операції процесу по заміні паркомату.

ТАБЛИЦЯ I. Системні операції по розмітці паркувальних місць

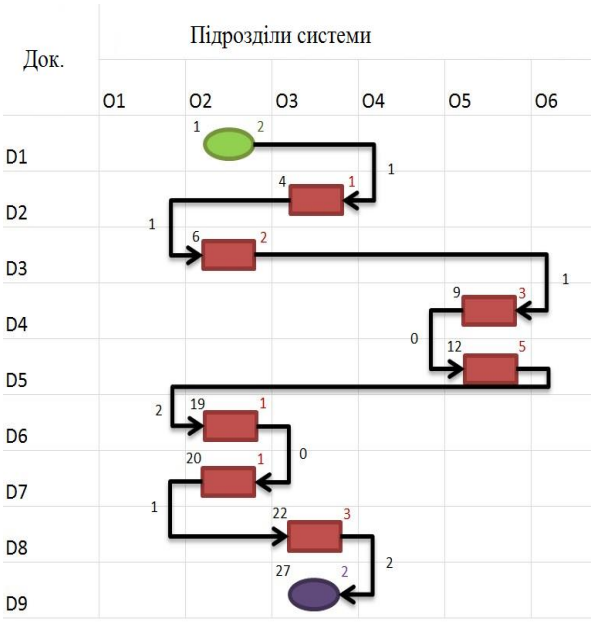
Документ	Зміст	Відповідальний
D1.O2	Встановлення контакту з клієнтом	Відділ обслуговування клієнтів
D2.O3	Відкриття внутрішнього клієнтського рахунку	Відділ звітування та разрахунків
D3.O2	Розміщення у хмарі проекту клієнта	Відділ обслуговування клієнтів
D4.O5	Впровадження технічних виправлень у проекті	Відділ територіального управління
D5.O5	Розмітка місця та надсилання документації	Відділ територіального управління
D6.O2	Затвердження виконаних послуг	Відділ обслуговування клієнтів
D7.O2	Надіслати відгук до відділу O3	Відділ обслуговування клієнтів
D8.O3	Розрахунок замовлення з клієнтом	Відділ звітування та разрахунків
D9.O3	Виплата заробітної плати	Відділ звітування та разрахунків

ТАБЛИЦЯ II. Системні операції по заміні паркомату

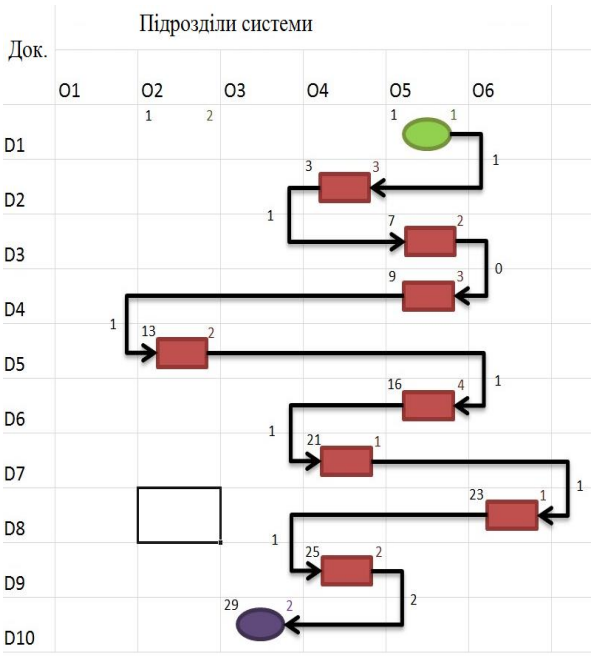
Документ	Зміст	Відповідальний
D1.O6	Реєстрація в системі повідомлення про нефункціонуючий паркомат	Відділ паркування
D2.O4	Відповідь на заявку - рішення заміни паркомату	Відділ технічної служби
D3.O5	Встановлення в системі плану розміщення нового паркомату	Відділ територіального управління
D4.O5	Підготовка кошторису	Відділ територіального управління
D5.O3	Прийняття кошторису витрат	Відділ звітування та разрахунків
D6.O5	Встановлення паркомату і відправлення інформації до відділу O4	Відділ територіального управління
D7.O4	Випробовування паркомату до відділу O6	Відділ технічної служби
D8.O6	Тест паркомату	Відділ паркування
D9.O4	Надсилання звіту робіт до відділу O3	Відділ технічної служби
D10.O3	Оплата витрат згідно кошторису	Відділ звітування та разрахунків

IV. Матрична модель

Матрична модель дозволяє візуалізувати перебіг виконання системних операцій в складі процесів підприємства, що виконуються у відповідних підрозділах в функції часу. На рис. 2 зображено матричні моделі процесів для: а) розмітки місць паркування та б) заміни паркомату.



а)



б)

Рис. 2. Матричні моделі процесів: а) розмітки місць паркування, б) заміни паркомату.

V. Модель суміщений граф часів

Здійснити оцінку повного обчислювального навантаження інформаційної системи управління дозволяє модель суміщеного часового графу виконання системних операцій процесів системи, яка для наведеного прикладу зображена на рис. 3.

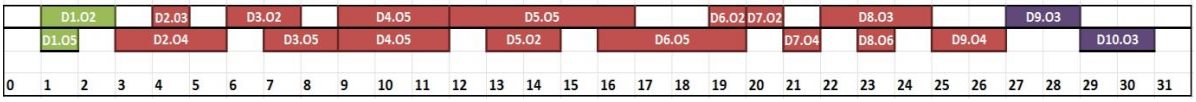


Рис. 3. Модель суміщеного часового графу виконання системних операцій процесів системи

VI. Блок-схема алгоритму

На основі моделі суміщеного часового графу будують блок-схему алгоритму виконання програми управління системою, яка із застосуванням об'єктно-орієнтованого програмування дозволяє здійснити швидку імплементацію програмного забезпечення. На рис. 4 наведено блок-схему алгоритму виконання системних операцій. Щоб уникнути неоднозначності позначень системних операцій для кожного з двох процесів, елементи процесу 1 позначено як "I", натомість елементи процесу 2 - "II".

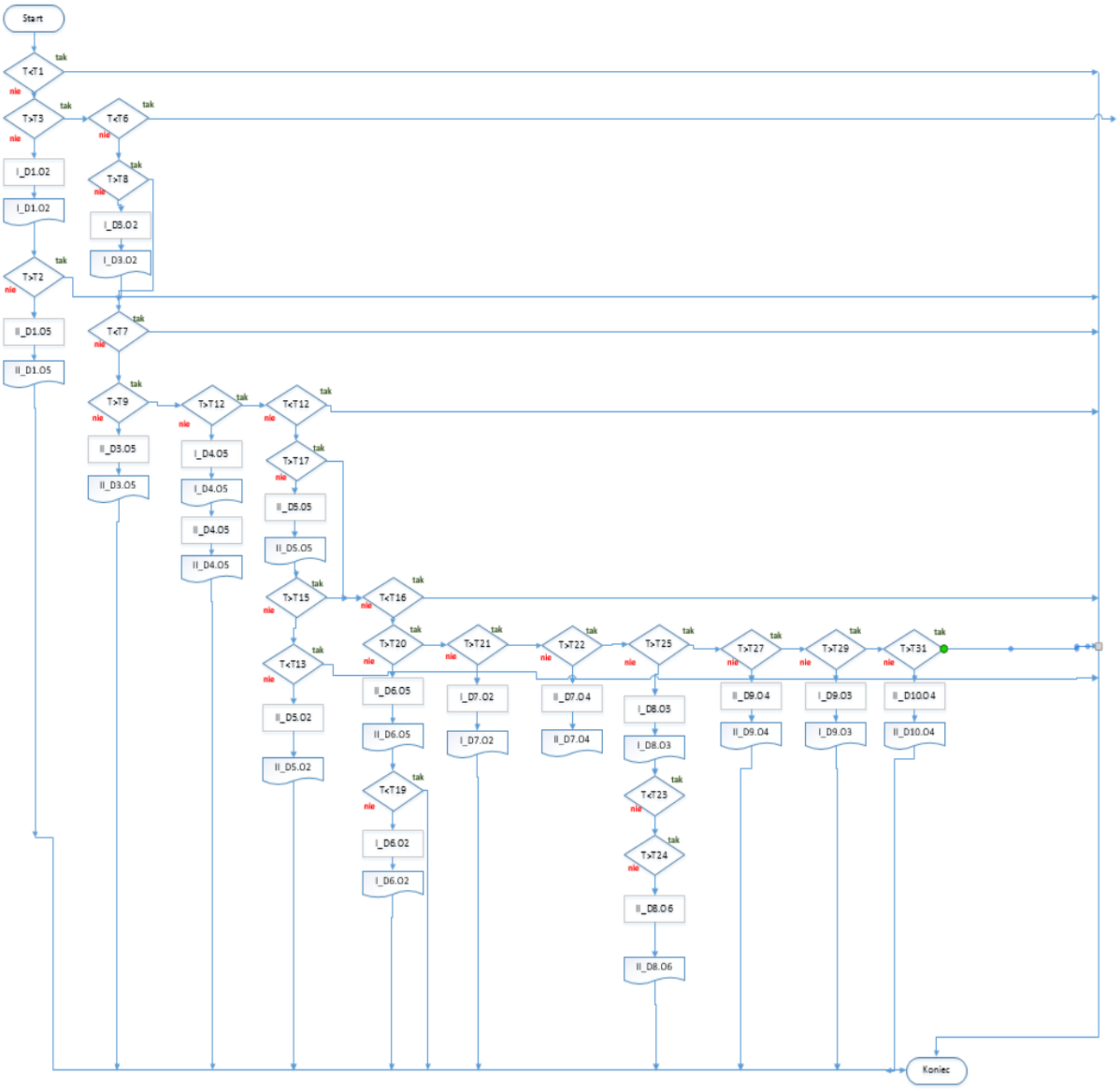


Рис. 4. Блок-схема алгоритму виконання системних операцій

VII. Симуляція процесів розробленої системи

Імітаційний аналіз для першого процесу розробленої системи здійнено в програмному середовищі BP Simulator [2]. З вязку з імплементацією проекту на польському підприємстві «Parkstop», імітаційні моделі відображені мовою оригіналу. Визначено окремі системні операції, часи тривалості їх виконання та виконавчі підрозділи (рис. 5). Симуляція дозволила оцінити затрати системи і показати середній час виконання кожного з процесів.

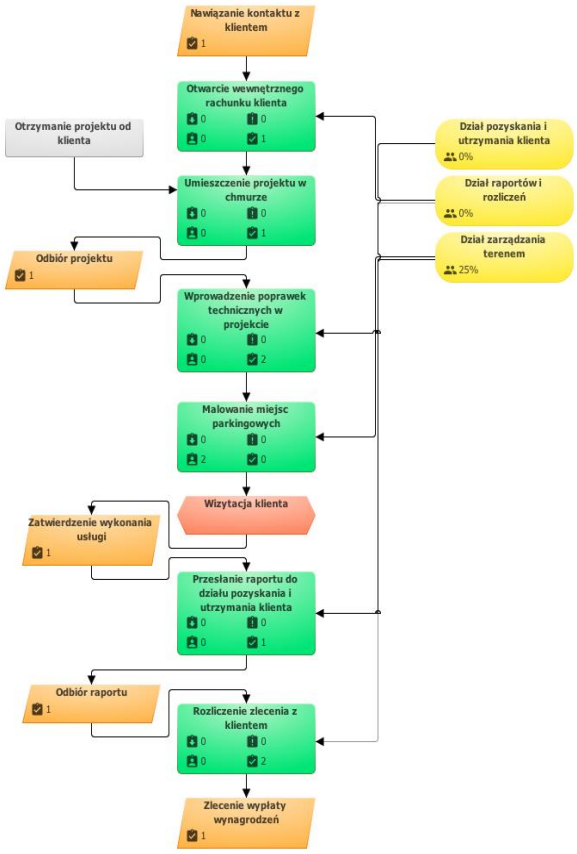


Рис. 5. Імітаційний аналіз першого процесу розробленої системи в програмному середовищі BP Simulator

Копія рапорту симуляції функціонування розробленої системи наведена на рис. 6.

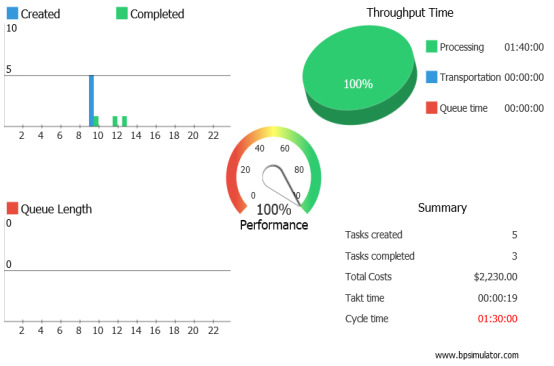


Рис. 6. Копія рапорту симуляції функціонування розробленої системи

VIII. Висновки

На базі запропонованих методів візуалізації перебігу системних операцій процесів управління складними системами в умовах міжсектрової кооперації закладено основи моделювання, які дозволили здійснити відображення стану та уможливили управління інформаційною системою в режимі реального часу. Візуалізація процесів управління дозволила зняти психологічний барєр та уникнути взаємного непорозуміння між замовником та розробником інформаційних систем, а також зредукувати кошти розроблення, впровадження та експлуатації таких систем.

Проаналізовано інфосистему управління компанією, яка надає послуги з паркування. Реалізація розробленої системи дозволила покращити інфообмін між окремими підрозділами і перейти на електронну систему реєстрації заявок і пропозицій. Завдяки впровадженню змін підвищилась конкурентоспроможність компанії, досягнуто покращення локування засобів, а функціональність системи адаптовано до ринкових стандартів.

Література

[1] Л. Петришин, Я. Николайчук, «Аналитическое моделирование информационных систем автоматизированного управления» в *Zarządzanie przedsiębiorstwem. Teoria i praktyka*: Kraków, / pod red. Wiesława Waszkielewicza; — Kraków: Wydawnictwa AGH, 2007. — ISBN 978-83-7464-153-1 — S. 268–275.

[2] BP Simulator [Online]. https://www.bpsimulator.com/run/ - режим доступу 16 липня 2018 р.

References

[1] L. Petrishin, Ya. Nikolaychuk, "Analytical modeling of information systems of automated control" in Zarządzanie przedsiębiorstwem. Teoria i praktyka: Kraków, / pod red. Wiesława Waszkielewicza; — Kraków: Wydawnictwa AGH, 2007. — ISBN 978-83-7464-153-1 — S. 268–275.

[2] BP Simulator [Online]. https://www.bpsimulator.com/run/ - режим доступу 16 липня 2018 р.

Оцінка складності побудови захисних графічних елементів на основі фрактальної геометрії

Іванна Дронюк
Кафедра автоматизованих систем управління
Львівський національний політехнічний університет
Львів, Україна
ivanna.m.droniuk@lpnu.ua

Артем Казарян
Кафедра систем автоматизованого проектування
Львівський національний політехнічний університет
Львів, Україна kag.software@gmail.com

The estimation of complexity protective graphic elements construction using fractal geometry

Ivanna Dronyuk
Automated Control Systems Department
Lviv Polytechnic National University
Lviv, Ukraine
ivanna.m.droniuk@lpnu.ua

Artem Kazaryan
Department of. Computer-Aided Design
Lviv Polytechnic National University
Lviv, Ukraine
kag.software@gmail.com

***Анотація*—У роботі розглянуто метод побудови унікальних захищених зображень на основі фрактальної геометрії. Для цього методу розроблено методику автоматизованої оцінки складності побудови захищених зображень. На цій основі реалізовано відповідне програмне забезпечення. Проведено тестування розробленої методики, що проілюстровано на рисунках. Зроблено порівняння складності побудови захищених зображень на основі фрактальної геометрії з іншими відомими методами на основі даної методики.**

***Abstract*—The paper considers the method of constructing unique protected images based on fractal geometry. For this method, the method of automated evaluation of the complexity of constructing secure images has been developed. On this basis, the software is implemented. The testing of the developed technique, illustrated in the drawings, was conducted. A comparison of the complexity of constructing protected images on the basis of fractal geometry with other known methods is made on the basis of this technique.**

Ключові слова—захисні графічні елементи, фрактальна геометрія, поліграфічний захист, оцінка складності геоиетричної побудови

Keywords—protective graphic elements, fractal geometry, polygraphical protection, estimation of complexity geometrical construction

I. Вступ

Для захисту поліграфічної продукції від підробки ефективним способом захисту є графічний. Проблеми захисту друкованих документів розглянуті у роботах [3-5], де запропоновано нові ефективні методи графічного захисту. Методи побудови захисних графічних елементів на основі Ateb- функцій розглянуті у роботі [6]. У розвиток цих методів нами запропоновано методи побудови захищених зображень на основі фрактальної геометрії [2]. Використовуючи властивість самоподібності фракталів та суцільне заповнення площини зображення, нами розроблений метод побудови унікальних захищених зображень, побудованих фракталами. Приклад роботи методу представлено на рис.1. Поряд з проблемою захисту друкованої продукції від підробки виникає проблема оцінки складності побудови захищеного зображення. Оскільки підробити можна все, тому для ефективності захисту важливим є співвідношення критеріїв «час»-«матеріальні затрати». Ця проблема також тісно пов'язана з оцінкою якості поліграфічної продукції [1]. Зрозуміло, що чим складніший метод побудови захисного зображення, тим більше часу та матеріальних ресурсів потребує його відтворення, а отже складнішим є це зображення для підроблення зловмисниками. Тому актуальним завданням є оцінка складності побудови захищених зображень. Метою даної роботи є розробка методу автоматизованої оцінки складності побудови захисних зображень на основі фрактальної геометрії та створення програмного забезпечення, що реалізує даний метод.

II. Метод оцінки складності побудови захисних графічних елементів

Відомо [4, 6], що побудова стандартних захисних сіток реалізується на основі звичайних афінних перетворень простору, до яких належать паралельне перенесення та поворот відносно осі. Будемо вважати, що коефіцієнт складності побудови для афінних

перетворень дорівнює одиниці. Оцінимо, побудовані розробленою інформаційною технологією на основі фрактальної геометрії, захисні сітки для захисту електронних та друкованих документів за критерієм складності побудови.

Уведемо позначення: коефіцієнт складності побудови паралельного перенесення позначимо k_{par} , а коефіцієнт складності побудови поворотом площини відносно осі k_{mov}. Тоді прийняті припущення, можна виразити наступними формулами $k_{par} = k_{mov} = 1$. Наприклад, представлена у роботі [1] на сторінці 38. Захисна сітка утворена паралельним перенесенням графіків гіперболічного Ateb-синуса у заданих припущеннях має коефіцієнт складності побудови, що дорівнює 1.

Побудова захисних елементів на основі фрактальних перетворень площини, метод, що описаний у [1, 2], містить такі перетворення площини як розтяг і стиск у певних областях площини. Нехай задана підобласть площини G_i розтягується або стискується у k разів. Тоді будемо вважати, що коефіцієнт складності побудови захисного елемента у цій підобласті дорівнює $k_i=k$. Нехай задана площина, що підлягає захисту, має N різних підобластей з різними коефіцієнтами розтягу чи стиску. Тоді сумарний коефіцієнт складності побудови k_{sum} визначимо як суму коефіцієнтів складності побудови кожної області

$$k_{sum} = \sum_{i=1}^{N} k_i. \qquad (1)$$

Якщо розглядати технологію побудови захисної сітки на основі фракталу, що будується на фракталі [1], то ця технологія крім розтягу і стиску містись ще повороти певних підобластей, що додатково ускладнює побудову захисної сітки такої підобласті. Будемо вважати, що складність побудови такої підобласті збільшується на емпірично заданий коефіцієнт α, де коефіцієнт α задовольняє умову $1 \le \alpha \le 1{,}5$. Тоді сумарний коефіцієнт складності побудови k_{sum} визначимо за наступною формулою

$$k_{sum} = \sum_{i=1}^{N} \alpha_i k_i. \qquad (2)$$

Розглянемо захищене зображення, утворене на основі фракталу за методом описаним у монографії [1] та представлене на рис.1. Для цього рисунку обчислимо коефіцієнт складності побудови запропонованим методом.

Для автоматизації оцінки складності побудови захисних фрактальних зображень нами було розроблене відповідне програмне забезпечення.

Результат роботи програми для виділення областей складності побудови показаний на рис.2. Як бачимо рис.1 має чотири області різної склановості побудови, які обчислені на основі оцінки контрастності вихідного зображення.

За контрасністю даний рисунок розбивається на 4 види областей:

1) область, що відповідає низькому рівню контрасту і відповідно початковому фракталу, приймаємо для цієї області коефіцієнт складності побудови $k_1 = 1$;

2) область, що відповідає середньому рівню контрасту і відповідно початковий фрактал стискається у 2 рази, приймаємо для цієї області коефіцієнт складності побудови $k_2 = 2$;

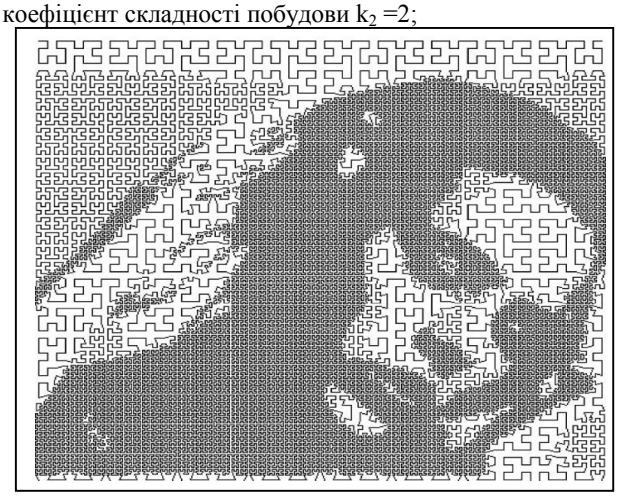


Рис. 1. Зображення, побудоване захисною сіткою на основі фракталів

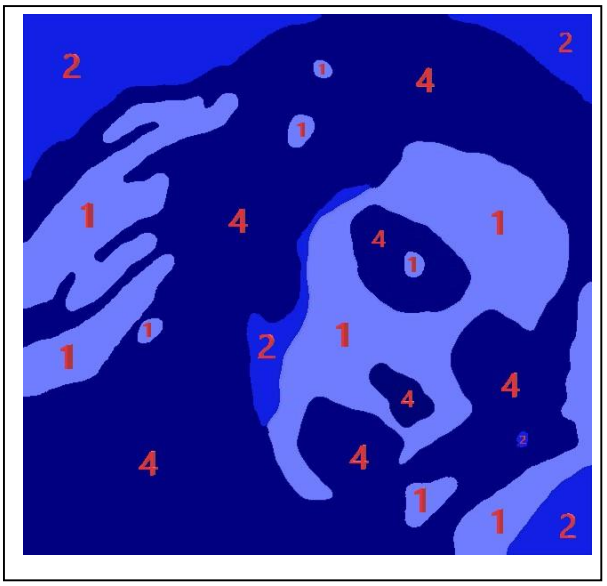


Рис. 2. *Розбиття зображення на різні області за критерієм складності побудови*

3) область, що відповідає високому рівню контрасту і відповідно початковий фрактал стискається у 4 рази, приймаємо для цієї області коефіцієнт складності побудови $k_3 = 4$;

4) область переходів між контрастами, відповідає областям, де фрактал деформується. Будемо вважати, що для цього виду області $k_1 = 1$ та $\alpha = 1{,}5$.

Для обчислення коефіцієнта складності побудови для областей 1-3 застосовуємо формулу (1) а для області 4 – формулу (2). Як видно з рис.2, вихідне зображення (див. рис.1) містить 3 області 1 виду, 9 областей 2 виду, 6 областей 3 виду і 10 областей 4 виду.

Тоді просумувавши результати формул (1) та (2) отримаєм коефіцієнта складності побудови захисної сітки на основі фрактальної геометрії ksum для зображення на рис.1 у вигляді

$$k_{sum}= 3*1+9*2+6*4+10*1,5=3+18+24+15=60$$

Очевидно, що збільшення градацій контрасності рисунку приведе до збільшення коефіцієнта складності побудови. Також збільшення кількості областей однакового рівня контрастності також збільшує коефіцієнт складності побудови захисної сітки на основі фракталів. Використовуючи властивість самоподібності фракталу коефіцієнт стиску фрактального зображення, а отже і коефіцієнт складності побудови захисної можна збільшувати до наперед заданої величини. Верхнє обмеження буде визначатися роздільчою здатністю друкарського обладнання. Для тестування розробленого методу оцінки складності побудови захисного зображення використаємо просте тестове зображення представлене на рис.3, яке містить усього дві чітко визначені області контрастності: область зліва – повністю біла, далі перехідна область та область справа – повністю чорна.

На рис.4 представлено перетворене зображення на основі тестового із рис.3 побудовою захисної фрактальної сітки. На рис.5 представлено перетворене зображення на основі тестового із рис.3 за допомогою плагіну Engraver фірми Panopticum.

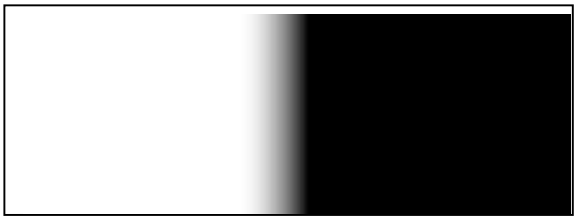


Рис. 3. Тестове зображення з двома рівнями контрасності

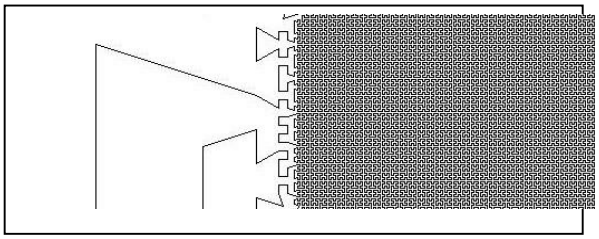


Рис. 4. Перетворене захищене зображення на основі тестового захисною сіткою на основі фракталів

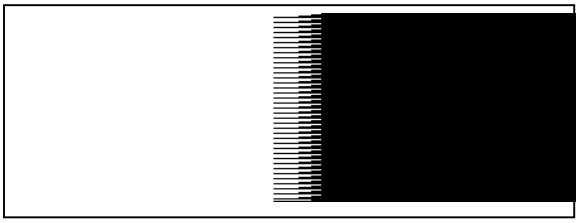


Рис. 5. Перетворене захищене зображення на основі тестового плагіном Engraver фірми Panopticum.

На рис. 6 приведено розрахунок показника складності побудови для захисних сіток, що побудовані запропонованим методом у випадку тестового зображення та 2 рівнів контрастності та 2 областей (див. рис. 3-5, а також методом розробленим у [6] та відомими програмами: фільтром Mezzotint програми обробки зображень Adobe Photoshop та плагін Engraver (фірми Panopticum). За обчисленнями побудовано відповідний графік, що показаний на рис.5 та візуально ілюструє отримані показники. Як видно з рис.5 найбільше значення показника складності побудови за розробленою методикою є для методу на основі фрактальної геометрії.

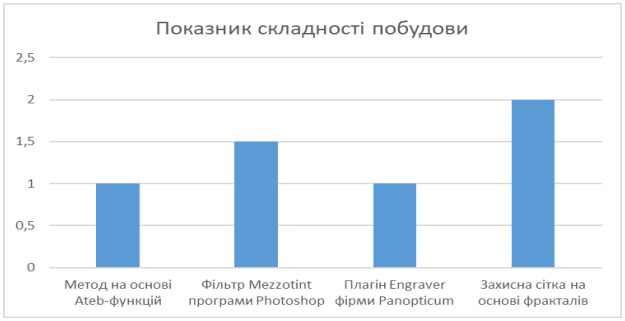


Рис. 6. Порівняння показника складності побудови для розробленого методу та відомих методів графічного захисту

Висновки

У роботі побудовано методику оцінки складності побудови захищених зображень на основі фрактальної геометрії. Для автоматизації оцінювання розроблено відповідне програмне забезпечення. Роботу методу проілюстровано відповідними рисунками. Для проведення порівняння складності побудови захищеного зображення використано тестове зображення. Тестове зображення було перетворене чотирма методами: методом на основі Ateb-функцій , методом на основі фрактальної геометрії, плагіном Engraver фірми Panopticum та фільтром Mezzotint програми Photoshop. Захищені зображення представлені на відповідних малюнках. На основі цих зображень здійснено оцінку складності побудови захищеного зображення, яка показала, що найвищий показник складності побудови має зображення утворене методом фрактальної геометрії. Таким чином на основі проведених досліджень, можна зробити висновок, що показник складності побудови захисних зображень для методу фрактальної геометрії на прикладі простого тестового зображення (рис.3) є не менш ніж на 30% більша, ніж інших відомих методів. Для складніших зображень це співвідношення буде значно вищим. Додатковими перевагами методу побудови захищених зображень на основі фрактальної геометрії є самоподібність частин зображення та заповнення усієї площини зображення.

ЛИТЕРАТУРА

[1] Дронюк І.М. Технології захисту інформації на матеріальних носіях: монографія/ І.М.Дронюк// Львів : Видавництво НУ»ЛП», 2017.-200с.

[2] Дронюк І.М., С. Квасниця, В. Калінчук Формування захисних зображень на основі фрактальної геометрії// Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології. - 2013. - 751. - С. 382-387.

[3] Дурняк Б.В. Інформаційна технологія формування графічних засобів захисту документів / Б.В. Дурняк , В.З. Пашкевич , В.І. Сабат, О.В. Тимченко. - Львів: Вид-во УАД, 2011.- 152 с.

[4] Запоточний В.Й. Технології захисту цінних паперів [Навч. посіб.] / В.Й. Запоточний. - Львів : Видавництво Національного університету <<Львівська політехніка>>, 2013. - 182 с.

[5] Назаркевич М.А., О. Троян Аналіз сучасних методів та видів графічного захисту друкованих документів//Вісник Націоального університету <<Львівська політехніка>>. Комп'ютерні науки та інформаційні технології, 2014. – 800. – С. 61 – 65.

[6] Назаркевич М.А. Методи підвищення ефективності поліграфічного захисту засобами Ateb-функцій [Текст] : монографія / Львів : Видавництво Національного університету <<Львівська політехніка>>, 2011. – 188с..

REFERENCES

[1] Dronyuk I.M. Technologies for protecting information on tangible media: monograph/ I.M.Dronyuk// 2017.-200p. (In Ukrainian)

[2] Dronyuk I.M., S. Kvasnycia, V.Kalinchuk Protected images construction based on fractal geometry// Visnyk NULP .Computer Science and Information Technology. - 2013. - 751. - P. 382-387.

[3] Durniak B.V.,Pashkevych V.Z.,Sabat V.I.., Tymchenko O.V Information technology for forming document protection grafics tools – Lviv: UPA Publishing, 2011.- 152 p. (In Ukrainian)

[4] Zapotochnyy V.Yo. Securities protection technologies // Lviv :NULP Publishing,-2013. - 182 p. Lviv :NULP Publishing,

[5] Nazarkevych M.A., Troyan O. Graphic protection of printed documents modern methods and types analysis // Visnyk NULP .Computer Science and Information Technology.-2014. – 800. – P. 61 – 65. (In Ukrainian).

[6] Nazarkevych M.A. Methods of increasing the efficiency of printing protection by means of Ateb-functions– Lviv :NULP Publishing, 2011. – 188с. (In Ukrainian).

Застосування дискретного трійкового симетричного вейвлет-перетворення для перетворення форми та цифрової обробки інформації у розподілених системах управління в умовах секторної кооперації

Артем Ізмайлов
кафедра інформатики
Прикарпатський національний університет
Івано-Франківськ, Україна
aiartefact@gmail.com

Любомир Петришин
кафедра управління
Науково-технологічний університет AGH
Краків, Польща
l.b.petryshyn@gmail.com

Application of discrete symmetric ternary wavelet transform for form transform and digital processing of information in dispersed management systems in terms of sector cooperation

Artem Izmailov
dept. of Computer Science
Precarpathian National University
Ivano-Frankivsk, Ukraine
aiartefact@gmail.com

Lubomyr Petryshyn
dept. of Enterprise Management
AGH University of Science and Technology
Cracow, Poland
l.b.petryshyn@gmail.com

***Анотація*—У роботі досліджено ефективність застосування дискретного трійкового симетричного вейвлет-перетворення на основі трійкових симетричних функцій для перетворення форми та цифрової обробки інформації за критерієм мінімуму ентропії деталізуючих коефіцієнтів. Дискретні вейвлет-перетворення є одним з найбільш ефективних методів аналізу та синтезу цифрових сигналів. Однак, кожне вейвлет-перетворення пристосоване для аналізу виключно певного класу сигналів і для інших сигналів може забезпечувати меншу ефективність обробки та аналізу. Відповідно, синтез та впровадження нових вейвлет-перетворень є актуальним завданням цифрової обробки інформації. У даному дослідженні проаналізована ефективність застосування синтезованого у попередніх роботах дискретного вейвлет-перетворення на основі трійкових симетричних функцій за критерієм мінімуму ентропії деталізуючих коефіцієнтів у порівнянні з існуючими дискретними вейвлет-перетвореннями. Доведено, що синтезоване вейвлет-перетворення за даним критерієм володіє вищою ефективністю застосування у випадку третини тестових сигналів. У випадку більше, ніж половини тестових сигналів, синтезоване вейвлет-перетворення забезпечує найвищу ефективність у задачах спектрального аналізу.**

***Abstract*—The paper deals with discrete wavelet transform based on symmetric ternary functions and its application efficiency in form transform and digital processing of information due to the criterion of entropy minimum of detail coefficients. Discrete wavelet transforms are one of the most effective ways to perform analysis and synthesis of digital signals. However, each wavelet transform is effective for analysis of certain class of signals and can be completely useless for analysis of another one. Therefore, synthesis and application of new wavelet transforms is an actual task of digital signal processing. In this research application effectiveness of formerly synthesized discrete wavelet transform based on symmetric ternary functions was tested due to the criterion of entropy minimum of detail coefficients in comparison to existing discrete wavelet transforms. It was shown that synthesized wavelet transform has higher application efficiency due to the described criterion in case of a third of the tested signals. For more than half of the tested signals synthesized wavelet transform has the best performance in tasks of spectral analysis.**

Ключові слова — перетворення форми, цифрова обробка інформації; дискретне вейвлет-перетворення;

трійкові симетричні функції, секторна кооперація, розподілені системи, управління

Keywords — form transform and digital processing of information; discrete wavelet-transform; symmetric ternary functions, sectoral cooperation, dispersed systems, management

I. Вступ

Перетворення форми та цифрова обробка інформації є ключовим елементом численних технічних систем, які використовуються у різних галузях управління, виробництва, зв'язку та медицини [1 – 6]. Відповідно, ефективні рішення у галузі перетворення форми та цифрової обробки інформації призведуть до підвищення ефективності перебігу процесів, які включають перетворення форми та цифрову обробку інформації, у прикладних галузях.

Одним із актуальних завдань перетворення форми та цифрової обробки інформації є обробка цифрових сигналів на основі вейвлет-перетворень [1 – 3, 7 – 9]. Відомо, що кожне вейвлет-перетворення пристосоване для обробки лише певного класу сигналів, тобто має обмежений спектр застосування [2, 7 – 9]. Звідси випливає, що актуальним завданням цифрової обробки інформації є синтез нових вейвлет-функцій та відповідних їм вейвлет-перетворень, які дозволять з вищою ефективністю проводити обробку конкретних цифрових сигналів, у тому числі тих, для яких існуючі методи працюють із недостатнім рівнем ефективності.

Аналіз останніх досліджень у галузі вейвлет-перетворень вказує на те, що дослідження щодо реалізації дискретних вейвлет-перетворень на основі трійкових симетричних функцій не проводились [1 – 3, 4]. Водночас, успішний синтез дискретного ортогонального перетворення на основі трійкових симетричних функцій [6] та дискретного вейвлет-перетворення на основі трійкових симетричних функцій [4] вказують на перспективність розвідок у даному напрямі. Крім цього, у роботі [4] доведено перспективність подальших досліджень ефективності застосування розробленого методу цифрової обробки інформації.

Метою дослідження є оцінювання ефективності застосування дискретного вейвлет-перетворення на основі трійкових симетричних функцій за критерієм мінімуму ентропії деталізуючих коефіцієнтів вейвлет-перетворення.

Наукова новизна отриманих результатів полягає в успішному проведенні оцінки ефективності застосування дискретного вейвлет-перетворення на основі трійкових симетричних функцій у порівнянні з найбільш уживаними вейвлет-перетвореннями за критерієм мінімуму ентропії деталізуючих коефіцієнтів вейвлет-перетворення.

II. Дискретне вейвлет-перетворення на основі трійкових симетричних функцій

Вейвлет-перетворення синтезується на основі системи функцій, які є стиснутими та зсунутими по осі абсцис (здебільшого представляє вісь часу) копіями деякої функції, яку називають материнським вейвлетом [2, 7, 8]. Якщо материнський вейвлет позначити, як ψ, то описана система функцій набуде вигляду (1) [8].

$$\psi_{m,n}(x) = a_0^{-m/2}\psi(a_0^{-m}x - nb_0), \tag{1}$$

де $a_0 \neq 1$ – параметр стиску, b_0 – параметр зсуву, $m, n \in Z$.

У випадку вейвлет-перетворення на основі трійкових симетричних функцій, параметр a_0 рівний *3*, а b_0 – *1*. Відповідно, вираз (1) для даного перетворення набуде вигляду

$$\psi_{m,n}(x) = 3^{-m/2}\psi(3^{-m}x - n). \tag{2}$$

У зв'язку з тим, що параметр стиску у виразі (2) рівний *3*, у дискретному вейвлет-перетворенні на основі трійкових симетричних функцій використовуються два материнські вейвлети. Перший материнський вейвлет $\psi 1$ визначається аналітичним виразом

$$\psi 1(t) = \begin{cases} -\sqrt{\frac{3}{2}}, t \in [0, \frac{1}{3}), \\ \sqrt{\frac{3}{2}}, t \in [\frac{2}{3}, 1), \\ 0, t \notin [0, \frac{1}{3}) \cup [\frac{2}{3}, 1). \end{cases} \tag{3}$$

Другий материнський вейвлет $\psi 2$ визначається аналітичним виразом

$$\psi 2(t) = \begin{cases} \frac{1}{\sqrt{2}}, t \in [0, \frac{1}{3}) \cup [\frac{2}{3}, 1), \\ -\sqrt{2}, t \in [\frac{1}{3}, \frac{2}{3}), \\ 0, t \notin [0, 1). \end{cases} \tag{4}$$

У якості масштабної функції для вейвлетів $\psi 1$ та $\psi 2$ обрано характеристичну функцію на проміжку [0, 1) (8), задану аналітичним виразом

$$\varphi(t) = \begin{cases} 1, t \in [0, 1), \\ 0, t \notin [0, 1). \end{cases} \tag{5}$$

Функції (3) – (5) породжують відповідні їм сімейства функцій за допомогою аналітичної залежності (2). Детальну інформацію відносно аналізу властивостей функцій (3) – (5) та синтезу на їх основі відповідного вейвлет-перетворення можна знайти у [4].

III. Ефективність застосування дискретного трійкового симетричного вейвлет-перетворення

Одним із завдань вейвлет-аналізу у системах цифрової обробки інформації є зменшення

надлишковості та стиснення даних [2, 7, 9]. Для оцінювання ефективності застосування вейвлет-перетворень у описаних задачах та їх здатності концентрувати енергію у апроксимуючих коефіцієнтах використовується критерій мінімуму ентропії деталізуючих коефіцієнтів вейвлет-перетворення [7, 9]

$$H = -\sum_{i=1}^{N}\left(\frac{d_i^2}{\sum_{j=1}^{N} d_j^2}\log_2\left(\frac{d_i^2}{\sum_{j=1}^{N} d_j^2}\right)\right), \qquad (6)$$

де N – загальна кількість деталізуючих коефіцієнтів по всіх рівнях вейвлет-перетворення, d_i – i-ий член послідовності деталізуючих коефіцієнтів всіх рівнів вейвлет-перетворення.

Дослідження ефективності застосування дискретного вейвлет-перетворення на основі трійкових симетричних функцій за критерієм (6) проводилося на множині з 34 тестових сигналів у порівнянні з дискретними вейвлет-перетвореннями на основі вейвлетів Хаара, Добеші 2-го, 3-го, 4-го порядків та біортогональних вейвлетів з параметрами 1.3, 2.2 та 3.7.

Проведений у роботі [4] аналіз ефективності дискретного вейвлет-перетворення на основі трійкових симетричних функцій за критерієм мінімуму середньоквадратичної похибки відновлення даних за частиною коефіцієнтів вказав на необхідність аналізу результатів досліджень ефективності з точки зору переваги синтезованого вейвлет-перетворення відносно кількості рівнів перетворення, оскільки у випадку багатьох тестових сигналів перевага даного перетворення зберігається лише до певного значення кількості рівнів перетворення.

Отримані за критерієм (6) результати порівняння ефективності вейвлет-перетворень вказують на наявність переваги вейвлет-перетворення на основі трійкових симетричних функцій над іншими вейвлет-перетвореннями, яка зберігається лише до певного значення кількості рівнів перетворення. Це зумовлює необхідність застосування описаного підходу до проведення аналізу переваги синтезованого вейвлет-перетворення за критерієм (6) відносно кількості рівнів перетворення. На рис. 1 наведені значення кількості рівнів перетворення, для яких вейвлет-перетворення на основі трійкових симетричних функцій зберігає перевагу за критерієм (6) над іншими проаналізованими вейвлет-перетвореннями у випадку кожного з тестових сигналів.

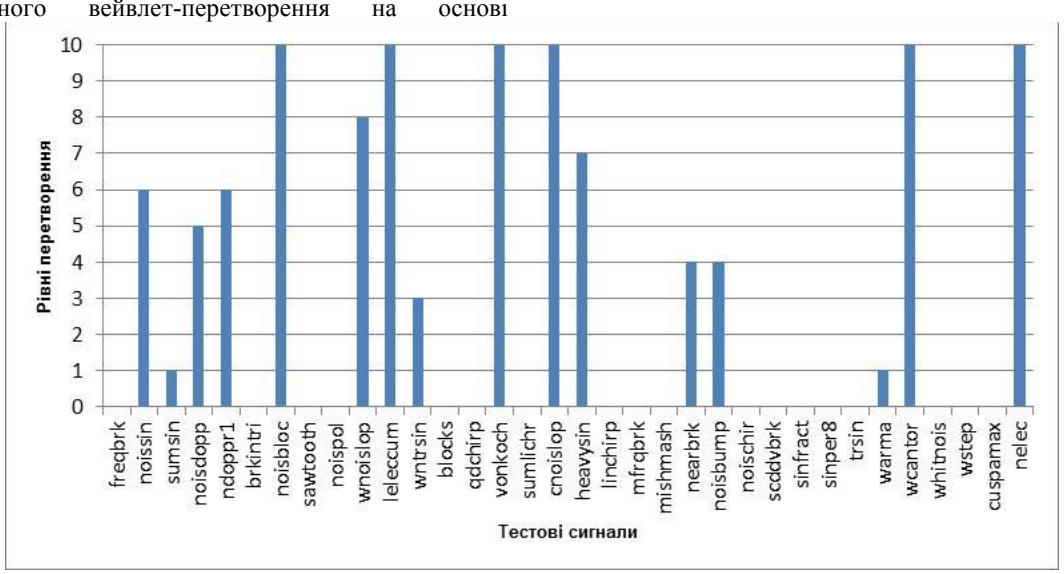


Рис. 1. Гістограма значень кількості рівнів вейвлет-перетворення, при яких дискретне трійкове симетричне вейвлет-перетворення має перевагу над іншими за критерієм мінімуму ентропії деталізуючих коефіцієнтів вейвлет-перетворення

Встановлено, що для повної декомпозиції сигналу (кількість апроксимуючих коефіцієнтів досягає мінімального для заданого вейвлет-перетворення значення і з кожним наступним рівнем перетворення не зменшується [2, 7, 8]) представленого множиною близько 1000±25 семплів біортогональними вейвлет-перетвореннями та вейвлет-перетвореннями Хаара та Добеші необхідно 10 рівнів перетворення, а у випадку вейвлет-перетворення на основі трійкових симетричних функцій – лише 7. Враховуючи, що кількість семплів переважної більшості використаних тестових сигналів лежить саме у даних межах, можна стверджувати, що показник у 6 рівнів перетворення вказує на фактично повну перевагу вейвлет-перетворення на основі трійкових симетричних функцій у даному випадку, зокрема, якщо додатково врахувати, що при переході з 6 до 7 рівнів перетворення, кількість утворених даним вейвлет-перетворенням апроксимуючих коефіцієнтів зменшується з 2 до 1.

З даних на рис. 1 випливає, що у випадку тестових сигналів noisbloc (прямокутні імпульси з шумом), leleccum (дані типу «потужність, яка споживається»), vonkoch (фрактальна крива Коха), cnoislop (забарвлений шум), wcantor (крива Кантора) та nelec (Дані типу «потужність, яка споживається» із шумом) синтезоване вейвлет-перетворення володіє вищою ефективністю за критерієм (6) у порівнянні з рештою

проаналізованих вейвлет-перетворень при всіх значеннях кількості рівнів перетворення. Це свідчить про вищу здатність даного вейвлет-перетворення концентрувати енергію у апроксимуючих коефіцієнтах і, відповідно, більш ефективне зменшення надлишковості та стиснення даних описаних типів.

Враховуючи наведені вище викладки про те, що перевагу синтезованого вейвлет-перетворення за критерієм (6) до 6 рівнів перетворення включно, допустимо наближено розглядати як повну, можна стверджувати, що, у загальному випадку, дискретне вейвлет-перетворення на основі трійкових симетричних функцій забезпечує менше до 63% значення ентропії деталізуючих коефіцієнтів для 29% протестованих сигналів.

Водночас, отримані дані (рис. 1) вказують на те, що для 53% тестових сигналів дискретне вейвлет-перетворення на основі трійкових симетричних функцій забезпечує максимальне значення ентропії деталізуючих коефіцієнтів. Це вказує на низьку здатність до концентрації енергії відповідних типів даних у апроксимуючих коефіцієнтах, але, водночас, на максимальний ступінь інформативності деталізуючих коефіцієнтів, у порівнянні з іншими вейвлет-перетвореннями, що зумовлює перевагу синтезованого перетворення у задачах спектрального аналізу.

Висновки

Дискретне вейвлет-перетворення на основі трійкових симетричних функцій завдяки своїй відмінній від інших вейвлет-перетворень структурі володіє рядом переваг. Зокрема, для певних типів даних (наприклад, крива Кантора) дане перетворення володіє вищою, у порівнянні з іншими вейвлет-перетвореннями, здатністю до зменшення надлишковості та стиснення даних, що підтверджується отриманими як за критерієм (6), так і у роботі [4] результатами.

Водночас, одержані результати вказують на високу інформативність деталізуючих коефіцієнтів, утворених синтезованим вейвлет-перетворенням. Це, з одного боку, обмежує застосування дискретного вейвлет-перетворення на основі трійкових симетричних функцій для задач стиснення із втратами даних відповідних типів. Однак, з іншого боку, наявність більш інформативних деталізуючих коефіцієнтів вказує на вищу ефективність застосування у задачах виявлення характеристик та особливостей сигналів, а також на перспективність використання даного вейвлет-перетворення у задачах очищення сигналів від шуму, зокрема, за допомогою техніки «м'якого» порогу.

Подальші дослідження полягають у аналізі ефективності застосування дискретного вейвлет-перетворення на основі трійкових симетричних функцій за допомогою відмінних від (6) критеріїв. Необхідним є, також, синтез згорткової форми даного вейвлет-перетворення з метою спрощення його імплементації у засобах цифрової обробки інформації. Проведення окреслених досліджень дозволять чітко визначити спектр застосування описаного вейвлет-перетворення.

Література

[1] E. Ifeachor, B. Jervis, Digital Signal Processing: A Practical Approach (2nd Edition), Pearson Education, 2002, P. 960.

[2] P.S. Addison, The Illustrated Wavelet Transform Handbook: Introductory Theory and Applications in Science, Engineering, Medicine and Finance (Second Edition) / P.S. Addison, CRC Press, 2016, P. 446.

[3] S. Prasad, Information Fusion in the Redundant-Wavelet-Transform Domain for Noise-Robust Hyperspectral Classification / S. Prasad, W. Li, J.E. Fowler, L.M. Bruce // IEEE Transactions on Geoscience and Remote Sensing. – September 2012. – Vol. 50, No. 9. – P. 3474-3486. doi: 10.1109/TGRS.2012.2185053

[4] A. Izmailov, L.Petryshyn, Discrete Symmetric Ternary Wavelet Transform and Its Application for Digital Information Processing in Dispersed Management Systems (in Ukrainian), Information Technologies and Computer Modelling: Proceedings of International Scientific Conference, Ivano-Frankivsk, V.P. Suprun, 2018, P. 152-155.

[5] A. Izmailov, L. Petryshyn, "Symmetric ternary functions and their application in orthogonal transforms," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, 2017, P. 836-841. doi: 10.1109/UKRCON.2017.8100364

[6] A. Izmailov, Application Effectiveness of Orthogonal Transform Based on Symmetric Ternary Functions for Digital Information Processing (in Ukrainian), Methods and Devices of Quality Control. - 2018. - № 1 (40). - P. 97-104.

[7] R.R. Coifman and M.V. Wickerhauser, Entropy-based algorithms for best basis selection, IEEE Transactions on Information Theory (Special Issue on Wavelet Transforms and Multiresolution Signal Analysis). – 1992. – Vol. 38, №3. – P. 1241-1243.

[8] I. Daubechies, Ten Lectures on Wavelets, CBMS-NSF Regional Conference Series in Applied Mathematics, Rutgers University and AT&T Bell Laboratories, 1992, P. 357.

[9] D. Salomon, Data Compression – The Complete Reference, Springer London, 2007, P. 1092.

Оцінка показників ефективності декодеру Turbo-Product-кодів на базі ПЛІС

Ярослав Крайник
Кафедра комп'ютерної інженерії
Чорноморський національний університет імені Петра Могили
Миколаїв, Україна
codebreaker7@ukr.net, yaroslav.krainyk@chmnu.edu.ua

Владислав Перов
Кафедра комп'ютерною інженерії
Чорноморський національний університет імені Петра Могили
Миколаїв, Україна
perov.vlad92@gmail.com

Evaluation of performance of Turbo-Product-Codes decoder based on FPGA

Yaroslav Krainyk
Department of Computer Engineering
Petro Mohyla Black Sea National University
Mykolaiv, Ukraine
codebreaker7@ukr.net, yaroslav.krainyk@chmnu.edu.ua

Vladyslav Perov
Department of Computer Engineering
Petro Mohyla Black Sea National University
Mykolaiv, Ukraine
perov.vlad92@gmail.com

***Анотація*—У даній роботі представлені результати дослідження щодо оцінки ефективності роботи декодеру Turbo-Product-кодів, який використовує комбінований метод декодування. Даний метод об'єднує сильні сторони жорсткого декодеру (швидкість ітерації декодування) з м'яким декодуванням (підвищена корегуюча здатність). Основною задачею даного декодеру є демонструвати результати по виправній здатності, які є кращими за результати жорсткого декодеру. У даній роботі представлена методика, яка використовувалась для отримання результатів з використанням програмних і апаратних засобів, а також засобів моделювання. Для проведення дослідження розроблений лабораторний стенд, який складався з двох модулів, який підключається до комп'ютеру і може отримувати дані для декодування. Даний стенд дозволяє не лише швидше отримувати результати декодування, а і проводити перевірку пропускної здатності декодеру, оскільки взаємодія між компонентами відбувається з використанням високошвидкісного інтерфейсу. Отримані результати демонструють перевагу методу декодування над жорстким декодером. Також визначені особливості роботи декодеру, які визначають обмеження щодо його максимальної виправної здатності відносно роботи з різними типами помилок та причини такої роботи декодеру відповідно до операцій, які використовуються у методі декодування.**

***Abstract*—Results of the investigation on effectiveness of Turbo-Product-codes decoder, which utilizes combined decoding method, performance is presented in this work. The method combines advantages of hard-decoder (speed of single decoding iteration) with improvements of soft-decoder (better error-correcting ability). The main purpose of this decoder is to demonstrate better performance than hard-decision decoder. We represent technique that has been used in the work to evaluate decoder properties. Both software and hardware resources are applied for this technique. Laboratory stand has been designed for experiments. The stand is comprised of two modules. The designed stand can be connected to computer, thus, computer can transfer data for decoding and receive the results. The stand also allows checking throughput of the decoder because of usage of high-speed interface. The achieved results claim about advantage of the developed decoder in comparison with hard-decision decoder. Additionally, peculiarities connected with maximum correcting ability of the decoder work have been identified.**

Ключові слова—декодер, Turbo-Product-коди

Keywords—decoder, Turbo-Product-codes

I. Вступ

Декодери кодів прямого виправлення помилок на даний момент є центральними елементами телекомунікаційних систем. Вони є одними з найскладніших компонентів на стороні отримуючого обладнання. Від того, яку швидкість декодування здатен забезпечувати декодер, залежить загальна швидкість передачі даних у системі. Для того, щоб мати можливість представити можливі режими роботи системи та її основні характеристики, на основі математичних операцій, які використовуються у ході декодування можливими варіантами є проведення моделювання спеціалізованими програмними засобами, або організація лабораторних тестувань з залученням апаратного забезпечення. У даній роботі використовуються обидва варіанти для того, щоб підтвердити коректність розгортання моделі на ресурси програмовних логічних інтегральних схем (ПЛІС). Представлена методика, відповідно до якої проводились дослідження, а також результати проведених досліджень.

До кодів з прямим механізмом виправленням помилок відносяться і коди, які отримали назву турбо-коди-добутки (англ. Turbo-Product-Codes – ТР-коди). Вони представляють собою коди, що містять горизонтальну та вертикальну компоненти коду (рядки та стовпці). Декодування відбувається за ітераціями і результат попередньої ітерації подається

на вхід новій ітерації, тому у назві наявна частина «Turbo».

У даній роботі представлені результати оцінки системи, яка описана у попередніх працях [1, 2]. Дана система представляє собою декодер, який комбінує м'який та жорсткий підхід для декодування TP-кодів. Він дозволяє об'єднати швидкість роботи жорсткого декодеру з більшою корегуючою здатністю декодеру, який працює з м'якими значеннями. Перш за все, такий декодер повинен забезпечувати кращу виправну здатність, ніж декодер жорстких рішень. У якості складових компонентів TP-кодів часто використовуються коди SECDED-коди (Single Error Correction Double Error Detection), які дозволяють виправити одиночну помилку та вказати на наявність подвійної помилки, проте не виправити її. Саме ці коди розглядаються у даній роботі. У ній представлені показники роботи системи за умови використання різних кодів. Проводиться перевірка роботи в різних умовах зашумленості каналу передачі даних. З практичної точки зору, це дозволить визначити, які коди доцільно використовувати за різних умов роботи системи.

II. Проведення дослідження

Методика проведення оцінки показників декодеру передбачає наявність наступних етапів:

- Генерація набору тестових даних на основі показників кодів для тестування. Відповідно, на даному етапі мають бути згенеровані дані для усіх кодів, декодування яких здатен проводити декодер.
- Визначення показників зашумленості каналу передачі даних. Для представлення цього показника можуть використовуватись різні фізичні показники, які у кінцевому результаті можуть бути приведені від одного до іншого (показник сигнал/шум для біту, для символу, імовірність помилки).
- Накладання шуму відповідно до обраного показника, який характеризує якість передачі даних у каналі. Крок, який здійснюється між попереднім та наступним показником для цього значення залежить від того, наскільки детальну характеристику необхідно отримати для досліджуваного декодеру.
- Передача зашумлених даних на вхід декодеру. У якості моделі реального декодеру, зазвичай, використовується програмне забезпечення, яке проводить однакові операцій з декодером, для якого проводиться тестування.
- Отримання декодованого повідомлення. На цьому етапі в якості виходу можуть використовуватись як м'які дані, так і жорсткі дані.
- Аналіз результуючих даних, отриманих на виході декодеру шляхом порівняння з початковим повідомленням. На цьому етапі, в основному, використовуються жорсткі дані, а м'які дані використовуються для того, щоб простежити загальний хід процесу декодування.

На першому етапі для генерації тестових даних може використовуватись довільний двовимірний масиву двійкових значень відповідної розмірності, які відповідають характеристикам коду. Після цього слова з даного масиву мають бути закодовані з використанням генеруючих матриць кодів. Відповідно, розмір масиву збільшується відповідно до показників довжин коду. Для представлення передачі по каналу з шумами проводиться відображення жорстких вхідних даних на м'які. Відображення відбувається на значення, що відповідають максимальному абсолютному значенню, яке використовується у системі, з присвоєнням відповідного знаку. Таким чином, для перевірки можуть використовуватись два початкові масиви: жорстких значень і м'яких значень.

На другому етапі визначається, наскільки якісним є канал передачі і які завади присутні у каналі. Для тестування можуть використовуватись різні типи помилок, які вносяться у початковий масив даних: просте інвертування, внесення зовнішнього впливу відповідно до значення амплітуди конкретного біту та інші техніки. Таким чином, на третьому етапі у повідомленні з'являються помилки/відмінності у порівнянні з початковим кодовим словом, які декодер має виправити.

Після цього мають бути реалізовані наступні етапи, які є ключовими для проведення оцінки. Програмне забезпечення, яке повністю повторює роботу декодеру з точки зору математичних операцій, що використовуються, зазвичай, є підготовленим заздалегідь, оскільки саме на його основі проводиться попереднє тестування якості алгоритму декодування. Дане програмне забезпечення може бути як звичайною консольною утилітою, так і повноцінною програмою з графічним інтерфейсом користувача. Проте, через можливі зміни, пов'язані з цільовою платформою декодеру, отримана апаратна реалізація може не завжди відповідати початковій версії програмної реалізації, тому важливим моментом є повна та цілковита відповідність операцій, які проводяться на обох платформах. Для більшою наочності та більшої інформативності дослідження доцільно проводити легування результатів окремих ітерацій декодування або, навіть, більш дрібних стадій обробки даних. Наявність такого функціоналу дозволяє проводити порівняння з результатами, які отримані у спеціалізованих засобах моделювання системи для ПЛІС на базі спеціально розроблених тестових оточень. Порівняння кожної окремої стадії обчислення є обов'язковою умовою для проведення подальших досліджень.

На виході програми отримується декодоване повідомлення у м'якому або жорсткому вигляді. Результуюча кількість помилок для випадку м'яких значень визначається на основі співпадіння знаку м'якого значення у вхідному та вихідному повідомленнях. Відмінності у абсолютних значеннях за умови співпадіння знаку не є суттєвими.

Проведення паралельного тестування з використанням як програмного, так і апаратного

забезпечення надає переваги у тому, що можна одразу проводити аналіз результатів декодування. Порівняння результатів декодування під час моделювання роботи ПЛІС є більш затратним з точки зору часу, який необхідний на моделювання. Саме тому під час виконання даного дослідження був зібраний лабораторний стенд, який складався з відлагоджувальної плати з мікросхемою ПЛІС, інтерфейсної плати для спрощення підключення між комп'ютером та платою. Структурна схема з'єднань між компонентами розробленого лабораторного стенду представлена на рис. 1.

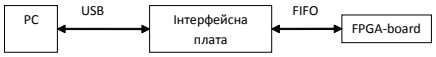


Рис.1.Структурна схема підключення компонентів стенду

Для зв'язку з комп'ютером використовується інтерфейс передачі даних USB 2.0. Максимальна швидкість передачі даних для даної специфікації становить 480 Мбіт/с. Інтерфейсна плата, яка працює в режимі FIFO (паралельний інтерфейс передачі даних) здатна, відповідно, до документації забезпечувати швидкість передачі даних близько 40 Мбайт/с. Це означає, що дані показники є достатньо близькими, оскільки у даному випадку враховується лише корисна інформація, що передається. Мікросхема ПЛІС на відлагоджувальній платі зчитує дані з використанням блоку FIFO, а оброблені дані передаються за допомогою того самого блоку. Це пов'язано з тим, що на інтерфейсній платі наявні буфери як для прийому, так і для передачі даних.

У якості складових компонентів для побудови лабораторного стенду використовувались:

- інтерфейс на плата FT2232H Mini Module;
- відлагоджувальна плата Altera DE0-SoC-Nano.

Інтерфейсний модуль має у своєму складі в якості основного компоненту мікросхему FT2232H. Дана мікросхема здатна працювати у двох режимах FIFO (синхронний та асинхронний) для забезпечення високої пропускної здатності. У цих режимах використовується паралельний інтерфейс передачі даних. Також дана мікросхема може працювати і в якості інтерфейсу для протоколів з меншою швидкістю передачі даних – UART, SPI, I2C, JTAG. Висока пропускна здатність інтерфейсу у даному випадку означає те, що можна не лише провести перевірку результатів декодування, а і оцінити пропускну здатність системи, що тестується.

У свою чергу, відлагоджувальна плата дозволяє працювати з модулем ПЛІС сімейства Cyclone V. Дана мікросхема, окрім частини програмовної логіки містить апаратні ядра мікропроцесору ARM (доступні два ядра). Завдяки цьому можна об'єднати обчислювальні потужності програмовної логіки з гнучкістю налаштувань процесора. На мікропроцесорній частині пристрою можливий, навіть, запуск операційної системи Linux. Дана плата містить достатню кількість логічних ресурсів для проведення тестування роботи декодерів деяких кодів з обраного набору. Для того, щоб мати можливість тестувати декодер при роботі з більшою довжиною кодового слова,необхідно використовувати мікросхему, яка надає більшу кількість ресурсів програмовної логіки (наприклад, Altera Stratix та ін.).

Зовнішній вигляд розробленого лабораторного стенду для декодеру ТР-кодів на базі ПЛІС представлено на рис. 2.

Рис.2. Зовнішній вигляд лабораторного стенду для проведення тестування

Підключення двох модулів організоване наступним чином. На відлагоджувальній платі наявний роз'єм, що відповідає за розташуванню пінам відомої плати Arduino Uno. У цей роз'єм вставляється перехідна макетна плата, на якій розміщений інтерфейсний модуль. Макетна плата забезпечує з'єднання між шиною даних і допоміжними сигналами на платі та модулем. Такий варіант з'єднання забезпечує надійну передачу сигналів між модулями при використанні високої тактової частоти.

Програмна складова для проведення тестування представляє собою скрипт на мові програмування Python, який окрім безпосередньо декодування вхідних даних, які попередньо були згенеровані та записані у текстовий файл. У текстовому файлі послідовно записана відповідна кількість пакетів. Даний файл використовується як для проведення тестування за допомогою скрипту, так і за допомогою спеціалізованих засобів моделювання (у даному випадку – MentorGraphics ModelSim 10.1). Як вже зазначалось засоби моделювання демонструють меншу швидкодію при моделюванні декодування великої кількості пакетів, тому вони використовуються на початковому етапі налагодження скрипту. Окрім цього, засоби моделювання дозволяють більш детально дослідити роботу кожного окремого модуля, який є складовою частиною декодеру. Як результат цього етапу за допомогою розробленого тестового оточення отримані вихідні файли декодованих пакетів, які порівнюються з результатами, які показує скрипт.

При моделюванні роботи декодеру використовувався розроблений опис декодеру мовою схемотехнічного опису VHDL. Саме цей опис на наступних етапах перенесений на мікросхему ПЛІС

для апаратного тестування роботи декодеру. Важливим є те, що основні модулі, які переносяться мають бути однаковими як для засобів моделювання, так і для апаратної реалізації на базі ПЛІС.

Проведено тестування для різних імовірностей помилки для 100 пакетів. Для тестування був обраний код-добутків (64,57)x(46, 39). Тестування проводилось з використанням розробленого скрипту на мові програмування Python. Для представлення результатів використовувалось програмне середовище gnuplot 5.1. Результуюча гістограма представлена на рис. 3.

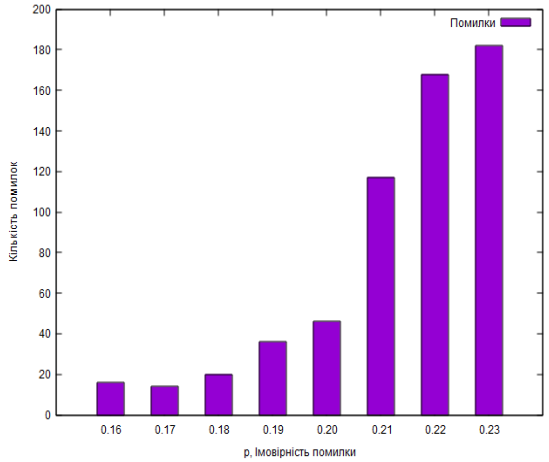


Рис.3.Гістограма залежності кількості помилок від імовірності помилки для тестових випадків для коду 64*46

Як видно з рисунку, кількість помилок при низькій імовірності є практично однаковою, тому можна зробити висновок, що результативність декодування залежить від характеру помилок, які утворюються.

Таке саме дослідження проведено для коду 32*22. Результати представлені на рис. 4.

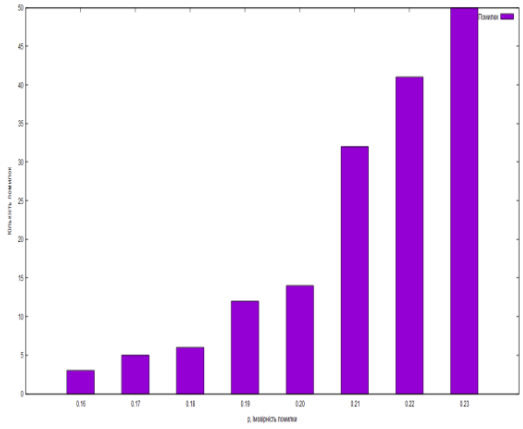


Рис.4.Гістограма залежності кількості помилок від імовірності помилки для тестових випадків для коду 32*22

У результаті проведення дослідження виявлено, що запропонований метод декодування дозволяє отримати вищу завадостійкість у порівнянні з жорстким декодером. Крім того, виявлені деякі особливості в роботі декодеру. За рахунок зменшення модулю при декодуванні протилежним декодером вдається виділити біти, які є більш імовірними помилковими бітами. Особливості роботи декодеру полягають у тому, що запропонований метод не завжди обирає коректний шлях декодування виділених бітів. Це призводить до ситуації, коли декодер показує відсутність помилок у вихідному слові, в той час як порівняння з початковим кодовим словом вказує на наявність помилок. Дану обставину необхідно враховувати, але оскільки ТР-коду застосовуються в тому числі в якості складових кодів, то такі помилки можуть бути виправлені декодерами на наступних рівнях.

III. Висновки

У даній роботі дається оцінка ефективності роботи декодеру ТР-кодів, який розроблений відповідно до положень представлених у роботах [1, 2]. Проведено тестування роботи декодеру в умовах різної зашумленості каналу для кодів довжиною 64 та 32 (горизонтальна і вертикальна компоненти мають однакову базову довжину кодового слова). При задані умов передачі використовувався показник імовірності інвертування біту. У результаті дослідження отримані показники роботи декодеру при роботі в різних умовах. Виявлено, що при зменшенні рівні шумів до визначеного рівня імовірність помилки фактично не залежить від даного показника, а залежить від того, які типи помилки виникають у кодовому слові. У випадку виникнення помилки, яка не може бути відкорегована декодером, вона залишається, незважаючи на зміну кількості ітерацій. Також визначено, які саме комбінації помилок не дозволяють провести виправлення вказаним декодером. За результатами досліджень, декодер є ефективним під час роботи з каналом передачі інформації, який має відносно низький рівень зашумленості. За даної умови він перевершує жорсткий декодер у виправній здатності. Тестування проводилось на базі розробленого лабораторного стенду, який складається з двох модулів. Лабораторний стенд здатен забезпечувати тестування роботи декодеру при пропускній здатності понад 200 Мбіт/с.

ЛІТЕРАТУРА

[1] Y. Krainyk, V. Perov, M. Musiyenko, “Low-Complexity High-Speed Soft-Hard Decoding for Turbo-Product Codes”, Electronics and Nanotechnologies-2017 (ELNANO-2017), Kyiv, Ukraine, 2017, pp. 471-474.

[2] Y. Krainyk, V. Perov, M. Musiyenko, Y. Davydenko, “Hardware-Oriented Turbo-Product Codes Decoder Architecture”, IDAACS-2017, Bucharest, Romania, 2017, pp. 151-154.

Питання побудови мов паралельного програмування

В.А. Святний
Донецький національний технічний університет
Покровськ, Україна
vsvjatnyj@gmail.com

А.С. Любимов
Донецький національний технічний університет
Покровськ, Україна
artemliubymov@gmail.com

О.М. Мірошкін
Університет Ульм
Ульм, Німеччина
miroshkinan@gmail.com

В.Г. Кушнаренко
Університет Ульм
Ульм, Німеччина
volodymyr.kushnarenko@uni-ulm.de

Question of parallel simulations language constructing

V.A. Svjatnyj
Donetsk national technical university
Pokrovsk, Ukraine
vsvjatnyj@gmail.com

A.S. Liubymov
Donetsk national technical university
Pokrovsk, Ukraine
artemliubymov@gmail.com

O.M. Miroshkin
Donetsk national technical university
Pokrovsk, Ukraine
miroshkinan@gmail.com

V.G. Kushnarenko
Ulm university
Ulm, Germany
volodymyr.kushnarenko@uni-ulm.de

***Анотація*—Аналіз етапів і наявних засобів моделювання складних динамічних систем (СДС) показав, що сучасні паралельні засоби відстають за рівнем сервісу від послідовних блоково-, рівняння- та об'єктно-орієнтованих (БО, РО, ОО) мов моделювання: розробники MIMD-симуляторів вимушені працювати на рівні мов програмування. Запропоновано концепцію розробки мов паралельного моделювання на основі аналогії між принципами функціонування послідовних мов і MIMD-паралельністю. Розв'язання систем рівнянь послідовною мовою відповідає MIMD-паралелізму і може інтерпретуватися як віртуальне призначення «Функціональний елемент мови – MIMD-процес». Показано трансформацію БО-специфікації Simulation-моделі СДС в структуру MIMD-процесів на прикладі моделі мережевого динамічного об'єкту з зосередженими параметрами (МДОЗП). Запропоновано трансформацію специфікацій БО-, РО- та ОО-симуляторів в віртуальні паралельні MIMD-симулятори. Введено віртуальну матрицю комутацій, яка формально описує всі зв'язки між процесами MIMD-симулятора, що відповідають функціональним елементам послідовних мов. Визначено девіртуалізацію як процес перетворення специфікацій віртуальних MIMD-симуляторів, що однозначно забезпечує реалізацію симуляторів на заданій цільовій паралельній обчислювальній системі, сформульовано основні теоретичні і практичні задачі цього процесу.**

***Annotation* – The analysis of the stages and available simulation tools of complex dynamic systems (CDS) showed that modern parallel tools lag behind the level of service from sequential block, equation and object-oriented (BO, EO, OO) simulation languages: MIMD simulators are forced developers work at the programming language level. The concept of developing parallel modeling languages based on the analogy between the principles of the functioning of consecutive languages and MIMD-parallelism is proposed. The solution of the systems of equations in the sequential language corresponds to MIMD-parallelism and can be interpreted as a virtual assignment "Functional language element - the MIMD-process". The transformation of the BO-specification of the simulation-model of CDS into the structure of MIMD-processes is shown on the example of a network dynamic object model with lumped parameters (NDOLP). The transformation of the specifications of BO-, EO- and OO-simulators into virtual parallel MIMD-simulators is proposed. A virtual matrix of commutations was entered, which formally describes all the relationships between the processes of the MIMD-simulator that correspond to the functional elements of sequential languages. De-virtualization is defined as the process of transforming the specifications of virtual MIMD-simulators, which uniquely provides the implementation of simulators on a given objective parallel computing system, the main theoretical and practical tasks of this process was formulated.**

Ключові слова—складна динамічна система, Simulation-модель, мови моделювання, функціональний блок, MIMD-симулятор, MIMD-процес, девіртуалізація.

Keywords–complex dynamic system, Simulation-model, modeling language, functional block, MIMD-simulator, MIMD-process, de-virtualization.

I. Вступ

Основні етапи та засоби моделювання складних динамічних систем (СДС) показано на рис. 1. *Математична модель СДС* [1] – це рівняння досліджуваних динамічних процесів і формальний опис топології системи (технологічні схеми, графи, структури систем автоматизації, вторинні топології як результати апроксимації систем з розподіленими параметрами та ін.). *Simulation-моделлю СДС* прийнято називати модель, приведену до форми, яку вимагають обчислювальні методи та програмно-апаратні засоби розв'язання систем рівнянь. З огляду на показники складності (велика розмірність систем рівнянь, просторова розподіленість і багатозв'язність параметрів, ієрархічність структур, різна фізична природа взаємодіючих процесів, різні методи апроксимації моделей відносно просторових координат та ін.) треба відзначити, що побудова Simulation-моделей СДС є нетривіальною задачею і

потребує суттєвої комп'ютерної підтримки. Вибором певного обчислювального методу зумовлюється дискретна Simulation-модель СДС, що в процесі апаратно-програмної імплементації трансформується в *симулятор СДС*.

Рис.1. Етапи та засоби моделювання складних динамічних систем

Послідовні симулятори СДС пройшли шлях від реалізацій засобами мов програмування [2] до засобів блоково-(БО), рівняння-(РО) та об'єктно-орієнтованих (ОО) мов моделювання [3,4,5]. Розробка паралельних MIMD-симуляторів ведеться, як і раніше, за допомогою мов програмування з використанням засобів бібліотек MPI, OpenMP для обміну даними та синхронізації MIMD-процесів. Внаслідок цього експерти предметних областей, що розробляють паралельні симулятори, вимушені працювати з засобами колишніх традиційних систем моделювання другого і третього поколінь [2], що за рівнем сервісу та дружності до користувачів поступаються послідовним мовам моделювання. В

теорії і практиці технологій паралельного моделювання (Parallel Simulation Technology, ParSimTech) однією з ключових проблем є розробка розподілених паралельних моделюючих середовищ (РПМС) з повнофункціональним програмним забезпеченням розробки, налагодження й експлуатації паралельних симуляторів СДС (Parallel Modeling and Simulation Software). Для того, щоб наблизитись за рівнем сервісу до засобів моделювання п'ятого покоління [1, 2], необхідно в РПМС мати мови паралельного моделювання, що забезпечують перетворення специфікацій моделей СДС в виконувані програмні модулі паралельних симуляторів і звільняють експертів предметних областей від питань вибору обчислювальних методів, побудови дискретних Simulation-моделей СДС та їх програмної реалізації.

II. Принципи розв'язання диференціальних рівнянь в мовах моделювання і MIMD-паралельність

Основою концепції розробки мов паралельного моделювання є аналогія між блоками, об'єктами та операторами БО -, ОО- та РО-мов моделювання та MIMD-процесами паралельних обчислювальних систем з розподіленим адресним простором. Аналогія між БО-специфікацією Simulation-моделі СДС і MIMD-принципом розпаралелювання показується на прикладі моделі простого мережевого динамічного об'єкту з зосередженими параметрами (МДОЗП), що описується системою рівнянь:

$$\begin{cases} X = Y_1 + Y_2 \\ K_x \dfrac{dX}{dt} + R_x X|X| + K_1 \dfrac{dY_1}{dt} + R_1 Y_1 |Y_1| = f(X) \\ K_x \dfrac{dX}{dt} + R_x X|X| + K_2 \dfrac{dY_2}{dt} + R_2 Y_2 |Y_2| = f(X) \end{cases}$$

Simulation-модель МДОЗП:

$$\begin{cases} X = Y_1 + Y_2 \\ \dfrac{d}{dt}\left(Y_1 + \dfrac{K_x}{K_1} X\right) = [f(x) - R_x X|X| - R_1 Y_1 |Y_1|]/K_1 \\ \dfrac{d}{dt}\left(Y_2 + \dfrac{K_x}{K_2} X\right) = [f(x) - R_x X|X| - R_2 Y_2 |Y_2|]/K_2 \end{cases}$$

За методом неявних функцій отримаємо БО-специфікацію Simulation-моделі у вигляді блок-схеми функціональних блоків, що необхідні для знаходження невідомих змінних X, Y_1, Y_2 (рис. 2).

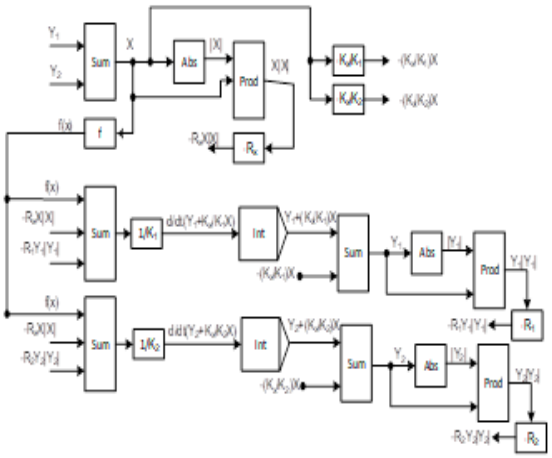


Рис.2. Блок-схема розв'язання системи рівнянь, БО-симулятор

Аналіз показує, що функціональному блоку БО-мови моделювання можна співставити MIMD-процес, що виконує операцію блоку і програмується за аналогічним алгоритмом. Принцип розв'язання систем рівнянь БО-мовою відповідає MIMD-паралелізму і може інтерпретуватися як віртуальне призначення «Функціональний блок – MIMD-процес» (рис. 3): кожному блоку БО-мови призначаємо MIMD-процес, який в точності виконує операції блоку; отримаємо множину **n** процесів, які зв'язуються між собою комунікаційним графом, що синтезується на основі схеми з'єднань між виходами і входами блоків БО-симулятора рис. 2.

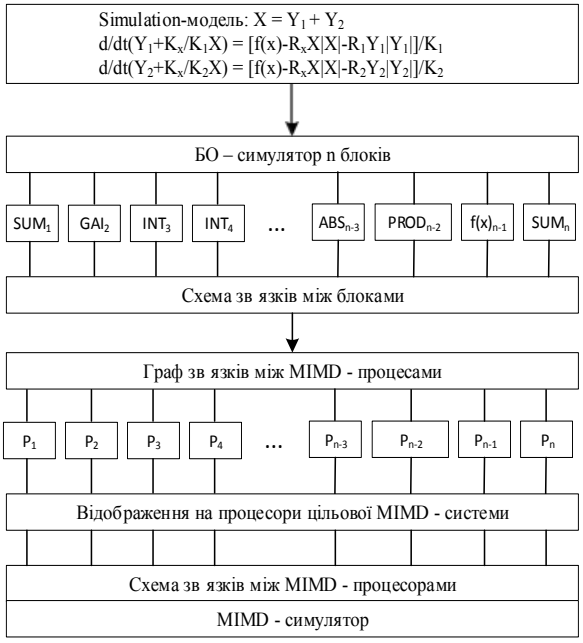


Рис. 3. MIMD-паралельність і принцип БО-мови, n – кількість блоків і процесів MIMD-симулятора

III. Трансформація специфікацій БО-, ОО-, та РО-симуляторів в віртуальні паралельні MIMD-симулятори

Віртуальний паралельний MIMD-симулятор – це структура MIMD-процесів, яка будується на основі запропонованих аналогій між БО-, ОО- та РО-специфікаціями. Пропонується підхід до трансформації мовних специфікацій в віртуальну структуру MIMD-процесів на основі векторів з'єднань для процесів Ti:

$$VST_i = (S_{i1}T_1\ S_{i2}T_2 \ldots S_{ik}T_k\ \ldots S_{in}T_n)$$

де i – номер процесу, i =1,2,…,n; S_{ik} – параметр комутації : S_{ik}=1 – якщо є зв'язок між процесами Ti ↔ Tk і S_{ik}= 0 – якщо зв'язок Ti ↔ Tk відсутній. Множина векторів VSTi для загальної структури БО-симулятора має вигляд:

$$\begin{cases} VST_1 = (S_{11}T_1\ S_{12}T_2 \ldots S_{1k}T_k\ \ldots S_{1n}T_n) \\ \ldots \\ VST_k = (S_{k1}T_1\ S_{k2}T_2 \ldots S_{kk}T_k\ \ldots S_{kn}T_n) \\ \ldots \\ VST_n = (S_{n1}T_1\ S_{n2}T_2 \ldots S_{nk}T_k\ \ldots S_{nn}T_n) \end{cases}$$

Simulation-модель описується системою рівнянь, кожне з яких є неявною функцією, що визначає невідому змінну і розв'язується відповідним блоком та по аналогії – MIMD-процесом Ti. Ця змінна VARTi, будучи вихідною величиною процесу Ti, є результатом певної операції над множиною змінних. В загальному специфікація віртуального MIMD-симулятора може бути представлена множиною операцій:

$$\begin{cases} VART_1 = FUNT_1(S_{11}VART_1\ S_{12}VART_2 \ldots S_{1n}VART_n) \\ \ldots \\ VART_k = FUNT_k(S_{k1}VART_1\ S_{k2}VART_2 \ldots S_{kn}VART_n) \\ \ldots \\ VART_n = FUNT_n(S_{n1}VART_1\ S_{n2}VART_2 \ldots S_{nn}VART_n) \end{cases}$$

Тут VARTi – вихідні результуючі змінні процесів Ti, і = 1,2, ..., n; FUNTi – операції процесів Ti над вхідними змінними, що подаються з виходів всіх інших процесів-учасників розв'язання системи рівнянь Simulation-моделі. Для подальших дій з трансформації специфікацій знадобиться віртуальна матриця комутацій

$$KM = \begin{pmatrix} S_{11} & S_{12} & \cdots & S_{1(n-1)} & S_{1n} \\ S_{21} & S_{22} & \cdots & S_{2(n-1)} & S_{2n} \\ & & \vdots & & \\ S_{k1} & S_{k2} & \cdots & S_{k(n-1)} & S_{kn} \\ & & \vdots & & \\ S_{n1} & S_{n2} & \cdots & S_{n(n-1)} & S_{nn} \end{pmatrix}$$

яка формально описує всі зв'язки між блоками БО-симулятора і між процесами MIMD-симулятора.
Ці формальні засоби можуть використовуватись і для трансформації ОО- та РО-симуляторів в відповідні віртуальні MIMD-симулятори.

IV. Девіртуалізація специфікацій віртуальних MIMD-симуляторів

Девіртуалізація – це перетворення специфікацій віртуальних MIMD-симуляторів, що однозначно визначає реалізацію симуляторів на заданій цільовій паралельній обчислювальній системі (ЦПОС) і потребує вирішення наступних основних теоретичних і практичних задач: розробка програм MIMD-процесів, що є аналогами елементів мов моделювання; синтез віртуальних комутаторів зв'язку між MIMD-процесами-аналогами та їх відображення в реальних системах зв'язку ЦПОС; апріорний аналіз специфікацій віртуальних MIMD-симуляторів на відповідність основним критеріям ефективності паралельних обчислень; архітектурно релевантна програмна імплементація; інтеграція з підсистемами РПМС [1, 8].

V. Висновки

Зростаючі вимоги предметних областей до методів і засобів моделювання стимулюють застосування високопродуктивних паралельних комп'ютерів існуючих і майбутніх MIMD -архітектур та викликають нові теоретичні та практичні проблеми технологій паралельного моделювання. Одним із аспектів проблеми дружності паралельних обчислювальних систем до експертів предметних областей є перехід від програмування паралельних симуляторів до їх побудови засобами мов моделювання. Запропонована концепція розробки мов паралельного моделювання базується на аналогії між MIMD-процесами та основними елементами послідовних мов моделювання. Реалізація концепції є перспективним напрямком розробок і досліджень в області паралельного моделювання складних динамічних систем.

Література

[1] Feldmann, L.P., Resch, M., Svjatnyj, V.A., Zeitz,M.: Software-Architektur für parallele Simulationsumgebungen. Plenarvortrag am ASIM'2014-Symposium Simulationstechnik (Berlin, 03.-05.09.2014), Tagungsband, S.3-7.

[2] Schmidt B.: Simulationssysteme der 5. Generation. SiP, Heft 1, 1994, S. 5-6.

[3] A. Angermann, M. Beuschel, M. Rau, U. Wohlfarth: Matlab-Simulink-Stateflow, 6.Auflage, Oldenbourg, München, 2009.

[4] Modelica – A Unified Object-Oriented Language for Physical Systems Modeling. Language Specification. Version 2.0, 2002.

[5] Johan Åkessona, Torbjörn Ekmanb, Görel Hedinc: Implementation of a Modelica compiler using JastAdd attribute grammars. Science of Computer Programming 75 (2010) p. 21–38.

[6] Advanced Continuous Simulation Language (ACSL). Reference Manuel, 4th Edition. Mitchel and Gauthier Associates, Concord, 1986.

[7] Kushnarenko,V., Resch, M., Svjatnyj, V., Wesner, S.: Zur Entwicklung des Gleichungslösersubsystems der verteilten parallelen Simulationsumgebung. ASIM'2014 in Berlin, Tagungsband 2, ARGESIM Report 43, Wien 2014, S. 357-363.

[8] V. Svjatnyj, V. Kushnarenko, O. Shcherbakov, M. Resch: Dekomposition der verteilten parallelen Simulationsumgebung. In: Проблеми моделювання й автоматизованого проектування. Наук. праці ДонНТУ, №1(10)-2(11). – Донецьк, 2012. – с. 227-234.

Визначення істинності продукційних правил в Erlang

Світлана Шаповалова
Кафедра автоматизації проектування енергетичних процесів і систем
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Київ, Україна
lanashape@gmail.com

Ольга Мажара
Кафедра автоматизації проектування енергетичних процесів і систем
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Київ, Україна
olyamazhara@gmail.com

Evaluations of production rules in Erlang

Svitlana Shapovalova
Automation of projection of power processes and systems
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
lanashape@gmail.com

Olga Mazhara
Automation of projection of power processes and systems
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
olyamazhara@gmail.com

***Анотація*—Дослідження присвячено реалізації продукційної системи представлення знань на основі вбудованих механізмів мови Erlang. Розглянуто основні концепції та базові підходи до реалізації співставлення за допомогою інкрементних алгоритмів Rete, Treat та LEAPS. Визначено, що LEAPS найменш ресурсоємний з точки зору використання пам'яті та швидкодії, однак має обмежене застосування внаслідок формування неповної конфліктної множини. В той же час дане обмеження не є принциповим для багатьох прикладних систем висновування. Представлено концепцію уніфікації термів та доведення істинності атомарних формул в Erlang. Наведено компоненти представлення шаблонів правил та робочої пам'яті в Erlang. Надано опис алгоритму визначення істинності умовної частини правила за стратегією LEAPS. Запропонованою реалізацією адаптованого алгоритму для мови Erlang. Представлений алгоритм дозволяє проводити паралельну обробку правил бази знань за рахунок відмови від збереження даних проміжних етапів. Його перевагою є простота реалізації з використанням вбудованих механізмів Erlang без побудови складних структур даних для представлення бази знань, які б потребували додаткових ресурсів для обробки. Запропонований спосіб дозволяє створити механізм логічного висновування, зокрема продукційних систем.**

***Abstract*— The research is devoted to the implementation of a production knowledge representation system based on embedded Erlang language mechanisms. The basic concepts and approaches to implementation of incremental match algorithms Rete, Treat, LEAPS are described. LEAPS is found to be the least resource-consuming in terms of memory and performance, but it has limited application due to the formation of incomplete conflict set. At the same time, this limitation is not essential for many applied inference systems. The concept of the unification of terms and the evaluation of the truth of atomic formulas in Erlang is presented. The components for presenting rule templates and working memory in Erlang are presented. The description of the algorithm for determining the truth of the conditional part of the rule according to the LEAP strategy is described. An implementation of the adapted algorithm for the Erlang language is proposed. The presented algorithm allows parallel processing of knowledge base rules due to the refusal to store data of intermediate stages of matching. Its advantage is the simplicity of implementation using Erlang's built-in mechanisms without building complex data structures for the presentation of a knowledge base that would require additional resources for processing. The proposed method allows to create the mechanism of logical inference, in particular production systems.**

Ключові слова—Rete, LEAPS, Erlang, співставлення зі зразком, продукційні системи

Keywords—Rete, LEAPS, Erlang , pattern match, production systems

I. Вступ

Інтелектуалізація програмного забезпечення є найпоширенішою тенденцією в галузі його розробки. Важливим напрямком можна виокремити проведення заключень для доведення гіпотези або досягнення мети. Найбільш універсальним способом представлення правил висновування є логічні формули. Окрім спеціалізованих засобів, які пристосовані для обробки таких формул, наприклад мови Prolog, розроблені універсальні моделі представлення знань, насамперед продукційна. Системи, засновані на множині правил, що описують предметну область, знайшли широке застосування при проектуванні експертних систем підтримки прийняття рішень (Recomrndstion systems), сервісів консультацій (Pre-Sales Advice), бізнес-застосунків (Advanced Business Rule) та інших галузей, де необхідне експертне заключення [1].

Представлення правил висновування як формул логіки предикатів є найбільш універсальним. При реалізації продукційної моделі представлення знань основною та найбільш ресурсоємною [2] задачею є визначення істинності умовної частини правил. Загальновживана її реалізація на основі Rete

алгоритму співставлення зі зразком або його модифікацій є складною; потребує побудови додаткових графових структур представлення умов на етапі прекомпіляції, а згодом значних ресурсів пам'яті та часу в процесі визначення істинності логічних виразів. Оптимізації Rete спрямовані насамперед на пришвидшення цього процесу (наприклад, за рахунок його розпаралелювання) та зменшення використовуваних ресурсів пам'яті. Останнім часом з'явився інтерес до створення подібних методів за рахунок апаратного прискорення та сучасних підходів до розробки розподіленого програмного забезпечення [3], [4], [5], [6], [7] .

Rete алгоритм був запропонований C. Forgy як універсальний метод співставлення для реалізації на будь-яких мовах програмування. Однак з того часу були розроблені нові мови високого рівня, які за своєю концепцією та вбудованими механізмами можуть реалізовувати продукційну модель без проміжних структур представлення бази знань з безпосередньою ефективною обробкою формалізованих записів продукційних правил в процесі висновування. Саме таким ефективним засобом програмування є мова Erlang. Однак і досі на її основі реалізації продукційних систем створюють за Rete алгоритмом [8]. Задача створення альтернативного способу представлення співставлення зі зразком з використанням вбудованих механізмів Erlang є актуальною та має практичне значення для розробки високоефективних та масштабованих систем висновування.

II. Підходи до співсталення зі зразком

В процесі логічного виведення за продукційною моделлю задаються або доводяться факти, які стосуються поточної задачі. Ці факти зберігаються в робочій пам'яті (WM - Working Memory). Правила бази знань мають умовну (ліву) та результативну (праву) частину. Правила вважають узгодженим з робочою пам'яттю, якщо її вміст в повній мірі визначає структуру антецеденту. Це умовна (ліва) частина правила описує шаблони, які містять константи та змінні. Дані робочої пам'яті узгоджуються з шаблонами правила, використовуючи ті самі константи на відповідних місцях [9].

Історично перший алгоритм співставлення зі зразком в продукційних системах відомий як "наївний". Для визначення правил, умовна частина яких істина на поточному кроці, сканується база знань і кожен умовний елемент правила порівнюється з вмістом робочої пам'яті. Це призводить до експотенціального зростання складності алгоритму зі збільшенням кількості правил в базі знань [10]. Недоліки наївного підходу стали мотивацією для створення інкрементних алгоритмів співставлення, які ґрунтуються на використанні інформації про виконання попередніх циклів логічного виведення. Необхідність збереження та обробки даних попередніх узгоджень призводить до компромісу щодо забезпечення швидкодії за рахунок витрат пам'яті. Найбільш широко відомими інкрементними підходами є Rete та Treat, формальне порівняння яких представлено в [11].

Для найгіршого випадку асимптотична складність Rete та Treat алгоритмів а термінах простору та часу $O(wm^c)$, де wm - розмір робочої пам'яті, c - максимальна кількість умовних елементів правила [12]. Конфліктний набір сам по собі має просторову складність найгіршого випадку $O(wm^c)$. Тому для зменшення затрат пам'яті необхідно в першу чергу уникнути обчислення повної конфліктної множини [12]. Для уникнення проблеми складності підходів нетерплячої оцінки D. Miranker запропонував алгоритм лінивої оцінки Leaps.

Алгоритми лінивої оцінки передбачають поєднання стратегії вирішення конфлікту з етапом пошуку активації для виконання таким чином, щоб на кожному циклі співставлення обчислювалося лише одне правило. Це дозволяє покращити асимптотичну просторову складність алгоритмів інкрементної оцінки для найгіршого випадку (worst-case asymptotic space complexity). Крім того попередні експериментальні результати вказують на значне підвищення швидкодії в порівнянні з класичними Rete та Treat алгоритмами [12]. Просторова складність найгіршого випадку для алгоритму лінивої оцінки $O(max(ts)*c)$, де ts - мітка часу, а $O(max(ts)$ - обмежена загальною кількістю змін робочої пам'яті [12]. В багатьох випадках немає потреби обчислювати всі варіанти підстановок змінних в шаблонах, достатньо діяти за стратегією LEAPS.

Мова Erlang дозволяє реалізувати обидва підходи способами, альтернативним існуючим, які базуються на Rete, Treat або LEAPS та їх модифікаціях. Ефективність такої реалізації забезпечується властивостями Erlang:

- механізмом співставлення - для уніфікації термів;
- механізмом легковагових потоків обчислень - для паралельної обробки правил БЗ;
- засобами функціонального програмування
- масштабованістю

Для реалізації співставлення зі зразком на основі вбудованих механізмів Erlang насамперед необхідно розв'язати задачу уніфікації термів.

III. LEAPS алгоритм визначення істинності антецеденту

Для алгоритмів нетерплячої оцінки (жадібних алгоритмів) надлишкові витрати за часом передбачають не лише обчислення конфліктної множини, але й менеджмент пам'яті та структур даних [13]. Це дозволяє висунути припущення, що зменшення затрат пам'яті може призвести до підвищення швидкодії системи [12]

Алгоритм лінивої оцінки передбачає пошук активації на основі пошуку в ширину за можливими узгодженнями умовних елементів. Після знаходження першої активації пошук призупиняється на час запуску знайденого правила. Так як запуск правила може призвести до змін робочої пам'яті, пошук в ширину повинен бути реалізованим з можливістю обробки динамічної зміни станів. Це досягається за

рахунок збереження стеку вказівників на стан пошуку. В процесі виконання пошуку за змінами робочої пам'яті, вказівники на результати додаються до стеку. Коли пошук за поточним елементом робочої пам'яті вичерпується, відповідні вказівники видаляються зі стеку. Згідно з [12] псевдокод алгоритму представлено на рисунку 1.

Фактично в стеці зберігаються поточні можливі підстановки для шаблонів умовних елементів правила p_i . Для кожного узгодженого умовного елемента встановлюється мітка пам'яті *timestamp* , яка вказує на те, коли елемент було додано до стеку. Ініціалізація стеку відбувається за початковим станом робочої пам'яті в довільному заздалегідь обраному порядку. Всі наступні елементи додаються в процесі узгодження. На кожному циклі співставлення зі зразком зі стеку отримується верхній елемент, що відповідає останньому узгодженню. Функція pop_stack повертає верхній елемент та видаляє його зі стеку. Даний елемент називається домінантним і подальше співставлення здійснюється на його основі за стратегією пошуку в ширину. Функція best_first виконує пошук за узгодженими елементами у порядку зворотному до порядку їх надходження до робочої пам'яті. Якщо вдалося знайти узгодження продукції, яке містить домінантний елемент – домінантний елемент повертається до стеку (push_stack), правило виконується (fire).

```
1.  p1, ..., pn: WME timestamps;
2.  begin Lazy Match;
3.    initialize stack;
4.    loop while stack not empty
5.      pn = pop_stack(p1, ..., pn−1)
6.      if stack not empty then
7.        best_first (p1, ..., pn−1, pn, found)
8.        if found then
9.          push_stack (pn, p1, ..., pn−1);
10.         fire (p1, ..., pn);
11.   end loop
12. end Lazy Match
```

Рис. 1 Базовий псевдокод LEAPS алгоритму

Згідно з [14] структури даних та принципи LEAPS алгоритму є складними для розуміння та реалізації. Можливо саме це завадило широкому його використанню в прикладних продукційних системах. Для ефективної реалізації алгоритму необхідна мова програмування, що підтримує концепції реляційних баз даних, такі як, наприклад, зв'язки (relations) та операції вибору з об'єднанням (select-project-join operators) [14]. Перша версія LEAPS алгоритму, запропонована Miranker та Batory, була реалізована у вигляді компілятору з бази знань, створеної для спеціалізованої оболонки OPS5, в набір програм на мові C [15]. Для уникнення складності з недоліками існуючих на той час мов програмування у вигляді недостатньої множини стандартних структур представлення даних, а також для спрощення розуміння алгоритму розробниками була створена версія LEAP алгоритму з використанням програмної абстракції курсор-контейнер (container-cursor programming abstractions) на базі компілятору структур даних P2 [14] . Однак P2 не є загальновживаною мовою програмування високого рівня і потребує від розробника додаткових зусиль на розуміння та інтеграцію реалізованих алгоритмів до існуючих програмних рішень.

Тому для Erlang на основі запропонованого механізму уніфікації термів та стратегій LEAPS підходу реалізовано адаптовану версію алгоритму співставлення зі зразком.

IV. Визначення істиності антецеденту в Erlang

Механізм визначення істинності логічних виразів насамперед реалізує уніфікацію термів атомарних формул антецеденту з відповідними термами шаблонів робочої пам'яті. Проблема полягає в тому, що антецедент може містити як зв'язані так і незв'язані терми. В робочій пам'яті всі терми зв'язані. Область дії змінних розповсюджується лише на поточне продукційне правило (тобто в межах одного антецеденту та консеквенту). Крім того в Erlang не можна задавати неосновні факти з незв'язаними параметрами. Тому для пристосування вбудованого механізму співставлення для уніфікації термів на етапі прекомпіляції всі змінні нумеруються та представляються у форматі кортежу *{var, N }*, де *N* номер змінної, який співпадає для всіх змінних з однаковим ім'ям (за зразком оболонки продукційних систем CLIPS).

Уніфікація двох термів успішна в двох випадках:

- якщо обидва терми є однаковими constant-термами (constant термами є атомарні константи або колекції атомарних констант – списки або кортежі);
- якщо терм антецеденту є змінною, а терм WM є константою. В такому випадку всі змінні продукційного правила , представлені однаковим номером, стають зв'язаними значенням цієї константи.

Для реалізації стратегії лінивої оцінки в записі шаблону WM достатньо зберігати лише один приклад підстановки атомарної формули. За умови реалізації моделі з повним конфліктним набором в шаблоні WM необхідно зберігати список зі всіх можливих підстановок. Окрім цього представлення кожної атомарної формули містить її знак sign (позитивний чи негативний) та тег часу timestamp, який відображає час доведення відповідного факту.

Представлення правил баз знань обмежене диз'юнктивною нормальною формою представлення умов висновування. При цьому умовною частиною одного правила є один диз'юнкт, тобто кон'юнктива атомарна зв'язка літералів. Таким чином, декілька правил можуть мати один і той самий консеквент. Консеквент містить список дій з модифікації робочої пам'яті на поточному кроці. До цих дій належать додавання доведених та видалення спростованих фактів.

При реалізації в Erlang доведення істинності атомарних формул за зразком мов Prolog та CLIPS відбувалося за двома концепціями: безпосереднє доведення за механізмом уніфікації та доведення істинності негативних шаблонів за постулатом замкненості світу.

V. Алгорим визначення істинності антецеденту в Erlang

Для реалізації в Erlang пропонується спрощена версія алгоритму, яка не передбачає збереження проміжних результатів узгодження. Пошук відбувається на основі стратегії глибини за новими узгодженнями умовних елементів. Обробка антецеденту поточного правила проводиться циклічно за його атомарними формулами, кожна з яких відмічена тегом tagName, який є ключем структури умовного елементу і не потребує додаткових витрат пам'яті для збереження. Псевдокод алгоритму представлено на рисунку 2.

1. $p_1, \dots, p_n : WME_1, \dots, WME_m, tags$
2. *begin Match;*
3. *loop for all* p_i *and* WME_i
4. *if* $p_1 == tag(WME_i)$
5. *unify* ($p_2, \dots, p_n$, WME_i, *WME, found)*
6. *if found then*
7. *fire* ($p_1, \dots, p_n$);
8. *end loop*
9. *end Match*

Рис. 2 Базовий псевдокод адаптованого алгоритму

Таким чином, кожне правило можна також вважати відміченим тегом, який фактично є відображенням назви структури першого умовного елементу. Аналогічний тег мають елементи робочої пам'яті. Зовнішній цикл обробки правил передбачає порівняння за даними тегами і забезпечує ранню відмову від правил, для яких в робочій пам'яті відсутні необхідні дані. Таким чином динамічно формується множина правил, які є кандидатам для узгодження. Для кожного з таких правил почергово запускається функція уніфікації *unify* . Якщо для правила було узгоджено решту шаблонів, функція уніфікації встановлює значення *found* істинним і виконується результативна частина даного правила. Після цього співставлення починається з початку. Функція уніфікації працює в межах одного правила і відповідає за узгодження константних значень та змінних. Спершу засобами мови Erlang виконується узгодження для констант та структур фактів за винятком змінних. Лише у випадку, коли доведено можливість узгодження константних значень на виконання запускається функція узгодження змінних, що також виконує перевірку аргументів за стратегією глибини серед елементів робочої пам'яті, які було узгоджено з константними значеннями.

LEAPS алгоритм передбачає збереження стеку узгоджених елементів, що фактично відповідає підходу до збереження узгодження константних значень в структурах даних Rete та Treat підходів. Це дозволяє досягти високої швидкодії. Однак, необхідність динамічного оновлення та сортування за мітками часу даної структури в процесі роботи співставлення ускладнює розпаралелювання даного підходу. Тому в адаптованій версії запропоновано відмовитися від збереження проміжних результатів узгодження, що наближує даний алгоритм до наївного. Це дозволяє виконувати доведення істинності антецеденту паралельно для кожного або ж для підмножини правил. В процесі співставлення на кожному циклі використовується статична поточна робоча пам'ять, для якої доступ відбувається лише в режимі зчитування. Таким чином запропонований спосіб засновується лише на базових компонентах продукційної системи, не вимагає додаткових структур даних, які потребують значних ресурсів пам'яті та часу обробки.

VI. Висновки

- Проведено аналіз методів співставлення зі зразком в продукційній моделі представлення знань. Обґрунтовано використання стратегії LEAPS для реалізації адаптованої версії в продукційній оболонці на базі Erlang.
- Запропоновано концепцію уніфікації термів в Erlang.
- Запропоновано спосіб співставлення зі зразком для доведення істинності умовної частини продукційного правила в Erlang.

Література

[1] Exys. Knowledge Automation Expert system Technology http://www.exsys.com/app_bizrules.html - [Electronic resources] - 2011

[2] C. L. Forgy, "On the Efficient Implementation of Production Systems," Carnegie-Mellon University, pp. 1–210, 1979.

[3] B. Cao, J. Yin, Q. Zhang, and Y. Ye, "A MapReduce-based architecture for rule matching in production system," Proc. - 2nd IEEE Int. Conf. Cloud Comput. Technol. Sci. CloudCom 2010, pp. 790–795, 2010.

[4] M. Peters, C. Brink, S. Sachweh, and A. Zündorf, "Rule-based reasoning on massively parallel hardware," CEUR Workshop Proc., vol. 1046, pp. 33–49, 2013.

[5] J. Y. Guo, C. Hwang, and M. S. Chen, "Using GPU to shorten the match time of rule reasoning based on rete algorithm," Proc. - 2016 IEEE Int. Symp. Comput. Consum. Control. IS3C 2016, no. 1, pp. 883–886, 2016.

[6] J. Wang, R. Zhou, J. Li, and G. Wang, "A Distributed Rule Engine Based on Message-Passing Model to Deal with Big Data," Lect. Notes Softw. Eng., vol. 2, no. 3, pp. 275–281, 2014.

[7] M. Peters, C. Brink, S. Sachweh, and A. Zündorf, "Scaling parallel rule-based reasoning," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8465 LNCS, pp. 270–285, 2014.

[8] Stefano 2014] A. Di Stefano, F. Gangemi, C. Santoro, and V. a Doria, "ERESYE : an Erlang Expert System Engine," Program, no. May, pp. 1–17, 2014.

[9] J. Klahr, P. Langley, and R. Neches, Production System Models of Learning and Development, 1989.

[10] Daniel P. Miranker. TREAT: A New and Efficient Match Algorithm for AI Production Systems. Pitman/Morgan Kaufmann, 1990.

[11] Shapovalova, S. I., Mazhara, O. O. Formalization of basic pattern matching algorithms in production systems. Eastern-European Journal of Enterprise Technologies, 4(3(76)), 22–27, 2015 doi:10.15587/1729-4061.2015.46571

[12] D. P. Miranker, D. a Brant, B. J. Lofaso, and D. Gadbois, "On the Performance of Lazy Matching in Production Systems," Proc. 1990 Natl. Conf. Artif. Intell., no. c, pp. 685–692, 1990.

[13] Lofaso, B. J., "Join Optimization in a Compiled OPS5 En-vironment," Tech. Report No. ARL-TR-89-19, Ap- plied Research Laboratories, The University of Texas at Austin, April, 1989

[14] D. Batory, "The LEAPS algorithms," Elements, pp. 1–15, 1994.

[15] D. Miranker and B. Lofaso, "The Organization and Performance of a TREAT Based Production System Compiler", IEEE Transactions on Knowledge and Data Engineering, March 1991

Автоматичне реферування текстів на природній мові

Катерина Морозова
кафедра математичного забеспечення комп'ютерних систем
Одеський національний університет ім. І.І. Мечникова
Одеса, Україна
morozova.kateryna@stud.onu.edu.ua

Ірина Шпінарева
кафедра математичного забезпечення комп'ютерних систем
Одеський національний університет ім. І.І. Мечникова
Одеса, Україна
ishpinareva@gmail.com

Ольга Геренко
кафедра математичного забезпечення комп'ютерних систем
Одеський національний університет ім. І.І. Мечникова
Одеса, Україна
gerenko_olga@ukr.net

Automatic texts summarization in natural language

Kateryna Morozova
Department of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
morozova.kateryna@stud.onu.edu.ua

Irina Shpinareva
Department of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
ishpinareva@gmail.com

Olga Gerenko
Department of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
gerenko_olga@ukr.net

***Анотація*—У статті розглянуто алгоритм для автоматичного реферування текстів на природній мові з застосуванням методів машинного навчання, зокрема за допомогою нейронних мереж з довгою-короткочасною пам'яттю LSTM. Визначено актуальність дослідження в напрямку подачі текстового документа в векторній формі з застосуванням методів Word2vec, GloVe та векторної моделі використовуючи «мішок термів» із застосуванням підходу побудови векторної моделі статичної міри TF-IDF. Процес отримання реферату складається з наступних етапів: вихідний текст перекладається в нижній регістр в якому видаляються стоп-слова і виконується стемінг; далі йде векторне подання обробленого тексту; рекурентна нейронна мережа LSTM приймає вектор вхідних слів і виводить векторне подання відповідне вхідний послідовності за допомогою навчання. Навчання нейронної мережі виконано за допомогою алгоритму зворотного поширення помилки розгорнутого в часі. Тестування системи здійснюється на корпусі текстів. Аналізуючи результати роботи системи можна відзначити, що нейронна мережа показала найкращий результат роботи використовуючи векторну форму GloVe.**

***Abstract*—The article deals with the algorithm for automatic texts summarization in natural language using machine learning methods, in particular, using neural networks with long-short term memory LSTM. The relevance of research is in the direction of supplying a text document in vector form which is determined using the methods Word2vec, GloVe and a vector model using the «bags of terms», using the approach of constructing the vector model of the static measure TF-IDF. The process of obtaining an abstract consists of the following steps. At the processing stage, the source text is transferred to the lower case, in which the stop words are deleted and stemming is performed. The result of the next step is the processed text vector representation. After this the LSTM recurrent neural network receives the input value vector of the words and outputs a vector representation corresponding to the input sequence through training. The neural network is trained using an algorithm for back propagation of an error deployed in time. The system is tested on the text corpus. Analyzing the results of the system, it can be noted that the neural network showed the best result using a vector representation of GloVe method.**

Ключові слова—реферування, векторне подання, Word2vec, GloVe, статистична міра TF-IDF, негативне семплірування, нейронна мережа, рекуррентна нейронна мережа, Long-Short-Term-Memory, функція активації, обробка природних мов, навчання мережі, тестування мережі.

Keywords—summarization, vector representation, Word2vec, GloVe, statistical metrics TF-IDF, negative sampling, neural network, recurrent neural network, Long-Short-Term-Memory, activation function, natural languages processing, network training, network testing.

I. ВСТУП

Електронна інформація грає все більшу роль у всіх сферах життя сучасного суспільства. В останні роки обсяг текстової інформації в електронному вигляді зріс настільки, що виникає загроза знецінення цієї інформації в зв'язку з труднощами пошуку необхідних відомостей серед безлічі доступних текстів. Розвиток інформаційних ресурсів Інтернет багаторазово посилює проблему інформаційного перевантаження. У цій ситуації особливо актуальними стають методи автоматизації реферування текстової інформації, тобто методи отримання стисненого уявлення текстових документів – рефератів (анотацій). Постановка задачі

автоматичного реферування тексту і відповідно спроби її вирішення з використанням різних підходів робилися багатьма дослідниками.

Дуже багато користувачів регулярно стикаються з необхідністю швидко переглядати великий обсяг документів і вибирати з них дійсно потрібні. Ця задача виникає і при роботі з текстовими базами даних, і при розбиранні електронної пошти, і при пошуку в Інтернеті. Часто буває, що в великих організаціях, особливо державних, правила діловодства наказують супроводжувати кожен важливий документ коротким описом.

Потреби в засобах автоматичного реферування відчувають: корпоративні системи документообігу, пошукові машини і каталоги ресурсів Інтернету, автоматизовані інформаційно-бібліотечні системи, канали мовлення, служби розсилки новин та ін.

Реферат (від лат. Referre – повідомляти, доповідати) – це скорочений зміст друкованого твору з основними фактичними даними і висновками. Реферат являє собою об'єктивне, позбавлене емоцій повідомлення інформації першоджерела на основі її смислової переробки. Він акцентує увагу на нових відомостях і визначає доцільність звернення до першоджерела.

Основними видами рефератів є: індикативні, критичні або оціночні і інформативні. Індикативні, що вказують тип інформації, мають сповіщальний характер. Критичні або оціночні оцінюють інформацію, що міститься в документі. До даного типу реферату відносяться огляди, що відображають не тільки суть джерела, а й думка про нього, що містить додаткові висновки, яких немає в оригіналі. Інформативні припускають конспективно виклад даних, представлених в первинному джерелі інформації.

У рефераті формулювання і узагальнення запозичуються з самого тексту оригіналу [1].

II. ПРОЕКТУВАННЯ СИСТЕМИ

Основні етапи роботи проектованої системи наведені на рис. 1.

Рис.1. Основні этапи проектування системи

Розглянемо більш детально кожен з етапів проектування системи.

Перш за все, необхідно провести аналіз текстового документа, який складається з попередньої обробки тексту.

Попередня обробка тексту складається з наступних етапів: переведення вхідного тексту в нижній регістр; видалення стоп-слів, тобто слів, що не несуть сенсу; стемінг, тобто відкидання змінної частини слова.

Отриманий текст перетворюється в векторне подання з застосуванням векторного збігу, алгоритмів GloVe або Word2vec або за допомогою статистичної міри TF-IDF.

Механізм побудови векторного збігу полягає в прийнятті до уваги того, які слова оточують слово, що розглядається. Це означає, що кожне слово буде визначатися його сусіднім словом зліва та справа. Математично це моделюється шляхом побудови матриці збігів.

Word2vec приймає в якості свого введення великий корпус тексту і створює векторний простір, зазвичай в кілька сотень вимірів, причому кожному унікальному слову в корпусі присвоюється відповідний вектор в просторі. Векторні уявлення розташовані в векторному просторі, так що слова, які мають спільні контексти в корпусі, розташовані в безпосередній близькості один від одного в просторі.

Перший крок алгоритму Word2vec полягає в читанні корпусу і розрахунку частоти входження *i* кожного слова в корпусі (тобто кількість разів, коли слово зустрілося в корпусі – і так для кожного слова). Отриманий масив слів сортується за частотою (слова зберігаються в хеш-таблиці), і видаляються рідкісні слова.

Другий крок алгоритму Word2vec полягає в побудові дерева Хаффмана. Дерево Хаффмана часто застосовується для кодування словника – це значно знижує обчислювальну і часову складність алгоритму.

На третьому кроці з корпусу читається субречення і проводиться субсемплірування найбільш частотних слів. Субречення – це якийсь базовий елемент корпусу, зазвичай – просто речення, але це може бути і абзац або навіть ціла стаття. Субсемплірування - це процес вилучення найбільш частотних слів з аналізу, що прискорює процес навчання алгоритму і сприяє значному збільшенню якості отриманої моделі. По субреченням прохід здійснюється за допомогою вікна (розмір вікна задається алгоритмом як параметр). Під вікном мається на увазі максимальна дистанція між поточним і передбачуваним словом в реченні. Тобто, якщо вікно дорівнює трьом, то аналіз буде проходить всередині блоку в три слова. Рекомендоване значення вікна – 9.

На четвертому кроці алгоритму необхідно застосувати нейронну мережу прямого поширення з функцією активації ієрархічний софтмакс і/або негативне семплірування. Ієрархічний софтмакс краще веде себе при роботі з не дуже частотними словами, але працює повільніше, негативне семплірування краще працює з частотними словами і краще для вектора слів невеликої розмірності (50-100), працює швидше.

Задача побудови моделі Word2vec виглядає наступним чином: максимізація близькості векторів слів (скалярний добуток векторів), які з'являються поруч один з одним, і мінімізація близькості векторів слів, що не з'являються поруч один з одним. Тобто це відношення добутку близькості слів контексту і цільового слова на суму добутку близькості всіх інших контекстів і цільового слова.

Проблема в тому, що вважати усі слова контексту дуже довго і складно – контекстів може бути безліч для кожного слова.

Негативне семплірування – один із засобів впоратися із заданою проблемою. Принцип полягає в тому, що не враховуються всі можливі контексти, а вибираються випадковим чином кілька контекстів.

Метод GloVe, представлений на рис. 2, складається з двох етапів. На першому відбувається збір статистики появи слів в одному контексті, чого не відбувається в Word2Vec, і завдяки цьому показуються найкращі результати, в тому числі і в задачі пошуку аналогій. Словам, що знаходяться на більшій відстані, присвоюється штраф обернено пропорційний відстані. На другому етапі проводиться факторизація, яка називається негативним семплюванням [2-3].

Міра TF-IDF визначає важливість речення на основі частот слів, що входять в нього. При цьому для того, щоб не враховувати слова, які зустрічаються у всіх документах використовується зворотна частота документа IDF, яка дорівнює логарифму відношення кількості документів до кількості документів в яких вони зустрілися. Якщо слово часто зустрічається в даному документі, то міра TF-IDF збільшує вагу слова, і зменшує вагу слова, якщо слово часто зустрічається в багатьох документах.

На рис. 2 представлено результат обчислення векторного подання для слова formula методом GloVe.

formula_49 0.51952 0.36551 0.025452 -0.1951 -0.698 0.47093 1.0037 -0.71102 0.59568 0.4361 0.18142 0.74148 0.064232 -0.77135 -0.4859 0.098925 -0.38343 -0.26062 0.019739 -1.2724 -0.24354 0.48015 -0.052788 0.41563 0.23525 -0.26637 -0.29295 0.063295 -0.3241 0.33523 -0.28421 -0.47776 -0.25373 -0.49716 1.2665 -0.056948 -0.054321 -0.30834 -0.79601 0.41223 0.12801 -0.048872 -0.60556 -0.72225 0.025741 -0.2503 -0.27343 1.015 0.33405 -0.40708 0.61678 -0.22844 0.59156 0.052866 -0.00049725 0.072001 -0.32558 0.48756 -0.6016 0.14807 -0.24816 0.38507 -0.28583 -0.089611 0.081894 0.021572 -0.10213 0.13035 -0.19308 0.52014 -0.65474 0.086185 -0.296 0.035527 -0.36587 0.2201 -0.3063 -0.23909 -0.79859 -0.99602 0.148 0.32126 0.74175 -0.79598 -0.07167 -0.36708 -0.22583 -0.14502 -0.5132 -0.02999 -0.40754 0.41496 -0.58612 -0.94321 -0.51316 0.20841 0.26117 -0.24436 -0.13086 0.12595 0.09813 0.24711 0.73207 -0.086551 -0.58214 0.47236 0.64539 -0.68593 0.25126 0.5638 0.10715 -0.53064 -0.14665 0.35799 -0.14139 0.033978 0.60213 -0.10138 0.34922 -0.034818 0.25573 0.30483 0.10324 -0.04604 1.0471 0.070872 0.080445 -0.20606 -0.52216 0.3066 0.090441 -0.6725 0.32591 -0.097589 0.16465 -0.27029 0.30082 -0.28223 -0.29891 0.60578 0.13203 0.15553 -0.78966 -0.31467 -0.14415 -0.93517 -0.11302 -0.18034 0.93259 -0.029786 -0.59878 -0.44598 -0.5018 0.19715 -0.48042 -0.064742 -0.030131 0.069196 -0.3741 0.1785 -0.58733 0.80838 -0.18974 -0.44845 -0.25945 -0.051967 0.77687 -0.56301 0.2724 0.38876 0.068384 0.11919 1.3691 0.23131 0.5467 0.29358 0.21479 0.63916 -0.11962 -0.18311 -0.39951 -0.1359 -0.42035 -0.69039 0.10507 -0.31148 0.26122 0.81869 -0.24747 0.52537 -0.022141 -0.82681 -0.58131 -0.19134 0.30522 -0.091688 0.44055 0.95577 -0.7985 -0.63559 -0.2905 -0.59506 0.0067817 -0.026231 0.74042 -0.065419 -0.49075 0.07653 0.271 -0.084782 -0.26219 0.34771 0.75797 0.02177 -0.54897 0.56393 0.13951 -0.10005 -0.33486 0.26776 -0.47954 0.16444 -0.19718 -0.16358 -0.0443 -0.2064 0.26854 0.2619 0.49099 0.47061 0.50445 0.33096 0.59112 -0.34117 -0.53375 1.0249 0.069123 0.61091 -0.08862 0.69628 0.25573 0.12004 -0.80578 0.32404 1.0341 -0.53147 0.31703 0.076164 0.21104 0.15529 -0.64391 0.2069 -0.35442 -0.97081 -1.3846 1.1875 -0.12946 0.27918 -0.3457 -0.11953 0.40894 -0.67621 0.5759 0.62123 -0.13904 -0.064351 -0.18573 0.54623 0.78426 -0.052013 0.048598 -0.41228 -0.033042 -0.18561 -0.40321 0.74202 0.87619 0.074738 0.31938 0.62563 -0.66416 -0.066583 -0.41327 -0.43621 -0.49331 0.053018 0.17621 -0.50915 0.27515 -0.6763 0.26457 0.18884 0.35361 0.49686 -0.026109 -0.55791
0.14982 -0.39115 0.25823 0.56237

Рис.2. Результат обчислення методом GloVe

Вага деякого слова пропорційна кількості вживання цього слова в документі і обернено пропорційна частоті вживання слова в інших документах колекції [4,5].

Для розрахунку числового значення TF-IDF необхідно обчислити: число входжень і слова в документі, загальна кількість слів у документі, кількість документів в корпусі, кількість документів, в яких зустрічається і слово.

Відносна частота зустрічальності і слова в тексті d

$$\mathrm{TF}(w; d) = \frac{n_i}{\sum_k n_k} \qquad (1)$$

де n_i – число входжень і слова в документ, $\sum_k n_k$ – загальне число слів в документі.

Інверсна частота w в довільній безлічі текстів D

$$\mathrm{IDF}(w; D) = \log \frac{|D|}{|(d_i|w_i)|} \qquad (2)$$

де D – кількість документів в корпусі, $(d_i|w_i)$ – кількість документів в яких зустрічається і слово.

Вага або значимість TF-IDF(w;d;D) слова w є Wd тексту d в загально тематичної колекції текстів D визначається за формулою

$$\mathrm{TFIDF}(w; d; D) = \mathrm{TF}(w; d)*\mathrm{IDF}(w; D) \qquad (3)$$

На рис. 3 представлені важливості термів в тексті про художника Мікеланджело, тобто результати міри TF-IDF.

0.30153436667111 - работы
0.30153436667111 - микеланджело
0.150767183335555 - считал
0.150767183335555 - гениальным
0.100511455557037 - скульптором
0.100511455557037 - прихоти
0.100511455557037 - приходилось
0.100511455557037 - пап
0.100511455557037 - картиной
0.100511455557037 - знания
0.100511455557037 - закончить
0.100511455557037 - доказательства
0.100511455557037 - буонарроти
0.100511455557037 - анатомии
0.0924424752233507 - художника
0.0924424752233507 - считали
0.0616283168155671 - картина
0.0616283168155671 - заниматься
0.0502557277785183 - чувствовал
0.0502557277785183 - церкви
0.0502557277785183 - фрески
0.0502557277785183 - флоренцию
0.0502557277785183 - физической
0.0502557277785183 - успел
0.0502557277785183 - уехал

Рис.3. Результат обчислення мірою TF-IDF

Отримане векторне уявлення подається на рекурентну нейронну мережу з довгої короткостроковою пам'яттю (LSTM) представлену на рис. 4. Переваги такого підходу в тому, що довжина вхідного тексту не обмежена. Рекурентна нейронна мережа LSTM приймає вектор вхідних значень слів $\{x_1,x_2,\ldots,x_t\}$, виводить векторне уявлення h $\{h_1,h_2,\ldots,h_t\}$ вхідної послідовності.

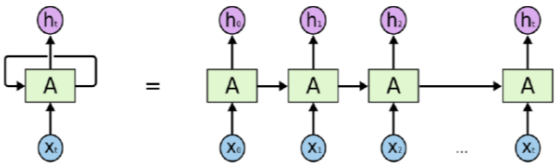


Рис.4.Рекурентна нейронна мережа з довгої короткостроковою пам'яттю розгорнута в часі

Мережа LSTM використовує механізм фільтрів. Цей механізм дає можливість регулювати надходження нової інформації в вектор стану c_t

мережі, а також висновок стану h_t мережі і оновлення її стану c_t. Вектори фільтрів мережі визначаються за такими формулами

$$i_t = \sigma(U_i \cdot x_t + W_i \cdot h_{t-1}) \quad (4)$$
$$f_t = \sigma(U_f \cdot x_t + W_f \cdot h_{t-1}) \quad (5)$$
$$o_t = \sigma(U_o \cdot x_t + W_o \cdot h_{t-1}) \quad (6)$$
$$C_t = \tanh(U_C \cdot x_t + W_C \cdot h_{t-1}) \quad (7)$$

де x – вхідна послідовність, h – вектор прихованого стану комірки мережі, U_i, U_f, U_o, U_C, W_i,W_f, W_o, W_C – матриці вагових коефіцієнтів фільтрів мережі i, f, o, g, індекс t – індекс елементу навчальної послідовності, i_t – вхідний вентиль, f_t – вентиль забування, o_t – вихідний вентиль, C_t – новий блок пам'яті, σ – сигмоїдальна функція активації , tanh – функція гіперболічного тангенса.

На підставі значень фільтрів мережі визначаються її вектор внутрішнього стану (внутрішньої пам'яті) і прихованого стану за такими формулами

$$c_t = \tanh(i_t \circ C_t + f_t \circ c_{t-1}) \quad (8)$$
$$h_t = \tanh(o_t \circ c_t) \quad (9)$$

де c_t – вектор внутрішнього стану комірки мережі, h_t – вектор прихованого стану комірки мережі, ∘ – операція по елементного добутку.

Оскільки значення вектора h_t мережі LSTM може виявитися більшим, внаслідок чого може виникнути насичення функції активації, яке призводить до малих значень похідної функції, що уповільнюють процес навчання мережі. Запобігти даний наслідок можна застосувавши функцію активації, яка не насичується. В результаті навчання мережі відбуватиметься швидше і точніше. Функція активації, заснована на логарифмах дозволяє уникати насичення при обробці великих значень і визначається формулою

$$f(x) = \begin{cases} \ln(x+1), x \geq 0 \\ -\ln(-x+1), x < 0 \end{cases} \quad (10)$$

Навчання мережі LSTM відбувається за допомогою методу зворотного поширення помилки. Алгоритм зворотного поширення помилки полягає в наступному: розрахувати вузел останнього рівня за формулою (11), розрахувати всі внутрішні вузли мережі за формулою (12), для всіх вузлів мережі обчислити зміни ваг по формулі (13) [6–9].

$$\delta_k = o_k(1 - o_k)(t_k - o_k), \quad (11)$$
$$\delta_j = o_j(1 - o_j) \sum_{k \in \text{Children}(j)} \delta_k w_{j,k}, \quad (12)$$
$$\Delta w_{i,j} = -\eta \delta_j o_j, \quad (13)$$

де $w_{i,j}$ – вага, яка стоїть на ребрі, що з'єднує i-й та j-й вузел, o_k – вихідний вузел останнього рівня мережі, o_j – вихід j-го вузла мережі; t_k – очікувану відповідь останнього рівня мережі, η – коефіцієнт навчання ($0 < \eta < 1$), δ_k – величина помилки на останньому рівні мережі, δ_j – величина помилки j-го вузла мережі.

Тестування системи здійснюється на корпусі текстів. Результат роботи системи представлено на рис. 5.

III. ВИСНОВОК

Система приймає текст, обробляє його і виводить короткий виклад поданого тексту. Перевагою рішення є здатність до автоматизованого самовдосконалення з мінімальним втручанням людини. Аналізуючи роботу системи можна відзначити, що нейронна мережа показала найкращий результат автоматичного реферування при векторному подані методом GloVe. Система недостатньо якісно реферує тексти великого обсягу, тому передбачено застосувати модифікацію з використанням не насичуючої функції активації засновану на логарифмах.

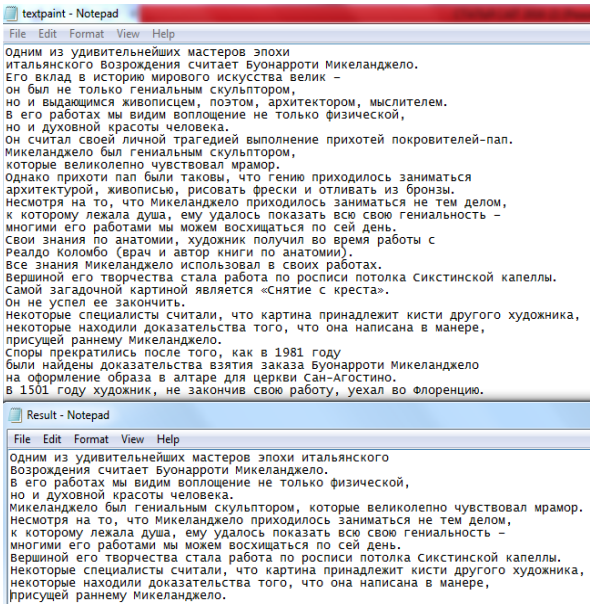


Рис.5.Тестування системи

ЛІТЕРАТУРА

[1] Abstract and summarizing. [Online]. Available: http://poznayka.org/s39440t1.html

[2] Word2Vec [Online]. Available: https://www.slideshare.net/HyunYoungLee3/word2-vec-81790245

[3] A Comprehensive Introduction to Word Vector Representations [Online]. Available: https://medium.com/ai-society/jkljlj-7d6e699895c4

[4] TF-IDF [Online]. Available: https://seonomad. net/slovar/tf-idf

[5] Spinareva I. M., Gerenko O.A, Morozova K. Y., "Classification of Texts in Natural Language by Neural Network", Issue. № 59. Collection of scientific works of the Military Institute of the Kyiv National University named after. T. Shevchenko - K .: VIKNU, 2018, p. 171-177

[6] I.D. Chernobayev, A.S. Surkov, A.Z. Pankratova (2018). Simulation of texts using recurrent neural networks [Online]. Available: http://old.nntu.ru/trudy/2018/01/065-073.pdf

[7] Recurrent neural networks in text analysis problems [Online]. Available: http://docplayer.ru/42578505-Rekurrentnye-neyronnye-seti-v-zadachah-analiza-tekstov.html

[8] LSTM - network of long short-term memory [Online]. Available: https://habr.com/company/wunderfund/blo g/331310/

[9] Huiting Zheng, Jiabin Yuan, Long Chen. (2017). Short-Term Load Forecasting Using EMD-LSTM Neural Networks with a Xgboost Algorithm for Feature Importance Evaluation [Online]. Available: http://www. mdpi.com/1996-1073/10/8/1168

Моделювання безпровідних сенсорних мереж для дослідження впливу типів маршрутизації на часові мережеві характеристики

Дарія Бондар
кафедра автоматизованих систем управління Національний університет «Львівська політехніка»
Львів, Україна
dasbu34@gmail.com

Ольга Федевич
кафедра автоматизованих систем управління Національний університет «Львівська політехніка»
Львів, Україна
olhafedevych@gmail.com

Іванна Дронюк
кафедра автоматизованих систем управління Національний університет «Львівська політехніка»
Львів, Україна
ivanna.m.droniuk@lpnu.ua

Квітослава Обельовська
кафедра автоматизованих систем управління Національний університет «Львівська політехніка»
Львів, Україна
obelyovska@gmail.com

Simulation of wireless sensor networks to investigate the routing types impact on network time characteristics

Daria Bondar
Automated Control Systems Department Lviv Polytechnic National University
Lviv, Ukraine
dasbu34@gmail.com

Olga Fedevych
Automated Control Systems Department Lviv Polytechnic National University
Lviv, Ukraine
olhafedevych@gmail.com

Ivanna Droniuk
Automated Control Systems Department Lviv Polytechnic National University
Lviv, Ukraine
ivanna.m.droniuk@lpnu.ua

Kvitoslava Obelovska
Automated Control Systems Department Lviv Polytechnic National University
Lviv, Ukraine
obelyovska@gmail.com

***Abstract*— Дослідження, аналіз та вдосконалення безпровідних сенсорних мереж є актуальною задачею. В даній роботі об'єктом досліджень є безпровідні сенсорні мережі, що відповідають стандарту IEEE 802.15.4. Досліджувався вплив типу маршрутизації (WiseRoute і Flooding) на часові показники безпровідної сенсорної мережі. Маршрутизація WiseRoute базується на використанні дерева маршрутів, що не допускає наявності петель, Flooding – це маршрутизація, при якій кожний пакет відсилається всім сусіднім вузлам, за винятком того вузла звідки він прийшов. Проведене дослідження показало, що збільшення кількості вузлів у безпровідних сенсорних мережах суттєво погіршує їх часові характеристики, як при використанні маршрутизації типу Flooding, так і при маршрутизації WiseRoute. При цьому використання маршрутизації типу WiseRoute в розглянутих нами прикладах мережі погіршувало часові показники мережі на (10 – 20) % порівняно з використанням маршрутизації Flooding. Позитивний вплив від використання маршрутизації Flooding порівняно з маршрутизацією типу WiseRoute більше проявляється у мережах з малою кількістю вузлів і з збільшенням кількості вузлів зменшується. Дослідження проводились за допомогою програмного засобу OMNeT++ та фреймоворку MiXiM.**

***Abstract*— Investigation, analysis and improvements of wireless sensor networks are of high importance nowadays. In given paper IEEE 802.15.4 wireless sensor networks are targeted. Impact of routing type (WiseRoute or Flooding) on network time characteristics was investigated. WiseRoute uses routes tree with no loops allowed. Flooding sends every packet to each neighbor node, except the sender node. Investigation shows that increase of network nodes number results in significant degradation of wireless sensor network time characteristics. This is true for both WiseRoute and Flooding routing. For the reviewed case studies WiseRoute shows a (10 – 20) % worse time characteristics comparing to Flooding. The positive effect from using Flooding is higher for the networks with smaller number of nodes and decreases as number of nodes grows up. Investigation was performed using OMNeT++ software and MiXiM framework.**

Keywords—безпровідні сенсорні мережі, сітчаста топологія, маршрутизація

Keywords—wireless sensor networks, mesh topology, routing

I. Вступ

Новітні інформаційні технології, що запроваджуються в виробництво та різні сфери людської діяльності, все частіше для передавання даних використовують безпровідне фізичне середовище. В останні роки у зв'язку з активним впровадженням Інтернету речей IoT (Internet of Things) особливо стрімкого росту зазнали безпровідні сенсорні мережі [1].

На сьогодні сенсорні безпровідні мережі вивчені ще не достатньо. Крім того сфера їх застосування постійно розширюється, вимоги до експлуатаційних характеристик підвищуються. Різні прикладні

застосування ставлять різні вимоги до конкретних показників сенсорних мереж. В зв'язку з цим важливим і актуальним є дослідження, аналіз та вдосконалення безпровідних сенсорних мереж.

В [2] наведені як комерційні, так і безкоштовні системи моделювання, які дають можливість провести моделювання безпровідної сенсорної мережі будь-якої складності.

В даній роботі об'єктом досліджень є безпровідні сенсорні мережі, що відповідають стандарту IEEE 802.15.4. Архітектура безпровідної сенсорної мережі, що досліджувалась, у відповідності з [3] показана на рис. 1.

Протоколи мережевого та прикладного рівнів відповідають специфікації ZigBee. Технологія ZigBee при невеликому енергоспоживанні підтримує сітчасту топологію з ретрансляцією і маршрутизацією повідомлень та надає можливість вибору алгоритму маршрутизації.

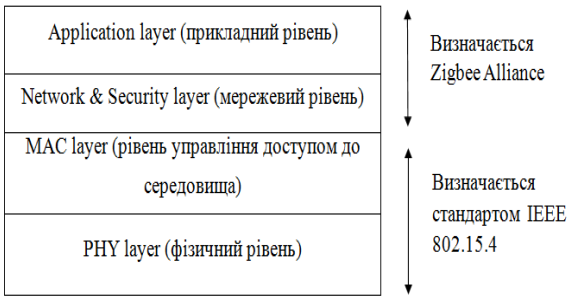


Рис.1.Архітектура безпровідних сенсорних мереж IEEE 802.15.4/ Zigbee

Маршрутизація має значний вплив на ряд характеристик безпровідної сенсорної мережі, про що свідчить велика кількість публікацій, присвячених аналізу впливу маршрутизації в різних мережах на різні експлуатаційні характеристики мереж. Одним з найважливіших параметрів, який є об'єктом дослідження різних безпровідних мереж, є затримки пакетів [4], нами досліджувався вплив типів маршрутизації (WiseRoute і Flooding) на часові показники сенсорних безпровідних мереж. Маршрутизація WiseRoute базується на використанні дерева маршрутів, що не допускає наявності петель, Flooding - це маршрутизація, при якій кожний пакет відсилається всім сусіднім вузлам, за винятком вузла звідки він прийшов.

II. Характеристика програмного забезпечення для комп'ютерного імітаційного моделювання роботи мережі

На сьогоднішній день відомою є досить велика кількість комерційних та вільно доступних програмних симуляторів комп'ютерних мереж. Ці всі різновиди програмного забезпечення мають свої переваги та недоліки, а також області застосування та популярність серед користувачів. Найбільшої уваги, з точки зору функціональних можливостей та фінансової доступності, заслуговують наступні: 1) J-Sim [5], 2) OMNeT++ [6], 3) NS-2 [7].

1) J-Sim – середовище для комп'ютерного імітаційного моделювання мереж, створене за допомогою мови програмування Java. Програмне забезпечення є компонентно-орієнтованим, у ньому будь-які об'єкти можуть відігравати роль компонентів: з'єднання, протокол, комп'ютер. Враховуючи цю властивість, кожен обраний компонент може бути як цілісним, так і складатись з довільної кількості інших компонентів. З'єднання між компонентами встановлюється з допомогою змодельованих портів. Доступними для використання є три типи з'єднань для портів. До моделі можна додавати власноруч створені компоненти, або використовувати існуючі компоненти, чи перевизначати їхні атрибути та методи за допомогою мови програмування Java.

2) OMNeT++ - це пакет програмного забезпечення, який є якісним інструментом для імітаційного моделювання роботи комп'ютерних мереж. OMNeT++ має в своєму розпорядженні ресурси для побудови комп'ютерних мереж різного масштабу та різної архітектури і топологій [8]. Це програмне забезпечення має велику базу даних мережевих елементів, готових до використання, які вже містять алгоритми моделювання та етапи обробки інформації про комп'ютерну мережу,

3) Середовище для імітаційного моделювання NS-2. Було створене за допомогою двох мов програмування C++ та OTcl. Остання дає змогу інтерпретувати сценарії роботи комп'ютерної мережі.

Для завдань моделювання безпровідних мереж оптимальним є середовище OMNeT++, оскільки воно дає змогу графічно візуалізовувати отримані результати, а також спостерігати за зміною параметрів імітаційного моделювання комп'ютерної мережі, що є необхідним для якісного оцінювання результатів короткострокового прогнозування пульсацій трафіку.

Дослідження проводились за допомогою програмного засобу OMNeT++ та фреймоворку MiXiM.

III. Моделювання мережі

Об'єктом моделювання була сітчаста мережа з різною кількістю станцій. Рис. 2 ілюструє безпровідну сенсорну мережу з 10-ма стаціонарними вузлами. Територія, на якій розгорталась мережа – 300 м х 300 м, інтенсивність трафіку – 1 пакет на секунду.

Всі пристрої використовують стандарт IEEE 802.15.4 (mixim.modules.node.Host802154) і Zigbee на мережевому рівні (netwLayer = 'Zigbee').

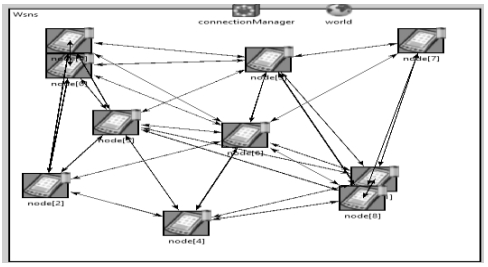


Рис.2. Безпровідна сенсорна мережа з 10-ма стаціонарними вузлами

Результати моделювання показали, що використання маршрутизації типу Flooding забезпечило кращі часові показники ніж використання маршрутизації типу WiseRoute.

Конкретні значення зменшення часових показників за рахунок вибору типу маршрутизації можуть бути визначені шляхом моделювання мережі, що досліджується, при заданих умовах її функціонування.

У мережі наведеного прикладу з 10-ма стаціонарними вузлами при застосуванні маршрутизації WiseRoute середнє значення максимальної затримки приблизно на 20 % більше ніж при використанні маршрутизації Flooding (рис.3).

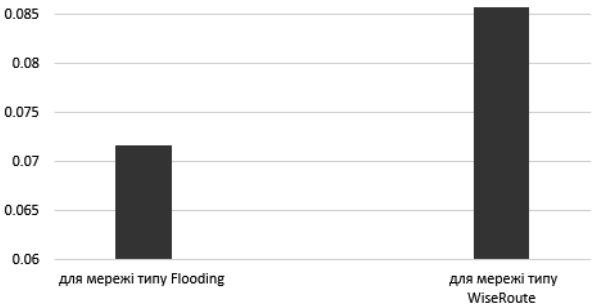


Рис.3.Середнє значення максимальної затримки для мереж з різним типом маршрутизації

Проаналізуємо вплив на даний ефект кількості вузлів в мережі. Для цього аналогічне дослідження проведено для мережі з 30-ма та 60-ма вузлами.

Результати моделювання, що показують значення максимальної затримки у вузлах мережі з 10-ма, 30-ма та 60-ма стаціонарними вузлами, при використанні маршрутизації типу Flooding показані на рис. 4.

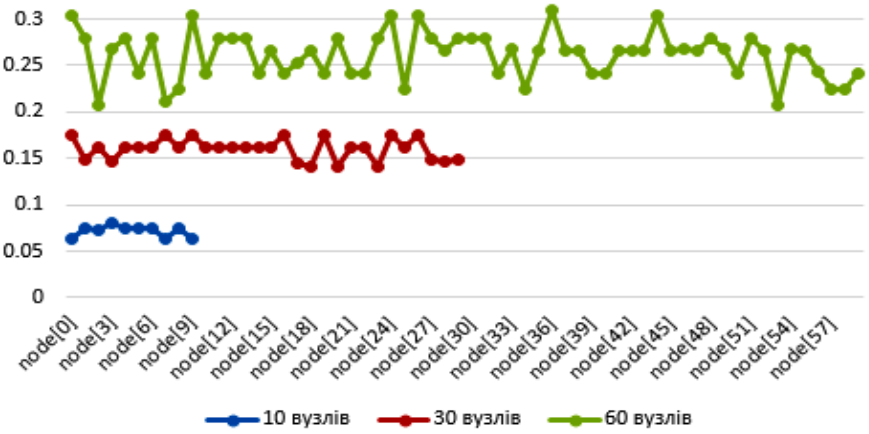


Рис.4.Максимальна затримка в вузлах мережі з маршрутизацією типу Flooding при кількості вузлів рівній 10, 30 та 60

Результати моделювання, що показують значення максимальної затримки у вузлах мережі типу WiseRoute з 10-ма, 30-ма та 60-а вузлами показані на рис. 5.

Середні значення максимальних затримок для мереж з різною кількістю вузлів при застосуванні маршрутизації WiseRoute та Flooding показані на діаграмі рис. 6.

Як видно з результатів, зі збільшенням кількості вузлів в мережі затримки суттєво зростають. При збільшенні кількості вузлів з 10 до 30 середнє значення максимальної затримки зростає дещо більше ніж в 2 рази, а при збільшенні кількості вузлів з 10 до 60 - дещо більше ніж в 3 рази. Проте вплив типу маршрутизації на погіршення часових показників навпаки є більшим в мережах з меншою кількістю вузлів. Якщо заміна маршрутизації Flooding на WiseRoute в безпровідній сенсорній мережі з 10 вузлами привела до збільшення середнього значення максимальної затримки на 19,6 %, то в мережі з 30 вузлами – на 15,3 %, а в мережі з 60 вузлами – на 9,2 %.

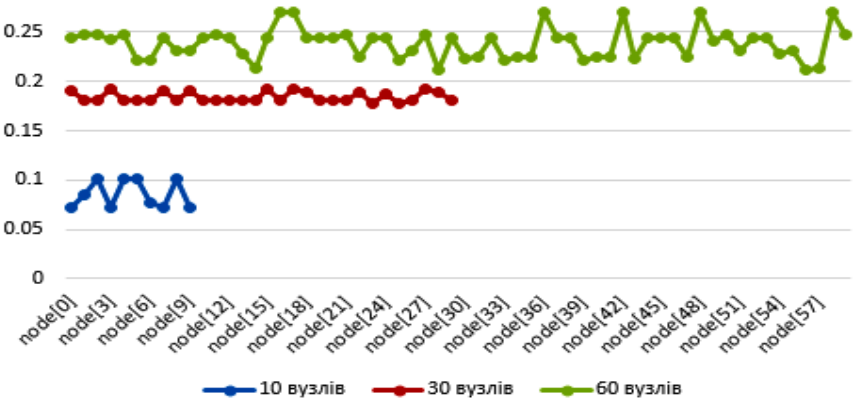


Рис.5. Максимальна затримка в вузлах мережі з маршрутизацією типу Wise Route при кількості вузлів рівній 10, 30 та 60

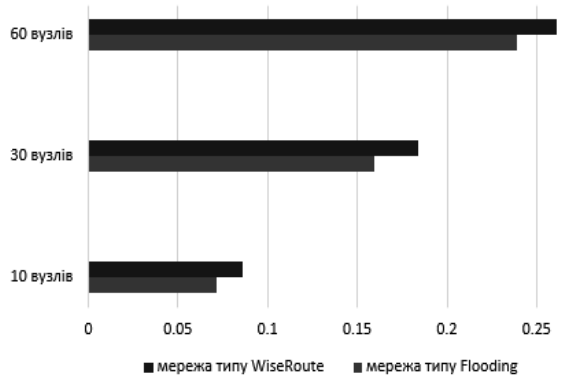


Рис.6. Середнє значення максимальної затримки для мереж з різним типом маршрутизації та різною кількістю вузлів

Результати моделювання показали, що з точки зору часових мережевих показників в усіх розглянутих прикладах маршрутизація типу Flooding дає кращі результати ніж маршрутизація типу WiseRoute. Слід відзначити, шо у процентному вимірі виграш від використання маршрутизації Flooding є більш значимий для безпровідних сенсорних мереж з меншою кількістю вузлів.

IV. Висновки

Проведене дослідження показало, що збільшення кількості вузлів у безпровідних сенсорних мережах суттєво погіршує їх часові показники, як при використанні маршрутизації типу Flooding, так і при маршрутизації WiseRoute. При цьому використання маршрутизації типу Flooding може забезпечити кращі часові показники ніж використання маршрутизації типу WiseRoute. Проте позитивний вплив від використання маршрутизації Flooding порівняно з маршрутизацією типу WiseRoute більше проявляється у мережах з малою кількістю вузлів і з збільшенням кількості вузлів зменшується.

Статтю підготовано за результатами виконання спільного українсько-австрійського науково-дослідного проекту "Моделювання трафіку і телекомунікаційних мереж".

ЛІТЕРАТУРА

[1] В.О. Власенко, “Методи побудови безпровідних сенсорних мереж”, Зв'язок, №2, 2017, С. 42-46.

[2] І.Б. Галелюка “Моделювання бездротових сенсорних мереж”, Комп'ютерні засоби, мережі та системи. № 14, 2015, С. 141-150.

[3] A. Cunha, A. Koubia, R. Severino, M. Alves, “Open-ZB: an open-source implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS”, 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASSI07), Pisa, Italy, October 2007, pp.1-12.

[4] M. Laner, J. Fabini, P. Svoboda, M. Rupp "End-to-end Delay in Mobile Networks: Does the Traffic Pattern Matter?"; Talk: ISWCS'13, Ilmenau, Germany; 08-26-2013 - 08-30-2013; in: "Proceedings of ISWCS'13", (2013), 5 pages.

[5] A. Sobeih et al, “An Integrated Environment for Simulation and Model Checking of Network Protocols”, Proceedings of the Parallel and Distributed Processing Symposium, CA, 2007, P.1-6.

[6] A. Varga “Ommet++ - discrete event simulation system”, Proceedings of the European Simulation Multiconference, 2001.

[7] DARPA/NSF. The network simulator - ns-2[Online]. Available: http://www.isi.edu/nsnam/ns/.

[8] J. N. Nurminen “Using software complexity measures to analyze algorithms - an experiment with the shortest-paths algorithms”, In Computers & Operations Research. Elsevier Science, 2003, pp 1121-1134.

REFERENCES

[1] V.O. Vlasenko, “Wireless sensor networks Construction Methods”, Zviazok, №2, 2017, C. 42-46. (In Ukrainian)

[2] I.B. Galeluka “Modelling of Wireless sensor networks”, Computer tools, networks and systems. № 14, 2015, C. 141-150. . (In Ukrainian)

[3] A. Cunha, A. Koubia, R. Severino, M. Alves, “Open-ZB: an open-source implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS”, 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASSI07), Pisa, Italy, October 2007, pp.1-12.

[4] M. Laner, J. Fabini, P. Svoboda, M. Rupp "End-to-end Delay in Mobile Networks: Does the Traffic Pattern Matter?"; Talk: ISWCS'13, Ilmenau, Germany; 08-26-2013 - 08-30-2013; in: "Proceedings of ISWCS'13", (2013), 5 pages.

[5] A. Sobeih et al, “An Integrated Environment for Simulation and Model Checking of Network Protocols”, Proceedings of the Parallel and Distributed Processing Symposium, CA, 2007, P.1-6.

[6] A. Varga “Ommet++ - discrete event simulation system”, Proceedings of the European Simulation Multiconference, 2001.

[7] DARPA/NSF. The network simulator - ns-2 [Online]. Available: http://www.isi.edu/nsnam/ns/.

[8] J. N. Nurminen “Using software complexity measures to analyze algorithms - an experiment with the shortest-paths algorithms”, In Computers & Operations Research. Elsevier Science, 2003, pp 1121-1134.

Методологія представлення соціальних проектів IT-індустрії

Тетяна Філатова
кафедра економічної кібернетики та інформаційних технологій
Одеський національний політехнічний університет
Одеса, Україна
filatova.321@gmail.com

Олексій Чернишов
кафедра системного програмного забезпечення
Одеський національний політехнічний університет
Одеса, Україна
oleksii.chernyshov@outlook.com

Methodology for the presentation of social projects in the IT industry

Tetiana Filatova
Department of Economic Cybernetics and Information Technologies
Odessa National Polytechnic University
Odessa, Ukraine
filatova.321@gmail.com

Oleksii Chernyshov
Department of Economic Cybernetics and Information Technologies
Odessa National Polytechnic University
Odessa, Ukraine
oleksii.chernyshov@outlook.com

***Анотація*—У даній роботі розглядається такий напрямок дослідження як методологія розробки та подання соціальних проектів IT-сфери. У сучасному світі створення і реалізація соціальних проектів стає невід'ємною частиною суспільства. Методологія визначення необхідного і корисного державі проекту дозволяє представити не тільки допомогу в рішенні різного роду завдань, а й здійснює уявлення соціального проекту IT-індустрії з найменшими витратами часу і впевненістю в актуальності і подальше використання даного проекту. Кожен проект будується з безлічі компонентів. У статті виділені основні аспекти, найбільш важливі при створенні нового соціального проекту. Складність полягає в необхідності різностороннього підходу, безліч фрагментів якого залежать виключно від обраної ідеї, цільової аудиторії, бізнес-моделі, команди і наявних початкових ресурсів. Розробка соціального проекту із застосуванням інформаційних технологій несе комплексний характер, який об'єднує підходи до створення, як програмного продукту, так і громадського нововведення. Подібні проекти повинні мати всі переваги підходів нових технологічних проектів, володіти масштабністю і гнучкістю системи, застосовувати нові види бізнес-моделей і підходів до проектування та розробки нових програмних продуктів на споживчому ринку.**

***Abstract*—In the given work, the methodology of development and presentation of social projects of IT-sphere are investigated. Nowadays, creation and realization of social projects becomes an integral part of society. The methodology of determining the necessary and useful state of the project provides not only assistance in solving various tasks, but also allows to implement projects of IT-industry with the least time and confidence in the relevance of this project. Each project is built from many components. The article highlights the main aspects that are most important when creating a new social project. The difficulty lies in the need for an integrated approach, with a multitude of fragments dependent solely on the chosen idea, target audience, business model, team and available initial resources. The development of such projects combines the creation of both the software product and the public innovation. Such projects should have all the advantages of the approaches of new technological projects, have the scalability and flexibility of the system, apply new types of business models and approaches to the design and development of new software products on consumer market.**

Ключові слова— проект; соціальний проект; ідея; програмний продукт; IT -область.

Keywords—project, social project, idea, software, IT-area

I. Визначення соціального проекту у сфері IT-індустрії

У сучасному світі створення і реалізація соціальних проектів стає невід'ємною частиною суспільства. Методологія визначення необхідного і корисного державі проекту дозволяє надати не тільки допомогу в рішенні різного роду завдань, а й здійснює уявлення соціального проекту IT-індустрії з найменшими витратами часу і впевненістю в актуальності і подальшому використанні даного проекту.

Для того, щоб визначити яким чином створити, уявити і реалізувати подібного роду проект, необхідно визначити основні етапи, які необхідно пройти від виникнення ідеї до реалізації.

Інформаційні технології в наш час здатні значно покращити життя людей. Забезпечивши нові підходи до соціальних проектів, можна значно підвищити їх ефективність і досягти нового рівня соціальної залученості громадян.

Соціальний проект - це реалізація ідеї, корисної для суспільства: країни, міста, людей і т.п. Соціальний проект в сфері інформаційних технологій має на увазі розробку інформаційної системи, програмного продукту, який має характерну суспільну цінність.

Визначення соціального проекту, концепції реалізації проектів в сфері інформаційних технологій розглянуті і представлені різними авторами і

дослідниками [1]. Крім цього, важливе значення приділяється універсальним принципам розгляду чи створення будь-яких проектів різних сфер життя, до яких може бути застосована єдина методологія [2]. Проаналізувавши існуючі проекти в області соціального спрямування, можна прийти до висновку про те, що в даний момент є актуальним розвиток громадських проектів в сфері інформаційних технологій. Мета їх створення не тільки допомога навколишнього світу в певних завданнях, а й надання послуг в цій сфері.

II. ОСНОВНІ АСПЕКТИ СОЦІАЛЬНИХ ПРОЕКТІВ

Розробка подібних проектів об'єднує в собі створення, як програмного продукту, так і громадського нововведення. Складність полягає в необхідності комплексного підходу, безліч фрагментів якого залежать виключно від обраної ідеї, цільової аудиторії, бізнес-моделі, команди і наявних початкових ресурсів.

Як приклад соціального-проекту в IT-області у статті приведено проект Helpy, що пройшов шлях від ідеї до реалізації у рамках проекту “Програміст 2018” та “Social IT” та являє собою волонтерську платформу [3].

Кожен проект будується з безлічі компонентів. Виділимо основні аспекти важливі при створенні нового соціального проекту:

- Ідея - при створенні будь-якого проекту, важливо визначити і проаналізувати те, для кого розробляється продукт, які є конкуренти на ринку і які переваги будуть у даного продукту в порівнянні з іншими;
- Команда - важливо, щоб учасники команди були зацікавлені метою проекту і активно брали участь в його розвитку, а також мали необхідні компетенції;
- Технічна реалізація - це стек технологій та принцип їх застосування, повністю залежить від ідеї проекту, навичок команди, початкових коштів і стратегії подальшого розвитку;
- Модель фінансування (бізнес модель) - при проектуванні потрібно виділити яким чином проект буде забезпечуватися необхідними засобами, що сприяють розвитку і підтримці проекту.

III. ЕТАПИ ВИЗНАЧЕННЯ ТА СТВОРЕННЯ IT-ПРОЕКТУ

Для створення будь-якого проекту необхідна команда зацікавлених в ідеї фахівців, або людей, які готові вчитися в процесі розробки. Формування команди - це важливий етап створення проекту і в випадках, коли кінцевих вимог до проекту не існує, першим етапом створення будь-якого соціального проекту є визначення команди.

У реальних умовах, початкова концепція проекту повинна формуватися перед збором команди. Для визначення актуальної теми необхідно скласти список з можливих ідей для розроблюваного проекту, наприклад, в ході мозкового штурму. Далі складаються критерії оцінки, які включають актуальність, соціальність і фінансові перспективи, а також включаються особисті переваги учасників команди. В результаті відбираються ідеї з максимальними показниками і, в ході дискусії, з них вибирається фінальна ідея проекту. На рис. 1 зображений макет, який дозволяє визначити експертним шляхом найбільш значимий проект. Подібну методику можна розглядати в різних предметних областях [2].

Название	Критерий 1	Критерий 2	...	Оценка по критерию 1	Оценка по критерию 2	...	Субъективная оценка (макс. 5)					Итог
							ФИО 1	ФИО 2	ФИО 3	ФИО 4	...	
Название 1	Описание 1.1	Описание 2.1	...	!оценка	!оценка	...	!оценка	!оценка	!оценка	!оценка	...	!сумма
Название 2	Описание 1.2	Описание 2.2	...	!оценка	!оценка	...	!оценка	!оценка	!оценка	!оценка	...	!сумма
...	...	...	...	...	...	...	...	...	...	...	...	...

Рис. 1. Макет експертного визначення вибору проекту

Варто відзначити, що підсумкова сума балів визначається формулою суми, по якій надалі ранжуються ідеї проектів. Лідером команди, або призначеним довіреною особою, визначаються критерії оцінки. Крім критеріїв оцінки, можна враховувати персональні оцінки команди, якщо її число дозволяє, тоді відповідальна особа повинна визначити скільки балів виділяється на кожен критерій і на кожного учасника. Результат відсортованої таблиці ідей представлений на прикладі проекту Helpy (див.рис. 2).

Коли ідея обрана, всі сили йдуть на продумування її концепції, що включає: визначення цільової аудиторії, бізнес-моделі, технічної реалізації, конкурентного аналізу та стратегії, яка визначає масштабованість, що має на увазі автоматизованість ключової діяльності проекту, і найближчі плани проекту. Для допомоги в цьому процесі зазвичай вдаються до підтримки менторів, людей з досвідом в тій, чи іншій сфері, пов'язаної з розробкою продукту, включаючи технічну реалізацію, монетизацію, дизайн, маркетинг і т.д.

Название	Описание	Бизнес-модель	Соц. значимость	Бизнес-модель	Субъективная оценка (макс. 5)				Итог
					A	C	B	K	
A Волонтёрская платформа	Наши клиенты - волонт	Проценты от оплаты деньгам	10	8	5	5	5	5	38
A Помощник для глухих	Приложение помогающ	Покупка приложения, и/или о	10	7	5	4	5	3	34
A Аналитик рынка труда	Сервис анализа рынка	Колаборации с компаниями,	9	7	5	5	4	3	33
K Поиск ближайшей помощи	Поиск волонтеров (мен	Процент с транзакций	10	7	4	3	4	4	32
O Сервис сдача в аренду снаряжения	Сервис который способ	Процент с аренды	7	7	5	2	5	4	30
A Трекер маршруток	Разработка приложени	Месячная подписка для клие	7	8	4	5	4	2	30
A Сервис оценки врачей и мед. учреж		Рейтинговая платформа	Реклама	8	6	5	3	4	3	29
B Сервис поиска работы для студенто		Платформа для поиска	Реклама, процент от компани	7	7	5	2	5	3	29
A Научное питание	Подбор диет по особен	Подписка (без рекламы, офф	8	9	4	5	1	2	29

Рис. 2. Результат представлення ідей проекту Helpy

Цільова аудиторія допомагає виділити необхідний функціонал проекту і його інформаційного продукту, також хороше розуміння споживача дозволяє визначити правильну бізнес-модель, технічну реалізацію і продумати стратегію розвитку. Конкурентний аналіз дозволяє більш наочно виділити слабкі і сильні сторони на ринку, що наочно показує, які сторони проекту необхідно покращувати. Для конкурентного аналізу досить виділити лідерів ринку і їх ключові сильні і слабкі сторони. Приклад

конкурентного аналізу запропонованого проекту Helpy представлений на рис. 3.

	Связь без посредников	Широкий охват аудитории	Публичный профиль
Helpy	+	+	+
IT-Volunteer	+	-	+
Ukrainian Volunteer service	-	+	-

Рис. 3. Конкурентний аналіз IT проекту Helpy

Бізнес-модель проекту може бути заснована на наступних принципах:

- Некомерційний підхід [4, Стаття 1] - підхід, який базується на сфері волонтерства, де всі витрати покриваються за рахунок благодійності; часто застосовується в класичних соціальних проектах, але робить проект вкрай залежним від людей і не надає належних ресурсів для підтримки технологічного проекту;
- Некомерційний підхід із залученням грантів і / або фінансування [4, Стаття 6] - підхід має на увазі існування проекту за рахунок грантів, або інвестицій від зацікавлених осіб; дозволяє розвиватися проекту в рамках, встановлених інвестором, що забезпечує підтримку, але і безліч обмежень, що стримують зростання проекту, або схиляють його розвиток у вигідне вкладнику русло;
- Комерційний підхід [5] - підхід, базується на наданні платних послуг; цей підхід здатний належним чином здатний забезпечити необхідними ресурсами технологічний проект, але вимагає наявності значного стартового капіталу і досвіду в створенні бізнесу;
- Комерційний підхід із залученням грантів і / або фінансування [5] - підхід, базується на наданні платних послуг з залученням інвесторів; незначний контроль над процесами організації, компенсується менторської допомогою, що надається інвесторами.

Основний етап - це розробка фінального продукту. Це комплексний процес, який вимагає належних знань технологій, а також вміння та досвіду проектування програмного забезпечення та управління ресурсами компанії. Цей етап може кардинально відрізнятися в залежності від обраної ідеї, бізнес моделі, команди і наявних фінансових ресурсів.

IV. РЕЗУЛЬТАТИ ПРЕДСТАВЛЕННЯ СОЦІАЛЬНОГО ПРОЕКТУ ІТ-ІНДУСТРІЇ

Результатом опису представленої методології може бути публічна платформа для волонтерів та організаторів Helpy, яка пройшла через всі описані етапи і отримала визнання фахівців в IT-області. Розроблений проект Helpy реалізований в рамках проекту Social IT і може зазнавати подальший розвиток і впровадження на базі створеного продукту.

Розробка соціального проекту із застосуванням інформаційних технологій несе комплексний характер, який об'єднує підходи до створення, як програмного продукту, так і громадського нововведення. Подібні проекти повинні мати всі переваги підходів нових технологічних проектів, володіти масштабністю і гнучкістю системи, застосовувати нові види бізнес-моделей і підходів до проектування та розробки нових програмних продуктів на споживчому ринку

ЛІТЕРАТУРА

[1] Пальчук В. Соціальні інформаційні комунікації і розвиток діяльності сучасних інформаційних центрів / В. Пальчук // Наукові праці V. I. Vernadsky National Library of Ukraine. - 2017. - Вип. 46. - С. 74-91. - Режим доступу: http://nbuv.gov.ua/UJRN/npnbuimviv_2017_46_7.

[2] Филатова Т. В. Модели формализованного сопоставления степени соответствия образовательно-квалификационных уровней для вузов различного уровня аккредитации // Матеріали міжнародної українсько-японської конференції з питань науково-промислового співробітництва, Том 2; 24—25жовтня 2013 р. — Одесса: ОНПУ, 2013. – 27 с.

[3] Новини благодійного фонду Колесникова // Результати благодійного проекту “Програміст 2018” — Київ: Фонд Бориса Колесникова, 2018. – 1с. – Режим доступу: http://kolesnikovfund.org/ru/news/1652.

[4] Закон України Про благодійну діяльність та благодійні організації від 06.11.2016 // Відомості Верховної Ради (ВВР), 2013, № 25, ст.252 – Режим доступу: http://zakon3.rada.gov.ua/laws/show/5073-17

[5] Ігнатович Неллі Іванівна, Гура Вікторія Леонідівна Зарубіжний досвід розвитку соціального підприємництва // Вісник Київського національного університету ім. Тараса Шевченка. Серія: Економіка. 2014. №165.

REFERENCES

[1] Palchuk, V. Social Information Communications and the Development of the Activity of Modern Information Centers. Naukovi pratsi Natsionalnoi biblioteky Ukrainy imeni V. I. Vernadskoho – Transactions of V. I. Vernadsky National Library of Ukraine, issue 46, pp. 74-91, 2017. Kyiv [in Ukrainian].

[2] Filatova T.V. Models of compare extent of matching to educational levels for universities of various levels of accreditation. Materials of international Ukrainian-Japanese Conference on question of Scientific and Industrial Cooperation (from October, 24th, to October, 25th, 2013), Odessa National Polytechnic University, part 3, pp. 27-29, [in Russian].

[3] The Boris Kolesnikov Foundation. (2018). “ The result of the beneficent project "Programmer 2018” [Online]. Available: http://kolesnikovfund.org/ru/news/1652.

[4] Zakon Ukrainy pro blagodiynu diyalnist ta blagodiyni jhganizatcii vid 06.11.2016 [Online]. Available: http://zakon3.rada.gov.ua/laws/show/5073-17

[5] N. Ignatovich, V. Gura. Zarubizhniy dosvid rozvitku sotsialnogo pidpriemnitstva. VIsnik Kiivskogo natsionalnogo universitetu im. Tarasa Shevchenka. Seriya: Ekonomika, vol.165, 2014.

Трійкові логічні та арифметичні пристрої на основі багатопорогового елемента багатозначної логіки

Юрій Гунченко,
Олександра Уханова
кафедра математичного забезпечення комп'ютерних систем
Одеський національний університет ім. І.І. Мечникова
Одеса, Україна
gunchenko@onu.edu.ua

Сергей Шворов
кафедра автоматики та робототехнічних систем
Національний університет біоресурсів і природокористування України
Київ, Україна
sosdok@i.ua

Юрій Берков
кафедра системного програмного забезпечення та технологій дистанційного навчання
Одеський національний університет ім. І.І. Мечникова
Одеса, Україна
bercov68@gmail.com

Ternary logical and arithmetic devices based on the multi-threshold element of multiple-valued logic

Yurii Gunchenko,
Oleksandra Ukhanova
dept. of Mathematical Support of Computer Systems Odessa I.I.Mechnikov National University
Odessa, Ukraine
gunchenko@onu.edu.u

Sergey Shvorov
dept. of Automation and Robotic Systems
National University of Life and Environmental Sciences of Ukraine
Kyiv, Ukraine
sosdok@i.ua

Yurii Bercov
dept. of the system software and technologies of distance learning
Odessa I.I.Mechnikov National University
Odessa, Ukraine
bercov68@gmail.com

***Анотація*—В роботі розглядається проблема побудови логічних та арифметичних пристроїв на основі багатозначних систем числення. Описується структура багатопорогового елемента багатозначної логіки (БПЕБЛ), принципи його функціонування та побудови на його основі систем трійкової логіки. Запропоновано базову структуру для побудови трійкових двомісних функцій, для якої описано вихідні сигнали запропоновано структуру, що реалізує трійковий сильний кон'юнктор. Отримані структури набагато простіши ніж існуючи відомі пристрої, отримано декілька пристроїв, які не було реалізовано раніше, а у порівнянні з існуючими, отримані структури мають у 2,5 – 4 разів менше елементів.**

***Abstract*— The paper considers the problem of constructing logical and arithmetic devices based on multiple-valued number systems. The structure of the multi-threshold element of multiple-valued logic (MTEMVL) is described, on the basis of which it is possible to construct logical and arithmetic devices for the number system of any value. One of the possible implementations of MTEMVL with four symmetrical thresholds is proposed, which can be used for rational construction of systems of the balanced ternary number system. This structure, unlike known ones, distinguishes five levels of input signals, or the sum of input signals, and has up to eight types of different outputs, combining which allows to obtain the specified functions and can effectively be used to implement triple-valued two-place functions. In this paper, structures are obtained that implement the ternary strong conjunction, as well as several other triplevalued two-place functions. The resulting structures are much simpler than existing known devices. A comparative analysis shows that several devices have been obtained that were not realized earlier, and compared to the existing ones, the structures obtained have 2.5 to 4 times less elements.**

***Ключові слова*—багатозначна система числення; трійкова симетрична система; трійковий сильний кон'юнктор; елемент багатозначної логіки**

***Keywords*— multiple-valued number system; balanced ternary number system; ternary strong conjunction; multiplevalued logic element**

I. Вступ

Одним з подальших розвитків сучасних обчислювальних систем є використання в них багатозначних (недвійкових) систем числення. При цьому найбільш перспективною з точок зору технології, розуміння та складності є трійкова система.

Відомо досить багато прикладів [1-5] побудови трійкових логічних, арифметичних та більш складних пристроїв, але досі не існує єдиного підходу до їх побудови та принципів синтезу. Був створений навіть повністю трійковий серійний комп'ютер [6].

Відомий багатопороговий елемент багатозначної логіки (БПЕБЛ) [7,8], на основі якого можлива реалізація елементів логіки будь-якої значності, але і поєднання різнозначних логічних елементів у єдиній системі.

Метою роботи є розгляд структури БПЕБЛ та побудова на його основі пристрою, що реалізує трійкову сильну кон'юнкцію.

II. Багатопороговий елемент багатозначної логіки

Узагальнена структура БПЕБЛ, на основі якої можна реалізувати логічні і арифметичні елементи для будь-якої багатозначної системи числення приведена на рис.1. На вхід блоку формування порогів (БФП) подаються k вихідних шин попередніх елементів, а n виходів поєднуються з входами n емітерних повторювачів (ЕП) 2.1…2.n, вихід кожного з яких з'єднано з входом щонайменше одного струмового перемикача (СП) 3.1…3.m, кожний з яких має два виходи, причому виходи всіх m струмових перемикачів у сукупності формують вихідну шину БПЕБЛ.

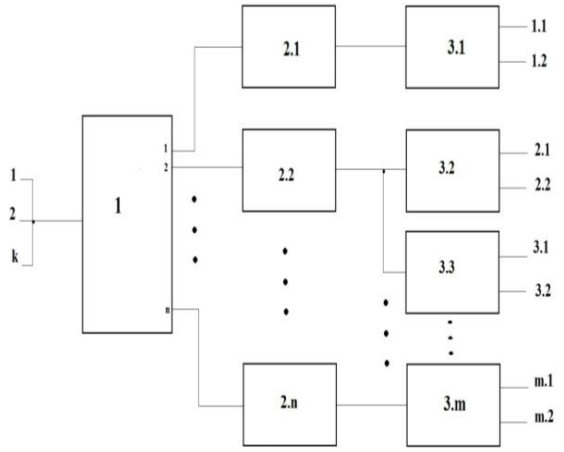


Рис. 1. Структурна схема багатопорогового елемента багатозначної логіки

1 – блок формування порогів, 2.1…2.n – емітерні повторювачі, 3.1…3.m – струмові перемикачі.

Особливості запропонованої структури:

- Система оперує не з потенціальними, а зі струмовими значеннями сигналів, тому виходи БПЕБЛ можуть об'єднуватися у довільній кількості, але подаватися сигнал може тільки на вхід одного елемента.
- Можливість формування будь якої кількості порогів, які БПЕБЛ в змозі розрізняти.

Від кількості порогів БФП залежить кількість рівнів вхідної змінної, які БПЕБЛ в змозі розрізнити й, відповідно, розрядність змінної або складність операцій, які можуть виконуватися.

Запропонована система працює таким чином. На вхід БФП 1 поступають k дискретних струмових сигналів I_j з попередніх елементів. Вони можуть приймати одне з типових значень (наприклад, для двійкової логіки таких значень буде два: $I_j = +1$, $I_j = 0$; для трійкової симетричної системи таких значень буде три: $I_j = +1$, $I_j = 0$, $I_j = -1$).

БФП формує необхідну кількість порогів n. Його n виходів з'єднуються з входами емітерних повторювачів (ЕП) 2.1…2.n. В залежності від результату додавання вхідних струмів $\sum I_j$ активується частка виходів БФП, і відповідні їм ЕП. Активні ЕП формують сигнали на підключених до них струмових перемикачів (СП) 3.1…3.m. В залежності від вхідного сигналу кожний СП формує стандартний струм $I_ф$ на одному зі своїх двох виходів.

Виходи струмових перемикачів можуть об'єднуватися у довільних комбінаціях для формування необхідної логіки функціонування багатопорогового елемента багатозначної логіки.

III. Використання БПЕБЛ для трійкової симетричної логіки

Для трійкової симетричної системи числення можливо використання БПЕБЛ з двома симетричними порогами, що дозволяє розрізняти три рівні вхідного сигналу. Але, для спрощення структур трійкових елементів пропонується використовувати БПЕБЛ з більшою кількістю порогів, що дозволить розрізняти більшу кількість рівнів вхідного сигналу.

Структура можливої реалізації БПЕБЛ з чотирма симетричними порогами і, відповідно, п'ятю рівнями наведена на рис.2. На вхід БФП поступають k дискретних струмових сигналів I_j з вихідних шин попередніх елементів.

$$k = k_{+1} + k_{-1} + k_0,$$

де k_{+1} – число сигналів, поточні значення яких +1, k_{-1} – число сигналів, поточні значення яких -1, k_0 – число сигналів, поточні значення яких 0.

В схемі може бути до чотирьох емітерних повторювачів (ЕП1…ЕП4) та декілька струмових перемикачів (СП1…СП4). На БФП може подаватися будь-яка кількість вхідних сигналів k. Значення напруг, що формуються на виходах ЕП і відповідно подаються на входи струмових перемикачів наведені у таблиці 1.

У таблиці 1 позначено «1» – активний сигнал (який впливає на СП), «0» – неактивний сигнал (який не впливає на СП) на виході відповідного ЕП.

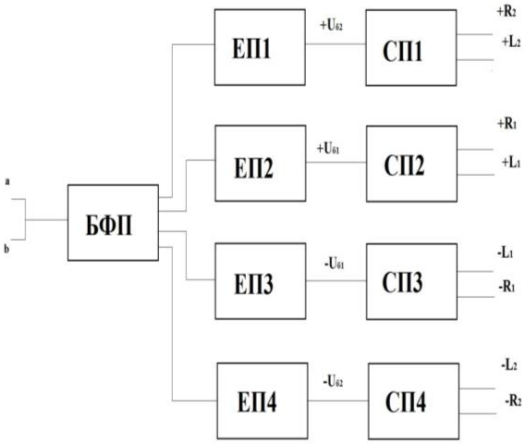


Рис. 2. БПЕБЛ з чотирма симетричними порогами

ТАБЛИЦЯ I. Значення напруг на виходах ЕП1…ЕП4

Сума вхідних струмів	ЕП1 (+Uб2)	ЕП2 (+Uб1)	ЕП3 (–Uб1)	ЕП4 (–Uб2)
– –	1	1	0	0
–	0	1	0	0
0	0	0	0	0
+	0	0	1	0
+ +	0	0	1	1

Вихідні сигнали СП, в залежності від вхідних змінних, фактично від функції terlev, можуть приймати вісім різних значень, які наведено у таблиці 2. Якщо сигнал на вході СП активний («1» по таблиці 1), на виході L відповідного СП формується струм, інакше – струм формується на виході R. СП у сукупності мають 8 виходів, комбінація яких може формувати необхідні логічні або арифметичні функції.

ТАБЛИЦЯ II. ВИХІДНІ СИГНАЛИ СП1…СП4

Сума вхідних струмів	**Вихідні сигнали струмових перемикачів**							
	СП1		***СП2***		***СП3***		***СП4***	
Terlev	$+R_2$	$+L_2$	$+R_1$	$+L_1$	$-R1$	$-L1$	$-R_2$	$-L_2$
– –	0	+	0	+	–	0	–	0
–	+	0	0	+	–	0	–	0
0	+	0	+	0	–	0	–	0
+	+	0	+	0	0	–	–	0
+ +	+	0	+	0	0	–	0	–

IV. РЕАЛІЗАЦІЯ ТРИЙКОВОЇ СИЛЬНОЇ КОН'ЮНКЦІЇ

В роботі отримано декілька структур логічних та арифметичних пристроїв для тійкової симетричної системи. Розглянемо використання запропонованої структури для побудови трійкового сильного кон'юнктора, основні параметри якого наведено у таблиці 3, де a і b – вхідні змінні, terlev – функція суми вхідних сигналів, $a\&_L b$ – вихідна функція. Для отримання вихідної функції достатньо об'єднати виходи (додати вихідні струми) –R2(ab), +R1(ab), –R1(ab), +L1(ab), значення яких також наведено у таблиці 3. Структура, яка реалізує сильний кон'юнктор, наведено на рис. 3.

БФП – блок формування порогів, ЕП1…ЕП3 – емітерні повторювачі, СП1…СП3 – струмові перемикачі. У запропонованої структури можливо використання БФП з трьома замість чотирьох порогів, та лише трьох струмових перемикачів.

ТАБЛИЦЯ III. Т ЗНАЧЕННЯ НАПРУГ НА ВИХОДАХ ЕП1…ЕП4

a	**b**	**terlev**	**$a\&_L b$**	**$-R_2(ab)$**	**$+R_1(ab)$**	**$-R_1(ab)$**	**$+L_1(ab)$**
–	–	– –	–	–	**0**	–	+
–	**0**	–	–	–	**0**	–	+
–	+	**0**	–	–	+	–	**0**
0	–	–	–	–	**0**	–	+
0	**0**	**0**	–	–	+	–	**0**
0	+	+	**0**	–	+	**0**	**0**
+	–	**0**	–	–	+	–	**0**
+	**0**	+	**0**	–	+	**0**	**0**
+	+	++	+	**0**	+	**0**	**0**

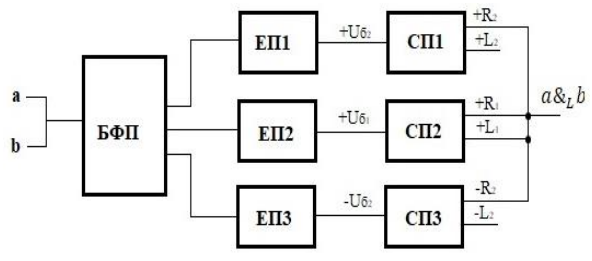


Рис. 3. Структура трійкового сильного кон'юнктора

Аналогічним чином можлива побудова інших логічних та арифметичних трійкових елементів. Невикористані виходи струмових перемикачів можливо застосувати в інших частинах більш складних систем.

V. ВИСНОВКИ

На основі запропонованої структури БПЕБЛ побудовано трійковий сильний кон'юнктор та деякі інші структури трійкових елементів. Отримані пристрої мають набагато простішу структуру та є більш логічно-потужними у порівнянні з відомими системами.

ЛІТЕРАТУРА

[1] Кушнеров А., Троичная цифровая техника. Ретроспектива и современность. Университет им. Бен-Гуриона Беэр-Шева, Израиль, 28.10.05

[2] Пат. 2394366 Россия, МПК (2006.01) H03K19/00. Пороговый элемент троичной логики и элементы на его основе. Опубл. 10.07.2010

[3] Левчук В.В., Малахов В.П., Гунченко Ю.О. Багатопороговий пристрій для реалізації логічно-арифметичних елементів багатозначних систем числення // Тези доповідей XIII Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє", Київ, 2017. – С. 51.

[4] Пат. 2015130589 Россия, МПК (2006.01) H03K19/00. Троичный реверсивный регистр сдвига. Опубл. 27.05.2016

[5] П.Ившин, С.Леготин, В.Мурашёв. Базовые троичные логические элементы. Снижение энергопотребления. [Електронний ресурс] – Режим доступу: http://www.electronics.ru/journal/2010/4

[6] Брусенцов Н.П. Об использовании троичного кода и трехзначной логики в цифровых машинах, Москва – 1969 г.

[7] Гунченко Ю., Левчук В., Кузніченко С., Олейник О., Концепція Побудови Логічних і Арифметичних Пристроїв для Багатозначних Логік // Міжнародна наук.-практ. конф. "Інформаційні технології та комп'ютерне моделювання", Івано-Франківськ, 2018. – С.216.

[8] Пат. UA 118735 Україна, МПК (2017.01) H03K19/00. Багатопорговий елемент багатозначної логіки / Гунченко Ю.О. Заявка 23.03.2017, опубл. 28.08.2017

REFERENCES

[1] A. Kushnerov, Trinity digital technology. Retrospective and modernity. University of. Ben-Gurion Beer-Sheva, Israel, 28.10.05

[2] Pat. 2394366 Russia, IPC (2006.01) H03K19 / 00. Threshold element of the ternary logic and elements based on it. Publ. 10.07.2010

[3] Levchuk V.V., Malakhov V.P., Gunchenko Y.O. Multipath device for the implementation of logical-arithmetic elements of multivalued numerical systems // Abstracts of the XIII International Scientific and Practical Conference "Military Education and Science: Present and Future", Kyiv, 2017. - P. 51.

[4] Pat. 2015130589 Russia, IPC (2006.01) H03K19 / 00. Trilogy reversible shift register. Publ. 27.05.2016

[5] P.Ivshin, S.Legotin, V.Murashev. Basic ternary logical elements. Reduced power consumption. [Online]. Available: http://www.electronics.ru/journal/2010/4

[6] Brusentsov N.P. On the use of the ternary code and three-digit logic in digital machines, Moscow - 1969.

[7] Gunchenko Y., Levchuk V., Kuznychenko S., Oleynik O., Concept of Constructing Logical and Arithmetic Devices for Multivariate Logic // International Science. Pract. conf. "Information Technologies and Computer Modeling", Ivano-Frankivsk, 2018. - P.216.

[8] Pat. UA 118735 Ukraine, MPC (2017.01) H03K19 / 00. Multi-party element of multivalued logic / Gunchenko Y.O. Application 23.03.2017, published 28.08.2017

Многомерные преобразования Грея

Белецкий Анатолий
Кафедра электроники
Национальный авиационный университет
Киев, Украина
abelnau@ukr.net

Multidimensional transformations Gray

Beletsky Anatoly
Department of Electronics
National Aviation University
Kiev, Ukraine
abelnau@ukr.net

***Аннотация*—По аналогии с алгоритмами дискретного преобразования Фурье рассмотрены варианты построения методов дискретных преобразований Грея (ДПГ) одномерных, или преобразования векторных данных, двумерных, или преобразования на плоскости, и трехмерных, или пространственные преобразования, в общем случае m-ичных числовых данных. Преобразования Грея (ПГ) трактуются, как обобщение понятия кодов Грея. В классической схеме процесс формирования прямых и обратных кодов Грея развивается по направлению слева направо. При этом старший (левый) разряд преобразуемого числа не меняется как при прямом, так и обратном преобразованиях. Предложена схема преобразования, обратная по направлению формирования классическому, названному левосторонним ПГ. В новом классе правосторонних ПГ при прямом и обратном преобразованиях сохраняется неизменным значение младшего (правого) разряда преобразуемого числа. Комбинация лево- и правосторонних ПГ (как прямых, так и обратных) совместно с операцией инверсной перестановки привела к возможности построения комбинированных или составных кодов Грея (СКГ). Применение СКГ оказалось весьма успешным в задачах определения структуры и взаимосвязи симметричных систем функций Уолша, дискретных Виленкина-Крестенсона функций, в криптографии, кодировании и в других приложениях.**

***Abstract*— In analogy with discrete Fourier transform algorithms, variants of constructing discrete Gray transformation (DPG) methods for one-dimensional, or vector data transformations, two-dimensional or plane transformations, and three-dimensional or spatial transformations, in the general case of m-ary numerical data, are considered. Gray's transformations (GT) are treated as a generalization of the concept of Gray codes. In the classical scheme, the process of forming the direct and inverse Gray codes develops from left to right. In this case, the highest (left) digit of the converted number does not change under both forward and reverse transformations. A transformation scheme is suggested that is inverse in the direction of formation of the classical, called left-handed GT. In the new class of right-handed GT, the value of the lower (right) digit of the converted number remains unchanged under forward and backward transformations. The combination of left- and right-hand PGs (both direct and inverse) together with the inverse rearrangement operation led to the possibility of constructing combined or composite Gray codes (CGC). The application of the CGC proved to be very successful in determining the structure and interrelation of symmetric systems of Walsh functions, discrete Vilenkin-Crestenson functions, in cryptography, coding, and in other applications.**

Ключевые слова—простые и составные коды Грея, матричная форма операторов Грея, дискретные преобразования Грея.

Keywords-simple and compound Gray codes, matrix form of Gray operators, discrete Gray transformations

I. Введение

Преобразования Грея (ПГ) трактуются далее, как обобщение понятия кодов Грея (КГ). Коды Грея, предложенные в 1953 году в ответ на запросы инженерной практики относительно построения оптимальных по критерию минимума ошибки неоднозначности преобразователей типа “угол-код” [1], на заре своего появления привлекли к себе внимание не только исследователей математиков, но и широкого круга разработчиков разнообразной электронной аппаратуры. Отличительная особенность кодов Грея состоит в том, что в двоичном пространстве (в двоичной системе счисления) при переходе от изображения одного числа к изображению соседнего старшего или соседнего младшего числа происходит изменение цифр (1 на 0 или наоборот) только в одном разряде числа. Такие коды относят к группе двоичных кодов с единичным расстоянием Хэмминга [2]. Код Грея не единственный в этой группе, но его применение в системах связи, аналого-цифрованых преобразованиях и в других областях науки и техники в силу ряда причин становилось предпочтительным.

Укажем на одну существенную особенность данного исследования. По-видимому, оказались вне поля зрения, как математиков, так и разработчиков электронной аппаратуры возможности построения кодов, противоположных по направлению формирования классическим КГ. В известной (классической) схеме процесс формирования прямых и обратных кодов развивается по направлению слева направо. При этом старший (левый) разряд преобразуемого числа не меняется как при прямом, так и обратном преобразованиях. Вместе с тем, можно

построить схему преобразования в общем случае m-ичных кодов, обратную по направлению формирования классическому (левостороннему) ПГ. В таком классе правосторонних преобразований при прямом и обратном преобразованиях сохраняется неизменным значение младшего (правого) разряда преобразуемого числа.

Комбинация лево- и правосторонних преобразований Грея (как прямых, так и обратных) совместно с операцией инверсной перестановки кодов привела к возможности построения комбинированных или составных кодов Грея (СКГ) [3]. Применение СКГ оказалось весьма успешным в задачах определения структуры и взаимосвязи симметричных систем функций Уолша [4], дискретных Виленкина-Крестенсона функций [5], в криптографии, кодировании и в других приложениях.

Уточним понятие многомерного преобразования Грея (МПГ). К одномерным преобразованиям Грея (ОПГ) будем относить преобразования целочисленных данных, сведенных в одномерные массивы (векторы). Под двумерными ПГ, являющимися простейшими формами МПГ, будем понимать преобразования двумерных массивов чисел (матриц, растровых изображений). Соответственно, трёхмерные ПГ есть преобразования трёхмерных массивов и т.д.

Главная задача данного исследования состоит в разработке концептуальных основ построения алгоритмов многомерных дискретных преобразований в общем случае m-ичных числовых данных, основанных на применении обобщенных преобразований Грея.

II. Одномерные преобразования Грея

Наиболее просто физическая суть классического прямого ОПГ раскрывается его структурно-логической схемой, пример которой для четырехточечного преобразования бинарных данных показан на рис. 1.

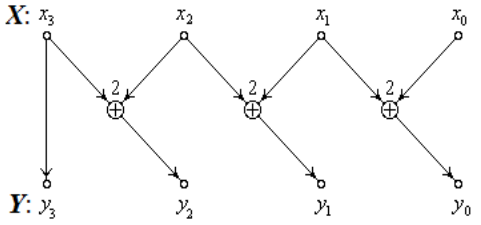


Рис. 1 Структурно-логическая схема алгоритма формирования прямого двоичного кода Грея левостороннего

Система алгебраических уравнений, отвечающих прямому левостороннему ОПГ (рис. 1), имеет вид:

$$\begin{aligned} y_3 &= x_3; \\ y_2 &= x_3 + x_2; \\ y_1 &= x_2 + x_1; \\ y_0 &= x_1 + x_0. \end{aligned} \qquad (1)$$

Формально разрешая модулярные уравнения (1) относительно входных переменных $\boldsymbol{X} = \{x\}$, с учетом того, что для двоичной системы счисления $-1 \pmod 2 = 1$, получим:

$$\begin{aligned} x_3 &= y_3; \\ x_2 &= y_3 + y_2; \\ x_1 &= y_3 + y_2 + y_1; \\ x_0 &= y_3 + y_2 + y_1 + y_0. \end{aligned} \qquad (2)$$

Обратные преобразования (2) отображаются схемой, представленной на рис. 2.

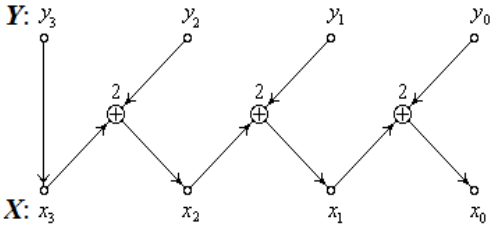


Рис. 2 Структурно-логическая схема алгоритма формирования обратного двоичного кода Грея левостороннего

Преобразования по Грею можно выполнять не только на множестве двоичных данных, но также и над числами с любым основанием системы счисления m. При переходе к m-ичному основанию в структурных схемах алгоритмов прямого преобразования Грея достаточно заменить поразрядный сумматор по модулю 2 на поразрядный сумматор по модулю m. Для структурных схем обратного преобразования Грея m-ичных данных недостаточно указанной выше замены поразрядных сумматоров. В самом деле, разрешая систему модулярных уравнений (1) относительно входных переменных $\boldsymbol{X} = \{x\}$, но теперь уже с учетом того, что $\boldsymbol{X}$ и $\boldsymbol{Y}$ являются m-ичными числами, имеем:

$$\begin{aligned} x_3 &= y_3; \\ x_2 &= (y_2 - x_3)_m; \\ x_1 &= (y_1 - x_2)_m; \\ x_0 &= (y_0 - x_1)_m, \end{aligned} \qquad (3)$$

где $(a)_m = a \pmod m$.

Системе уравнений (3) отвечает структурная схема преобразования, показанная на рис. 3.

Из систем уравнений (1) – (3), в равной степени как из соответствующих им схемам (на рис. 1 – 3), видно, что процесс ПГ развивается по направлению слева направо. По этой причине классические преобразования Грея названы левосторонними. Альтернативными классическим ПГ являются так называемые правосторонние преобразования [3-5], способ формирования которых иллюстрируется на рис. 4 и 5

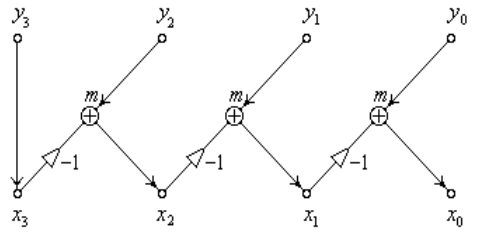


Рис. 3 Структурно-логическая схема алгоритма формирования обратного $m-$ичного кода Грея левостороннего

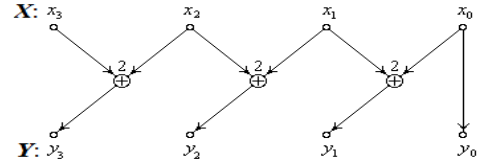


Рис. 4 Структурно-логическая схема алгоритма формирования прямого двоичного кода Грея правостороннего

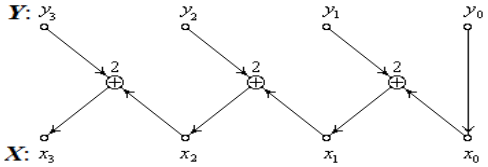


Рис. 5 Структурно-логическая схема алгоритма формирования обратного двоичного кода Грея правостороннего

Каждое из рассмотренных преобразований можно представить в матричной форме в таком общем виде:

$$\boldsymbol{Y} = \boldsymbol{X} \cdot \boldsymbol{G}; \qquad \boldsymbol{X} = \boldsymbol{Y} \cdot \bar{\boldsymbol{G}},$$

где $\boldsymbol{G}$ – оператор (матрица) прямого и $\bar{\boldsymbol{G}}$ – обратного преобразования.

Сведем основные операторы Грея в табл. 1, дополнив её рядом дополнительных операций.

Матричные формы операторов Грея третьего порядка показаны в табл. 2.

Операторов Грея, представленных в табл. 1 и 2, а также СКГ, составленных на их основе, достаточно для построения полного дерева (рис. 6) систем функций Уолша восьмого порядка (являющееся также деревом индикаторных матриц (ИМ) третьего порядка). Буквенно-цифровые символы, расположенные в узлах (кружочках) контуров дерева, представляют собой идентификаторы матриц Уолша (или ИМ).

ТАБЛИЦА 1. Группа простых операторов Грея

Обозначение оператора	***Выполняемая операция***
0(e)	Сохранение исходной комбинации
1	Инверсная перестановка
2	Прямое левостороннее ПГ
3	Обратное левостороннее ПГ
4	Прямое правостороннее ПГ
5	Обратное правостороннее ПГ
6	Циклический сдвиг на один разряд вправо
7	Циклический сдвиг на один разряд влево

ТАБЛИЦА 2. Матричные формы простых операторов Грея

$0=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$	$2=\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}$	$4=\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}$	$6=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$
$1=\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$	$3=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}$	$5=\begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix}$	$7=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$

Индикаторными матрицами $\boldsymbol{J}_w$ систем функций Уолша $\boldsymbol{W}$ являются правосторонне симметрические (0,1)-матрицы (то есть матрицы, симметричные относительно вспомогательной диагонали), невырожденные над F_2.

Порядки систем Уолша N и их ИМ n связаны целочисленной показательной функцией по основанию 2, т. е. $N = 2^n$, где $n \geq 1-$ натуральное число.

Такими же простыми операторами Грея, как в табл. 2, но уже четвертого порядка, и на их основе – составными кодами Грея, удаётся получить все 448 ИМ и, соответственно, — систем функций Уолша 16-го порядка.

Любая система Уолша $N-$го порядка может быть образована соответствующей перестановкой строк (или столбцов) матрицы Уолша-Пэли $\boldsymbol{P}$, что наглядно иллюстрируется графом взаимосвязи систем на рис. 6. Номер строки k_w системы $\boldsymbol{W}$, в которую перемещается k_p-я строка матрицы Пэли $\boldsymbol{P}$, можно найти по формуле:

$$k_w = k_p \cdot \boldsymbol{J}_w, \quad k_p = \overline{0, N-1},$$

из которой, как следствие, вытекает

Утверждение 1: Произвольная система Уолша $N-$го порядка $\boldsymbol{W}$ однозначно определяется её индикаторной матрицей $n-$го порядка $\boldsymbol{J}_w$.

Базисные функция $k-$го порядка $p(k,t)$ дискретного аргумента (времени) t систем Уолша-Пели в пространстве ***оригиналов*** $\boldsymbol{P} = \{p(k,t)\}, \quad k,t = \overline{0, N-1},$ ***вычисляются рекуррентными соотношениями [4]:***

- для четных функций

$$p(2k,t) = p\left(k,(2t)_N\right)$$

- для нечетных функций

$$p(2k+1,t) = p(2k,t) \cdot p(1,t)$$

Начальными условиями для $p(k,t)$ являются:

$$p(0,t) = +1, \quad p(1,t) = \begin{cases} +1, & n = \overline{0, N/2-1}; \\ -1, & n = \overline{N/2, N-1}. \end{cases}$$

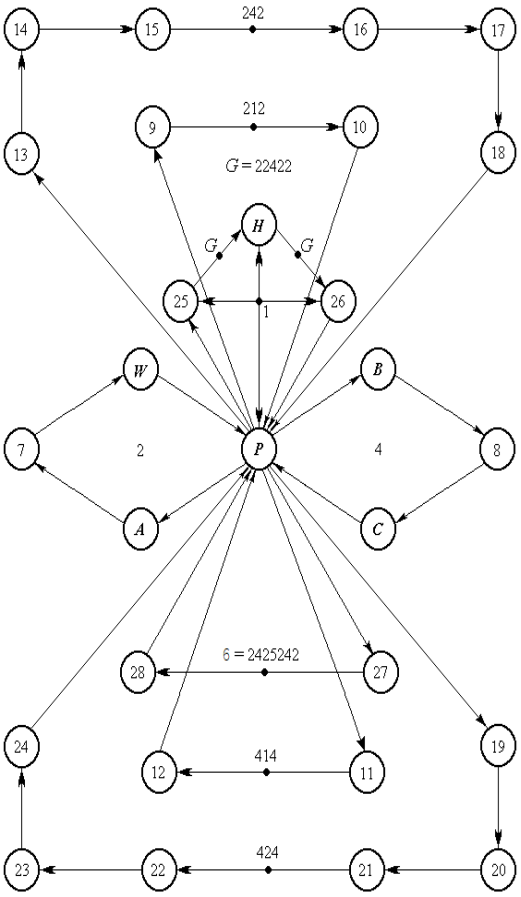


Рис. 6 Полный граф Пэли-связанных систем Уолша восьмого порядка

III. Аксиоматические основы преобразований Грея и *M*-последовательности

Сформулируем ряд фундаментальных положений, которые составляют основу построения теории ПГ.

Аксиома 1. Произвольный код Грея (простой или составной) является образующим элементом мультипликативной циклической группы.

Аксиома 2. Оператор $\perp$ правостороннего транспонирования осуществляет разворот квадратных матриц относительно вспомогательных диагоналей.

Лемма 1. Составному коду Грея $\boldsymbol{G}\cdot\boldsymbol{G}^T$, где $\boldsymbol{G}$ — матричная форма произвольного СКГ, отвечает левосторонне симметрическая матрица.

Доказательство. Из того, что $(\boldsymbol{A}\cdot\boldsymbol{B})^T=\boldsymbol{B}^T\cdot\boldsymbol{A}^T$, следует, что $\left(\boldsymbol{G}\cdot\boldsymbol{G}^T\right)^T=\left(\boldsymbol{G}^T\right)^T\cdot\boldsymbol{G}^T=\boldsymbol{G}\cdot\boldsymbol{G}^T$, которое справедливо, если только $\boldsymbol{G}\cdot\boldsymbol{G}^T$ — левосторонне симметрическая матрица. ■

Лемма 2. Правостороннее транспонирование $\perp$ СКГ эквивалентно инверсии этого кода, которое сводится к обращению порядка следования простых кодов Грея.

В самом деле, $\left(g_1\cdot g_2\right)^{\perp}=g_2{}^{\perp}\cdot g_1{}^{\perp}=g_2\cdot g_1$, так как любой простой код Грея g является симметричным относительно вспомогательной диагонали. ■

Лемма 3. Симметричному СКГ отвечает правосторонне симметрическая матрица преобразования.

Доказательство. По определению симметричным составным является код $\boldsymbol{G}_s=\boldsymbol{G}\cdot\omega\cdot\boldsymbol{G}^{\perp}$, в котором $\boldsymbol{G}$ – произвольный СКГ, а ω – ядро, являющееся простым или симметричным составным кодом Грея. Имеем

$$\boldsymbol{G}_s^{\perp}=\left(\boldsymbol{G}\cdot\omega\cdot\boldsymbol{G}^{\perp}\right)^{\perp}=(\boldsymbol{G}^{\perp})^{\perp}\cdot\omega^{\perp}\cdot\boldsymbol{G}^{\perp}=\boldsymbol{G}\cdot\omega\cdot\boldsymbol{G}^{\perp}=\boldsymbol{G}_s.\blacksquare$$

Утверждение 2: Существуют СКГ, образующие циклические группы максимального порядка L, (*m*-последовательности) определяемого соотношением $L=2^n-1$, где n – порядок индикаторных матриц простых кодов, являющихся компонентами СКГ. Назовем *примитивными* относительно ИМ n – го порядка те СКГ, последовательность степеней которых, начиная с нулевой степени, образует *m*-последовательность. Примерами таких кодов (см. рис. 6), являются симметричные 242 и 424 коды. $M-$ последовательности генерируют также отдельные несимметричные СКГ. В качестве примера укажем код $\boldsymbol{G}=1\cdot g$, в котором g – один из простых кодов с идентификаторами $2-5$, представленных в табл. 2. Дополнительные сведения относительно несимметричных примитивных составных кодов приведены в табл. 3.

ТАБЛИЦА 3. Примитивные составные коды Грея

$n=16$	$n=32$	$n=64$	$n=128$	$n=256$
2224244	2225355	2252435	2425535	22533435
2225524	2225535	2433435	2433534	22534335
2252435	2244424	2435225	2435334	24334225
2255535	2255524	2522534	22524224	25224334
2433435	2442224	25224334	22533334	2222535224

IV. Дискретные преобразования Грея

Введем по аналогии с термином «дискретные преобразования Фурье» (ДПФ) термин *дискретные преобразования Грея* (ДПГ), разделяя их на *одномерные*, или преобразования векторных данных, *двумерные*, или преобразования на плоскости, и *трехмерные*, или пространственные ДПГ. Наиболее полезным оказывается всё же обобщение на случай двух измерений, поскольку оно широко применяется при обработке изображений.

Как и двумерное ДПФ двумерное ДПГ можно вычислить последовательно по двум измерениям. С этой целью достаточно определить одномерные ДПГ всех строк изображения, а затем вычислить в результирующем «изображении» одномерные ДПГ всех столбцов. При этом результаты одномерных ДПГ нужно записывать на место исходных данных для этих ДПГ.

Аналогичным образом осуществляется трёхмерное ДПГ, которое сводится к последовательности таких преобразований. Предположим, что исходные данные, назовём их *пикселями*, «упакованы» в трехмерный контейнер с попарно ортогональными осями координат i, j и k . Сначала проводятся ДПГ над исходными пикселями, содержащимися, например, во всех векторах контейнера, коллинеарных оси i . Затем вычисляются ДПГ над данными предыдущего преобразования и расположенными в векторах, коллинеарных оси j . И, наконец, на заключительном этапе выполняется ДПГ данных, которые находятся в ячейках векторов контейнера, коллинеарных оси k .

V. Выводы

Несмотря на более чем полувековую (1953 г.) историю своего открытия коды Грея всё ещё далеки от завершения. Предлагаемые в данной работе дополнения классических кодов Грея так называемыми правосторонними и составными кодами существенно расширяют границы применения преобразований Грея во многих областях науки и техники.

ЛИТЕРАТУРА

[1] F. Gray," Pulse code communication". — Pat. USA, # 2632058, 1953.

[2] R. V. Hamming, "Coding and Information Theory", Prentice-Hall, 1980, ISBN 0131391399

[3] А. Я. Белецкий, "Коды Грея." — К.: Изд-во «КИТ», 2002. — 150 с.

[4] А. Я. Белецкий, "Комбинаторика кодов Грея." — К.: Изд-во «КВІЦ», 2003. — 508 с.

[5] А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий, "Преобразования Грея." Монография. В двух томах. Т.1. Основы теории. — К.: Изд-во «НАУ», 2007. — 412 с.; Т.2. Прикладные аспекты. — К.: Изд-во «НАУ», 2007. — 644 с.

REFERENCES

[1] F. Gray," Pulse code communication". — Pat. USA, # 2632058, 1953.

[2] R. V. Hamming, "Coding and Information Theory", Prentice-Hall, 1980, ISBN 0131391399

[3] A. Ya. Beletsky, "Gray codes." — Kiev, Publishing house "KIT", 2002. — 150 p.

[4] A. Ya. Beletsky, " Combinatorics of Gray codes." — Kiev, Publishing house "KVIC", 2003. — 508 p.

[5] A. Ya. Beletsky, A. A. Beletsky, E. A. Beletsky, "Gray transformations." Monograph. In two vol. V.1. Fundamentals of Theory. — Kiev, Publishing house "NAU", 2007. — 412 p.; V.2. Applied aspects. — Kiev, Publishing house "NAU", 2007. — 644p.

Оценка эффективности реализации IT приложения на гибридной облачной платформе

Людмила Волощук
каф. Математического обеспечения компьютерных систем
ОНУ им.И.И.Мечникова
Одесса, Украина

Ольга Розновец
каф. Математического обеспечения компьютерных систем
ОНУ им.И.И.Мечникова
Одесса, Украина

Evaluation of the effectiveness of the implementation of IT applications on a hybrid cloud platform

L.A. Voloshchuk
Dep. of Mathematical Support of Computer Systems
Odesa I.I. Mechnikov National University,
Odesa, Ukraine
lavstumbre@gmail.com

O.I. Roznovets
Dep. of Mathematical Support of Computer Systems
Odesa I.I. Mechnikov National University,
Odesa, Ukraine
olga.roznovets@gmail.com

***Аннотация*—Облачные технологии и платформы активно развиваются и становятся все более востребованными. Наибольшую популярность последнее время завоевывают гибридные облака и мультиоблачные услуги, в которых реализуется распределенное размещение ИТ-инфраструктуры предприятия частично на облачных платформах, частично на локальных вычислительных мощностях заказчика. Для принятия решения о возможности частичной миграции ИТ-инфраструктуры в облако возникает задача выбора правильного сочетания частных и облачных решений в единой архитектуре приложений и собственно ИТ-среде предприятия в целом. Поэтому важно иметь методологический инструментарий, который поможет сделать обоснованный выбор. В работе рассмотрены возможности применения методики оценки эффективности частичной миграции подсистем приложения в «облако» [4] на примере построения гибридной облачной архитектуры Системы ведения документации кафедр ВУЗа. Использование предложенного в методике подхода позволило получить два альтернативных варианта гибридной облачной архитектуры на основе процесса декомпозиции исходной монолитной архитектуры приложения. Сравнение альтернативных вариантов облачных архитектур проведено в соответствии с совокупностью технических нефункциональных критериев, представляющих собой требования к функционированию системы в целом и их весовыми значениями. Для получения интегрированной оценки эффективности работы в гибридном «облаке» приложения используется Метод Анализа Иерархий (МАИ), который позволяет провести многокритериальный анализ и выбрать лучшее облачное архитектурное решение. Оценки технической эффективности, полученные с учетом принятых экспертных суждений о значимости критериев, подкритериев и альтернатив позволили получить эффективную гибридную облачную архитектуру Системы ведения документации кафедр ВУЗа.**

Abstract—Cloud technologies and platforms are actively developing and becoming more and more in demand. Lately, the hybrid clouds and multi-cloud services are the most popular, in which distributed allocation of the company's IT infrastructure is realized partly on cloud platforms, partly on the customer's local computing facilities. To make a decision on the possibility of a partial migration of IT infrastructure to the cloud, the problem of choosing the right combination of private and cloud solutions in a single application architecture and the IT environment of the enterprise as a whole arises. So it is important to have a methodological tool that will help in making a valid choice. The possibilities of applying the methodology for estimating the effectiveness of partial migration of application subsystems to the "cloud" [4] using the example of the construction of a hybrid cloud architecture of the Document management system of the university chairs are considered in the paper. The use of the approach suggested in the methodology has allowed obtaining two alternative versions of the hybrid cloud architecture based on the decomposition process of the initial monolithic application architecture. Comparison of alternative cloud architectures is carried out in accordance with a set of technical non-functional criteria, which are requirements for the functioning of the system as a whole, and their weight values. To obtain an integrated assessment of the effectiveness of the application in a hybrid cloud, the Analytic Hierarchy Process (AHP) is used, which allows conducting multi-criteria analysis and choosing the best cloud architectural solution. Estimates of technical efficiency, received taking into account the accepted expert judgments about the importance of criteria, subcriteria and alternatives, allowed to obtain an effective hybrid cloud architecture of the Document management system of the university chairs.

Keywords— hybrid cloud platforms, application migration to the cloud, evaluation of the efficiency of migration to the cloud

Ключевые слова – гибридные облачные платформы, миграция приложения в облако, оценка эффективности миграции в облако

I. Введение

Облачные технологии и платформы активно развиваются и становятся все более востребованными. С понятием облачных вычислений связывают такие сервис-предоставляющие технологии, как инфраструктура как сервис (“Infrastructure as a Service” или “IaaS”), платформа как сервис (“Plaatform as a Service”, “PaaS”), программное обеспечение как сервис (“Software as a Service” или “SaaS”).

Помимо различных способов предоставления сервисов различают несколько вариантов развёртывания облачных систем. Частное облако (private cloud) - используется для предоставления сервисов внутри одной компании. Публичное облако (public cloud) - используется облачными провайдерами для предоставления сервисов внешним заказчикам. Смешанное облако (hybrid cloud) - совместное использование двух вышеперечисленных моделей развёртывания.

Наибольшую популярность последнее время завоевывают гибридные облака и мультиоблачные услуги, в которых реализуется распределенное размещение ИТ-инфраструктуры предприятия частично на облачных платформах, частично на локальных вычислительных мощностях заказчика. Для принятия решения о возможности частичной миграции ИТ приложения в облако возникает задача выбора правильного сочетания частных и облачных решений в единой архитектуре приложений и собственно ИТ-среде предприятия [1].

Вопросы поддержки принятия решения о возможности миграции приложений в облачную инфраструктуру с точки зрения требований к экономической эффективности, к безопасности системы и техническим возможностям облачной реализации рассматриваются в ряде работ [2,3].

В статье [4] предложена методика предварительной оценки эффективности частичной миграции на облачную платформу отдельных модулей и подсистем приложений, основанная на структурной декомпозиции архитектуры приложения, проведения технико-экономической экспертной оценки эффективности миграции отдельных подсистем, приложения на основе совокупности нефункциональных требований к эксплуатации системы и, собственно, вычислении итоговой оценки эффективности реализации приложения в гибридном облаке с использованием Метода анализа иерархий (МАИ)[5].

В данной работе рассматривается применение вышеизложенного подхода для принятия решения о частичной миграции в публичное облако Системы для ведения документации кафедр ВУЗа.

II. Выбор альтернативных вариантов гибридной облачной архитектуры Системы ведения документации кафедр ВУЗа

Кафедра, как важнейшее подразделение ВУЗа, выполняя учебную, методическую, научную и организационную работу со студентами по ходу учебного процесса, сталкивается с большим объемом соответствующей документации,которую необходимо формировать, сопровождать, хранить, а для принятия управленческих решений – анализировать [6]. Внедрение автоматизированной системы для работы с документацией кафедры позволяет решить многие проблемы. Однако, реализация полнофункциональной автоматизированной системы представляет собой процесс создания специализированного программного обеспечения, что является достаточно сложной задачей, требующей привлечения больших материальных и интеллектуальных ресурсов. Поэтому применение современных информационных технологий, выбор эффективной облачной архитектуры создаваемой системы, что непосредственно влияет на требуемый объем затрат при ее реализации, является актуальным.

Система ведения документации кафедр ВУЗа должна содержать модули и компоненты такие как база данных документов кафедры и архивных материалов, сервер приложений с модулями, реализующими бизнес логику системы. сервисы и службы для расширения функциональных возможностей и обеспечения сохранности информации, клиентские приложения для типовых пользователей с соответствующими функциональными возможностями.

Классическая монолитная сервис-ориентированная архитектура системы представлена на рис. 1.

Рис.1. Архитектура системы ведения документации кафедр ВУЗа

Исходя из описания базовой архитектуры можно представить на рассмотрение следующие альтернативные варианты облачной гибридной реализации системы:

- альтернативный вариант архитектуры А1, в котором частично на облачную платформу выносятся подсистема бизнес логики ведения документации, функционально поддерживающие ее облачные сервисы и уровень представления, а в локальной инфраструктуре остаются подсистема бизнес логики архивации и собственно база данных системы ведения документации кафедры;

- альтернативный вариант архитектуры А2, в котором частично на облачную платформу выносится операционная часть БД системы, при этом, историческая архивная часть БД остается на локальном сервере, на облачную платформу также перемещаются подсистема бизнес логики ведения документации, функционально поддерживающие ее облачные сервисы и уровень представления.

Таким образом, на сравнение выносится два альтернативных варианта реализации гибридной облачной архитектуры А1 и А2.

III. Определение иерархии критериев для оценки технико-экономической эффективности миграции в «облако»

Существенное влияние на архитектуру системы оказывают нефункциональные требования (NFR - non-functional requirement). Это требования, которые могут использоваться для оценки функционирования системы, а не для конкретного ее поведения. Они определяют архитектурно значимые требования, называемые также атрибутами качества. В соответствии с отобранной совокупностью критериев в используемой методике[4] и требованиями к рассматриваемой системе определим следующие критерии и подкритерии оценки технической эффективности реализации гибридной облачной архитектуры Системы ведения документации кафедры.

Критерий «Хранение данных» включает подкритерии долговременность хранения, пропускная способность, централизация хранения данных.

Критерий «Требования к доступу» включает подкритерии доступность, степень пульсации трафика, пропускная способность канала, секретность.

Определим значения приведенных критериев.

Долговременность хранения (Retention policy) – политика хранения, требование, которое определяют срок хранения в памяти различных данных системы.

Пропускная способность (CCU, number of concurrent users) – требование, определяющее количество пользователей, которые могут работать параллельно с системой.

Централизация хранения данных (Data centralization) – определяет требование к централизации или возможность распределенного хранения информации системы.

Доступность (Availability) – характеристика системы, определяющая требование гарантированного обслуживания путём уменьшения или управления сбоями и минимизацией времени плановых простоев.

Степень пульсации трафика (Traffic pulsation degree) – определяет требование необходимой пропускной способности, в том числе при пиковой нагрузке.

Пропускная способность канала (Channel bandwidth) – физическая характеристика коммуникационного канала, показывающая, какой объем данных может быть передан через этот канал в единицу времени; влияет на стоимость аренды канала.

Секретность (Security) – определяет требования к безопасности системы, в том числе аутентификация, авторизация пользователя, защита от атак.

В качестве критериев экономической эффективности гибридной облачной архитектуры будем принимать:

- начальные затраты – стоимость разработки системы;
- текущие затраты – стоимость эксплуатации системы.

К уменьшению этих затрат необходимо стремиться. Опыт использования облачных технологий определил следующие тенденции:

- начальные затраты на создание системы и ее аппаратно-программной платформы в случае реализации в корпоративном ЦОД значительно выше, чем при облачной реализации;
- текущие затраты на эксплуатацию системы в облаке в перспективе 5 лет дороже на 30% – 40%, чем эксплуатация этой же системы в локальной инфраструктуре предприятия, а в перспективе 1 года они примерно равны.

Проведем построение иерархии выбранных критериев оценки технико-экономической эффективности (рис.2).

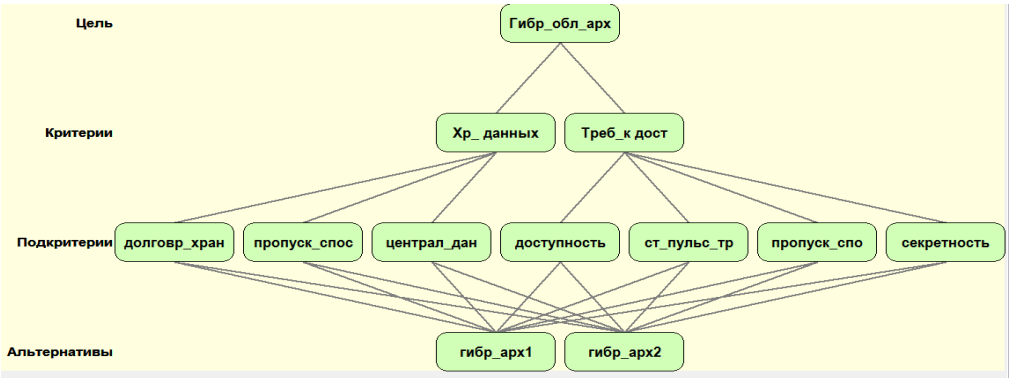


Рис.2 Иерархия критериев оценки техникой эффективности реализации гибридных облачных архитектур А1 иА2

При сравнении критериев и подкритериев, выделенных альтернативных гибридных облачных архитектур используется шкала экспертных суждений МАИ, приведенная в таблице 1. В соответствии со значениями оценок в шкале субъективных суждений при сравнении выделяются наиболее значимые и важные критерии и подкритерии.

ТАБЛИЦА 1. ШКАЛА ЭКСПЕРТНЫХ СУЖДЕНИЙ СРАВНЕНИЯ

Значение	Определение
1	А и В одинаково важны
3	А незначительно важнее, чем В
5	А значительно важнее В
7	А явно важнее В
9	А по своей значительности абсолютно превосходит В
2, 4, 6, 8	Промежуточные значения

При сравнении определенных выше критериев можно определить следующие экспертные суждения:

- хранение данных незначительно важнее требований к доступу -3;
- долговременность хранения явно важнее, чем пропускная способность - 7;
- долговременность хранения значительно важнее, чем централизация хранения данных – 5;
- централизация хранения данных незначительно важнее, чем пропускная способность – 3;
- доступность незначительно важнее, чем степень пульсации трафика – 3;
- доступность одинаково важна с пропускной способностью канала –1;
- секретность явно важнее, чем доступность – 7;
- степень пульсации трафика незначительно важнее пропускной способности канала – 3;
- секретность абсолютно превосходит степень пульсации трафика - 9;
- секретность явно важнее пропускной способности -7.

По результатам сравнения критериев и подкритериев составим матрицы сравнений.

ТАБЛИЦА 2. ОЦЕНКА ОТНОСИТЕЛЬНЫХ ПРИОРИТЕТОВ КРИТЕРИЕВ

Цель – гибр.арх.	ХД	ТД	Вектор приоритетов
Хранение данных(ХД)	3/4	3/4	3/4(0.750)
Требования к доступу(ТД)	1/4	1/4	1/4(0.250)

Вектор приоритетов показывает, что именно мы предпочитаем. В нашем примере наиболее предпочтительными являются критерий «Хранение данных».

ТАБЛИЦА 3. ОЦЕНКА ОТНОСИТЕЛЬНЫХ ПРИОРИТЕТОВ ПОДКРИТЕРИЕВ «ХРАНЕНИЕ ДАННЫХ»

Хранение данных	ДХ	ПС	ЦД	Вектор приоритетов
Долговременность хранения(ДХ)	35/47	7/11	15/19	0.7235
Пропускная способность(ПС)	5/47	1/11	1/19	0.0833
Централизация данных(ЦД)	7/47	3/11	3/19	0.1932

В группе критерия «Хранение данных» наиболее предпочтительным является подкритерий «Долговременность хранения».

ТАБЛИЦА 4. ОЦЕНКА ОТНОСИТЕЛЬНЫХ ПРИОРИТЕТОВ ПОДКРИТЕРИЕВ «ТРЕБОВАНИЕ К ДОСТУПУ»

Требования к доступу	Д	СТП	ПСК	С	Вектор приоритет
Доступность(Д)	1	3	1	1/7	0.1239
Степень пульсации трафика(СПТ)	1/3	1	1/3	1/9	0.0509
Пропускная способность канала(ПСК)	1	3	1	1/7	0.1239
Секретность(С)	7	9	7	1	0.7013

В группе критерия «Требования к доступу» наиболее предпочтительным является подкритерий «Секретность».

IV. ОЦЕНКА АЛЬТЕРНАТИВНЫХ ВАРИАНТОВ ГИБРИДНОЙ ОБЛАЧНОЙ АРХИТЕКТУРЫ ПО НАБОРУ КРИТЕРИЕВ

Проведем сравнение альтернативных гибридных облачных архитектур А1 и А2 поочередно для каждого из отобранных подкритериев. В качестве желаемой эффективности гибридной облачной архитектуры будем принимать уменьшение стоимости разработки и эксплуатации системы. При сравнении архитектур будем руководствоваться обзорами услуг облачных провайдеров и рекомендациями экспертов в области облачных технологий.

При сравнении по подкритерию «Долговременность хранения» – архитектура А2 явно эффективнее(7) архитектуры А1, так как историческая архивная часть БД будет храниться локально, что позволяет снизить требование по срокам сохранения данных в операционной части БД, уменьшить стоимость эксплуатации системы за счет сокращения стоимости размещения и обслуживания архива, как достаточно дорогого сервиса, в облачном хостинге.

При сравнении по подкритерию «Пропускная способность» архитектура А1 одинакова с архитектурой А2 (1).

При сравнении по подкритерию «Централизация хранения данных» – архитектура А1 значительно более требовательна к централизации по сравнению с архитектурой А2(5).

При сравнении по подкритерию «Доступность» – архитектура А2 явно важнее архитектуры А1(7).

При сравнении по подкритерию «Степень пульсации трафика» – архитектура А2 значительно важнее по сравнению с архитектурой А1(5), так как «Облако» значительно эффективнее решает вопросы пульсации трафика.

При сравнении по подкритерию «Пропускная способность канала» – архитектура А2 явно важнее архитектуры А1, так как нет пересылки данных(7).

При сравнении по подкритерию «Секретность» – архитектура А2 значительно превосходит архитектуру А1(5), так как архитектура А1 предполагает обеспечение безопасности данных локально с соответствующими затратами при эксплуатации системы, в архитектуре А2 безопасность данных и системы обеспечивает облачных провайдер, что может быть значительно дешевле, с учетом почасовой оплаты.

V. Вычисление общей оценки МАИ альтернативных вариантов гибридной облачной архитектуры системы ведения документации кафедр ВУЗа.

Проведем вычисление оценки МАИ для каждого варианта альтернативной гибридной облачной архитектуры. Общий балл каждой из архитектур системы рассчитывается как сумма произведения его относительного приоритета по каждому критерию и относительного приоритета соответствующего критерия.

$$S_x = \sum_{i=1}^{M} \sum_{j=1}^{N_i} (P_i) * (p_{ij}) * (s_{ijx}) \qquad (1)$$

где S_x –МАИ-балл для х-й подсистемы приложения; M – число групп критериев; N_i –число элементов в i-ой группе критериев; P_i – значение приоритета i-ой группы критериев; p_{ij} – значение приоритета j-го критерия, принадлежащего i-ой группе критериев; s_{ijx} – балл сравнения х-й альтернативной архитектуры приложения по j-му критерию в i-ой группе критериев.

На рис.3 приведены результаты вычислений оценки МАИ для альтернативных вариантов А1 и А2 гибридной облачной архитектуры в виде круговой диаграммы.

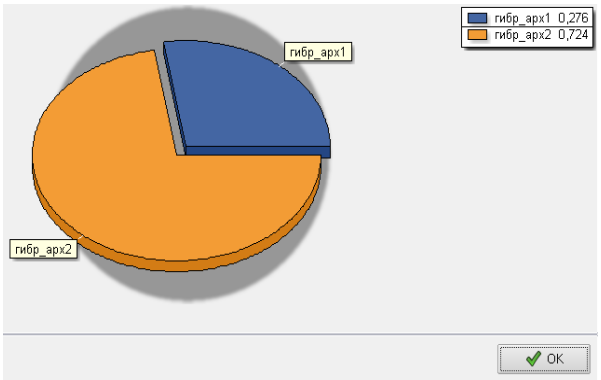


Рис.3. Диаграмма результатов вычислений оценок МАИ

Результаты экспертной оценки показывают, что более эффективной для реализации, удовлетворяющей всем выдвинутым техническим критериям, является гибридная облачная архитектура А2.

Выводы

В результате применения методики [4] оценки эффективности миграции подсистем приложения в «облако» для анализа целесообразности частичной миграции в «облако» Системы ведения документации кафедр ВУЗа получены оценки технической эффективности для двух альтернативных вариантов А1 и А2 гибридной облачной архитектуры.

Эффективность гибридной облачной архитектуры А2 с учетом принятых экспертных суждений о значимости критериев, подкритериев и альтернатив оценена величиной 72.4%, то есть является более целесообразной для реализации.

Процесс применения методики [4] и проведения расчетов в соответствии с МАИ [5] определил особую значимость выбранных нефункциональных технических критериев оценки и экспертных суждений о их значимости для исследуемых гибридных облачных архитектур ИТ приложений. Это определяет перспективную дальнейшую задачу формирования экспертной базы данных критериев, их весовых баллов и рекомендаций облачных провайдеров по применению их для различных классов ИТ приложений.

Применение методики[4] позволяет формализовать и упростить процесс принятия решения о построении гибридной облачной инфраструктуры приложения.

Литература

[1] Paola Doebel. Hybrid IT: avoiding 'cloud cliff' by finding the right mix. Why Hewlett Packard Enterprise is banking on a shift towards hybrid IT adoption. [Електронний ресурс] – Режим доступа: http://www.businesstimes.com.sg/hub/empowering-enterprise/hybrid-it-avoiding-cloud-cliff-by-finding-the-right-mix – 17.01.2018

[2] Bridges Deb. Assessing the suitability of enterprise applications for migration to the cloud [Online]. Available:: https://www.ibm.com/developerworks/ru/library/cl-assessport/ – 02.03.2012

[3] Разумников С.В. Модель поддержки принятия решений о миграции корпоративных приложений в облачную среду // Труды Вольно экономического общества России. – 2015 (194). – с. 490-502

[4] Волощук Л.А. Поддержка принятия решений о реализации приложений в гибридной облачной инфраструктуре./ Л.А.Волощук, О.И. Розновец, Д.Д.Волощук //Інформатика та математичні методи в моделюванні, 2018. – Т.8,№1. –С.86-97

[5] Саати Т. Принятие решений. Метод анализа иерархий / пер. с англ. Р.Г. Вачнадзе. —М.: Радио и связь, 1993. — 278 с.

[6] Малахов, В.Є. Сервіс-орієнтований інформаційний ресурс кафедри ВНЗ в гібридній хмарній інфраструктурі. / В.Є.Малахов, Л.А.Волощук //Інформатика та математичні методи в моделюванні, 2017. – Т.7,№3. –С.240-249

Многослойный генератор ландшафта

Артем Григорян
кафедра математического обеспечення компьютерних систем
Одесский национальный университет им. И.И.Мечникова
Одесса, Украина
grigoryan.artem.j@gmail.com

Евгений Малахов
кафедра математического обеспечення компьютерних систем
Одесский национальный университет им. И.И.Мечникова
Одесса, Украина
eugene.malakhov@onu.edu.ua

Multilayer Landscape Generator

Artem Grigoryan
Dept. of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
grigoryan.artem.j@gmail.com

Eugene Malakhov
Dept. of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
eugene.malakhov@onu.edu.ua

***Аннотация* — в ряде предметных областей таких, как управление кризисными службами, существует необходимость моделирования некоторой части окружающего мира, её визуализации с целью прогнозирования развития природных явлений, катастроф или стихийных бедствий. В коммерческой сфере аналогичная задача стоит при создании некоторых видеоигр. Основой таких моделей является мир или местность, сгенерированная случайным или псевдослучайным образом.**

Целью работы является создание многослойного генератора ландшафта, в котором каждый слой обладает специфическими свойствами. Генерация проходит в четыре этапа: создание слоя, создание маски, фильтрация и «склейка» с другими слоями. Каждый слой представляет собой карту высот, полученную одним из трёх способов: случайная генерация с помощью генератора шумов, использование данных программы Shuttle Radar Topography Mission, импорт некоторого графического файла. С каждым слоем ассоциирован слой-маска, который ограничивает влияние слоя на другие слои. Кроме того, каждый слой может быть подвергнут фильтрации, например, для сглаживания рельефа, поворота слоя на некоторый угол, отражения по вертикали или горизонтали и т.п. Так как для генерации случайной карты высот требуется генератор шумов, было приятно решение создать генератор, который имеет возможность расширения с использованием плагинов.

***Abstract* — in array of subject areas such as the management of crisis services, there is a necessity of some part of the surrounding world model, its visualization in order to predict the development of natural phenomena, disasters or natural disasters. In the commercial sphere, a similar task is worthwhile when creating some video games. The basis of such models is the world or locality generated in a random or pseudo-random manner.**

The aim of the work is to create a multi-layered landscape generator, in which each layer has specific properties. Generation takes place in four stages: creating a layer, creating a mask, filtering and "splicing" with other layers. Each layer is a map of heights, obtained in one of three ways: random generation using a noise generator, the use of Shuttle Radar Topography Mission data, the import of a certain graphic file. Each layer is associated with a mask layer, which limits the effect of the layer on the other layers. In addition, each layer can be filtered, for example, to smooth out the relief, rotate the layer to some angle, reflect vertically or horizontally and so on. Since a noise generator is required to generate a random heights map, it was decided to create a generator that can be expanded using plug-ins.

Ключевые слова — генерация ландшафта, генерация шума, бесшовные карты высот, многомерный шум.

Keywords — landscape generation, noise generation, seamless height maps, multidimensional noise.

I. Введение

Согласно исследованию Oxfam [1] за 2011 год, которое затронуло более чем 140 стран. За почти треть века зафиксирован заметный рост климатических катастроф: с 133 в 1980 году до 350 в 2010. После 1975 года в результате катастроф и стихийных бедствий погибло более 2,2 миллионов человек. Две трети смертей были вызваны катастрофами, связанными с климатом. В предыдущем исследовании Oxfam, проведенном в 2009 году, природные бедствия каждый год в среднем затрагивали порядка четверти миллиарда человек.

Причём, подавляющее большинство катастроф – 98% были климатическими.

Также согласно исследованию Interactive Software Federation of Europe[2] за 2008 год, в ходе которого была собрана статистика 5 различных регионов в результате опроса людей в возрасте от 16 до 49 лет, выяснив, что видеоигры находятся в числе самых популярных способов проведения досуга. Около 40 процентов опрошенных заявили, что играют от 6 до 14 часов в неделю. 72 процента опрошенных используют видеоигры в качестве развлечения. 57 процентов опрошенных отмечают, что подобный способ развлечения помогает им стимулировать воображение, а 45 процентов заявили, что видеоигры заставляют их думать.

Две вышеперечисленные предметные области объединяет задача генерации ландшафта, в первом случае, для проведения симуляции в уникальных географических условиях, при этом стоит задача генерации максимально правдоподобного ландшафта, учитывая множество свойств реальной окружающей среды, таких как: температура, давления, скорость и направление ветра и т.д. Во втором случае задача состоит в том, что необходимо создать продуманный ландшафт, который будет подходить под игровой дизайн, и будет обладать необходимыми для видеоигры свойствами. Целью работы является создание и реализация метода генерации ландшафта, которой мог бы удовлетворить следующие условия:

- Ландшафт должен делиться на тайлы, для возможности масштабирования детализации генерируемой поверхности, каждый тайл – это небольшой участок строго заданного размера.
- В каждом тайле должна содержаться информация, которая могла бы меняться в зависимости от предметной области, с помощью плагинов.
- При генерации должна быть возможность создания существующего ландшафта, или приближенного к нему.
- Необходима возможность создания случайного, однако однотипного ландшафта, который отличался бы в деталях, однако глобальная структура, которого была бы изначально заданна.

II. Обзор методов в системах генерации ландшафта

К системам генерации ландшафта можно отнести следующие программные продукты:

A. Bryce

Bryce – как в 3D-редакторах, основу сцены в Bryce составляют объекты: в отношении объектов можно применять булевы операции, управлять их освещением, присваивать материалы-текстуры и т.п. Однако, наряду со стандартными примитивами, в пакете имеются и особые объекты, представляющие собой части пейзажа: облака, плоскость земли и воды, горы и камни [3].

B. Vue 5 Esprit

Vue 5 Esprit – для создания рельефа можно автоматически сгенерировать какой-нибудь вариант горного ландшафта с помощью модуля Terrain, который в свою очередь использует генератор шума, а можно воспользоваться редактором рельефа и создать нужный рельеф вручную при помощи специальных инструментов. Для этого сначала задается приблизительная форма поверхности (каньон, дюны и т.п.), а затем результат корректируется специальными средствами. По окончании работы, для придания рельефу большей естественности, можно дополнить его каменными глыбами и наложить специальные эффекты, позволяющие имитировать различные варианты эрозии. Возможна генерация ландшафта на основе обычной карты высот [4].

C. World Builder

Создание ландшафта начинается с формирования рельефа в окнах проекций. Сначала из набора векторных линий строится каркас будущей местности, затем полученная векторная система фрактализуется путем добавления в нее случайных элементов по определенному фрактальному закону, а потом вычисляется положение всех элементов ландшафта относительно уровня моря, в результате чего формируется пространственный каркас моделируемой местности. Созданный рельеф можно сгладить, применить к нему эрозию, покрыть его снегом или льдом и т.п. Можно внедрить в готовый ландшафт и дороги, для чего нужно просто нарисовать соответствующую дороге кривую [5].

D. VistaPro

Основой построения рельефа являются цифровые карты высот DEM (Digital Elevation Maps). Можно воспользоваться существующими картами высот из американских баз данных Geological Survey и NASA и создать, например, реальный пейзаж Большого каньона или Фудзиямы. Можно обратиться к встроенному генератору рельефа, который предложит бесконечное число вариантов случайно сформированных карт высот, а можно отсканировать топографическую карту любой местности и импортировать ее в форматах PCX, BMP и TGA — по такой карте VistaPro самостоятельно создаст карту высот и сформирует на ее основе рельеф. Полученный рельеф можно подвергнуть эрозии, сгладить и т.д. При желании несложно экспортировать полученный пейзаж в трехмерную программу моделирования и рендеринга [6].

E. Terragen

Все составляющие пейзажа (рельеф, вода, облака, атмосфера, освещение) представлены в виде отдельных слоев, которые последовательно наносятся друг на друга и могут быть скорректированы на всех стадиях его подготовки. Рельеф местности определяется картой высот, которую можно нарисовать самостоятельно, сгенерировать автоматически или импортировать из другого приложения. К тому же для каждого из названных параметров имеется очень большое количество

настроек, и от каждой из них зависит конечный результат [7].

F. GenesisIV

GenesisIV – в пакете реализованы поддержка баз данных ГИС, возможности фотореалистического рендеринга и применение инструментов картографии, вследствие чего программа в основном ориентирована не на художников, а на тех пользователей, которые работают с геоинформационными системами, поскольку GenesisIV предоставляет им привычные инструменты для визуализации ландшафтов по ГИС-данным. Так, GenesisIV можно воспользоваться для быстрого создания пейзажей на основе реальных данных из базы данных карт высот, что позволит наглядно представить ту или иную информацию для клиентов компании (при этом подключать художника не потребуется).

G. Анализ методов

Так как любой ландшафт можно представить в виде карты высот, то при генерации ландшафта главной задачей является именно её создание. По результатам анализа методов, которые используют вышеперечисленные системы, можно сделать вывод, что они в основном использует три варианта получения карты высот:

1) генератор шума

Преимущества:

- большая вариативность генерируемой поверхности;
- масштабируемость;
- возможность тонкой настройки генераторов;
- возможность создания бесконечного ландшафта;
- скорость создания.

Недостатки:

- отсутствие сходства с реальным ландшафтом;
- сложность создания бесшовного ландшафта.

2) созданная вручную карта высот

Преимущества:

- возможность создания бесшовного ландшафта;
- точная настройка параметров и свойств карты.

Недостатки:

- сложность;
- скорость;
- невозможность создания бесконечного ландшафта.

3) импортированая из геоинформационных систем

Преимущества:

- сходство с реальным ландшафтом;

Недостатки:

- невозможность создания бесшовного ландшафта;
- невозможность создания бесконечного ландшафта;
- большой объем хранимых данных.

III. Технология генерации многослойного ландшафта

Технология, положенная в основу многослойного генератора ландшафта должна предоставить возможность комплексного или последовательного использования различных методов генерации среды таким образом, который обеспечит нивелирование недостатков отдельных методов. Технология генерации состоит из четырёх этапов.

A. Первый этап. Создание слоев

Первым этапом является создание слоев, путем генерации базовой поверхности. В рамках данной технологии базовыми способами генерации были выбраны: генерация с помощью шумов, импорт карт высот и использование карты высот, полученных в результате миссии Shuttle Radar Topography Mission[8].

Однако в разрабатываемом продукте все методы подключаются с помощью системы плагинов, что даёт возможность в зависимости от предметной области, использовать для генерации поверхности любые существующие методы и алгоритмы. Например, такие как Diamond-Square, предложенный компанией Mojang AB.

B. Второй этап. Создание маски слоя

На втором этапе создается маска для каждого слоя. Маска слоя – двухмерная матрица, которая состоит из вещественных чисел в диапазоне [0,1]. В дальнейшем маска слоя применятся к базовой поверхности, тем скрывая ненужные участки генерируемой ранее поверхности. Таким способом мы можем сгенерировать случайный ландшафт, с неслучайной местностью. По умолчанию маска слоя должна быть “белой”, и никаким образом не влиять на слой. Маску слоя можно создать в ручном режиме, закрашивая области специальной кистью, подгрузить готовую маску, или сгенерировать.

C. Третий этап. Применение фильтров

На третьем этапе к слою можно применить различные фильтры, которые так же должны иметь возможность расширения с помощью плагинов. Фильтр – любая операция над слоем, к примеру, переворот на n градусов, или же отражение по оси. Так же должны быть предусмотрены фильтры, для выделения, и сглаживания частот.

D. Четвертый этап. Склейка слоев и постообработка

На последнем этапе выполняется склеивание слоев. Имея набор бинарных, арифметических операции а, также дополнительные операции, которые поставляются в виде плагинов, мы можем использовать их комбинацию для того, чтобы получить результирующую поверхность. Операции описываются с помощью функций от двух аргументов.

После склейки слоев, в каждом тайле ландшафта, генерируется необходимые свойства. Базовыми свойствами является температура, влажность, биом. Все свойства являются настраиваемыми. Карта

температур является произведением градиентного и фрактального шума, что придает реализма, разбиение на широты. Аналогичным образом относительно высоты тайла корректируется температура. Карта влажности представляет собой фрактальный шум, скорректированный, относительно высоты тайла. Биом определяется согласно классификации Уиттекера (рис.3.1) на основе средней годовой влажности и средней годовой температуры. Помимо базовых свойств тайла, можно задать постобработку полученного ландшафта. Например, для решения задачи прогнозирования стихийных бедствий введен модуль, который позволяет генерировать на полученном ландшафте некоторую инфраструктуру, такую как населенные пункты и дороги. Населенные пункты, представлены в трех вариациях: город, поселок городского типа, село, отличия заключаются в наличие различных средств, и их объема, для ликвидации последствий стихийных бедствий. Дороги представлены двух типов: междугородняя магистраль, и обычная дорога. Свойства тайла и варианты постобработки можно дополнить с помощью плагинов.

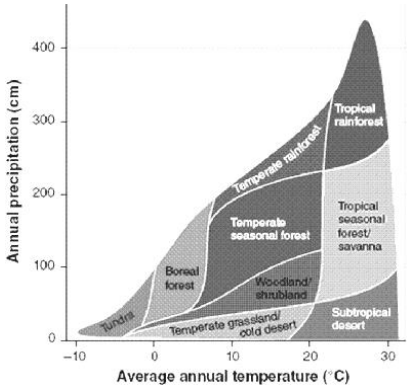


Рис.1. Классификация Уиттекера

E. Ключевые модули и особенности многослойного генератора ландшафта

1) генератор шума

Одним из ключевых модулей является генератор шумов, который создает базовую поверхность для слоя. Генератор должен в себя включать возможность использование любого, из следующего видов шумов: Value Noise; Perlin Noise; Simplex Noise; Cubic Noise; Cellular Noise; White Noise.

Каждый из шумов порождает отличную от другого шума текстуру, которую можно использовать для генерации различных типов местности. К примеру, для получения ландшафта в виде типичного океанического острова можно использовать шум Перлина с наложенной на него маской в виде радиального градиента, размещенного в центральной области карты. Для имитации береговой линии с эрозией можно использовать белый шум, а для имитации сглаженного океанического дна – сотовый шум.

2) бесшовные карты высот

Для создания карт на таких поверхностях как тор, сфера, цилиндр, требуется бесшовный вариант шума. Для выполнения данной задачи, принято решение использовать многомерный шум, спроецированный в пространство с меньшей размерностью. Для данной цели используется лента Мебиуса (1), которая позволяет добиться бесшовности по одной из осей и восьмерка Клейна (2), с помощью которой можно добиться бесшовности по двум осям.

$$\begin{aligned} x(u,v) &= \left(1+\frac{v}{2}\cos\frac{u}{2}\right)\cos u,\\ y(u,v) &= \left(1+\frac{v}{2}\cos\frac{u}{2}\right)\sin u,\\ z(u,v) &= \frac{v}{2}\sin\frac{u}{2}, \end{aligned} \tag{1}$$

где *x, y, z* – координаты для многомерного шума; *v* – задает расстояние от края ленты; *u* – отклонение от центральной линии ленты.

$$\begin{aligned} x(r,u,v) &= \left(r+\cos\frac{u}{2}\sin v-\sin\frac{u}{2}\sin 2v\right)\cos u\\ y(r,u,v) &= \left(r+\cos\frac{u}{2}\sin v-\sin\frac{u}{2}\sin 2v\right)\sin u\\ z(r,u,v) &= \sin\frac{u}{2}\sin v+\cos\frac{u}{2}\sin 2v \end{aligned} \tag{2}$$

где *x, y, z* – координаты для многомерного шума; *r* – константа, выбранный радиус круга; *v* – обозначает положение около 8-образного сечения; *u* – задаёт угол на плоскости XY.

Это позволяет адресоваться к какой-либо точке бесшовной поверхности для генерации шума путём задания двухмерных координат *u* и *v* в виде параметров.

IV. Вывод

На основе предложенных методов была спроектирована система, которая позволяет генерировать ландшафт, используя существующие методы, которые возможно подключать с помощью плагинов, а также накладывать на них различные фильтры и маски. Созданный в рамках проекта программный продукт может быть использован для симуляции природных явлений, катастроф, стихийных бедствий в системах управления кризисными службами (МЧС, медицины катастроф и пр.), а также для создания реалистичного ландшафта местности в видеоиграх или кинематографе. Технология плагинов обеспечивает дальнейшее развитие и расширение функционала системы не только со стороны разработчиков, но и обычными пользователями, которые ознакомились со спецификацией модулей.

ЛИТЕРАТУРА

[1] Weather cataclysm became four times larger [Online]. Available: http://news.bbc.co.uk/hi/russian/sci/tech/newsid_7111000 /7111805

[2] Research shows growing videogame popularity in Europe. [Online]. Available: https://www.gamesindustry.biz/articles/resear ch-shows-growing-videogame-popularity-in-europe

[3] Kitchens, Susan A. and Gavenda, Victor, Real World Bryce 4, page 18, Peachpit Press, 2000

[4] Magic of digital painting Vue 5 Esprit [Online].Available: https://itc.ua/articles/magiya_cifrovoj_zhivopisi_vue_5_esprit_19336/

[5] Kantrowitz, Barbara; Ramo, Joshua Cooper (Aug 28, 1994). "Garage-Band Programmers".

[6] VistaPro [Online]. Available: https://en.wikipedia.org/w/index.php?title=VistaPro&oldid=848538413

[7] Terragen 3. Planetside Software. 24 September 2014.

[8] Farr, T. G., et al. The Shuttle Radar Topography Mission, Rev. Geophys., 45, RG2004.

Исследование аппаратной реализации метода регистрации активности блоков LUT в составе FPGA-базированных устройств

Константин Защелкин
Кафедра компьютерных интеллектуальных систем и сетей
Одесский национальный политехнический университет
Одесса, Украина
const-z@te.net.ua

Александр Дрозд
Кафедра компьютерных интеллектуальных систем и сетей Одесский национальный политехнический университет
Одесса, Украина
drozd@ukr.net

The study of hardware realization for activeness registration method of lut units including in FPGA-based devices

Kostiantyn Zashcholkin
Department of Computer Intelligent Systems and Networks
Odessa National Polytechnic University
Odessa, Ukraine
const-z@te.net.ua

Oleksandr Drozd
Department of Computer Intelligent Systems and Networks
Odessa National Polytechnic University
Odessa, Ukraine
drozd@ukr.net

***Аннотация*—Рассмотрены вопросы контроля целостности FPGA-базированных компонентов компьютерных систем. Отмечено, что одним из наиболее опасных видов нарушения целостности FPGA проектов является внедрение в проект вредоносных аппаратных закладок. Отмечено, что закладки могут быть имплантированы в систему в моменты ее плановой модификации, т.е. тогда, когда не действует контроль целостности, основанный на применении хэш-сум. Перед запуском контроля целостности необходима уверенность в том, что закладка не была внедрена в систему во время очередной плановой модификации. Рассмотрен метод, предназначенный для выявления возможных областей локализации вредоносных закладок в пространстве FPGA-базированных компонентов систем критического применения. Метод выполняет предварительную обработку проекта с целью выявления подмножества блоков LUT, в которых возможно локализованы схемы закладок. Указанный метод основан на анализе активности элементарных вычислительных блоков FPGA-базированной системы – блоков LUT (Look Up Table). Метод предполагает добавление в проект дополнительной схемы регистрации активности блоков LUT. Выполнен анализ возможных способов построения указанной схемы. Оценены достоинства, недостатки и ограничения вариантов реализации схемы. Выполнено сравнение предложенных схем и оценка целесообразности их использования.**

***Abstract*— The problems of the FPGA-based components integrity monitoring in safety-critical systems are considered. One of the most dangerous types of FPGA-based system integrity violation is the Hardware Trojans implantation. And a method necessary to detect the probable areas of hardware Trojans location in the space of FPGA-based components of computer systems is described. The method performs the preliminary project processing on the level of elementary computational units of FPGA-based system – LUT units (Look Up Table). The goal of the method is to detect the LUT unit subsets in which the Trojans' circuits are probably located. The presented method is based on the analysis of LUT unit activeness, i.e. the registration of value changes at these units outputs. The method offers to enter an extra circuit of LUT unit activeness registration in a project. The analysis of the possible ways of entering the mentioned circuits has been performed, and the advantages, disadvantages and restrictions of different circuit variants estimated.**

Keywords—FPGA, LUT, компьютерные системы критического применения, контроль целостности

Keywords—LUT-oriented architecture, FPGA, Safety-Critical Systems, Integrity Monitoring

I. Введение

Микросхемы FPGA находят значительное применение в качестве элементной базы для построения компьютерных систем, управляющих техническими объектами повышенного риска. Компьютерные системы такого рода принято называть системами критического применения [1]. Выбор FPGA для построения систем критического применения обусловлен, во-первых, возможностью изменения функций системы путем ее перепрограммирования, а во-вторых, более высокими показателями производительности, чем у микропроцессоров и микроконтроллеров [2]. Первый из указанных факторов позволяет выполнять функциональную оптимизацию системы без необходимости ее долговременного вывода из рабочего состояния. Это упрощает процессы: обновления функций системы;

устранения выявленных в процессе эксплуатации системы дефектов; выполнения оптимизации отдельных функций системы.

Одним из важных первичных атрибутов гарантоспособности для систем критического применения является *целостность* – свойство исключать непредусмотренные изменения системы и предоставляемых ею сервисов [3]. Изменения функционирования микросхем типа FPGA возможно только путем модификации их программного кода, из чего следует определение программного кода, как основного носителя целостности FPGA-базированных устройств. Таким образом, контроль целостности программного кода FPGA-базированных компонентов находится в наборе наиболее существенных составляющих обеспечения гарантососособности систем, построенных из таких компонентов.

II. Обзор публикаций и цель работы

Для систем критического применения одним из наиболее опасных видов нарушения целостности [4] является скрытая злонамеренная имплантация в систему аппаратных закладок (Hardware Trojans) [5]. Для FPGA-базированных систем закладки представляют собой скрытно внедренные в систему фрагменты вредоносного программного кода. Эти фрагменты создают в пространстве FPGA схему, которая обеспечивает вредоносную функцию закладки. Указанная схема может создавать искусственные неисправности в работе системы или осуществлять утечку конфиденциальной информации, обрабатываемой системой [6].

Внедрение закладки в FPGA-базированную систему может происходить как на этапе эксплуатации системы, так и на этапе ее проектирования. На этапе эксплуатации закладка имплантируется в программный код микросхемы FPGA. На этапе проектирования закладка представляет собой имплантированный в проект фрагмент высокоуровневого описания (HDL и/или схемотехнического описания), которое, в конечном итоге, транслируется в программный код.

Целостность проекта FPGA-базированной системы обычно обеспечивается путем получения хэш-сум для отдельных файлов проекта или для всего проекта целиком [7]. При этом хэш-суммы (при помощи, которых выполняется мониторинг целостности) прикрепляются к соответствующим файлам проекта или помещаются в структуру проекта. На этапе эксплуатации целостность программного кода FPGA-базированной системы может обеспечиваться либо отдельным файлом хэш-сумы, либо путем встраивания хэша непосредственно в программный код в виде цифрового водяного знака [8]. Имплантация вредоносной закладки в проект (систему) находящийся под мониторингом целостности, нарушает целостность и, следовательно, приводит к обнаружению факта имплантации. Однако в процессе проектирования описание системы модифицируются. В процессе эксплуатации возможно перепрограммирование системы. Такие легальные (разрешенные) изменения требуют остановки мониторинга целостности, внесения изменений, пересчета хэш-сум и повторного запуска мониторинга. Именно в моменты времени, когда из-за выполнения разрешенных изменений системы мониторинг целостности не осуществляется, возможно внедрение закладки в систему. Таким образом, перед повторным запуском мониторинга должно быть доказано, что в период приостановки мониторинга, в систему не были внесены непредусмотренные изменения (например, в виде вредоносных закладок).

Процесс выявления вредоносных закладок осложнен тем, что закладки обычно: а) замаскированы под аппаратные ресурсы, обеспечивающие основную функцию системы; б) создаются таким образом, чтобы усложнить их обнаружение в процессе тестирования системы; в) не проявляют себя в процессе эксплуатации системы до момента наступления события активации закладки.

В работе [9] предложен метод предварительной обработки проекта FPGA-базированной системы с целью выявления вероятных областей размещения вредоносных закладок в системах критического применения. Метод позволяет уменьшить область поиска закладки в пространстве микросхемы FPGA. Указанный метод основан на анализе активности элементарных вычислительных блоков FPGA-базированной системы – блоков LUT (Look Up Table) [10]. Основные положения метода базируются на том, что системы критического применения проектируются для функционирования в двух режимах: нормальном и аварийном. При этом компоненты систем функционируют в каждом из этих режимов на разных множествах входных слов [1]. Метод ориентирован на наиболее вероятный сценарий атаки на систему, при котором закладка проявляет себя только в аварийном режиме. В этих условиях наличие статистики активности вычислительных блоков LUT дает возможность анализировать изменение динамики участия этих блоков в вычислительном процессе, в каждом из режимов работы системы на характерных наборах входных слов. Метод предполагает добавление в проект дополнительной схемы регистрации активности блоков LUT.

Цель данной работы состоит в: а) исследовании возможных способов построения схемы, обеспечивающей выполнение указанного метода; б) формировании рекомендаций к выбору среди этих способов в зависимости от требований к условиям применения метода.

III. Основная часть работы

Метод, предложенный в работе [9] основан на встраивании в пространство целевой микросхемы FPGA схемы, которая регистрирует активность блоков LUT в процессе функционирования FPGA-базированной системы. Информация о активности блоков LUT может быть извлечена из схемы регистрации и использована методами последующего анализа для принятия решения о наличии или отсутствии вредоносных закладок, а также для точного выявления областей их размещения в пространстве микросхемы FPGA.

Схема регистрации активности блоков LUT состоит из одинаковых фрагментов, подключаемых к

выходам анализируемых блоков LUT (рис.1). Каждый из фрагментов состоит из двух подсхем:

- *подсхемы обнаружения активности блока LUT*, которая выдает на свой выход единичный сигнал только в том случае, если имеет место изменение значения на выходе анализируемого подсхемой блока LUT;
- *подсхемы фиксации активности*, которая фиксирует во внутренней памяти факт наличия или отсутствия изменений выходного сигнала блока LUT. Этот факт фиксируется в виде одноразрядного значения: нулевое значение соответствует отсутствию изменений выходного сигнала блока LUT, единичное – свидетельствует о том, что такое изменение имело место.

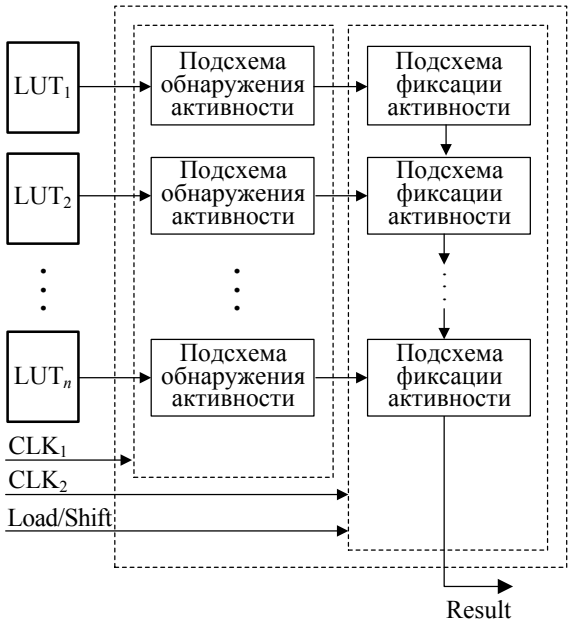


Рис. 1. Обобщенная структура схемы регистрации активности блоков LUT

Элементы внутренней памяти подсхем фиксации образуют сдвиговый регистр, из которого считывается двоичный вектор зарегистрированных активностей блоков LUT. Каждый разряд этого вектора закреплен за конкретным блоком LUT, что позволяет локализовать активные и пассивные блоки проекта.

В данной работе предлагается два базовых варианта реализации рассмотренной схемы в среде FPGA. Подсхемы обнаружения активности в обоих вариантах совпадают. Эти подсхемы состоят из синхронного D-триггера и элемента суммирования по модулю два. На выходе элемента суммирования по модулю два формируется логическая единица только в случае изменения значения на выходе блока LUT.

Базовые варианты схем отличаются способом построения схем фиксации активности. На рис. 2 представлен базовый вариант схемы, обеспечивающий фиксацию активности блока LUT посредством входа установки синхронного D-триггера (далее – первый вариант). В случае, если имеет место изменение входного значения, на выходе элемента суммирования по модулю два возникает единичное значение, которое передается на вход установки триггера подсхемы фиксации. В результате триггер подсхемы фиксации переходит в состояние логической единицы. После этого состояние данного триггера уже не зависит от изменений значения на выходе элемента суммирования по модулю два.

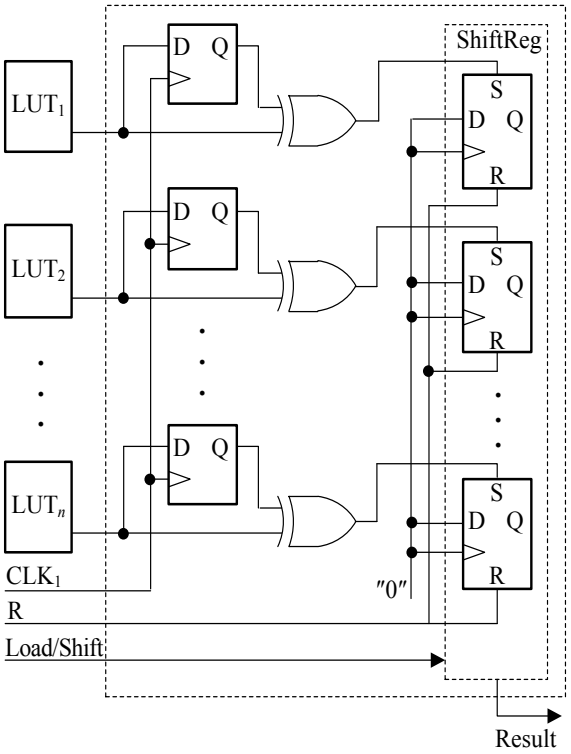


Рис. 2. Вариант схемы с обеспечением фиксации активности посредством входа установки триггера (первый вариант)

На рис. 3 представлен второй базовый вариант схемы, обеспечивающий фиксацию активности блока LUT посредством информационного входа триггера подсхемы фиксации. На информационном входе указанного триггера размещается элемент ИЛИ, охваченный обратной связью с выхода триггера. Такое подключение необходимо для невозможности перевести триггер в состояние логического нуля после его перехода в состояние логической единицы, которое фиксирует факт активности блока LUT.

Анализ рассмотренных базовых схем состоял в их синтезе и временном моделировании с последующим сравнением и оценкой затрат оборудования, а также результатов постсинтезного моделирования. Синтез и моделирование производились в системе проектирования Intel Quartus для целевых микросхем FPGA семейств Altera Cyclone II – Cyclone IV.

Затраты оборудования в среде FPGA оценивались в виде количества элементов памяти и вычислительных блоков LUT, использованных в соответствующих синтезированных схемах. В результате синтеза схем было установлено, что количество элементов памяти для обеих схем совпадает и составляет два элемента на каждый фрагмент схемы. Количество вычислительных блоков

LUT для первого (V_1) и второго варианта схемы (V_2) составляет соответственно:

$$V_1 = 2 + 5n;\ \ V_2 = 1 + 2n,$$

где n – количество фрагментов схемы.

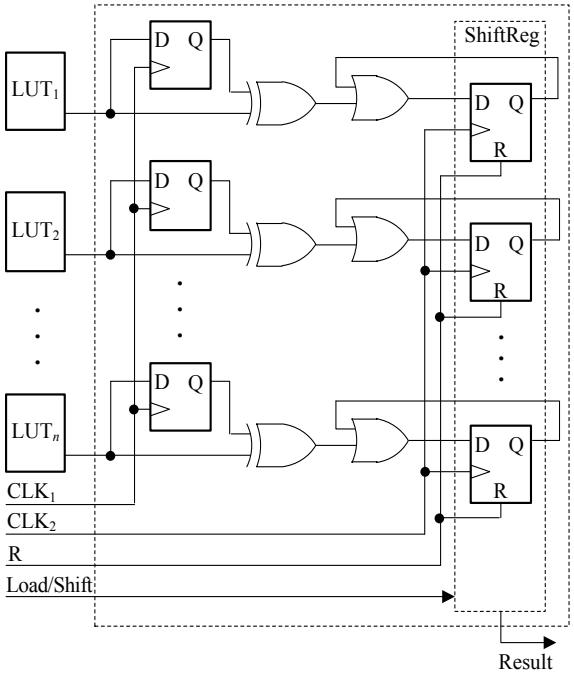


Рис. 3. Вариант схемы с обеспечением фиксации активности посредством информационного входа триггера (второй вариант)

Больший объем оборудования первого варианта схемы обусловлен спецификой реализации входа асинхронной установки триггеров в структуре микросхем FPGA. Такой вход отсутствует в явном виде в триггерах микросхем FPGA, рассматриваемых семейств. Функциональность триггера, обеспечиваемая асинхронным входом установки, искусственно реализуется через вход приема данных триггера при помощи дополнительной подсхемы, занимающей 4 блока LUT.

Однако, несмотря на указанный недостаток, первый вариант схемы имеет следующие преимущества по сравнению со вторым:

- дает возможность организовать более простую, и обеспечивающую меньшую задержку, конструкцию сдвигового регистра для извлечения результатов регистрации активности;
- в первом варианте схемы фиксация активности происходит асинхронно относительно функционирования подсхемы обнаружения активности. Во втором же варианте фиксация выполняется под управлением синхросигнала CLK_2, длина периода которого должна быть не больше длины регистрируемого изменения сигнала на выходе блока LUT.

Таким образом, в зависимости от требований условий применения рассмотренных схем регистрации активности блоков LUT может быть выбран один из базовых вариантов схем: вариант требующий меньших затрат оборудования (второй вариант) или вариант, не требующий тактирования подсхем фиксации активности и обладающий меньшей задержкой сдвига при получении результирующих данных (первый вариант).

IV. Выводы

В работе рассмотрены возможные варианты схемотехнической реализации метода [9], предназначенного для получения информации об активностях блоков LUT в FPGA-базированном устройстве. Метод применяется для решения задачи предварительной обработки проекта при поиске места локализации вредоносных аппаратных закладок.

Предложены два варианта схемы регистрации активности блоков LUT, отличающиеся затратами оборудования, способом фиксации обнаруженной активности и сложностью сдвигового регистра, необходимого для получения результирующих данных. Выполнено сравнение предложенных схем и оценка целесообразности их использования.

References

[1] A. Drozd, V. Kharchenko, S. Antoshchuk, J. Sulima and M. Drozd, "Checkability of the digital components in safety-critical systems: problems and solutions," IEEE East-West Design & Test Symposium, Sevastopol, Ukraine, 2011, pp. 411-416.

[2] W. Vanderbauwhede and K. Benkrid, (eds.), High-performance computing using FPGAs, New-York: Springer, 2016, 774 p.

[3] V. Kharchenko, V. Sklyar and E. Brezhniev, "Safety of information and control systems and infrastructures", Palmarium Academic Publishing, 2013.

[4] K. Zashcholkin and O. Ivanova, "LUT-object integrity monitoring methods based on low impact embedding of digital watermark," Proceedings of 2018 IEEE 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018, pp. 519-523.

[5] D. Mukhopadhyay and R. Chakraborty. Hardware Security: Design, Threats, and Safeguards, Boca Ration, Chapman and CRC, 2014, 542 p.

[6] M. Tehranipoor, H. Salmani and X. Zhang, Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection, Springer, 2013.

[7] J. Vacca, Computer and information security, 2nd edition, USA, Waltham: Morgan Kaufmann Publishers, 2013, 1280 p.

[8] F. Shih. Digital Watermarking and Steganography: Fundamentals and Techniques, 2nd edition, CRC Press, 2017.

[9] K. Zashcholkin and O. Drozd, "The detection method of probable areas of hardware trojans location in FPGA-based components of safety-critical systems," Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT'2018, 2018, pp. 220-225.

[10] J. Andina, FPGAs: Fundamentals, Advanced Features, and Applications in Industrial Electronics, CRC Press, 2017, 266 p.

Метод выявления и классификации дефектов в микролитографии

Михаленко Владислав
Факультет математики, физики и информационных технологий
ОНУ им. И.И. Мечникова
Одесса, Украина
mikhalenko.vladislav@stud.onu.edu.ua

Пенко Валерий
Факультет математики, физики и информационных технологий
ОНУ им. И.И. Мечникова
Одесса, Украина
vpenko@onu.edu.ua

Microlithography hotspot detection and classification method

Vladyslav Mykhalenko
Faculty of Mathematics, Physics and Information Technology
Odessa I.I. Mechnikov University
Odessa, Ukraine
mikhalenko.vladislav@stud.onu.edu.ua

Valerii Pienko
Faculty of Mathematics, Physics and Information Technology
Odessa I.I. Mechnikov University
Odessa, Ukraine
vpenko@onu.edu.ua

***Аннотация*—Современные микрочипы характеризуются экстремально малыми значениями проектной нормы, что приводит к возникновению брака в процессе изготовления интегральных схем. В 2000-х, с увеличением сложности чипов, стала чаще возникать проблема в процессе экспонирования масок: инструмент микролитографии (свет) начал проявлять волновую природу при обработке шаблонов с очень малой проектной нормой. Анализ проектных решений перед началом производства позволяет в какой-то мере решить данную проблему. Особенностью задачи выявления и классификации дефектов является отсутствие единого подхода к классификации существующих типов дефектов, это обусловлено сильным разнообразием этих областей. Современные методы, выявляющие и прогнозирующие местоположение дефектов, помимо неплохих результатов обладают недостатками, которые выражены в точности, длительности анализа, количестве ложных срабатываний. В данной работе предлагается метод для решения задачи выявления и классификации таких дефектов. Он базируется на использовании нейросетевого классификатора. Применяемые в данной работе свёрточные нейронные сети эффективно решают задачу классификации при условии заранее известного множества классов, что в данной задаче представляет самостоятельную проблему. Для выявления классов был использован метод симуляции процесса микролитографии. Исходные данные представлены в цифровом формате GDSII. Для осуществления симуляции они были конвертированы в пиксельные изображения. Процесс выявления классов осуществлялся эмпирически на основе экспертных оценок. Перед подачей на вход нейросетевого классификатора эти данные кодируются специальным образом. Это позволяет снизить размерность задачи (количество нейронов первого слоя).**

***Abstract*—Modern microchips can be characterized by extremely small resolution, which leads to integrated circuits manufacturing defect appearance. In the 2000s, due to increase of chips complexity, the problem in masks exposure began to arise more often: the main microlithography tool (light) began to exhibit a wave nature during the small resolution designs processing. Pre-manufacturing microlithography design analysis allows to resolve this issue. Due to a huge variety of known defects, a lack of the unified approach to defects classification increases the complexity of problem formalization. Modern defects detection and prediction methods, in addition to good results, have disadvantages, that are expressed in accuracy, analysis duration and the number of false positives. Defect identification and classification method is proposed in this paper. It is based on the use of the neural network classifier. The convolutional neural networks can effectively solve the classification problem in case of classes set availability. This is an independent task in this problem. To identify the classes, the microlithography process simulation was used. The initial data is represented in GDSII digital format. In order to perform the simulation, it was converted to pixel images. Classes identifying process was carried out empirically on the expert assessments basis. Before passing to the neural network classifier this data is encoded in a special way. This allows us to reduce the dimensionality of the problem (input layer neurons number).**

Ключевые слова—дефект, проектная норма, микролитографический проект, микролитография, GDSII, экспонирование маски, симуляция, микрочип

Keywords—hotspot, resolution, microlithography design, microlithography, GDSII, mask exposure, simulation, microchip

I. ВВЕДЕНИЕ

Микрочипы являются базой практически для всей современной электроники: они представляют собой электронную схему произвольной сложности, которая размещается на полупроводниковой основе

(подложке). Одной из основных технологий, используемых в изготовлении интегральных схем является *оптическая микролитография* - процесс формирования контактных дорожек путем экспонирования содержимого маски на подложку. В размеченных областях размещаются схемотехнические элементы. Любой микрочип характеризуется максимально допустимым размером контактных дорожек – проектной нормой. В микрочипах последних поколений эта характеристика находится в пределах 10-14 нм [1,2].

Современная индустрия изготовления микрочипов достигла высокой степени автоматизации всех производственных процессов и максимально приблизилась к предельным возможностям используемых инструментов. Область, в которой нарушается логика функционирования интегральной схемы принято называть ***hotspot***. Основным источником дефектов является инструмент микролитографии (***свет***): он проявляет неопределенность в процессе экспонирования шаблона из-за очень близкого расположения элементов на интегральной схеме.

Для преодоления такого рода ограничений в процессе изготовления микрочипов внедрялись технологии, направленные на коррекцию исходных шаблонов с целью минимизации возможности возникновения брака (например, Optical Proximity Correction [3]). Это, в некоторой степени, уменьшило проблему возникновения hotspot и позволило микролитографии сохранить актуальность, как подхода к изготовлению чипов. Однако задача выявления потенциальных hotspot сохраняет свою актуальность, т.к. с уменьшением проектной нормы, возрастает вероятность их возникновения. Основные усилия были направлены на предварительный анализ проектных решений, что дает возможность уменьшить вероятность получения бракованной продукции и сохранить ресурсы.

Все подходы, решающие задачу выявления и классификации hotspot, можно разделить на три направления:

- *Симулирующие процесс микролитографии* – имеют высокую вычислительную сложность и требуют больших вычислительных ресурсов;
- *Pattern Matching методы* – заранее выявленные hotspot используются в качестве шаблонов для сопоставления и поиска дефектов;
- *Machine Learning методы* –как правило используют нейросетевые классификаторы и имеют большую перспективу в решении данной задачи [4]

Каждое из направлений имеет как преимущества, так и недостатки: точность, время работы и перспектива выявления новых видов hotspot. Существующие методы дают достаточно хорошие результаты [5,6,7]. Открытым остается вопрос их применимости к проектным решениям с меньшими масштабами.

Целью данной работы является разработка и реализация системы для классификации и выявления, дефектов в микролитографических проектах. Объектом исследования в рамках данной работы являются микролитографические проекты с содержащейся в них информацией.

Предмет исследования – дефекты, возникающие в при изготовлении интегральных схем, то есть в процессе экспонирования маски на полупроводниковую подложку.

В последующих пунктах будут описаны основные идеи и этапы функционирования разрабатываемой системы.

II. ДЕФЕКТНЫЕ ОБЛАСТИ HOTSPOT

A. Типы hotspot

Следует отметить, что не все искажения, возникающие в процессе экспонирования, нарушают логику работы микрочипа. При этом в данной предметной области существует классификация критических областей по виду топологических искажений:

- *Bridging* - появление контакта между находящимися рядом несовместимыми элементами ИС;
- *Pinching* - ухудшение или полное исчезновение контакта между частями целостного элемента интегральной микросхемы.

Каждый из указанных типов, по характеру проявления, может быть жестким и мягким (*hard* и *soft* соответственно) [8]. Более наглядно типы HS приведены на Рис.1

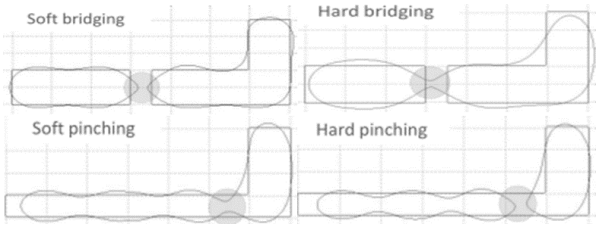


Рис. 1. Типы hotspot по характеру топологического влияния

Следует отметить, что на возникновение прведенных на Рис.1 примеров повлияли находящиеся в близи графические примитивы. Достаточно часто примеры hotspot предоставляются в виде окресности с расположенной в них дефектной областью, так как именно близко расположенные элементы играют ключевую роль в возможности возникновения брака [9].

B. Особенности задачи выявления и классификации hotspot

Вся информация в проектных решениях представляется в виде графических примитивов. Топологический анализ в таком случае не дает эффективных результатов: высока вероятность ложных выводов. Использование нескольких подходов к прогнозированию местоположения hotspot требует наличия оценочных характеристик, которые бы в достаточно наглядной форме позволяли оценивать качество и эффективность анализа. В

рамках решения рассматриваемой задачи существуют термины, для обозначения результатов анализа:

- *Hot spots* – фактическое множество дефектных областей в конкретном проектной решении;
- *Prediction* – прогноз, множество областей микролитографического проекта, которые потенциально являются критическими.

Вместе Hot Spots и Prediction формируют ключевые характеристики, для оценки эффективности работы методов, выявляющих hotspot:

- *HIT* - корректно выявленные hotspot;
- *MISS* – hotspot, которые были упущены при анализе исходного микролитографического проекта;
- *EXTRA* – области, которые ошибочно были определены как hotspot.

При этом EXTRA охватывает множество ошибок первого рода, MISS – ошибки второго рода. Еще одной важной характеристикой является время выполнения анализа Рис.2.

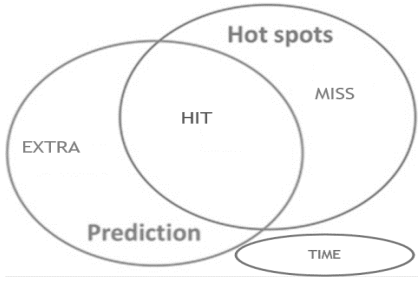


Рис. 2. Оценочные характеристики в рамках решения задачи выявления hotspot

Особенностью задачи выявления и классификации hotspot является отсутствие какой-либо типизации, существующих дефектных областей – это важным дополнительным условием при решении задачи классификации. В существующих методиках [4,5] типизация производится эмпирически авторами.

III. ИДЕИ И ПРИНЦИПЫ РАБОТЫ СИСТЕМЫ

A. Основные этапы функционирования

Работа классифицирующей модели может быть разделена на два основных этапа: обучение (калибровка) с учителем и непосредственная классификация входных данных. В качестве классификатора предполагается использование свёрточной нейронной сеть: это обусловлено характером представления данных в микролитографических проектах [11]. Этап обучения (Рис.3) подразумевает наличие обучающей выборки, которая будет состоять из закодированного представления микролитографического проекта и поставленного ему в соответствие выделенного класса hotspot. Рассмотрим это более подробно.

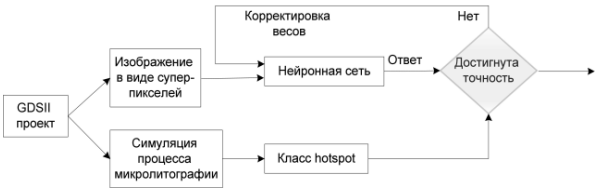


Рис. 3. Упрощенная схема процесса обучения нейросетевого классификатора

B. Кодирование исходных данных

Сегодня самым популярным форматом цифрового представления микролитографических проектов считается GDSII формат. За 40 лет ему удалось закрепиться в индустрии производства интегральных микросхем: подавляющее большинство микролитографических проектов представлено именно в нем. Данные представляются в виде графических примитивов (точек, линий, многоугольников, блоков) [10].

В таком виде информация о микролитографическом проекте не может быть использована свёрточными нейронными сетями [11]. Для этого была разработана процедура пикселизации GDSII проекта в точечное изображение. При этом исходные размеры анализируемой области могут достигать 1200x1200 пикселей. Такая размерность существенно скажется на скорости обучения нейронной сети. Потому мы предлагаем кодировать исходные данные *супер-пикселями* – исходное изображение разбивается на блоки фиксированного размера: размер которых выбирается таким образом, чтобы максимальное количество линий, попадающих в блок, не превышало двух. Исходя из визуального анализа примеров микролитографических проектов, предполагается выделение около 16 классов супер-пикселей. Такой подход позволит сократить размерность входных данных до 60 раз: коэффициент зависит от размеров исходного изображения и блока. Пример работы кодировщика приведен на Рис.4.

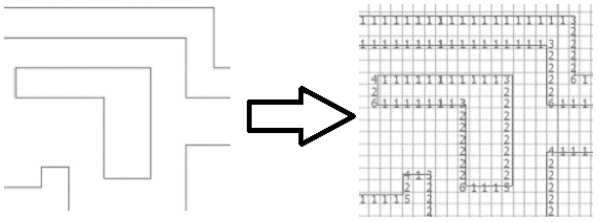


Рис. 4. Наглядный пример кодирования исходных данных (1 – горизонтальная линия, 2 – вертикальная, 3,4,5,6 – комбинация из двух линий, образующих прямой угол)

C. Классификация hotspot

Для обеспечения полноценного обучения нейронной сети наличие закодированных данных является недостаточным, необходимо иметь классы hotspot. Для решения данной подзадачи предлагается произвести субъективную классификацию hotspot. Для этого предполагается проведение симуляции воздействия оптического инструмента на содержимое микролитографического проекта. Поведение луча было сильно упрощено – это связано с ограниченностью знаний о нюансах процесса

микролитографии. Предполагается, что энергия луча подчиняется нормальному распределению (1).

$$g(x) = ae^{\frac{-(x-b)^2}{c^2}} \quad (1)$$

где a, b, c это числовые параметры: при этом a указывает высоту колокола, b отвечает за сдвиг по оси абсцисс, относительно начала координат, c – определяет ширину колокола функции Гаусса.

Таким образом, каждый пиксель исходного изображения наделяется значением энергии, которая будет накапливаться в процессе прохождения луча по контурам шаблонов образуя размытие в пределах текущего контура. В результате на изображении появляются области с критически высоким значением энергии (возникают в пределах слишком близко расположенных примитивов). Это рассматривается как критерий классификации hotspot. Далее исходные изображения с подобными «скоплениями» энергии объединяются в классы. Пример приведен на Рис.5.

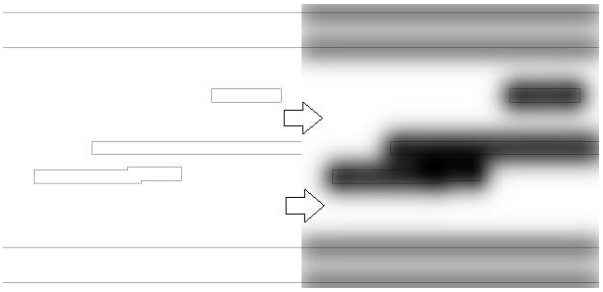


Рис. 5. Пример симуляции процесса микролитографии

Выявленные таким образом классы hotspot, позволили сформировать традиционное для нейросетевых подходов обучающее множество в виде пар (кодированный микролитографический проект и класс, к которому он относится).

ЗАКЛЮЧЕНИЕ

Индустрия изготовления интегральных схем нуждается в эффективных и точных решениях проблемы выявления hotspot. Развитие искусственного интеллекта предоставило гибкий и хорошо обучаемый инструмент, использование которого актуально для данной задачи. Существующие подходы уже дают положительные результаты, но их универсальность и гибкость не продемонстрирована в изученных ресурсах. Предложенные подходы и идеи являются перспективными для получения высокого уровня производительности и точности разрабатываемой системы выявления hotspot.

ЛИТЕРАТУРА

[1] news.sumsung.com – ‘Samsung Starts Industry’s First Mass Production of System-on-Chip with 10-Nanometer FinFET Technology’, Октябрь 17, 2016 [Электронный ресурс]. Режим доступа: https://news.samsung.com/global/samsung-starts-industrys-first-mass-production-of-system-on-chip-with-10-nanometer-finfet-technology;

[2] Mark Bohr, 14 nm Process Technology: Opening new horizonts (Intel), 2014 - 53 p.

[3] Smith, Bruce W., and Kazuaki Suzuki, eds, Microlithography: science and technology. Vol. 126. CRC press, 2007. – 864 p.

[4] Duo Ding, Xiang Wu, Joydeep Ghosh, David Z., Machine Learning based Lithographic Hotspot Detection with Critical-Feature Extraction and Classification IEEE International Conference on Integrated Circuit Design and Technology, Декабрь 2009 - 219-222 pages.

[5] Duo Ding EPIC: Efficient Prediction of IC Manufacturing Hotspots With a Unified Meta-Classification Formulation - 17th Asia and South Pacific Design Automation Conference Jan. 30 Февраля 2012.

[6] Moojoon Shin, Jee-Hyong Lee, CNN Based Lithography Hotspot Detection, International Journal of Fuzzy Logic and Intelligent Systems, Vol. 16, No. 3, Сентябрь 2016, pp. 208-215

[7] W.-Y. Wen, J.-C. Li, S.-Y. Lin, J.-Y. Chen, and S.-C. Chang, "A fuzzy-matching model with grid reduction for lithography hotspot detection," IEEE TCAD, vol. 33, no. 11, pp. 1671--1680, 2014

[8] Mark A. McCord, Stanford University Michael J. Rooks, Handbook of Microlithography: Micromachining and Microfabrication Institution Of Engineering And Technology, Январь 1997 – 776 p.

[9] William Andrew, Handbook of VLSI Microlithography: Январь 1991 – 671 p.

[10] GDSII Stream Format Manual Documentation №B97E060, Release 6.0, Фераль 1987, Calma – 47 p.

[11] Nielsen M., ‘Neural Networks and Deep Learning’, 2015. [Электронный ресурс]. Режим доступа - http://neuralnetworksanddeeplearning.com/

REFERENCES

[1] news.sumsung.com – ‘Samsung Starts Industry’s First Mass Production of System-on-Chip with 10-Nanometer FinFET Technology’, October 17, 2016 [Online]. Available - https://news.samsung.com/global/samsung-starts-industrys-first-mass-production-of-system-on-chip-with-10-nanometer-finfet-technology;

[2] Mark Bohr, 14 nm Process Technology: Opening new horizonts, Intel, 2014 - 53 p.

[3] Smith, Bruce W., and Kazuaki Suzuki, eds. Microlithography: science and technology. Vol. 126. CRC press, 2007. – 864 p.

[4] Duo Ding, Xiang Wu, Joydeep Ghosh, David Z., Machine Learning based Lithographic Hotspot Detection with Critical-Feature Extraction and Classification IEEE International Conference on Integrated Circuit Design and Technology, Dec 1 2009 - 219-222 pages.

[5] Duo Ding EPIC: Efficient Prediction of IC Manufacturing Hotspots With a Unified Meta-Classification Formulation - 17th Asia and South Pacific Design Automation Conference Jan. 30 2012-Feb. 2 2012.

[6] Moojoon Shin, Jee-Hyong Lee CNN Based Lithography Hotspot Detection International Journal of Fuzzy Logic and Intelligent Systems, Vol. 16, No. 3, September 2016, pp. 208-215

[7] W.-Y. Wen, J.-C. Li, S.-Y. Lin, J.-Y. Chen, and S.-C. Chang, "A fuzzy-matching model with grid reduction for lithography hotspot detection," IEEE TCAD, vol. 33, no. 11, pp. 1671--1680, 2014

[8] Mark A. McCord, Stanford University Michael J. Rooks, Handbook of Microlithography: Micromachining and Microfabrication Institution Of Engineering And Technology (January 1, 1997) –776 p.

[9] William Andrew, Handbook of VLSI Microlithography: January 1991 – 671 p.

[10] GDSII Stream Format Manual Documentation №B97E060, Release 6.0, February 1987, Calma – 47 p.

[11] Michael Nielsen ‘Neural Networks and Deep Learning’, 2015. [Online]. Available - http://neuralnetworksanddeeplearning.com/

Система шифрования на основе контекстно зависимых и регулярных грамматик

С.В Орлов
каф.МОКС, ФМФИТ
ОНУ им.И.И.Мечникова
Одесса,Украина
serorlov@ukr.net

The encryption system based on context-sensitive and regular grammars

S.V Orlov
Department of mathematical support of computer systems
Odessa National University
Odessa, Ukraine
serorlov@ukr.net

***Аннотация*—Будем рассматривать систему шифрования с открытым ключом. Используем метод раскрашивания. Для построения системы шифрования достаточно и бинарного раскрашивания. При этом шифруются лишь биты. Символы текста уже кодируются при помощи этих битов. Обычно рассматривается теория построения именно подобных алгоритмов. В подобных работах чаще всего не уделяется серьезного внимания практике. При бинарной раскраске существенно удлиняется зашифрованный текст. Ведь для каждого символа для кодирования используется обычно 8 бит. Каждый бит шифруется, словом длиной существенно большей единицы. В данной статье рассматривается система шифрования с 33 цветами раскраски. Это позволит существенно, минимум на порядок, сократить длину шифрованного текста. Помимо теории будет уделяться внимание практическому построению системы шифрования. Для каждой буквы русского алфавита будет отдельным конечным автоматом сгенерировано свое множество слов. Эти слова языка могут использоваться для зашифровки букв. Будет браться следующее слово из языка, если кодируемый символ встречается следующий раз. Контекстно-зависимой грамматика будет использоваться для фильтрования множества слов сгенерированных для шифрования букв. Подобное фильтрование позволит существенно повысить устойчивость системы шифрования от взлома.**

***Abstract* —We will consider the public key encryption system. We use the coloring method. To build an encryption system, binary colorization is sufficient. In this case, only bits are encrypted. The text characters are already encoded using these bits. Usually, the theory of constructing exactly similar algorithms is considered. In such works, most often not paid serious attention to practice. With binary coloring, the encrypted text is significantly extended. After all, for each character for encoding, usually 8 bits are used. Each bit is encrypted, with a word that is much longer than one. This article deals with an encryption system with 33 coloring colors. This will significantly reduce the length of the encrypted text, at least on the dowel. In addition to the theory, attention will be paid to the practical construction of an encryption system. For each letter of the Russian alphabet, its own set of words will be generated by a separate finite state machine. These words can be used to encode letters. The next word from the language will be taken if the encoded character occurs next time. Context-sensitive grammar will be used to filter a set of words generated for encryption of letters. Such filtering will significantly improve the stability of the encryption system from hacking.**

Ключевыеые слова — конечный автомат, шифрование, контекстно-свободная, регулярная, грамматика

Keywords — finite state machine, encryption, context-sensitive, regular, grammar

I. ВВЕДЕНИЕ

Будем рассматривать систему шифрования с открытым ключом. Используем метод раскрашивания. Для построения системы шифрования достаточно и бинарного раскрашивания. Так в работе [1] рассматривается теория построения именно подобных алгоритмов и без построения практических примеров. В данной статье рассматривается система шифрования с 33 цветами раскраски - для каждой буквы русского алфавита. И помимо теории будет уделяться внимание практическому построению системы шифрования. Существенное повышение крипто устойчивости будет осуществляться за счет применения контекстно-зависимой грамматики для фильтрования множества слов, сгенерированных для шифрования букв.

II. МЕТОД ШИФРОВАНИЯ

Подберем группу детерминированных конечных автоматов:

$DKA_i=\{V_s , V_t ,D_i, S\}$ i-тый конечный автомат,

где V_s – множество состояний;

V_t – входной алфавит;

D_i – функции переключения и выхода;

S – начальное состояние.

Собственно говоря, мы имеем частный случай конечных автоматов - детерминированные конечные распознаватели. Удобнее рассматривать их запись в виде таблиц. Будем использовать функции

выхода ={“Допустить”,” Отвергнуть”}. Выход по символу конец строки “CR” не будем использовать в автоматах.

Для генерации множества слов шифрующих i-тую букву алфавита будем использовать автоматы DKA_i, где $i=\overline{1,33}$. Очередное появление этой буквы будет зашифровано следующим словом из данного множества.

Упростить процесс создания конечных автоматов можно введя нулевой, шаблонный автомат DKA_0. Частично заполним исходный автомат функциями переключения состояний, например до половины. Оставшиеся клетки оставим пустыми. Тогда все остальные автоматы DKA_i можно построить, используя шаблонный, нулевой DKA_0 следующим образом [2]:

1) Множество клеток с функциями выхода ”Допустить” не должны пересекаться для DKA_i

2) Алфавит V_t может быть существенно шире, чем исходый. Ведь алфавит входного потока автомата не обязан вообще содержать буквы шифруемого текста. Поэтому можно использовать, например, Unicode символы в качестве V_t .

3) Функции ”Допустить” могут располагаться в одинаковых столбцах DKA_i. Тогда возможна неоднозначность при выборе очередного автомата для расшифрования.Однако вероятность получения двух разных легальных версий расшифрованного текста достаточного размера исчезающе мала. Очевидно, что устойчивость ко взлому такой системы шифрования будет существенно выше.

4) Функции переключения оставим одинаковыми для всех автоматов DKA_i

Полученные DKA_i приведем, если это необходимо. Для чего объединим эквивалентные и удалим недостижимые состояния. Процесс приведения актуален еще и как дополнительная проверка на корректность задания множества автоматов.

Каждому автомату DKA_i можно поставить в соответствие регулярные языки $L(DKA_i)$ для которых

$$\bigcap_{i=1} L(DKA_i)=\{\emptyset\} \quad , i=\overline{1,33} \qquad (1)$$

Последовательность входных символов однозначно определяет позицию, в которую автомат попадает под ее воздействием. Обратное утверждение не верно. Это очевидно по построению, так как:

a) Каждая из ”Допукающих” клеток DKAi определяет множество языка L(DKAi), в общем случае счетное.
b) Эти множества не пересекаются.

Полученные множества языков L(DKAi) не пересекаются и содержат не пересекающиеся множества слов. Каждый i-тый язык будет использоваться для кодировки i-той буквы алфавита, где $i=\overline{1,33}$.

Для шифрования очередной буквы с номером i будет использоваться следующее слово из $L(DKA_i)$. В идеале в одной шифровке для шифрования буквы лучше не использовать одно и то же слово языка.

Теоретически количество слов в одном языке может быть счетно. Однако, даже не используя Unicode (см. вариант-2), можно быть уверенным, что для шифрования текста приемлемого размера сгенерировать достаточно объемные множества слов языка не сложно.

Для данного алгоритма существует проблема удлинения зашифрованного текста.

Замечание 1. Для данного алгоритма раскраски в 33 цвета проблема удлинения зашифрованного на порядок менее значима, чем для черно-белой раскраски битов 0,1.

III. Пример шифрования и дешифрования

Для удобства будем все пустые клетки автомата считать выходом «Отвергнуть». Шаблонный нулевой автомат DKA_0 приводить не будем, но переключения во всех автоматах и часть пустых клеток будут одинаковы во всех DKA. Это упрощает автоматизацию при создании множества DKA_i, $i=\overline{1,33}$. Любая из распознанных DKA_i строк может использоваться для кодирования i-той буквы русского алфавита. Приведем для некоторых букв конечные распознаватели.

ТаблицаI. Конечный автомат для кодирования «E»

DKA_6-автомат кодирования буквы «E»							
«E»	a	b	c	d	e	f	g
S_0	S_3	S_0		S_2		S_3	
S_1			S_5		S_2		«Доп»
S_2		S_3			S_1	S_5	
S_3	S_0	S_4					S_0
S_4			S_5	S_2	S_3		S_1
S_5			S_2	S_0			

Распознаватель DKA_6 будет допускать такие строки $L(DKA_6)$ ={bbbdeg, aabdeg, deg, fgfbgg, dfceg, …}.

ТаблицаII. Конечный автомат для кодирования «K»

DKA_{12}-автомат кодирования буквы «K»							
«K»	a	b	c	d	e	f	g
S_0	S_3	S_0	«Доп»	S_2		S_3	
S_1			S_5		S_2		
S_2		S_3			S_1	S_5	
S_3	S_0	S_4					S_0
S_4			S_5	S_2	S_3		S_1
S_5			S_2	S_0			

Распознаватель DKA_{12} будет допускать такие строки $L(DKA_{12})$ ={bbc, c, aac, decdc, fgbbbc, dfdc, …}.

Для кодирования буквы «C» постоим автомат DKA_{19} .Распознаватель DKA_{19} будет допускать такие строки $L(DKA_{19})$ ={bbbdd, abdd, dd, fbccd, abcd, …}.

Распознаватель DKA_{20} будет допускать такие строки $L(DKA_{20})$ ={bbdfb, abcb, dfb, fbcb, …}.

Некоторые символы могут повторяться в допустимых строках счетное число раз. Например «b»

в первых строчках каждого из приведенных множеств. То есть мы можем теоретически этими автоматами сгенерировать счетное множество шифрующих их слов для каждой из букв.

ТаблицаIII. Конечный автомат для кодирования «С»

DKA_{19}-автомат кодирования буквы «С»							
«С»	a	b	c	d	e	f	g
S_0	S_3	S_0		S_2		S_3	
S_1			S_5		S_2		
S_2		S_3		«Доп»	S_1	S_5	
S_3	S_0	S_4					S_0
S_4			S_5	S_2	S_3		S_1
S_5			S_2	S_0			

Таблица IV. Конечный автомат для кодирования «Т»

DKA_{20}-автомат кодирования буквы «Т»							
«Т»	a	b	c	d	e	f	g
S_0	S_3	S_0		S_2		S_3	
S_1			S_5		S_2		
S_2		S_3			S_1	S_5	
S_3	S_0	S_4					S_0
S_4			S_5	S_2	S_3		S_1
S_5		«Доп»	S_2	S_0			

Так как функции выхода «Допустить» в примере не располагаются в одном столбце для разных автоматов, то можно заметить, что строки, шифрующие одинаковые буквы кириллицы заканчиваются на одинаковые буквы алфавита V_t. Один из вариантов шифрования слова «ТЕКСТ» может выглядеть следующим образом:

bbdfb deg c dd dfb

Очевидно, что пробелы я оставил лишь для наглядности дальнейшего процесса дешифровки. Удобнее дешифровывать текст с конца. Последняя латинская малая буква зашифрованного текста определяет DKA_i , при помощи которого шифровали последнюю заглавную букву русского алфавита. В случае неоднозначности обусловленной пунктом 3 усложнение будет не существенным.

Так как последняя у нас буква «b», то для шифровки использовалось множество $L(DKA_{20})$ и поэтому последней расшифрованной буквой будет «Т». Из этого множества подходит лишь слово «dfb». Слово «bbdfb» не подходит, так как нет букв «dd».

Последняя буква из оставшейся не расшифрованной строки «d». Значит, для шифровки использовалось множество $L(DKA_{19})$ и следующей с конца расшифрованной буквой будет «С». Из этого множества подходит лишь слово «dd».

Последняя буква из оставшейся не расшифрованной строки «c». Значит, для шифровки использовалось множество $L(DKA_{12})$ и следующей с конца расшифрованной буквой будет «К». Из этого множества подходит лишь слово «c».

Последняя буква из оставшейся не расшифрованной строки «g». Значит, для шифровки использовалось множество $L(DKA_6)$ и следующей с конца расшифрованной буквой будет «Е». Из этого множества подходят слова «deg». Однако, вспоминая о зацикливании буквы «b» в первом слове каждого из множеств $L(DKA_i)$ получим, что и слово «bdeg» возможно. Однако следующая расшифровка для оставшейся строки, в этом случае, предполагает завершение слова на букву «f». Таких слов у нас нет, поэтому остается лишь вариант шифрования при помощи слова «deg».

Последняя буква из оставшейся не расшифрованной строки «b». Значит, для шифровки использовалось множество $L(DKA_{20})$ и поэтому следующей с конца расшифрованной буквой будет «Т». Из этого множества подходит лишь слово «bbdfb». В результате дешифровки получим слово «ТЕКСТ».

Практическая реализация алгоритма получения множества языков $L(DKA_i)$ для кодирования букв затруднена. Ведь конечные автоматы DKA_i распознают слова, поданные на их вход. Вручную в статье подобрать подходящие слова не сложно. А какие именно слова подавать на вход автоматов в программе реализующей подобный алгоритм? Ведь множества должны быть достаточно мощными, так как от этого зависит качество шифрования. А поток случайных слов, поданный на вход автомата, не гарантирует быстрого и эффективного создания результирующих множеств.

Однако известно, что каждому конечному автомату DKA_i можно поставить в соответствие регулярную грамматику, генерирующую тот же язык $L(DKA_i)$. И алгоритм получения такой грамматики не так уж сложен. А вот уже процесс генерации из аксиомы грамматики очередного слова как раз нами и будет использоваться, возможно, в комбинации с конечным автоматом.

IV. ПОВЫШЕНИЕ КРИПТОУСТОЙЧИВОСТИ СИСТЕМЫ ШИФРОВАНИЯ

Полученная система шифрования будет не достаточно устойчива к взлому. В системе шифрования с открытым ключом языки $L(DKA_i)$ являются секретным ключом. Однако получив, каким либо образом, некоторое количество шифрующих слов из множества $L(DKA_i)$ можно попытаться восстановить конечный автомат DKA_i. Причем задача восстановления автомата из набора слов будет не сложной P-полной.

Для получения открытого ключа следует модифицировать языки $L(DKA_i)$. Известно, что конечные автоматы позволяют распознавать регулярные языки. В соответствии с классификации языков по Хомскому это языки 3 класса. Контекстно-зависимые языки являются языками 1 класса. Известно[3], что пересечение языков контекстно-зависимого и регулярного является языком 1 класса. Попытка взлома системы шифрования на основе полученных слов из множества языка контекстно-

зависимого является «трудной» NP-полной задачей [4].

Создадим контекстно-зависимые грамматики $КЗ_i$, где $i=\overline{1,33}$. Каждая из этих грамматик генерирует некоторое множество слов - язык $L(КЗ_i)$. Важно подобрать языки, имеющие не пустое пересечение с $L(DKA_i)$.

$$L(КЗ_i) \cap L(DKA_i)=L(G_i)\neq\{\emptyset\}, \text{ где } i=\overline{1,33} \quad (2)$$

Задаче не такая уж и сложная. Можно, например, считать гласные и согласные латинские буквы разными скобками (открывающими/закрывающими) и в некотором случае, в зависимости от контекста проводить их «балансировку».

Очевидно, что пересечения языков $L(G_i)$ можно использовать как «открытый» ключ для шифрования.

Каждому контекстно-зависимому языку можно поставить в соответствие машину Тьюринга с конечной лентой. На практике можно использовать упрощенные контекстно-зависимые алгоритмы. Например, «балансировать скобки» в достаточно простых легко определяемых контекстах. Тогда сама балансировка уже контекстно-свободная задача, для которой не сложно построить автомат с магазинной памятью $АМП_i$.

Реализация алгоритма поиска подмножеств слов определяющих открытый ключ будет предполагать для каждого $i=\overline{1,33}$:

1) Генерацию слов языка $L(DKA_i)$ с использованием, как конечного автомата, так и регулярной грамматики.

2) Поиск требуемого контекста в словах

3) Отсеивание слов автоматом с магазинной памятью $АМП_i$.

Поиск требуемого контекста в словах задача не всегда тривиальная для контекстно-зависимых грамматик. Подобные грамматики преобразуют, в промежуточных цепочках вывода слова, некоторые последовательности в зависимости от контекста. Но там могут быть и правила контентно-свободные. Поэтому, в некоторых случаях, преобразования возможны и без учета контекста. Вариантов таких преобразований может быть счетное множество.

Однако, в нашем случае, надо учитывать тот факт, что контекстно-зависимая грамматика подбирается специальным образом. Одним из критериев создания этой грамматики и является простота поиска контекста, для которого и производится отсеивание. То есть можно, например, для аксиомы грамматики написать единственное правило с определением контекста. Остальную часть правил грамматики взять контекстно-свободной. В правой части остальных правилах грамматики не использовать аксиому или делать это только тщательно просчитав последствия для усложнения поиска контекста. В этом случае контекст генерируемых слов грамматики будет легко определять.

Другим вариантом решения данной проблемы может быть использование расширений контекстно-свободных грамматик

Известно, что синтаксический блок транслятора проводит обычно, не только синтаксический анализ, но и семантический. Возможностей контекстно-свободной грамматики для этих целей не достаточно. Например, контекстно-свободные грамматики не используются для поиска ошибок подобных повторному использованию метки с тем же именем. Для описания алгоритмов такого анализа используются расширения контекстно-свободных грамматик. Эти расширения уже не являются контекстно-свободными и принадлежат классу, как минимум контекстно-зависимых грамматик.

Однако расширенные грамматики, используемые для описания алгоритма синтаксического блока, обладают одним важным для нас свойством. Этим грамматикам, не смотря на то, что они не являются контекстно-свободными, можно поставить в соответствие автомат с магазинной памятью. Примером такой грамматики является атрибутивная транслирующая грамматика – L(1).

Для этой грамматики, генерирующей некоторое множество слов, всегда можно построить автомат с магазинной памятью распознающий то же множество слов.

В случае создания открытого ключа при помощи фильтрации множеств подобными расширенными грамматиками пункт 2, поиск требуемого контекста в словах, можно будет опустить.

Зачем вообще такие ухищрения при фильтрации множеств созданных конечными автоматами. Дело в том, что непосредственное использование контекстно-зависимых грамматик является достаточно трудоемкой задачей. Как построение и использование эквивалентной машины Тьюринга с конечной лентой. А вот создание и работа автоматов конечного и с магазинной памятью задача достаточно простая. Подобные автоматы и работают быстро.

Литература

[1] Н.Ф. Богаченко, Р.Т.Файзуллин, “Автоматы грамматики алгоритмы”, Омск:Наследие,2006.,104с.

[2] С.В.Кондакова, С.В. Орлов, “Пример построения возможно односторонней функции на основе контекстно-свободной и регулярных грамматик“, сборник научных трудов “Науковий часопис НПУ імені М.П.Драгоманова. Серія 1. Фізико-математичні науки”, вып.13(2), 2012, с. 77-84

[3] John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman, “Introduction to automata theory, languages, and computation”, Addison-Wesley, 2001., 521p.

[4] М.Герри, Д.Джонсон, “Вычислительные машины и трудно разрешимые задачи”, М.:Мир,1982. ,419с.

REFERENCES

[1] N.F. Bogachenko, RT Fayzullin, "Automata of grammar algorithms", Omsk: Heritage, 2006., 104p.

[2] S.V. Kondakova, S.V. Orlov, "An example of constructing a possibly one-way function based on context-free and regular grammars", collection of scientific papers " Scientific journal of the MP Drahomanov NPU. Series 1. Physics and Mathematics, issue 13 (2), 2012, p. 77-84

[3] John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman, "Introduction to automata theory, languages, and computation", Addison-Wesley, 2001., 521p.

[4] M.Gerry, D.Johnson, "Computing Machines and Hardly Solvable Problems", M.: Mir, 1982. , 419p.

Моделирование динамики реактора производства витамина B_6

Алексей Стопакевич
Кафедра «Информатики и управления защитой информационных систем»
Одесский национальный политехнический университет
Одесса, Украина
stopakevich@opu.ua

Елена Улицкая
Кафедра «Компьютерных технологий автоматизации»
Одесский национальный политехнический университет
Одесса, Украина
ulitskaja@opu.ua

Modeling the dynamics of continuous stirred-tank reactor of B_6 vitamin production

Oleksii Stopakevych
Department of "Informatics and management of information systems protection"
Odessa National Polytechnic University
Odessa, Ukraine
stopakevich@opu.ua

Olena Ulitska
Department of "Computer technologies of automation"
Odessa National Polytechnic University
Odessa, Ukraine
ulitskaja@opu.ua

***Аннотация*—Рассматривается вопрос аналитического составления нелинейной модели динамики реактора производства витамина B_6 для дальнейшего синтеза системы управления. Используя законы действующих масс и химической термодинамики, модель составляется в виде системы дифференциальных уравнений, а их порядок определяется порядком реакции, протекающей в химическом реакторе. Процесс моделируется в классе нелинейных систем с сосредоточенными параметрами. Управляемыми параметрами являются концентрация конечного продукта, температура в реакторе и уровень продукта. Управлениями являются расходы концентрированной азотной кислоты, суспензии пиридона с уксусным ангидридом, охлаждающей воды в рубашку реактора. Модель дополнена аппроксимацией номограммы Колбрука-Уайта, для возможности учёта изменения коэффициента гидравлического трения в зависимости от скорости потока жидкости. Изменение коэффициента гидравлического трения обусловлено сущностью процесса регулирования, при котором в зависимости от степени открытия регулирующего органа протекает разное количество управляющего потока. Составлена модель комплексного влияния регулирующего органа на поток жидкости в трубопроводе с учётом скорости потока и коэффициента гидравлического трения, выбранной линейной или равнопроцентной расходной характеристикой регулирующего органа. Моделирование химического реактора с учетом нелинейных свойств системы дает результаты, отличающиеся от упрощенного представления системы.**

***Abstract* — The issue of analytical compilation of continuous stirred-tank reactor nonlinear model of vitamin B6 production for further synthesis of the control system is considered. Using the laws of acting masses and chemical thermodynamics, the model is compiled in the form of a differential equations system, and their order is determined by the order of the reaction proceeding in the chemical reactor. The process is modeled in the class of nonlinear systems with lumped parameters. The controlled parameters are the concentration of the final product, the temperature in the reactor and the product level. Controls are the consumption of concentrated nitric acid, a suspension of pyridone with acetic anhydride, cooling water in the jacket of the reactor. The model is supplemented by approximating the Colebrook-White nomogram, in order to consider the change in the coefficient of hydraulic friction as a function of the flow rate of the fluid. The change in the coefficient of hydraulic friction is due to the essence of the control process, in which, depending on the degree of opening of the valve, a different amount of the control consumption flows. A model of the complex influence of the valve on the flow of liquid in the pipeline is drawn up. It takes into account the flow velocity and the coefficient of hydraulic friction selected by the linear or equal-percentage flow characteristic of the valve. Modeling a chemical reactor with nonlinear properties of the system gives results that differ from the simplified representation of the system.**

Ключевые слова — нелинейная модель, химический реактор, витамин B_6.

Keywords - nonlinear model, chemical reactor, vitamin B6.

I. Введение

Актуальность разработки прецизионной САУ реактором синтеза витамина B_6 обусловлена тем, что витамин B_6 является ценным веществом для фармацевтической, пищевой и сельскохозяйственной отраслей промышленности. Хотя витамин B_6 можно создавать разными способами, но его перспективное промышленное производство основано на химическом синтезе. Процесс производства завершается нитрованием пиридона, подаваемого в виде суспензии с уксусным ангидридом в химический смесительный реактор непрерывного действия с рубашкой. Для фармацевтической промышленности требуется витамин стабильного состава с минимальным количеством примесей. Важным этапом построения

системы управления химическим реактором непрерывного действия, обеспечивающей стабильный состав продукта на выходе, является разработка математической модели динамики объекта управления.

II. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ХИМИЧЕСКОГО РЕАКТОРА

Реактор синтеза витамина B_6, с точки зрения моделирования представляет собой реактор идеального перемешивания, в который поступают потоки концентрированной азотной кислоты и суспензии пиридона с уксусным ангидридом. Реакция взаимодействия пиридона с кислотой является экзотермической, поэтому в реакторе предусмотрена рубашка для охлаждения смеси. Реакция нитрования является реакцией первого порядка [1].

Математическая модель реактора составлена на основе стандартных уравнений химической кинетики и термодинамики химических реакций [17]. Модель имеет вид:

$$\frac{dx_1}{dt} = \frac{(u_1 \cdot \rho_1 + u_2 \cdot \rho_2 - k_0 \cdot \sqrt{\frac{x_1}{S}} \cdot \rho)}{\rho}$$

$$\frac{d(x_1 \cdot x_2)}{dt} = u_1 \cdot C_1 + u_2 \cdot C_2 - k_0 \cdot \sqrt{\frac{x_1}{S}} \cdot x_2 - x_1 \cdot k \cdot e^{-\frac{E}{R \cdot (273 + x_3)}} \cdot x_2^n$$

$$\frac{d(x_1 \cdot x_3)}{dt} = \frac{\left(\sum_{i=1}^{2} u_i \cdot \rho_i \cdot c_i \cdot T_i - k_0 \cdot \sqrt{\frac{x_1}{S}} \cdot \rho \cdot c \cdot x_3 + x_1 \cdot k \cdot e^{-\frac{E}{R \cdot (273 + x_3)}} \cdot x_2^n \cdot H \right)}{c \cdot \rho} - \frac{c_в \cdot \rho_в \cdot u_3 \cdot (x_3 - x_4)}{c \cdot \rho}$$

$$\frac{dx_4}{dt} = \frac{c_в \cdot \rho_в \cdot u_3 \cdot (T_в - x_4) + S \cdot k_t \cdot (x_3 - x_4)}{c_в \cdot \rho_в \cdot V_в}$$

Принятые обозначения параметров модели и их номинальные значения приведены в табл. 2. Отдельно обозначим переменные, режимные значения которых подлежат заданию. Такими переменными будут $y_i = x_i$, i=1, 2, 3.

ТАБЛИЦА 1. ПАРАМЕТРЫ ПРОЦЕССА НИТРОВАНИЯ ПИРИДОНА

Параметр	Описание	Номинал	Ед.измерения
u_1	расход азотной кислоты	0,0028	$м^3/с$
u_2	расход суспензии пиридона	0,0106	$м^3/с$
u_3	расход хладагента	0,012	$м^3/с$
x_1	объём смеси в реакторе	4,8	$м^3$
x_2	молярная концентрация B_6	0,132	$кмоль/м^3$
x_3	температура н B_6	41	ºC
x_4	температура воды в рубашке	15	ºC
F	расход B_6	0,0152	$м^3/с$
C_1	молярная концентрация HNO_3	0,61	$кмоль/м^3$
C_2	молярная концентрация пиридона	0,129	$кмоль/м^3$
T_1	температура HNO_3	20	ºC
T_2	температура суспензии пиридона	41	ºC
k	константа скорости	$1{,}6 \cdot 10^{11}$	$с^{-1}$
E	энергия активации	83,25	кДж/моль
R	универсальная газовая постоянная	8,31	Дж/(моль·ºC)
n	порядок реакции	1	–
H	тепловой эффект нитрования	$1{,}5 \cdot 10^3$	Дж/моль
c	теплоёмкость B_6	1550	Дж/(кг·ºC)
ρ	плотность B_6	1431	$кг/м^3$
c_1	теплоемкость HNO_3	1744	Дж/(кг·ºC)
$ρ_1$	плотность HNO_3	1400	$кг/м^3$
c_2	теплоемкость суспензии пиридона	1529	Дж/(кг·ºC)
$ρ_2$	плотность суспензии пиридона	1696	$кг/м^3$
S	площадь теплообмена	14,6	$м^2$
k_t	коэффициент теплопередачи к воде	947	$Вт/(м^2 \cdot ºC)$
$V_в$	объём воды в рубашке	0,585	$м^3$
$c_в$	теплоемкость воды в рубашке	4179	Дж/(кг·ºC)
$ρ_в$	плотность воды в рубашке	992,1	$кг/м^3$
$T_в$	температура воды на входе	8	ºC

Приведём модель к стандартному виду. Для этого введем вектор–столбец *g*, который содержит правые части ДУ системы (1), и матрицу А, относящуюся к левой части ДУ. Тогда получим модель в виде:

$$\frac{dx_i}{dt} = A^{-1} \cdot g$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_2 & x_1 & 0 & 0 \\ x_3 & 0 & x_1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad A^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\frac{x_2}{x_1} & \frac{1}{x_1} & 0 & 0 \\ -\frac{x_3}{x_1} & 0 & \frac{1}{x_1} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} \frac{dx_1}{dt} \\ \frac{dx_2}{dt} \\ \frac{dx_3}{dt} \\ \frac{dx_4}{dt} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\frac{x_2}{x_1} & \frac{1}{x_1} & 0 & 0 \\ -\frac{x_3}{x_1} & 0 & \frac{1}{x_1} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix} \quad (1)$$

$$g_1 = \frac{(u_1 \cdot \rho_1 + u_2 \cdot \rho_2 - k_0 \cdot \sqrt{\frac{x_1}{S}} \cdot \rho)}{\rho}$$

$$g_2 = u_1 \cdot C_1 + u_2 \cdot C_2 - k_0 \cdot \sqrt{\frac{x_1}{S}} \cdot x_2 - x_1 \cdot k \cdot e^{-\frac{E}{R \cdot (273 + x_3)}} \cdot x_2^n$$

$$g_3 = \frac{\left(\sum_{i=1}^{2} u_i \cdot \rho_i \cdot c_i \cdot T_i - k_0 \cdot \sqrt{\frac{x_1}{S}} \cdot \rho \cdot c \cdot x_3 + x_1 \cdot k \cdot e^{-\frac{E}{R \cdot (273 + x_3)}} \cdot x_2^n \cdot H \right)}{c \cdot \rho} -$$

$$- \frac{c_в \cdot \rho_в \cdot u_3 \cdot (x_3 - x_4)}{c \cdot \rho}$$

$$g_4 = \frac{c_в \cdot \rho_в \cdot u_3 \cdot (T_в - x_4) + S \cdot k_t \cdot (x_3 - x_4)}{c_в \cdot \rho_в \cdot V_в}$$

Таким образом, разработана аналитическая нелинейная математическая модель динамики химического реактора непрерывного действия производства витамина B_6.

III. Разработка модели изменения коэффициента гидравлического сопротивления

Для расчета гидравлического трения λ в круглых трубах при изменении расхода, и, следовательно, изменения числа Рейнольдса, разработана специальная процедура. В качестве входных параметров процедура использует текущее значение числа Рейнольдса (Re), а также отношение внутреннего диаметра трубопровода к эквивалентной шероховатости трубы ($n_э$=D/$\Delta_{экв}$). Тело процедуры представляет собой аппроксимацию известной номограммы Колбрука–Уайта для определения коэффициента гидравлического трения λ, а также уравнение Стокса и аппроксимацию переходного режима. Для диапазона чисел Re>4000 разработанная нами модель имеет вид ($x = \ln(n_э)$):

$$\lambda = \frac{1.91 \cdot 10^4 \cdot x^{-5.2} + 39}{1000} + \frac{184.2 \cdot x^{-0.26} - 131.7}{1000} \cdot \left(1 - e^{-\lg(\mathrm{Re}) - \frac{\lg(4000)}{1.1410^{13} \cdot e^{-\left(\frac{x-56.5}{10.8}\right)^2}}} \right) \quad (2)$$

Для диапазона чисел Re<2000 при моделировании используется уравнение Стокса:

$$\lambda = 64 / \mathrm{Re} \quad (3)$$

Для диапазона чисел 2000<Re<4000 используется уравнение вида:

$$\lambda = 0.629 \cdot e^{-0.00216 \mathrm{Re}} + 0.0137 \cdot e^{-0.000274 \mathrm{Re}}. \quad (4)$$

Результат моделирования изображен на рис. 1 и соответствует номограмме Колбрука-Уайта [2].

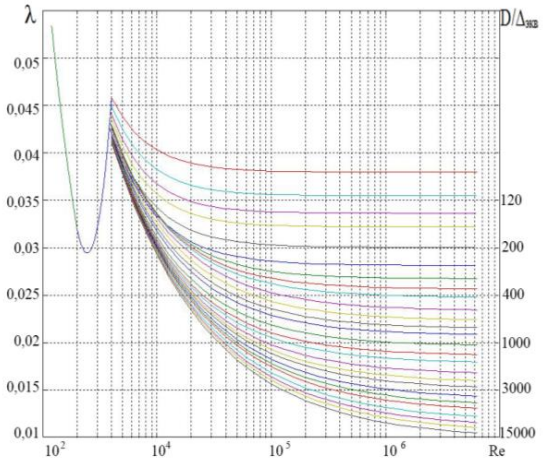


Рис. 1. Полученный график зависимости функции λ=f(Re, D/$\Delta_{экв}$)

При моделировании установлено отличие линейной и равнопроцентной расходных характеристик регулирующих органов, построенных с использованием переменного значения λ, от тех же характеристик, построенных с использованием усредненного значения λ. Переменное значение λ рассчитывалось по полученной аппроксимации.

IV. Разработка модели изменения расхода среды в регулирующем органе

Для окончательного получения влияния регулирующего органа (РО) на поток жидкости в трубопроводе с учётом скорости потока и λ, выбранной линейной или равнопроцентной расходной характеристикой РО, используется аналитическая модель вида:

$$Q = \sqrt{\frac{-K \cdot \gamma + \sqrt{K^2 \cdot \gamma^2 + 4 \cdot (K-1) \cdot Q_{\max}^2 \cdot \gamma}}{2 \cdot (K-1)}}, \quad (5)$$

где Q – объёмный расход среды, м3/с; Qmax – максимальный расход в системе при полностью открытом РО; γ – вспомогательный коэффициент; К – коэффициент, зависящий от формы пропускной характеристики РО.

Коэффициент К равен для линейной $K = 1/S^2$ и равнопроцентной $K = e^{7.82 \cdot (1-S)}$ пропускной характеристики РО, где S – степень открытия РО, (0<S<1) [3].

Вспомогательный коэффициент равен:

$$\gamma = \frac{(P_н - P_к + \Delta P_h) \cdot \pi^2 \cdot D^5}{8 \cdot \rho \cdot \left(\sum \xi \cdot D + L \cdot \lambda \right)}, \quad (6)$$

где Рн – начальное давление в линии, Па; Рк – конечное давление в линии, Па;

ΔPh – гидростатический напор, Па; ξ – коэффициент местного гидравлического сопротивления; ρ – плотность потока, кг/м3; L – длина прямых участков трубопровода, м; λ – коэффициент гидравлического трения; D – диаметр трубопровода, м.

Таким образом, полученные зависимости (5-6), позволяют учесть нелинейную зависимость расхода от степени открытия РО.

Результаты моделирования смесительного реактора непрерывного действия с использованием уравнений (1-6) представлены на рис.2.

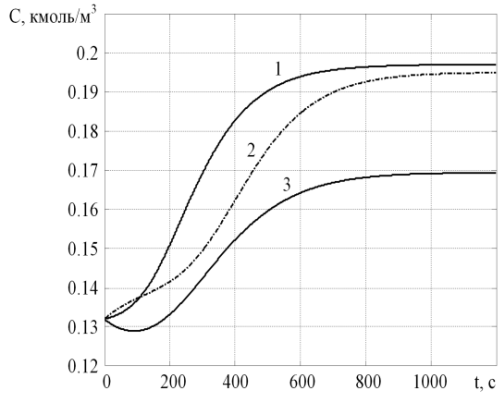


Рис. 2. Изменение молярной концентрации нитропиридона при нанесении возмущений (1 – увеличении расхода пиридона на 10%, 2 – уменьшении плотности пиридона на 15%, 3 – уменьшении молярной концентрации пиридона на 15%)

Выводы

1. Разработана модель химического реактора фармацевтической промышленности для синтеза витамина B_6, учитывающая взаимное влияние параметров, термодинамику и кинетику химической реакции, её порядок в соответствии со стандартами построения моделей химических реакций.

2. Разработана модель влияния характеристик регулирующего органа на поток управляющей жидкости, которая характеризуется учётом нелинейной зависимости расхода от степени открытия регулирующего органа.

3. Разработана модель изменения коэффициента гидравлического трения от расхода среды. Модель получена на основе аппроксимации номограммы Колбрука-Уайта. Показана высокая степень совпадения модели с оригиналом. Преимуществом разработанной модели учёта изменения коэффициента гидравлического трения является возможность её использования непосредственно в процессе управления.

Литература

[1] Коротченкова, Н. В. Витамины гетероциклического ряда. Строение, свойства, синтез, химическая технология [Текст]/ Н. В. Коротченкова, В. Я. Самаренко. – СПб: Изд–во СПХФА, 2006. – 80 с.

[2] Rennels, D. Hudson Pipe Flow: A practical and Comprehensive Guide [Text]/ D.Rennels, H. Hobart. – Hoboken, NJ: John Wiley & Sons, Inc., 2012. — 312 p.

[3] Казинер, Ю. Я. Арматура систем автоматического управления [Текст] / Ю.Я.Казинер, М. С. Слободкин. – М.: Машиностроение, 1977. – 136 с.

References

[1] Korotchenkova, N.V. Vitamins of the heterocyclic series. Structure, Properties, Synthesis, Chemical Technology [Text] / N.V.Korotchenkova, V.Y. Samarenko. - SPb: Publishing house of SPHFA, 2006. - 80 p.

[2] Rennels, D. Hudson Pipe Flow: A practical and Comprehensive Guide [Text]/ D.Rennels, H. Hobart. – Hoboken, NJ: John Wiley & Sons, Inc., 2012. — 312 p.

[3] Kaziner, Y.Y. Armature of automatic control systems [Text] / Y.Y.Kaziner, M.S. Slobodkin. - M .: Mechanical engineering, 1977. - 136 p.

Исследование топологических свойств масштабно-инвариантных эластичных сетей

Удовенко С.Г.
каф. Информатики и компьютерной техники ХНУЭ
Харьков, Украина
serhiy.udovenko@hneu.net

Шергин В.Л.
каф. Искусственного интеллекта ХНУРЭ
Харьков, Украина
vadim.shergin@nure.ua

Чалая Л.Э.
каф. Искусственного интеллекта ХНУРЭ
Харьков, Украина
larysa.chala@nure.ua

Загребельная М.Ф.
каф. Информационных технологий УкрГУЖТ
Харьков, Украина

On topological properties of elastic scale-free networks

Udovenko S.G.
Informatics and Computer Engineering dept.
KNUE
Kharkov, Ukraine
serhiy.udovenko@hneu.net

Shergin V.L.
Artificial Intelligence dept.
KHNURE
Kharkov, Ukraine
vadim.shergin@nure.ua

Chala L.E.
Artificial Intelligence dept.
KHNURE
Kharkov, Ukraine
larysa.chala@nure.ua

Zagrebelna M.F.
Information Technologies dept.
UkrSURT
Kharkov, Ukraine

***Аннотация*—Рассмотрена модель эластичной масштабно-инвариантной сети. Основной особенностью эластичных сетей являются разные относительные темпы роста числа узлов и связей между ними. Использование эластичности позволяет расширить область применения моделей масштабно-инвариантных сетей, в частности, позволяет строить модели плотных масштабно-инвариантных сетей. Важным топологическим свойством безмасштабных сетей является количество простых циклов, в частности, треугольных. Получена аналитическая зависимость количества циклов длиной три от размера сети и коэффициента эластичности. Показано, что зависимость количества циклов от размера сети обладает скейлинговыми свойствами. Она соответствует степенному закону, показатель которого линейно зависит от коэффициента эластичности. Проведён численный эксперимент по определению количества треугольных циклов в эластичных сетях для разных значений коэффициента эластичности. Результаты моделирования подтверждают корректность теоретических выводов.**

***Abstract*—A model of an elastic scale-free network is studied. The main feature of elastic networks is using different relative growth rates of nodes and links. Using the elasticity allows us to expand the scope of models of scale-free networks. For example, makes it possible to generate scale-free models for dense networks. An important topological property of scale-free networks is the number of simple cycles, in particular, triangular ones. An analytical dependence of the number of cycles of length three on the network size and the elasticity coefficient is obtained. It is shown that the number of cycles is subject to scaling. It follows asymptotically a power law with the exponent that depends linearly on the elasticity coefficient. A numerical experiment was performed to determine the number of triangular cycles in elastic networks for different values of the elasticity coefficient. The results of the simulation confirm the correctness of theoretical conclusions.**

Ключевые слова—масштабно-инвариантная сеть; предпочтительное присоединение; эластичность; треугольные циклы; скейлинг

Keywords—scale-free network; preferential attachment; elasticity; triangular loops; scaling

I. Введение

Теория масштабно-инвариантных сетей (англ. – scale-free networks) является относительно новой областью исследований сложных систем [1, 2]. В таких сетях распределение узлов по количеству связей является асимптотически степенным. Известно, что степенной характер такого распределения является характерным признаком наличия у сети фрактальных свойств [3]. Эти факторы обусловливают теоретический интерес к исследованию масштабно-инвариантных сетей. С другой стороны, многие сети реального мира являются безмасштабными, например, социальные сети, сети цитирований научных работ, некоторые транспортные сети, сети межбелковых взаимодействий и т. д. [1]. Таким образом, исследования масштабных сетей имеют весомую практическую значимость.

В основе моделей масштабно-инвариантных сетей находятся две базовые концепции: концепция роста и концепция предпочтительного присоединения. Самой популярной и простой моделью таких сетей является модель Барабаши-Альберт [1, 4]. В то же время классические модели масштабно-инвариантных сетей обладают рядом существенных недостатков и ограничений [5]. Ключевым из них является то, что в таких моделях средняя степень узла предполагается постоянной, в то время, как для большинства реально существующих сетей эта величина увеличивается с ростом сети. В работах [5, 6] предложено расширить перечень основных концепций масштабно-инвариантных сетей понятием эластичности, позволяющим учесть различие в темпах роста числа узлов и связей между ними. Модель эластичных

масштабно-инвариантных сетей представлена в разделе II.

Коэффициент скейлинга распределения узлов по числу связей существенно зависит от того, являются ли источником добавленных рёбер существующие случайно выбранные узлы, или же только новый узел, и варьируется от $\theta = 1 + 2/\lambda \le 3$ [5] до $\theta = 1/(1-\lambda/2) \ge 3$. В настоящей работе рассматривается второй из указанных частных случаев.

Как отмечено в [7], распределение узлов по числу связей является не единственным топологическим свойством сетей, подверженным скейлингу. Число простых циклов (длиной три или более) является одной из наиболее важных характеристик такого рода. В разделе III получена теоретическая оценка количества циклов длиной три в эластичных масштабно-инвариантных сетях.

II. Модель эластичной масштабно-инвариантной сети

Наиболее известной моделью масштабно-инвариантной сети является модель Барабаши-Альберт основанная на следующих базовых правилах [1,4]:

- на каждом временном шаге t в сеть добавляется новый узел (концепция роста) и соединяется с m существующими узлами;
- правило предпочтительного связывания: вероятность того, что новый узел будет присоединён к существующему узлу с номером k, пропорциональна его степени $D(k,t-1)$, т.е. количеству связей, уже имеющихся у данного узла:

$$p_{k,t+1}^{single} = \frac{D(k,t)}{\sum_k D(k,t)} = \frac{D(k,t)}{2E(t)}, \qquad (1)$$

где $E(t)$ – количество рёбер на шаге t перед добавлением узла с номером $t+1$.

Для моделей такого типа характерно постоянство числа добавляемых связей ($m = const$), однако в сетях реального мира средняя степень узла (количество связей в сети) имеет тенденцию возрастать с ростом сети и со временем наблюдения. В классических моделях масштабно-инвариантных сетей эта зависимость либо не рассматривается, либо рассматривается как внешний фактор. В результате такие модели отражают свойства реальных сетей лишь на узком интервале их масштаба. Кроме того ключевые свойства модели безмасштабной сети (например, показатель скейлинга) оказываются зависимыми от параметра m, имеющего масштаб.

Рассмотрим возможность модификации данной модели с применением концепции эластичности, в соответствии с которой относительные темпы роста узлов и рёбер отличаются друг от друга, а количество добавляемых рёбер $m(t)$ не является константой [6].

Обозначим число вершин, имеющих степень k, как $N(k,t)$, их общее число в момент времени t как $N(t)$, а общее число рёбер как $E(t)$.

Коэффициент эластичности λ ($1 \le \lambda < 2$) определяется как отношение относительного прироста числа ребер к относительному приросту числа вершин (со сдвигом на шаг назад):

$$\lambda = \frac{\delta E(t)}{\delta N(t-1)} = const \qquad (2)$$

Так как единицей измерения времени является количество узлов, т. е. $N(t) \equiv t$, то

$$\frac{E(t+1)-E(t)}{E(t)} = \lambda \frac{N(t)-N(t-1)}{N(t-1)} = \frac{\lambda}{t-1} \qquad (3)$$

Решение (3) имеет вид [3, 5]:

$$E(t) = \frac{\Gamma(t+\lambda-1)}{\Gamma(t-1)\Gamma(\lambda+1)}, \quad t > 1. \qquad (4)$$

При этом в момент времени $t = 1$ $E(1) = E(2) = 1$, что соответствует тому, что изначально сеть состоит из двух узлов, соединенных одним ребром.

Из (4) следует, что математические ожидания количества ребер, добавляемых в моменты $t+1$ и t, можно определить следующим образом:

$$m(t+1) = \lambda \frac{E(t)}{t-1} \qquad (5)$$

$$m(t) = \frac{\Gamma(t+\lambda-2)}{\Gamma(t-1)\Gamma(\lambda)} \qquad (6)$$

Важно отметить, что показатель распределения узлов по их степеням существенным образом зависит от того, как выбираются узлы-источники добавляемых ребер. Ими могут быть только новый узел, или же, помимо него, также и ранее добавленные. В данной работе рассматривается первый случай, как более простой.

Обозначим как $D(k,t)$ среднее число связей узла с номером k в текущий момент времени t. Рассматривая процесс добавления связей как процесс Бернулли с вероятностью успеха в одиночном испытании (1), получим:

$$p_{k,t+1} = p_{k,t+1}^{single} \cdot m(t+1) \qquad (7)$$

С учетом (1) и (5) получаем:

$$p_{k,t+1} = D(k,t) \cdot \frac{\lambda/2}{t-1} \qquad (8)$$

Математическое ожидание прироста степени узла k равно вероятности (8) того, что новый узел будет связан с узлом k, поэтому

$$D(k,t+1) - D(k,t) = D(k,t) \cdot \frac{\lambda/2}{t-1} \qquad (9)$$

Начальное условие имеет вид:

$$D(k,k) = m(k) \qquad (10)$$

Решение (9) - (10) имеет вид:

$$D(k,t) = \frac{\Gamma(k-2+\lambda)\cdot\Gamma(t-1+\lambda/2)}{\Gamma(k-1+\lambda/2)\cdot\Gamma(t-1)\cdot\Gamma(\lambda)}, \quad k \geq 2 \qquad (11)$$

при этом $D(1,t) = D(2,t)$.

Асимптотически, при больших значениях k и t

$$D(k,t) \approx \frac{t^{\lambda/2}\cdot k^{\lambda/2-1}}{\Gamma(\lambda)} \qquad (12)$$

Таким образом, средняя степень узла, вошедшего в сеть в момент времени k, уменьшается с ростом k по асимптотически степенному закону с показателем

$$\theta^{rank} = 1-\lambda/2 \qquad (13)$$

На рис. 1 приведены результаты пошагового моделирования эластичной масштабно-инвариантной сети из $t = 65536$ узлов при коэффициенте эластичности $\lambda = 3/2$.

Здесь точками показаны значения степеней узлов, полученные в процессе моделирования, а сплошная линия соответствует регрессионной прямой. Можно отметить, что полученная зависимость близка к теоретически предсказанной асимптотике (12), имеющей в данном случае вид:

$$\log D(k) = -0.25\cdot\log k + 8.4385 \qquad (14)$$

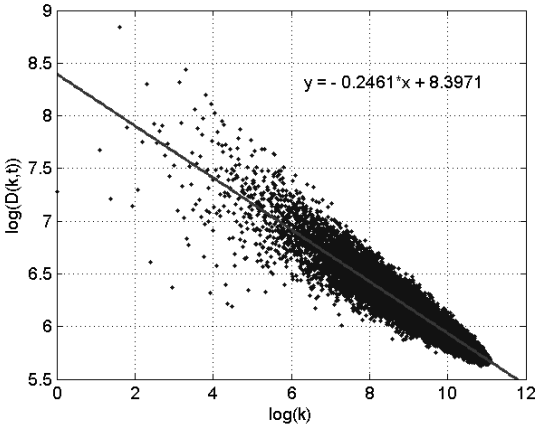


Рис. 1. Зависимость степени узла от времени входа в эластичную сеть

Путём сортировки узлов по убыванию их степеней получено ранговое распределение степеней узлов, эластичной сети (рис. 2). Очевидно, что экспериментальные данные (показанные точками) с большой точностью соответствуют прогнозируемой асимптотической зависимости (14), показанной сплошной линией.

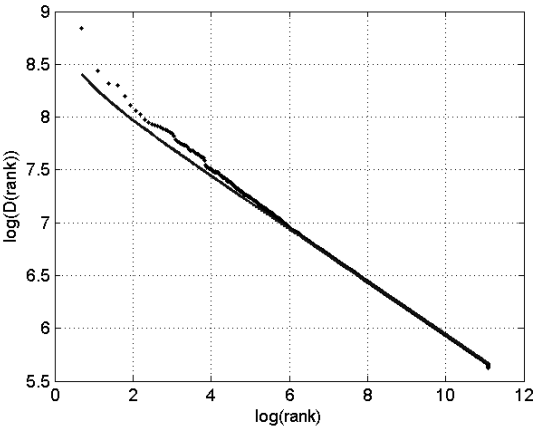


Рис.2. Ранговое распределение степеней узлов эластичной сети

Ранговому распределению с показателем (13) соответствует частотное распределение с функцией вероятности, имеющей степенной хвост с показателем

$$\theta = 1/\theta^{rank} = 1/(1-\lambda/2) \qquad (15)$$

В рассмотренном числовом примере $\lambda = 3/2$, таким образом, $\theta^{rank} = 1/4$ и $\theta = 4$, что больше, чем для неэластичной модели Барабаши-Альберт, имеющей степенной хвост с показателем $\theta = 3$.

Подставляя (11) в (8), получим точное и асимптотическое значения вероятности присоединения нового узла $t+1$ к существующему узлу k:

$$p_{k,t+1} = \frac{\lambda\cdot\Gamma(k-2+\lambda)\cdot\Gamma(t-1+\lambda/2)}{2\cdot\Gamma(\lambda)\cdot\Gamma(k-1+\lambda/2)\cdot\Gamma(t)} \qquad (16)$$

$$p_{k,t+1} \approx C(\lambda-1)(k\,t)^{\lambda/2-1} \qquad (17)$$

где

$$C = \frac{\lambda}{2(\lambda-1)\cdot\Gamma(\lambda)} \qquad (18)$$

III. Оценка количества циклов длиной три в эластичных масштабно-инвариантных сетях

Масштабно-инвариантные сети (при $m > 1$ или $\lambda > 1$) содержат при $t \to \infty$ циклы любого размера. В рассматриваемом частном случае, когда источником всех новых связей являются только новые узлы, все новые циклы всегда содержат вновь добавляемый узел. Новый цикл длиной три формируется тогда и только тогда, когда новый узел присоединится к двум узлам, уже связанным между собой. Вероятность того, что узлы, включенные в сеть в моменты времени k и $t+1$, связаны между собой, определяется формулами (16)-(17). Прирост количества циклов длиной три равен вероятности того, что новый узел $t+1$ соединится с двумя существующими узлами i и j, умноженной на вероятность того, что эти узлы уже связаны:

$$\Delta N_3(t) = N_3(t+1) - N_3(t) = \sum_{i=2}^{t} \sum_{j=1}^{i-1} p_{i,t+1} p_{j,t+1} p_{j,i} \quad (19)$$

Заменив суммы в (19) интегралами, можно записать уравнение скорости прироста циклов в виде:

$$\frac{dN_3(t)}{dt} \approx \int_{i=0}^{t} di \int_{j=0}^{i} C^3 (\lambda - 1)^3 (ijt)^{\lambda - 2} dj \quad (20)$$

Из уравнения (20) находим асимптотическую оценку количества циклов длиной три в эластичной сети:

$$N_3(t) = \frac{1}{6} \left(C \cdot t^{\lambda - 1} \right)^3 \quad (21)$$

Более точная оценка (21) имеет вид

$$N_3(t) = \frac{1}{6} \left(C \cdot \frac{\Gamma(t - 2 + \lambda)}{\Gamma(t-1)} \right)^3 \quad (22)$$

Был проведен численный эксперимент по определению количества треугольных циклов в эластичных сетях размером от $t = 8$ до $t = 4096$ и коэффициентом эластичности (λ) от 1.025 до 1.975 . На рис. 3. точками показаны экспериментальные значения количества циклов длиной три при $\lambda = 3/2$. Значения, соответствующие теоретической оценке (22), показаны сплошной линией.

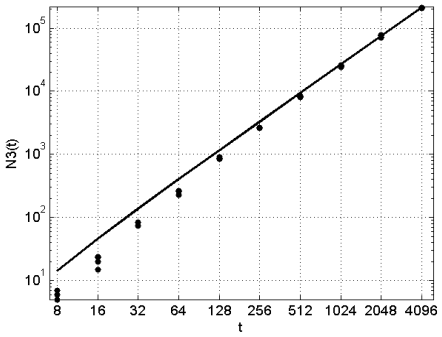


Рис. 3. Количество циклов длиной три в зависимости от размера эластичной сети при $\lambda = 3/2$

Зависимость $N_3(\lambda)$ близка к экспоненциальному закону. На рис. 4 показаны экспериментальные данные и теоретическая оценка, соответствующие сети размером t = 4096.

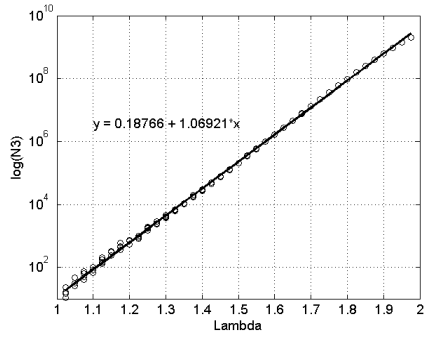


Рис. 4. Количество циклов длиной три в зависимости от коэффициента эластичности

Для сравнения отметим, что согласно [7] математическое ожидание количества циклов длиной три для сети Барабаши-Альберт составляет

$$N_3^{BA}(t) = \frac{1}{6} \left(\frac{m}{2} \log(t) \right)^3 \quad (23)$$

Результаты эксперимента показывают, что точность прогнозирования повышается с увеличением размера сети.

Выводы

Рассмотрена модель масштабно-инвариантной эластичной сети, важным топологическим свойством которой является количество циклов. Основной особенностью эластичных сетей являются разные относительные темпы роста связей и узлов, которые позволяют расширить область применения моделей безмасштабных сетей. Коэффициент эластичности представляет собой масштабную меру плотности графа, более естественную, чем обычно используемая средняя степень.

Получена аналитическая зависимость числа циклов от размера сети и коэффициента эластичности. Проведен численный эксперимент по определению количества треугольных циклов в эластичных сетях для разных значений коэффициента эластичности. Результаты моделирования подтверждают корректность теоретических выводов.

Показано, что зависимость количества циклов от размера сети соответствует степенному закону, а его масштабный коэффициент линейно зависит от коэффициента эластичности. Проведенные исследования могут быть полезными при создании масштабно-инвариантных моделей для сетей различного функционального назначения.

Перспективным направлением дальнейших исследований является обобщение полученных результатов для эластичных сетей с различными источниками добавления ребер.

References

[1] Dorogovtsev S. N., Mendes J. F. F. (2003). Evolution of Networks: From Biological Networks to the Internet and WWW – Oxford, USA: Oxford University Press, 2003. – 280 p.

[2] Choromański, K.; Matuszak, M.; MięKisz, J. (2013). Scale-Free Graph with Preferential Attachment and Evolving Internal Vertex Structure. Journal of Statistical Physics. 151 (6): 1175–1183.

[3] Shergin V. L., Chala L. E., Udovenko S. G. (2018). Fractal dimension of infinitely growing discrete sets. Advanced Trends in Radioelecrtronics Telecommunications and Computer Engineering (TCSET), no. 348.

[4] Albert, R., Barabasi A.-L. (2002). Statistical mechanics of complex networks: Rev. Mod. Phys. - V. 74. - p. 42-97.

[5] Shergin V. L., Chala L. E. (2017). The concept of elasticity of scale-free networks. Proc. Problems of Infocommunications. Science and Technology (PIC S&T), no. 62.

[6] Leung C. C., Chau, H. F. (2012). Weighted accelerated growth model of complex networks. International Journal of Modern Physics B. 21. 10.1142/S0217979207045219.

[7] Bianconi, Ginestra & Capocci, Andrea. (2003). Number of Loops of Size h in Growing Scale-Free Networks. Physical review letters. 90. 078701. 10.1103/PhysRevLett.90.078701.

Introducing WILLIAM: a system for inductive inference based on the theory of incremental *compression*

Arthur Franz* af@occam.com.ua
Michael Löffler* ml@occam.com.ua
Alexander Antonenko*† aa@occam.com.ua
Victoria Gogulya* vg@occam.com.ua
Dmytro Zaslavskyi*‡ dz@occam.com.ua

*Odessa Competence Center for Artificial intelligence and Machine learning (OCCAM) Odessa, Ukraine

†dept. of Mathematical Support of Computer Systems, Odessa National Mechnikov University, Odessa, Ukraine

‡Faculty of Mathematics, Physics and Information Technologies, Odessa National Mechnikov University, Odessa, Ukraine

***Abstract*—We introduce WILLIAM — a new system for data compression that is based on a formal mathematical theory of incremental compression. The theory promises to find short descriptions in an incremental and efficient way while still being applicable to a wide range of data. We have used abstract syntax trees of selected Python operators in order to define a representation language. We present some practical tests of the theory with encouraging results.**

***Index Terms*—incremental compression, data compression, Kolmogorov complexity, inductive inference**

I. Introduction

The ability to compress data is an important problem in both science and industry. Apart from saving memory space, data compression is tightly tied to inductive inference and artificial intelligence, since it requires intelligence in order to find regularities in data, which in turn leads to short representations (see [1], [2]).

Kolmogorov has proved that the concept of the shortest description is well defined and depends on the description language only up to an additive constant. The length of the shortest description is known as the (plain) Kolmogorov complexity of the data, which corresponds to optimal compression. In spite of substantial efforts in this area, progress is impeded by the fact that compression is possible only when a description, i.e. program, is found that captures regularities in the data. However, any language that is able to express all possible programs is Turing complete, such that the search within such a vast space becomes intractable.

In theory, there exist universal search methods, such as Levin Search, that are able to find short descriptions of data and require the execution of all lexicographically ordered programs until a solution is found. For the better or worse, Levin Search has the optimal order of computational complexity [3]. Nevertheless, the obvious slowness of this method, hidden in the big "O" notation, seems to be the price for its generality.

In order to alleviate that problem, we have developed a theory of incremental compression [4], that finds intermediate, increasingly shorter descriptions of data. Remarkably, it is guaranteed to find the shortest description (to some precision) by assembling it from short and mutually orthogonal features. In spite of the fact that those intermediate descriptions are incomputable, they can be approximated in practice, where the whole compression algorithm promises to be both general and efficient.

In this paper, we summarize the theoretical results expressed in the language of algorithmic information theory and also present a practical implementation of the proposed algorithm, WILLIAM: a Python-written system for data compression and inductive inference. Since this is work in progress, we include some modest results and discuss them in relation to the theory and future work.

II. Incremental compression

Consider strings made up of elements of the set $\mathcal{B} = \{0, 1\}$ with ϵ denoting the empty string. $\mathcal{B}^*$ denotes the set of finite strings over $\mathcal{B}$. Denote the length of a string x by $l(x)$. Since there is a one-to-one map $\mathcal{B} \leftrightarrow \mathcal{N}$ of finite strings onto natural numbers, strings and natural numbers are used interchangeably.

The universal, prefix Turing machine U is defined by

$$U\left(\langle y, \langle i, p\rangle\rangle\right) = T_i\left(\langle y, p\rangle\right), \tag{1}$$

where T_i is i-th machine in some enumeration of all prefix Turing machines and $\langle ., .\rangle$ is some one-to-one map $\mathcal{N} \times \mathcal{N} \leftrightarrow \mathcal{N}$. This means that $f = \langle i, p\rangle$ describes some program on a prefix Turing machine and consists of the number i of the prefix Turing machine and its input parameter p and y is some additional parameter. We will use the shortcut $U\left(\langle x, f\rangle\right) \equiv f(x)$. The conditional (prefix Kolmogorov) complexity is given by

$$K(x|y) := \min_s \left\{l(s) :\ U\left(\langle y, s\rangle\right) = s(y) = x\right\} \tag{2}$$

This means that $K(x|y)$ is equal to the shortest description of string x given string y on a universal, prefix Turing machine. The unconditional (prefix Kolmogoro23.5v) complexity is defined by $K(x) \equiv K(x|\epsilon)$. Up to this point, we have followed the standard definitions as given in e.g. [2].

Our theory of incremental compression has been presented in [4], which we summarize here.

Definition 1: Let f and x be finite strings and $D_f(x)$ the set of **descriptive maps** of x given f:

$$D_f(x) = \{f' : f(f'(x)) = x,\, l(f) + l(f'(x)) < l(x)\} \quad (3)$$

If $D_f(x) \neq \emptyset$ then f is called a **feature** of x. The strings $p \equiv f'(x)$ are called **parameters** of the feature f. f^* is called **shortest feature** of x if it is one of the strings fulfilling

$$l(f^*) = \min\{l(f) : D_f(x) \neq \varnothing\} \quad (4)$$

and f'^* is called **shortest descriptive map** of x given f^* if

$$l(f'^*) = \min\{l(g) : g \in D_{f^*}(x)\} \quad (5)$$

Lemma 1:

Let f^* and f'^* be the shortest feature and shortest descriptive map of a finite string x, respectively. Further, let $p \equiv f'^*(x)$. Then

1) $l(f^*) = K(x|p)$ and
2) $l(f'^*) = K(p|x)$.

Theorem 1 (Feature imcompressibility):

The shortest feature f^* of a finite string x is incompressible:

$$l(f^*) - O(1) \leq K(f^*) \leq l(f^*) + O(\log(l(f^*))). \quad (6)$$

Theorem 2 (Independence of features and parameters):

Let f^* and f'^* be the shortest feature and descriptive map of a finite string x, respectively. Further, let $p \equiv f'^*(x)$. Then,

$$K(f^*|p) \approx K(f^*), \quad (7)$$

$$K(p|f^*) \approx K(p), \quad (8)$$

$$K(f^*, p) \approx K(f^*) + K(p) \quad (9)$$

where the "$\approx$" sign denotes equality up to logarithmic terms in complexity.

We conclude that features and parameters do not share information about each other, therefore the description of the (f^*, p)-pair breaks down into the simpler task of describing f^* and p separately. Since Theorem 1 implies the incompressibility of f^* and $U(\langle p, f^* \rangle) = x$, the task of compressing x is reduced to the mere compression of p.

Let us describe the compression scheme of the binary string x. Denote $p_0 \equiv x$, and start an iterative process of compression: let f^*_{i+1} be a shortest feature of p_i, f'^*_{i+1} is a shortest corresponding descriptive map and $p_{i+1} = f'^*_{i+1}(p_i)$. We will continue this process until some p_s is not compressible (for example, $p_s = \epsilon$) and obtain $x = f^*_1(f^*_2(\cdots f^*_s(p_s)))$. One of the main theoretical results shows that this representation approximates the Kolmogorov complexity up to logarithmic terms, i.e. achieves near optimal compression.

III. Description of the algorithm

In the following we will describe the current state of WILLIAM, which is work in progress and will change considerably in future. The main goal of this project is to implement our theory of incremental compression in practice and to construct intelligent agents using the inductive reasoning capabilities that follow from the ability to compress data. For example, it has been shown formally that combining optimal compression (in the form of Solomonoff induction [5], [6]) with reinforcement learning leads to maximally intelligent agents [1].

A. The alphabet

As a language we have used trees of Python operators, which can be converted to abstract syntax trees, compiled and executed by Python itself. At the core, we use an alphabet of currently 36 Python operators, such as `range`, `add`, `mult`, `join`, `map`, `equal`, `and`, `or`, `ifelse` etc. Each operator can be called and knows its arity and type specifications, i.e. the types of variables that can be it's input and output. The currently allowed types are integer, float, string, bool and callable functions, which can be put into lists and tuples. Each operator knows whether and how it can be inverted. For example, `range(4) = [0,1,2,3]`, thus given the list as *induction target*, the input `4` can be inferred. Often, an operator can only be inverted if *conditioned* on some of its inputs. For example, `add(3,4) = 7` can be inverted, if the target `7` is given and the first or second input is conditioned on (i.e. it can be solved for the other input). Sometimes inversion leads to several solutions. For example, if `concat(a,b) = [0,1,2]`, then possible solutions are `a = [], b = [0,1,2]`; `a = [0], b = [1,2]`; `a = [0,1], b = [2]` or `a = [0,1,2], b = []`. Therefore, the inversion of operators is implemented as a Python generator, which yields all possible results. The resulting language defined by that alphabet is completely functional (not declarative).

B. Composite operators

The alphabet can be dynamically extended by defining trees made up of them, so that a tree can act as a single operator. Such new operators are called *composite operators*. They can be executed and also inverted depending on the invertibility and conditions of the participating operators at the nodes. In order to invert a composite, it has to be computed, which if its inputs have to be given, i.e. are conditioned and which can be computed. For example, the composite function $y = x_1 - x_2 + x_3 * x_4$ can be inverted given 3 out of 4 variables, which lead to the inverse functions $F_1 = (y - x_1 + x_2)/x_4$, $F_2 = (y - x_1 + x_2)/x_3$, $F_3 = y - x_1 - x_3 * x_4$ and $F_4 = y + x_2 - x_3 * x_4$. A special activation propagation algorithm has been deployed in order to implement such composite inversions. Composites can then be reused as single operators at the nodes of even larger trees – *hypertrees*.

C. Tree search

Given the alphabet with its respective arity and type specifications an exhaustive search for trees made up of those operators can be performed with the constraint that the output of an operator is fed into an input of another operator with a compatible type specification. Two versions of tree search have been implemented. The first is a depth-first search of all perfect trees at given depth. The second version is a description length sorted (=biased) tree search where trees of increasing description length are found. This

is important since we want to find simple trees first. For example, a degenerate, non-branching depth-4-tree of four unary operators may be simpler than a general depth-3-tree.

D. Search for parameters

After some tree has been constructed, it is used as a single composite operator and corresponds to a feature, as defined in our theory. WILLIAM tries to find inputs (=parameters) to the composite tree (=feature), such that the output matches the target. There are three ways of finding parameters that are currently implemented.

The first and the least efficient, tries to cycle through all combinations of parameters. For example, if the composite requires 5 integer parameters then all integer combinations up to a certain maximal size are attempted.

The second way uses the reasoning of the incremental compression theory: it uses the composite operator (feature f) and the target x in order to *compute* the parameters p. In general, some parameters have to be conditioned on, while the others can be inferred, which corresponds to solving an equation for unknown variables. WILLIAM takes those parameters that have to be known and computes all combinations like in the first version and infers all the other parameters by inverting the composite. Essentially, the descriptive map f' is given by the conditioned parameters p_c and the composite tree itself (for example, inversion of $\texttt{add}(p_c, p_i) = 7$ is possible, if p_c is known).

The third way is to use so-called biased permutation, where the generation of parameters is sorted by their description length.

E. Description length

The description length of various data sets is computed in the following way. Integers n are encoded with the Elias delta code [7], whose length is

$$l(n) = \lfloor \log_2(n) \rfloor + 2 \lfloor \log_2 (\lfloor \log_2(n) \rfloor + 1) \rfloor + 1 \quad (10)$$

Floats are approximated by fractions up to a given precision by minimizing the sum of the description lengths of nominator and denominator, which are integers. Chars are described by the Elias code of their ASCII number. The description length of iterable structures such as strings, lists and tuples consisted of basic elements is simply the sum of the lengths of each element plus description length of the length of the iterable structure.

Beyond data sets, elementary operators and the trees of them that define composite operators have to be described. The information needed to specify an elementary operator is simply $\lceil \log_2(N) \rceil$ where N is the length of the alphabet, currently $N = 36$. Since each operator knows the number if its inputs/children, a tree made up of operators can be described by assigning a number $0, \ldots, N-1$ to each operator and writing those numbers in sequence, assuming a depth-first enumeration order.

F. Inductor and incremental compression

Currently, WILLIAM can function in two modes. In the universal search mode, WILLIAM acts as simple inductor that find descriptions of a target string x in the form of an operator tree f and its parameters p, while trying to minimize the total description length $l(f) + l(p)$. In the incremental mode, WILLIAM tries to find trees f with short description lengths and compute parameters by inverting the tree. Here, only $l(f)$ is minimized while p is allowed to be long, merely bounded by the compression condition $l(f) + l(p) < l(x)$. The parameter list then becomes a new target.

More precisely, let x be an initial target, which is represented in the form of $x = f_1(p_1)$ where f_1 is an operator tree and p_1 is a list of parameters fulfilling $l(f_1) + l(p_1) < l(x)$. This procedure is repeated: $p_1 = f_2(p_2)$, $p_2 = f_3(p_3)$ etc. in accordance with the idea of incremental compression to use short features. In this way, we obtain a list of trees that can be executed subsequently, and form a composition of functions $f_1(f_2(\cdots f_s(p_s)))$ each fulfilling the compression condition $l(f_{i+1}) + l(p_{i+1}) < l(p_i)$. We call such lists/rows of trees *alleys*.

IV. Experiments

In the following, we present some test cases of what has been achieved.

A. Examples of induced functions

All trees up to depth 2 were searched through. We choose some target, then run the inductor in the universal search mode and give some examples of induced functions, the number of attempts to find this representation and compression ratio (in percents of target description length), see *Table I*. The compression ratio is required to be greater than zero, since we enforce the compression condition. w/hints means that we have used hints by limiting the set of basic functions in the inductor. In the condition "without inversion" all parameter combinations up to a certain threshold have been searched through exhaustively. In the "with inversion" condition, some of the parameters can be inferred by computing them from the target and from the conditioned inputs.

It is quite evident that guessing both the function tree and appropriate inputs to the tree is quite computationally expensive. However, when inputs can be computed by inversion, the search is much faster and also can solve problems that could not be solved before. This reflects the $p = f'(x)$ operation in the theory.

B. Example of an induced alley

Consider the target x from *Table II*. It is complex enough, such that an exhaustive search for a representation quickly becomes intractable. However, in the incremental compression mode, WILLIAM can still find a solution. It has first found a function $f_1(a, b, c, d)$ (in the form of an operator tree) and its parameter list $p_1 = [a, b, c, d]$. Both f_1 and p_1 are given in *Table II* and together they form the representation

$$x = \texttt{insert}(\texttt{range}(0, 6), 11, [12, 13, \ldots, 22, 8, \ldots, 8]),$$

which is shorter than the initial target x. In the current version of WILLIAM, the new target is a concatenated list of parameters (denoted by $\mathrm{c}(p_1)$), so at step two the new target is set to

$$\mathrm{c}(p_1) = [0, 6, 11, 12, 13, \ldots, 22, 8, \ldots, 8].$$

TABLE I
EXAMPLES OF INDUCED FUNCTIONS

Target	Some induced function	Attempts without inversion	Attempts with inversion	Compression
'111111'	str(111111), *(6,'1')	not found, 1290	4, 8	53%, 57%
[1,2,4,8,16,32,64,128,256]	power(2, range(9))	669071	196	70%
'aaaaazzzzz'	5 * 'a' + 5 * 'z'	not found	2136	53%
[0.0,1.0,...,99.0]	map(float,range(100))	866, w/hints	3, w/hints	97%
[33,35,37,39,15,14,...,6]	range(33,41,2)+range(15,5,-1)	not found	3021	49%

TABLE II
EXAMPLE OF AN ALLEY

Denotation	Function	List of parameters
x		[11,11,11,11,11,11,12,13,14,15,16,17,18,19,20,21,22,8,8,8,8,8]
$f_1\,(a,b,c,d)\,,p_1$	insert(range(a,b),c,d)	[0,6,11,[12,13,14,15,16,17,18,19,20,21,22,8,8,8,8,8]]
$f_2\,(a,b,c,d)\,,p_2$	insert(range(a,b),c,d)	[14,19,8,[0,6,11,12,13,14,15,16,17,18,19,20,21,22]]
$f_3\,(a,b,c,d)\,,p_3$	insert(range(a),b,range(c,d))	[5,[14,19,8,0,6],11,23]

After running the inductor on the new target we obtain a new feature $f_2\,(a,b,c,d)$ and its parameter list p_2 such that $\mathrm{c}(p_1) = f_2\,(p_2)$. Using $\mathrm{c}(p_2)$ as the new target we obtain $f_3\,(a,b,c,d)$ and p_3. This process can be continued but the inductor did not find a shorter representation of $\mathrm{c}(p_3)$ in this example. Overall, the final description of the target x contains features (functions) f_1, f_2, f_3, a parameter p_3 and some information that allows to obtain initial versions of p_i from the concatenated forms $\mathrm{c}(p_i)$, by saving the indices of each parameter in the concatenated list $\mathrm{c}(p_i)$.

V. DISCUSSION

Previously, we have developed a theory of incremental compression that promises the existence of an efficient and general data compression algorithm. In this publication, we have sketched our new system WILLIAM that aspires to realize that algorithm in practice. WILLIAM is much more complex than described here, but a full description of its functionality is beyond the scope of this paper. Still, it is very much work in progress, so that we have been able to demonstrate some modest capabilities for inducing short descriptions on some examples without yet being able to run a systematic comparison with industrial standards for compression algorithms. Also, a detailed match to the theory in order to test the derived theorems would be useful as well as the further development of a computable version of the theory. Nevertheless, the inductive capabilities using alleys have shown the emergence of fairly deep trees, which would be practically impossible to find using exhaustive search. This is an encouraging confirmation of the theory's efficient compression abilities.

REFERENCES

[1] M. Hutter, *Universal Artificial Intelligence: Sequential Decisions based on Algorithmic Probability*. Berlin: Springer, 2005. 300 pages, http://www.hutter1.net/ai/uaibook.htm.

[2] M. Li and P. M. Vitányi, *An introduction to Kolmogorov complexity and its applications*. Springer, 2009.

[3] L. A. Levin, "Universal sequential search problems," *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 115–116, 1973.

[4] A. Franz, "Some theorems on incremental compression," in *International Conference on Artificial General Intelligence*, pp. 74–83, Springer, 2016.

[5] R. J. Solomonoff, "A formal theory of inductive inference. Part I," *Information and control*, vol. 7, no. 1, pp. 1–22, 1964.

[6] R. J. Solomonoff, "A formal theory of inductive inference. Part II," *Information and control*, vol. 7, no. 2, pp. 224–254, 1964.

[7] P. Elias, "Universal codeword sets and representations of the integers," *IEEE transactions on information theory*, vol. 21, no. 2, pp. 194–203, 1975.

Формирование помехоустойчивых перестановочных кодов на основе факториальных чисел

А.А. Борисенко
Сумский гос. университет
Сумы, Украина
5352008@ukr.net

А.Е. Горячев
Сумский гос. университет
Сумы, Украина
a.goriachev@ekt.sumdu.edu.ua

М.С. Ермаков
Сумский гос. университет
Сумы, Украина

Я.В. Ярошенко
Сумский гос. университет
Сумы, Украина

Б.В. Артюх
Сумский гос. университет
Сумы, Украина

Generation of noise immune permutation codes based on factorial numbers

O.A. Borysenko
Sumy State University
Sumy, Ukraine
5352008@ukr.net

A.E. Goryachev
Sumy State University
Sumy, Ukraine
a.goriachev@ekt.sumdu.edu.ua

M.S. Ermakov
Sumy State University
Sumy, Ukraine

Y.V. Yaroshenko
Sumy State University
Sumy, Ukraine

B.V. Artyukh
Sumy State University
Sumy, Ukraine

***Аннотация* — В работе предлагается новый метод формирования помехоустойчивых кодов на основе перестановок, использующий факториальную систему счисления. Изложены основы теории факториальных систем счисления и приведен метод их получения. Даны примеры арифметических операций над факториальными числами. Рассмотрен быстродействующий метод преобразования факториальных чисел в перестановки. Достоинством данного метода получения перестановок на основе факториальных чисел является простая практическая реализация, как в программном, так и в аппаратном виде. Применение рассмотренного метода эффективно при переборе перестановок с большим количеством содержащихся в них элементов. Рассмотрены в общем виде методы обнаружения и исправления ошибок в перестановочных кодах. Произведена оценка помехоустойчивости перестановок. Из нее следует, что с ростом длины перестановок количество запрещенных состояний все более преобладает над разрешенными состояниями. Следовательно более высокой помехоустойчивостью обладают перестановки с большой длиной, которая достигается на практике применением факториальных систем счисления. Показано, что перестановки способны шифровать передаваемую или хранимую информацию, то есть надежно ее защищать от несанкционированного доступа. При этом защита информации сочетается с ее помехоустойчивым кодированием.**

***Abstract*—The paper proposes a new method for the generation of noise-immune codes based on permutations using a factorial number system. The basis of the factorial numbers systems theory is stated and the method of their obtaining is given. Examples of arithmetic operations over factorial numbers are given. A fast-acting method of transformation of factorial numbers into permutations is considered. The advantage of this method of permutations generation based on the factorial numbers is a simple practical implementation, both in software and in hardware. The application of the considered method is effective in enumeration the permutations with a large number of elements contained therein. General methods of detecting and correcting errors in permutation codes are considered. The noise immunity of permutations is estimated. According to it, with the increase in the length of the permutations, the number of forbidden states increasingly prevails over the permitted states. Consequently permutation with great length have higher noise immunity, which is achieved in practice using the factorial number systems. It is shown that permutations are capable of encrypting transmitted or stored information, that is, can reliably protect it from unauthorized access. In this case, the protection of information is combined with its noise immunity encoding.**

Ключевые слова — перестановки, системы счисления, помехоустойчивое кодирование

Keywords — permutations, numerical systems, noise immunity coding

I. Введение и постановка задачи.

Перестановка – широко распространенный математический объект, использующийся в различных разделах теоретической и прикладной математики. На

перестановках построена абстрактная алгебра, а также решение ряда задач комбинаторной оптимизации, к которой относится и задача коммивояжера, известная еще как задача отыскания гамильтонова цикла минимальной стоимости во взвешенном неориентированном графе [1]. При этом область применения перестановок в оптимизационных математических задачах продолжает расширяться.

Однако, кроме математических задач, перестановки широко применяются и имеют хорошую перспективу дальнейшего применения в практических задачах защиты информации от несанкционированного доступа [2]. Наряду с этим перестановки успешно решают задачи помехоустойчивого кодирования, так как по своей природе содержат избыточную информацию, что позволяет относительно легко находить и устранять ошибки в передаваемых с их помощью сообщениях [3,4]. Кроме того, перестановки позволяют сочетать решения задач помехоустойчивого кодирования с эффективной защитой информации от несанкционированного доступа. Оценка эффективности таких систем может производиться по специальному обобщенному критерию, учитывающему как эффект от помехоустойчивого кодирования, так и от защиты информации [5]. В совокупности все эти возможности перестановок делают задачу их эффективного построения в случайном или заданном порядке полезной и нужной.

На сегодня существует множество способов построения перестановок. К ним относится метод вложенных циклов, транспозиции смежных элементов, поиск с возвращением и другие [1]. Эти методы, так или иначе, используют операции над элементами перестановок, преобразующими их из одной перестановки в другую. Недостаток этих методов – относительно высокая сложность алгоритмов и невысокая скорость получения перестановок, снижающаяся с ростом их разрядности. А ведь нередко скорость обработки и передачи информации является основным требованием к алгоритмам, использующим в своей работе перестановки. Поэтому в настоящее время продолжается поиск простых и быстродействующих методов формирования перестановок.

Одним из таких относительно недавно появившихся эффективных методов построения перестановок является метод, использующий для порождения перестановок факториальные числа, от которых по специальным алгоритмам осуществляется переход к перестановкам [6, 7]. Особенно важна при этом задача формирования перестановок в возрастающем или убывающем порядке. Однако в известных работах, использующих факториальные числа, решающих указанную задачу, имеющиеся алгоритмы не рассчитаны на большую длину формируемых перестановок. А они как раз то наиболее и востребованы на практике. Кроме того, существующие методы порождения перестановок практически не используют факториальный счет, который способен существенно ускорить упорядоченное формирование большого количества перестановок, особенно при применении для этой цели схемных решений. В таком случае скорость формирования перестановок по сравнению с программной реализацией сильно возрастает. Поэтому задача разработки методов быстрого формирования перестановок рассчитанных как на программную, так и схемную реализацию с использованием, в том числе и факториального счета, становится на сегодня актуальной задачей. Именно на решение этой задачи и направлена данная работа.

II. Теоретические аспекты формирования факториальных чисел

Факториальным числом является число, использующее в качестве весовых коэффициентов факториалы цифр, которые в каждом разряде i = 0,1, …, $n-1$ могут принимать значения от 0 до i. Соответственно числовая (нумерационная) функция факториальных чисел $x_{n-1}x_{n-2}...x_i...x_1x_0$ имеет вид [7]:

$$N = x_{n-1}\times(n-1)! + x_{n-2}\times(n-2)! + ... + \\ + x_i \times i! + ... + 1\times 1! + 0\times 0!, \qquad (1)$$

$$0 \le x_i \le i,\ 0 \le i \le n-1.$$

Например, 6-разрядное факториальное число = 3 4 0 0 1 0 представляется с помощью нумерационной функции как

$$N = 3\times5! + 4\times4! + 0\times3! + 0\times2! + 1\times1! + 0\times0! = \\ = 360 + 96 + 1 = 457.$$

Из выражения (1) и примера на него следует, что если количество разрядов в факториальном числе равно n, то в старшем n – 1 разряде максимальная цифра будет равна n – 1, а в нулевом – 0. Тогда максимальное значение, которое может принять факториальное число,

$$N_{\max} = (n-1)\times(n-1)! + (n-2)\times(n-2)! + \mathrm{L} + \\ + 1\times1! + 0\times0! = n! - 1 \qquad (2)$$

Соответственно диапазон представимых чисел при учете нулевого числа

$$P = n! = N_{\max} + 1. \qquad (3)$$

Например, максимальное значение шестиразрядного факториального числа

$$N_{\max} = 5\times5! + 4\times4! + 3\times3! + 2\times2! + 1\times1! + 0\times0! = \\ = 600 + 96 + 18 + 4 + 1 = 719.$$

При этом диапазон представимых шестиразрядных факториальных чисел

$$P = n! = N_{\max} + 1 = 6! = 6 \times 5 \times 4 \times \times 3 \times 2 \times 1 = 720.$$

Для практики имеет значение перебор всех факториальных чисел, начиная с 0 и до максимального значения $N_{\max}$, который может идти в возрастающем или убывающем порядке. Алгоритм последовательного формирования всех n– разрядных факториальных чисел из диапазона P в порядке возрастания состоит из следующих шагов:

1. Формируется первое факториальное число, состоящее из n нулей. Нулевой разряд для всех факториальных чисел без исключения равен 0.

2. Происходит запись 1 в первый разряд.

3. Если в i - м разряде, i = 1, …, n - 1, находится цифра меньшая чем i , то следующее число получается добавлением в этот разряд 1.

4. Если в i - м разряде, $i = 1, \ldots, n - 1$, находится цифра равная i, то при добавлении к ней единицы, возникает 1 переноса в $i + 1$ разряд. При этом i - й разряд, а с ним и все младшие разряды факториального числа обнуляются. Переход к пункту 2.

5. При появлении во всех n разрядах цифр, соответствующих номеру разряда i, формирование факториальных чисел заканчивается, так как получено наибольшее факториальное число равное $n! - 1$.

III. Получение перестановок на основе факториальных чисел

Ценным свойством факториальных чисел является то, что с их помощью относительно легко организовывается переход к перестановкам. В работах [6,7] был предложен метод получения перестановок на основе факториальных чисел, отличающийся относительной простотой, однако скорость их получения в ряде случаев была недостаточной. Метод, описываемый ниже, позволяет поднять скорость преобразования факториальных чисел в перестановки и содержит следующие шаги:

1. Первый элемент перестановки, крайний слева, совпадает с цифрой старшего разряда факториального числа (крайняя цифра слева) и хранится в соответствующей ячейке памяти, хранящей перестановки.

2. Соседняя младшая цифра со старшим разрядом факториального числа сравнивается с уже полученным первым элементом перестановки, и если она больше или равна ему, то происходит ее увеличение на 1. В противном случае она записывается в памяти как новый элемент перестановки по соседству с предыдущим.

3.Третья цифра факториального числа сравнивается с двумя уже полученными ранее элементами перестановки, и если она меньше их обоих, то представляется как третий элемент перестановки. Если она больше их обоих, то факториальная цифра увеличивается на 2 единицы сразу и полученный результат воспринимается как третий элемент перестановки.

4. Если же факториальная цифра равна или больше только одного элемента перестановки из двух, то она увеличивается на 1 и сравнивается с элементом, который до этого был больше ее. Если она и теперь будет меньше его, то она считается 3 элементом перестановки, а если наблюдаться равенство с этим элементом, то факториальная цифра еще раз увеличивается на 1 и после этого считается 3 элементом перестановки.

5. Четвертый, пятый и так далее элементы перестановки получаются по аналогии с получением 3 элемента. Отличие состоит в том, что если очередная факториальная цифра больше 3, 4 и т. д. элементов перестановки, то к ней параллельно добавляются числа 3, 4 и так далее, что значительно увеличивает скорость преобразования факториальных чисел в перестановки по сравнению с методом, описанным ранее в [6].

6. Последний элемент перестановки может быть найден в виде разности заранее известной постоянной суммы n элементов перестановки и суммы уже полученных $(n - 1)$ элементов перестановки. Это при большой длине перестановок может повысить скорость их получения.

Например, если необходимо преобразовать в перестановку факториальное число $N = 3\ 4\ 0\ 0\ 1\ 0$, то в соответствии с приведенным методом преобразования получим перестановку 3 5 0 1 4 2. Этот результат вытекает из того, что первый слева элемент перестановки 3 совпадает с аналогичной цифрой факториального числа, представляющей старший его разряд $(n - 1)$. Поэтому эта цифра 3 остается в перестановке в качестве ее первого элемента. При сравнении второй цифры 4 $(n - 2)$ разряда факториального числа с первым элементом перестановки 3 получаем, что она больше его $(3 < 4)$. Следовательно, эта цифра 4 увеличивается на 1 и становится вторым элементом перестановки, то есть он будет равен 5. Третья цифра факториального числа 0, взятая со стороны старших разрядов, меньше предыдущих двух элементов перестановки 3 и 5. Поэтому она записывается в перестановку без изменений как ее третий элемент. Четвертая цифра 0 факториального числа равна третьему элементу перестановки, т. е. 0, и меньше двух предыдущих элементов перестановки 3 и 5. Поэтому она, увеличиваясь на 1, становится равной 1 и в таком виде выступает как 4 элемент перестановки. Аналогично получается пятый элемент перестановки: цифра 1 первого разряда факториального числа сравнивается сначала с 0 и 1, и так как она больше 0 и равна 1, то сразу увеличивается на 2, становясь равной 3. Затем 3 сравнивается с первым элементом перестановки 3 и так как при этом наблюдается равенство цифр, то элемент 3 увеличивается на 1, становясь равным 4. Больше в имеющихся элементах перестановки нет элемента меньшего или равного 4. Поэтому эта цифра 4 становится пятым элементом перестановки. Цифра 0 нулевого разряда факториального числа равна третьему элементу перестановки 0 и поэтому, увеличиваясь на 1, становится равной 1. Полученная единица, сравнивается с четвертым элементом перестановки, равным 1, и вследствие их равенства увеличиваясь на 1, принимает значение 2. Так как оставшиеся элементы перестановки 3, 4, 5 по своему значению больше 2, то 2 становится шестым элементом перестановки. Окончательный результат в виде перестановки из элементов 3 5 0 1 4 2 получен.

Значение 2 последнего элемента перестановки можно получить и иначе. Для этого надо взять сумму всех элементов перестановки из 6 элементов, равную 15 и вычесть из нее сумму 5 элементов перестановок, полученных из факториального числа до нулевого разряда. Она равна 13. Тогда последний элемент перестановки будет равен числу $15 - 13 = 2$. Ответ совпадает с полученным выше результатом.

Очевидно, что практическая реализация данного метода получения перестановок на основе факториальных чисел достаточно проста, как в программном, так и в аппаратном виде. Однако аппаратные средства дают возможность по сравнению с программной реализацией значительно поднять скорость преобразования, что актуально для задач комбинаторной оптимизации, например задач расписания.

IV. Обнаружение ошибок в перестановках

Обратим внимание, что в рассматриваемой перестановке имеется 6 различных элементов. Появление 2 одинаковых элементов в перестановке, например, двух 1, как в последовательности элементов: 3 1 0 4 1 2 – это уже есть признак ошибки. Ее легко исправить, так как сумма значений элементов для всех возможных перестановок одинакова, в данном случае она равна 15. Для этого от 15 надо отнять сумму цифр в ошибочной перестановке 11 и полученную разницу следует добавить к ошибочному элементу. Какой из двух элементов является ошибочным, выявляется другим способом, например, использованием контроля по модулю 2. Есть и другие более изощренное методы обнаружения и исправления ошибок на основе перестановок [3, 4].

Все они исходят из того, что у них, как и в любом помехоустойчивом коде, есть запрещенные и разрешенные состояния. Количество разрешенных состояний равно диапазону факториальных чисел длины n – P = n!. Соответственно количество запрещенных состояний равно n^n – n!. Очевидно, что их количество с ростом n резко возрастает.

Преобладание количества запрещенных состояний над разрешенными состояниями при росте их длины говорит о более высокой помехоустойчивости перестановок с большой длиной, которая легко достигается на практике применением факториальных систем счисления. Другие методы порождения перестановок не приспособлены для их порождения при большой длине.

V. Защита информации с помощью перестановок

Перестановки путем замены одних элементов другими элементами способны шифровать передаваемую или хранимую информацию и тем самым способны достаточно надежно ее защищать от несанкционированного доступа. Ключами в этом случае могут выступать магические квадраты, что значительно усложняет вскрытие шифра. При этом защита информации сочетается с ее помехоустойчивым кодированием, что позволяет сочетать с помощью перестановок две функции – защиту от помех и несанкционированного доступа. На сегодня существует мало кодов, обладающих данными свойствами, хотя попытки их создания были и неоднократные.

VI. Выводы

Несмотря на то, что рассмотренный метод получения перестановок на основе операций счета над факториальными числами предполагает в общем виде их перебор, в нем все же достигается существенное повышение скорости работы за счет использования арифметической операции сложения не только с 1, а и другими целыми числами. Также кроме быстродействия следует учесть простоту реализации данного метода и соответственно его перспективность для решения переборных задач, как при полном переборе всех решений, так и при частичном. Особенно применение данного метода эффективно при переборе перестановок с большим количеством содержащихся в них элементов. В перспективе для решения задач на перестановках могут быть введены различные ограничения, что требует проведения дополнительных исследований на основе решения данной задачи перебора.

Литература

[1] Э. Рейнгольд, Ю. Нивергельт, Н. Део., Комбинаторные алгоритмы: теория и практика, М.: Мир, 1980, 477 с.

[2] А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов., Криптография: скоростные шифры, СПб.: БХВ-Петербург, 2002, 244 с.

[3] А.Е. Горячев, "Обнаружение ошибок в перестановках", Вісник СумДУ. Технічні науки, 2009, №3, с.169 – 174.

[4] А.А. Борисенко, А.Е. Горячев, Е.Л. Онанченко, "Обнаружение и исправление ошибок в перестановках", Міжнародна науково-практична конференція "Інформаційні технології та комп'ютерна інженерія", Вінниця: ВНТУ, 2010, с. 348 – 349.

[5] Alexei A. Borisenko, Vyacheslav V. Kalashnikov, Nataliya I. Kalashnykova, y Alexey E. Goryachev, Chapter 11: A Generalized Criterion of Efficiency for Telecommunication Systems., M. Favorskaya and Lakhmi Jain (Eds.), Computer Vision in Advanced Control Systems Using Conventional and Intelligent Paradigms (Springer Series: Intelligent Systems Reference Library, ISSN 1868-4394), Springer-Verlag, Alemania, 2014, vol. 1, pp. 353 – 373. http://www.springer.com/series/8578

[6] О.А. Борисенко, І.А. Кулик, О.Є. Горячев, "Електронна система генерації перестановок на базі факторіальних чисел", Вісник СумДУ. Технічні науки,2007, № 1, с.183 – 188

[7] A. A. Borisenko, V. V. Kalashnikov, I. A. Kulik, A.E. Goryachev, "Generation of Permutations Based Upon Factorial Numbers", Eighth International Conference on Intelligent Systems Design and Applications. Kaohiung, Taiwan, 2008, p. 57 – 61.

References

[1] E. Reingold, Y. Nivergelt, N. Deo, Combinatorial Algorithms: Theory and Practice, Moscow: Mir, 1980, 477 p. (in Russian)

[2] A.A. Moldovyan, N.A. Moldovyan, N.D. Guts, B.V. Izotov., Cryptography: high-speed ciphers, St. Petersburg: BKhV-Petersburg, 2002, 244 p. (in Russian)

[3] A.E. Goryachev, "The detection of errors in permutations," Visnyk Sumdu. Technical sciences, 2009, №3, p.169-174. (in Russian)

[4] A.A. Borisenko, A.E. Goryachev, E.L. Onanchenko, "Detection and correction of errors in permutations", International scientific and practical conference "Informational technologies and computer engineering", Vinnitsa: VNTU, 2010, p. 348-349. (in Russian)

[5] Alexei A. Borisenko, Vyacheslav V. Kalashnikov, Nataliya I. Kalashnykova, y Alexey E. Goryachev. Chapter 11: A Generalized Criterion of Efficiency for Telecommunication Systems. – M. Favorskaya and Lakhmi Jain (Eds.), Computer Vision in Advanced Control Systems Using Conventional and Intelligent Paradigms (Springer Series: Intelligent Systems Reference Library, ISSN 1868-4394), Springer-Verlag, Alemania, 2014, vol. 1, pp. 353 – 373. http://www.springer.com/series/8578

[6] O.A. Borisenko, I.A. Kulik, O.E. Goryachyov, "Electronic system of generation of permutations on the basis of factorial numbers", Visnyk Sumdu. Technical sciences, 2007, No. 1, p. 183 - 188 (in Ukrainian)

[7] A.A. Borisenko, V. V. Kalashnikov, I. A. Kulik, A.E. Goryachev, "Generation of Permutations Based Upon Factorial Numbers", Eighth International Conference on Intelligent Systems Design and Applications. Kaohiung, Taiwan, 2008, p. 57 – 61.

Parallel time step control of lines method for the evolution equations

Olga Dmytriyeva
Donetsk National Technical University, Pokrovsk, Ukraine
Research Centre for Simulation Technology (Simtech),
Stuttgart, Germany
olha.dmytriieva@donntu.edu.ua

Nadiia Huskova
Donetsk National Technical University, Pokrovsk, Ukraine
Higher Technical School of the University of Applied Sciences,
Bingen, Germany
huskovanadiia@gmail.com

The problems of obtaining solutions for partial differential equations with the help of the method of lines are considered, which is a semi-discrete method with discretization over spatial variables. Such an approach made it possible to effectively implement a large class of evolutionary equations. The problems of solving the received SODEs by collocation block methods are considered, allowing to provide an effective parallel implementation. Moreover, all the advantages of the solution (parallel step control, local error control, stability of the solution) are realized for the case of partial derivatives without significant increase in computational complexity.

Keywords — evolution equations, method of lines, Cauchy problem, parallel step control, block methods, τ-refinement

I. INTRODUCTION

In this work, the main attention is focused on the control of the step of integration over time (τ-refinement) in the realization of the method of lines for partial differential equations by collocation block difference schemes. The method of straight lines [1-2] for simplicity of presentation is considered using the example of a one-dimensional parabolic equation and is a semi-discrete method with discretization in terms of spatial variables, ensuring the reduction of the original evolution equation with partial derivatives

$$\frac{\partial u}{\partial t} = a^2 \frac{\partial^2 u}{\partial x^2} + f(x,t), x \in [x_0, \mathrm{L}], \quad t \in [t_0, T] \qquad (1)$$

with initial condition of the form

$$u(x, t_0) = q(x), \qquad (2)$$

boundary conditions of the first, the second or the third kind of Cauchy problem

$$u' = \varphi\big(t, u(t)\big), u(t_0) = u_0, t \in [t_0, T], \qquad (3)$$

described by a system of ordinary differential equations (SODE). Such an approach allows us to effectively implement a large class of evolutionary equations. However, after reducing the partial differential equation to the Cauchy problem for SODE, problems arise that were not characteristic of the original problem. So, if we consider explicit implementation patterns, then the choice of the step of integration over time is determined by the fulfillment of the Courant condition [3] and directly depends on the step size over the spatial variable. For the case of implicit difference schemes, the time step is regulated by the physical nature of the problem being solved and the order of approximation of the difference scheme(s).

When it comes to numerical solution of the generated ODEs system, additional possibilities arise related to approximation of higher order (p-refinement), local error control and automatic change of integration step (τ-refinement). A significant influence on the error of the resulting solution will also be provided by questions related to the step change over the spatial variable (h-refinement). However, in this case, a simple reduction of the spatial step by a certain coefficient γ leads to an increase in the dimension of the formed SODE by the same coefficient, which considerably complicates the solution. Therefore, in this section we will consider questions related only to τ-refinement, which is especially important for the numerical solution of rigid differential equations. At the same time, the issues of correlating the errors of the results and the time spent on obtaining the solution are relevant.

II. CONTROLLING THE STEP ON COLLOCATION SCHEMES WHEN IMPLEMENTING EVOLUTION EQUATIONS BY THE METHOD OF LINES

The approaches considered in [4-5], connected with the control of the local error based on the comparison of solutions obtained with different orders in coinciding points of the block, is very effective in solving non-rigid equations and systems and can be used to estimate the error of the solution obtained. If we obtain a priori estimates of the integration step to ensure a given accuracy before the count begins, then it can be asserted that in any part of integration the error obtained does not exceed the specified error. But, unfortunately, this approach cannot provide a change in the integration step at the time of invoice. This question becomes most relevant when the desired function (s) at individual areas of integration is characterized by different rates of change. In this case, it is advisable to use the adaptable step for integration, which does not allow to provide the calculated collocation schemes [6]. To eliminate this drawback, new calculation schemes can be introduced, which will also be based on interpolation polynomials whose degrees coincide with the number of collocation points, and the values of the polynomials at these points coincide with the right-hand sides of the differential equation at the calculated points [5-6]. But the collocation points do not necessarily have to be a uniform grid, although it is desirable (but not necessary) that they be related to each other by some proportionality factors, for example, powers of two. Since it is a question of multi-step methods, it is necessary to select a set of points forming a support block

$$t_{n,i} = t_{n,0} + i\tau_n \in \left[t_{n,-m+1}, t_{n,0}\right],$$
$$i = -(m-1), -(m-2), \ldots, 0,$$

as well as two sets of points that will form the calculation blocks

$$t_{n,i}^{(1)} = t_{n,0} + i\tau_{n_1} \in [t_{n,0}, t_{n,s_1}], i = 1,2,\dots,s_1,$$

$$t_{n,i}^{(2)} = t_{n,0} + i\tau_{n_2} \in [t_{n,0}, t_{n,s_2}], i = 1,2,\dots,s_2.$$

The simplest way to do this is to associate the integration steps τ_{n_1} and τ_{n_2} with the relations $\tau_{n_1} = 2\tau_{n_2}$. Then the dimensions $s_2 = 2s_1$. should be fulfilled between the dimensions of the calculated blocks. The account, as in the previous case, will be executed in parallel for two computational schemes with the same dimensions of the reference blocks and with the dimensions of the calculated blocks that differ in s_2/s_1 times. The canonical form of multi-step collocation methods with the number of reference points m and the number of calculated points s_1 and s_2, respectively, will have the form

$$u_{n,i}^{(1)} = u_{n,0} + \tau_n \sum_{j=1-m}^{0} b_{i,j}^{(1)} F_{n,j} + \tau_{n_1} \sum_{j=1}^{s} a_{i,j}^{(1)}\ F_{n,j}^{(1)},$$

$$i = 1,2,\dots,s_1, \qquad (4)$$

$$u_{n,i}^{(2)} = u_{n,0} + \tau_n \sum_{j=1-m}^{0} b_{i,j}^{(2)} F_{n,j} + \tau_{n_2} \sum_{j=1}^{s} a_{i,j}^{(2)}\ F_{n,j}^{(2)},$$

$$i = 1,2,\dots,s_2,$$

where $u_{n,i}^{(1)}, u_{n,i}^{(2)}$ – are approximate values of the solution of the Cauchy problem (3) at the points $t_{n,i}^{(1)}, t_{n,i}^{(2)}$ respectively,

$\tau_n, \tau_{n_1}, \tau_{n_2}$ – are the steps of integration in the reference block, in blocks of dimension s_1 and s_2, respectively,

$F_{n,j} = \varphi(t_n + j\tau, u_{n,j})$ – are the right-hand sides of the equation (3) at the points, $j = -(m-1), -(m-2), \dots, 0$,

$F_{n,j}^{(1)} = \varphi(t_n + j\tau_{n_1}, u_{n,j}), j = 1,2,\dots,s_1,$

$F_{n,j}^{(2)} = \varphi(t_n + j\tau_{n_2}, u_{n,j}), j = 1,2,\dots,s_2,$

$a_{i,j}^{(1)}, b_{i,j}^{(1)}, a_{i,j}^{(2)}, b_{i,j}^{(2)}$ – coefficients of the design schemes (4).

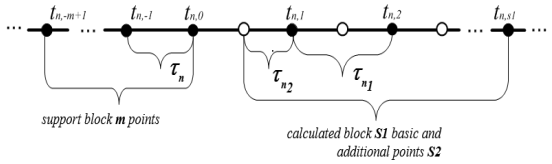


Fig. 1. Scheme of fixing the reference, calculated and intermediate points

To delineate the calculated and sought-for points, appropriate notation and representation of them in the vector form were implemented.

$U_n = \{u_{n,j}\},\ n = 1,2,\dots,\quad j = -(m-1), -(m-2), \dots, 0$ – the vector of counted points,

$U_{n+1} = \{u_{n,j}\},\ n = 1,2,\dots,\ j = 1,2,\dots,s_1$ – the vector of the required points for the dimension of the block s_1,

$V_{n+1} = \{u_{n,j}\},\ n = 1,2,\dots,\quad j = 1,2,\dots,s_2$ – is the vector of the desired points for the dimension of the block s_2,

$$F_{n,j} = \varphi(t_n + j\tau_n, u_{n,j}),\ n = 1,2,\dots,$$
$$j = -(m-1), -(m-2), \dots, 0,$$

$$F_{n+1,j} = \varphi(t_n + j\tau_{n_1}, u_{n,j}), n = 1,2,\dots,j = 0,1,\dots,s_1,$$

$\Psi_{n+1,j} = \varphi(t_n + j\tau_{n_2}, u_{n,j}),\ n = 1,2,\dots,j = 0,1,\dots,\ s_2$ – respectively, the right-hand sides of equation (6) at known and sought-for points,

$A^{(1)}, B^{(1)}, A^{(2)}, B^{(2)}$ – are the matrices of the coefficients of the difference schemes,

$U_{n,0} = (u_{n,0})e$ – is the solution at the point $t_{n,0}$,

e – is a unit vector of dimension s.

Then in vector form the system of equations (4) for the case under consideration will have the following form

$$U_{n+1} = U_{n,0} + \tau_n B^{(1)} F_n + \tau_{n_1} A^{(1)} F_{n+1}, \qquad (5)$$

$$V_{n+1} = U_{n,0} + \tau_n B^{(2)} F_n + \tau_{n_2} A^{(2)} \Psi_{n+1}.$$

To begin the calculation, it is necessary to enter a set of reference values, which can be determined by a one-step method that provides the required accuracy of calculations. Then the search for a numerical solution can be reduced to a solution at each step of two nonlinear systems of equations (5), with a sequential definition of the vectors U_1, V_1, U_2, V_2 ... After determining the unknown coefficients and forming the matrices $A^{(1)}, B^{(1)}$ with dimensions $s_1 \times m$ and $s_1 \times s_1$, $A^{(2)}, B^{(2)}$ with dimensions $s_2 \times m$ and $s_2 \times s_2$, computations by a multi-step block method represented in the form of systems (5) can be reduced to the following iterative processes

$$U_{n+1}{}^{(1)} = U_{n,0}e + \tau_n B^{(1)} F_n, \qquad (6)$$

$$U_{n+1}{}^{(r+1)} = \left(U_{n,0}e + \tau_n B^{(1)} F_n\right) + \tau_{n_1} A^{(1)} F_{n+1}{}^{(r)},$$

$$n = 1,2,\dots,r = 1,2,\dots s_1,$$

$$V_{n+1}{}^{(1)} = U_{n,0}e + \tau_n B^{(2)} F_n,$$

$$V_{n+1}{}^{(r+1)} = \left(U_{n,0}e + \tau_n B^{(2)} F_n\right) + \tau_{n_2} A^{(2)} \Psi_{n+1}{}^{(r)},$$

$$n = 1,2,\dots,r = 1,2,\dots s_2.$$

The systems in (6) require preliminary determination of the values of the vector U_0 at the reference points of the initial block. Determination of the initial values $U_{n+1}{}^{(1)}$, $V_{n+1}{}^{(1)}$ in the calculation blocks is carried out on the basis of the multi-step predictor method of Adams, which allows increasing the accuracy of the initial approximation. The computation of the approximate values $U_{n+1}{}^{(r+1)}, V_{n+1}{}^{(r+1)}$ of the solution of the Cauchy problem in each next computation block is carried out iteratively and independently. After obtaining the solution in the next block, the obtained values are compared in coinciding points. The magnitude of the norm of the discrepancy between the values of approximate solutions in the coinciding s_1 nodes of the main block is decisive for deciding on the step size.

Just as in the formation of multi-stage collocated block difference schemes, which are used to solve the initial Cauchy problem, when reducing equations (1), for controlling the integration step, it is necessary to first build several calculation schemes, namely: basic design schemes corresponding to integration with unchanged step, as well as the schemes to which the calculation will be transferred in case of providing an increase or reduction of the step. In this case, the steps for increasing the step (stretching) will characterize the changes only in the calculation block, and the reduction schemes will make changes both to the design and reference blocks. In fact, the generation of these schemes is reduced to the determination of the calculation coefficients and is carried out once, before the beginning of the calculations, implying their repeated use in solving various problems. For each type of difference schemes, the developed software system allows determining the maximum order of approximation and estimating the a priori error value at the nodes of the calculation block.

III. Numerical Realization of the Method of Lines with Variable Time Step Control (T-Refinement)

Experiments to control the step of integration with respect to the time variable (τ-refinement) were carried out for different values of the discretization step in space, based on the value of (h-refinement), the number of equations n in the SODEs (n=10, n=20, n=40). For test problems with a known exact solution, exact values were used to form values at m initial points. For cases where there was no exact solution, the required sets of initial values were determined by a one-step method with comparable accuracy. As the initial approximations $F_{n,1}, F_{n,2}, \dots, F_{n,s}$, the values calculated with the help of the predictor Adams [7] were used for the next calculation block. In conducting numerical experiments, in addition to the main indicators, the ratio of the number of effective steps to the total number of counts was also estimated.

Test problem 1. The already known test problem [8] (1) with initial condition

$$u(x,0) = sin(\pi x) + \sin(k\pi x), \quad (7)$$

boundary conditions of the first kind

$$u(0,t) = u(L,t) = 0, \quad (8)$$

with known exact solution

$$u(x,t) = e^{-\pi^2 a^2 t} sin(\pi x) + e^{-\pi^2 a^2 k^2 t} sin(k\pi x)$$

was considered as experimental. As the stiffness parameter, the values $k = 1,2, \dots ,10$.

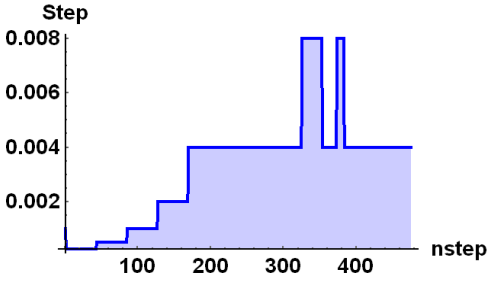


Fig. 2. Automatic change of the integration step for the problem (1, 7-8), $n = 10,\ k = 2, \varepsilon = 10^{-6}$

As shown in [8], methods without step control for such values of the parameter $k > 1$ cannot provide the declared accuracy of the calculation. In fig. 2-3 graphs of step change in time variable, obtained during the implementation of the test task using the system of difference schemes (6) with the dimensions of the reference and calculation blocks 2×2 and 2×4 are constructed.

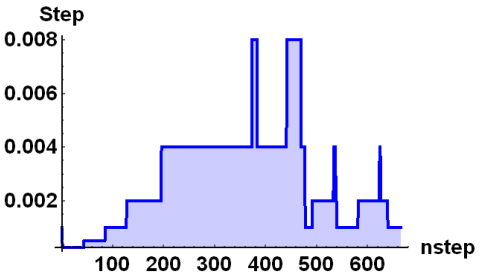


Fig. 3. Automatic change of the integration step for the problem (1, 7-8), $n = 10,\ k = 10, \varepsilon = 10^{-6}$

The dynamics of the step change was also investigated depending on the discretization step in space, the stiffness parameter k, which took values in the interval $1 \div 10$, and the value of the given global error ε.

Test problem 2. The test was performed for a parabolic equation with the known exact solution described in [9]. We consider a special case of the heat equation (1) with the values of the parameters $L = 1, T = 1, a = 1$, with the initial condition

$$u(x,0) = sin(\pi x/L), \quad (9)$$

boundary conditions of the first kind (8), and the known exact solution

$$u(x,t) = e^{-\left(\pi^2/L^2\right)t} sin\left(\frac{\pi x}{L}\right).$$

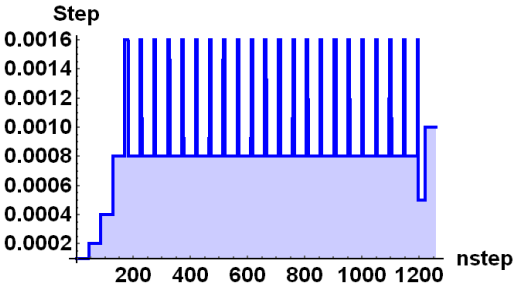


Fig. 4. Automatic change of the step for the problem (1, 8-9) in the method of lines, $n = 10, \varepsilon = 10^{-6}$

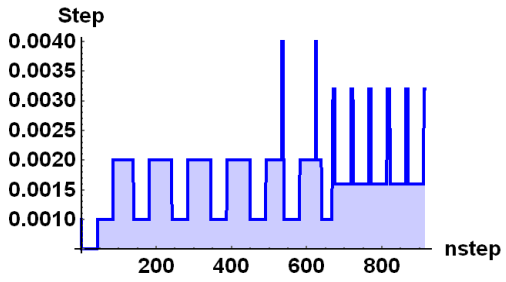


Fig. 5. Automatic change of the step for the problem (1, 8-9) in the method of lines, $n = 20, \varepsilon = 10^{-6}$

The experiment is aimed at conducting a comparative analysis of the results of numerical implementation using direct ones with an exact solution. The dynamics of the step change was investigated depending on the discretization step in space $h = L/n$, which determined

the dimension of the system of ordinary differential equations $n = 10, 20, 40$. Different consequences of global error ε were set. The method of lines was realized using difference schemes (6) with reference and calculation dimensions 2×2 (2×4) and 3×3 (3×6) (fig. 4-5).

Test problem 3. Testing was carried out for the test problem Schisser [9]. We consider the heat equation (1) over space intervals $-5 \le x \le 5$ and in time $0 \le t \le 1$, with the parameter $a = 1$, using the initial condition

$$u(x,0) = \frac{1}{2}e^{-(x-1)^2} + e^{-(x+2)^2}, \qquad (10)$$

with the known exact solution, with the boundary conditions on the left-Dirichlet and on the right-Neumann

$$u(-5,t) = 0, \;\; \partial u(5,t)/\partial x = 0. \qquad (11)$$

The dimension of the system of ordinary differential equations for the method of lines was chosen for the values $n = 10, 20{,}40$. These values of n determined the discretization step with respect to the space $h = L/n$. The value of the global error ε was set at the level $\varepsilon = 10^{-6}, \varepsilon = 10^{-9}$. To implement the method of lines, difference schemes (6) with dimensions of the reference and computational blocks 2×2 (2×4) and 3×3 (3×6) were used. The results of numerical simulation are presented in the form of step change diagrams (fig. 6).

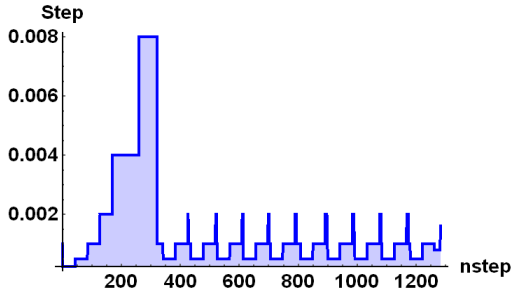


Fig. 6. Automatic change of the integration step for the problem (1, 10-11) in the method of lines, $n = 20, \varepsilon = 10^{-6}$

In all the model experiments performed for this task, in addition to the requirements for retaining a given error, indicators were monitored that ensure the decision to change the step size (the inertia parameter, the number of iterations to refine the solution by the Newton method, the closeness of the current local error to the limit value, effective steps to the total number of counted, etc.). The obtained results testify to the high effectiveness of the proposed approach, which is based on the use of multi-step collocation block schemes with variable dimensions of support blocks and calculation blocks for automatic step control (τ-refinement) in the method of lines.

IV. Conclusions

The investigations carried out in this section have made it possible to propose new approaches to solving the problem of parallel control over the step of integration over a variable time in the realization of the method of lines for partial differential equations by collocation block difference schemes. For controlling the time variable step in evolution equations is based on the use of multi-step multi-point collocation block schemes with uneven arrangement of nodes connected by some proportionality coefficients. When modeling with the help of such schemes, the local error of numerical integration was estimated as the norm of the discrepancies of the solutions obtained with different order of approximation at coinciding points of the computational blocks. The value of the received error and the state of the values of the indicators were used to decide on the size of the next step in the variable time. This made it possible to provide the specified accuracy at each site. If it is necessary to shorten the step length, in the calculation schemes, the previously calculated values were used as intermediate ones, which made it possible to significantly reduce the number of computational operations.

For the automatic generation of computing circuits, a software system based on the use of the integro-interpolation method has been developed, which makes it possible to generate the coefficients of difference equations with arbitrary dimensions of computational and reference blocks, with the possibility of transition to stretching-step compression schemes. The numerical solution for each calculation block was carried out by means of an iterative process, to accelerate the convergence, the initial approximations were determined using the Adams predictor method. The theoretical positions given in the paper are supported by experimental studies on test problems with known exact solutions.

Acknowledgment

The material presented in this report is the result of research conducted at the Research Centre for Simulation Technology (Simtech) of the University of Stuttgart, Germany. The authors are extremely grateful to the director of the SimTech Institute, the president of the International Association of Applied Mathematics and Mechanics, Professor Wolfgang Ehlers, for many years of support and the opportunity to conduct research.

References

[1] W. Schiesser, Method of Lines Analysis of Turing Models, 2017, World Scientific Publishing Co., 268 p.

[2] F. Shakeri and M. Dehghan, "The method of lines for solution of the one-dimensional wave equation subject to an integral conservation condition", J. Comp. & Math. with Applications, vol. 56, № 9, pp. 2175-2188, 2008.

[3] L. Feldman, A. Petrenko and O. Dmytriyeva, "Numerical methods in computer science", 2006, Kyiv, Publishing group BHV, 480 p.

[4] O. Dmytriyeva, "Parallel simulating of dynamic objects with lumped parameters", 2014, Kharkiv: "Noulidg", 335 p.

[5] O. Dmytriyeva, "Parallel numerical methods for modeling dynamic objects", 2016, Pokrovsk, "DonNTU", 384 p.

[6] O. Dmytriyeva, "Control of integration step for parallel realization of generalized collocation block methods", J. Radio-electronic and computer systems, vol. 69, № 5, pp. 119-123, 2014.

[7] A. Samarskii and A. Gulin, "Numerical methods", 1989, 432 p.

[8] J. Cash, "New finite difference schemes for parabolic equations", J. Society for Industrial and Applied Mathematics, vol. 21, № 3, pp. 433-446, 1984.

[9] W. Schiesser, Differential Equation Analysis in Biomedical Science and Engineering, 2014, John Wiley & Sons, 440 p.

Hyperbolic Zeta function of lattice over quadratic field

Nikolay N. Dobrovolskiy
Department of applied mathematics and Informatics
Tula State University
Tula, Russia
nikolai.dobrovolsky@gmail.com

Nikolay M. Dobrovolskiy
Department of algebra, mathematical analysis and geometry
Tula State Lev Tolstoy Pedagogical University
Tula, Russia
dobrovol@tspu.tula.ru

Irina Yu. Rebrova
Department of algebra, mathematical analysis and geometry
Tula State Lev Tolstoy Pedagogical University
Tula, Russia
i_rebrova@mail.ru

***Abstract*— This work consists of two main parts. In the first part, which presents the introduction, given a fairly comprehensive overview of the theory of the hyperbolic Zeta-function of lattices. Unlike earlier reviews is that most of the results of the General theory particularized to two-dimensional case. This is done because the main goal of this lattice is quadratic fields. And these lattices are two-dimensional.In the second part we investigate the behavior of the hyperbolic Zeta-function of the lattice Λ(t) of the quadratic field when the growth parameter t. For applications of the theory of hyperbolic Zeta-function lattices to estimate the error of the approximate integration on the class of by using generalized parallelepipedal nets with weights it is important to have assessment through growing the determinant of the lattice. In this work, we derived a new asymptotic formula for the hyperbolic Zeta function lattices of quadratic fields. The peculiarity of this formula is that it has a main two-term member and remaining a member with the assessment of incoming constants. In this formula more specific correlation between the hyperbolic Zeta function of lattices of quadratic fields and quadratic field characteristics as: the Zeta function of the Dedekind principal ideals of a quadratic field, the derivative of the Zeta-function of Dedekind principal ideals of a quadratic field, quadratic field by the regulator and the fundamental unit of the quadratic field. A similar result is obtained for the hyperbolic Zeta function of a three-dimensional lattice corresponding to a purely real cubic field.**

Keywords—lattice, hyperbolic zeta function of lattice, net, hyperbolic zeta function of net, quadrature formula, parallelepiped net, method of optimal coefficients.

I. HYPERBOLIC ZETA FUNCTION OF LATTICES

The term hyperbolic lattice Zeta function was introduced in 1984 N. M. Dobrovolsky in works [9], [10], which initiated the systematic study of the functions $\varsigma_H(\Lambda|\alpha)$. We reformulate the General results obtained in these papers on the case of two-dimensional lattices. provided.

In particular, lower bounds for the hyperbolic Zeta functions of an arbitrary two-dimensional lattice:

$$\varsigma_H(\Lambda|\alpha) \ge C_1(\alpha)(\det\Lambda)^{-1} \quad npu \quad 0 < \det\Lambda \le 1,$$

$$\varsigma_H(\Lambda|\alpha) \ge C_2(\alpha)\frac{\ln\det\Lambda}{(\det\Lambda)^{\alpha}}\, npu \quad \det\Lambda > 1,$$

where – constants that depend only from α.

An upper bound for the hyperbolic Zeta function is proved s-dimensional lattice:

$$\varsigma_H(\Lambda|\alpha) \le C_3(\alpha)C_4(\Lambda)^2 \quad npu\ q(\Lambda) = 1,$$

$$\varsigma_H(\Lambda|\alpha) \le C_5(\alpha)\frac{\ln q(\Lambda)+1}{q(\Lambda)^{\alpha}} \quad npu\ q(\Lambda) > 1.$$

For the hyperbolic Zeta function of the lattice $\Lambda(t,F)$ in the work [6] by Dobrovolsky N. M., Vankova V. S. and Kozlova S. L. an asymptotic formula was obtained, which in the two-dimensional case is as follows

$$\varsigma_H(\Lambda(t,F)|\alpha) = \frac{2(\det\Lambda(F))^{\alpha}}{R}\left(\sum_{(w)}\frac{1}{|N(w)|^{\alpha}}\right)\frac{\ln\det\Lambda(t,F)}{(\det\Lambda(t,F))^{\alpha}} + O\left(\frac{1}{(\det\Lambda(t,F))^{\alpha}}\right)$$

where the R – the regulator of the field F and the amount $\sum_{(w)}\frac{1}{|N(w)|^{\alpha}}$ summation is performed on all the main ideals of the ring *F*.

In the first phase of research, from 1984 to 1990, the study of the $\varsigma_H(\Lambda|\alpha)$ function was performed only for real $\alpha > 1$ .Since 1995, works Dobrovolsky N. M., Rebrovo I. Y. And Roshchenya A. L. [7] began a new stage in the study of hyperbolic Zeta function $\varsigma_H(\Lambda|\alpha)$: first, as of functions of a complex parameter α, and second, as a function on the metric space of lattices.

Thus, the most General definition of a hyperbolic Zeta-functiontion of a two-dimensional Λ lattice for a complex α next.

Definition 1. The hyperbolic Zeta function of the lattice Λ is called function $\varsigma_H(\Lambda|\alpha), \alpha = \sigma + it$, specified when $\sigma > 1$ is absolutely convergent

$$\varsigma_H(\Lambda|\alpha) = \sum_{\substack{\vec{x}\in\Lambda,\\ \vec{x}\neq 0}} (\bar{x}_1 \cdot \bar{x}_2)^{-\alpha},$$

where for all real values *x* we assume $\bar{x} = \max(1,|x|)$.

By Abel's theorem hyperbolic Zeta function the lattices can be represented in the following integral form

$$\varsigma_H(\Lambda|\alpha) = \alpha\int_1^{\infty}\frac{D(t|\Lambda)dt}{t^{\alpha+1}},$$

where $D(T/\Lambda)$ – number of nonzero lattice points Λ in hyperbolic cross $K_2(T)$.

The norm spectrum of the lattice Λ the set of norm values on non-zero points is called lattices Λ:

$$N_{sp}(\Lambda)=\{\lambda|\lambda=N(\overset{\mathrm{r}}{x}),\overset{\mathrm{r}}{x}\in\Lambda\setminus\{\overset{\mathrm{r}}{0}\}\}.$$

Correspondingly truncated norm spectrum of the lattice Λ — set of values truncated norm on non-zero lattice points:

$$Q_{sp}(\Lambda)=\{\lambda|\lambda=q(\overset{\mathrm{r}}{x}),\overset{\mathrm{r}}{x}\in\Lambda\setminus\{\overset{\mathrm{r}}{0}\}\}.$$

The truncated norm spectrum is a discrete numerical set, that is

$$Q_{sp}(\Lambda)=\{\lambda_1<\lambda_2<\mathrm{K}<\lambda_k<\mathrm{K}\}\ and\ \lim_{k\to\infty}\lambda_k=\infty.$$

It is obvious that $N(\Lambda)=\inf_{\lambda\in N_{sp}(\Lambda)}\lambda,\quad q(\Lambda)=\min_{\lambda\in Q_{sp}(\Lambda)}\lambda=\lambda_1.$

The order of the spectrum point is the number of lattice points with the specified norm value. If such the lattice points are infinitely many, then say that the point the spectrum has an infinite order. The order of the point λ the norm spectrum is denoted by $n(\lambda)$, and the order of the point λ the norm of the truncated spectrum, respectively, through $q(\lambda)$.

Hyperbolic Zeta function of an arbitrary lattice Λ can be represented as a Dirichlet series:

$$\varsigma_H(\Lambda|\alpha)=\sum_{\overset{\mathrm{r}}{x}\in\Lambda\setminus\{\overset{\mathrm{r}}{0}\}}(\overline{x}_1\cdot\overline{x}_2)^{-\alpha}=\sum_{\overset{\mathrm{r}}{x}\in\Lambda\setminus\{\overset{\mathrm{r}}{0}\}}q(\overset{\mathrm{r}}{x})^{-\alpha}=$$

$$=\sum_{k=1}^{\infty}q(\lambda_k)\lambda_k^{-\alpha}=\sum_{\lambda\in Q_{sp}(\Lambda)}q(\lambda)\lambda^{-\alpha}.$$

From this equality it follows that for any complex $\alpha = \sigma + it$ in the right half-plane ($\sigma > 1$) defined regular function of a complex variable, given definition 1, and the inequality holds

$$|\varsigma_H(\Lambda|\alpha)|\le\varsigma_H(\Lambda|\sigma).$$

II. Asymptotic formula for an algebraic lattice

We denote by $\varsigma_{D_0}(\alpha|F)$ the Zeta function of the Dedekind of the main ideals of the quadratic field F:

$$\varsigma_{D_0}(\alpha|F)=\sum_{(w)}|N(w)|^{-\alpha},$$

then

$$\varsigma'_{D_0}(\alpha|F)=-\sum_{(w)}\ln|N(w)|\cdot|N(w)|^{-\alpha}.$$

Theorem 1. Asymptotic equality holds

$$\varsigma_H(\Lambda(t)|\alpha)=\frac{2(\det\Lambda)^{\alpha}}{R}\cdot\frac{\ln\det\Lambda(t)}{(\det\Lambda(t))^{\alpha}}-$$

$$-\frac{2(\det\Lambda)^{\alpha}}{R(\det\Lambda(t))^{\alpha}}\left(\ln(\det\Lambda)\varsigma_{D_0}(\alpha|F)+\varsigma'_{D_0}(\alpha|F)\right)+$$

$$+\frac{2(\det\Lambda)^{\alpha}\varsigma_{D_0}(\alpha|F)}{R(\det\Lambda(t))^{\alpha}}\left(\theta_1(\alpha)+\frac{\theta_2(\alpha)}{sh\left(\frac{\alpha R}{2}\right)}\right),$$

where $|\theta_1(\alpha)|\le 1$ and $\left(\varepsilon_0^{(1)}\right)^{-\frac{\alpha}{2}}\le\theta_2(\alpha)\le\left(\varepsilon_0^{(1)}\right)^{\frac{\alpha}{2}}$, ε_0 – the fundamental unit of the quadratic field F and R – the regulator of this field.

In the monograph [11], a similar asymptotic formula for the hyperbolic Zeta function of the lattice of a purely real cubic field is proved. Let F be a purely real cubic field, $F^{(1)}=F,F^{(2)},F^{(3)}$ are a set of its conjugate fields and for any algebraic number Θ from F, $\Theta^{(1)}=\Theta,\Theta^{(2)},\Theta^{(3)}$ are a set it algebraically conjugate numbers. Through F we denote the ring of algebraic integers of the cubic field F.

Consider an algebraic lattice $\Lambda=\left\{\left(\Theta^{(1)},\Theta^{(2)},\Theta^{(3)}\right)\middle|\Theta\in\ddot{y}_F\right\}$.

Since for any non-zero integer algebraic number Θ from F we have $\left|\Theta^{(1)}\cdot\Theta^{(2)}\cdot\Theta^{(3)}\right|=N(\Theta)\ge 1,$ then $q(\Lambda)=1.$

For an arbitrary $t>1$ we consider an algebraic lattice $\Lambda(t)=\left\{\left(\Theta^{(1)}t,\Theta^{(2)}t,\Theta^{(3)}t\right)\middle|\Theta\in\ddot{y}_F\right\}$.

It is clear that $q(\Lambda(t))=t^3$. Since $\det\Lambda(t)=t^3\det\Lambda,$ then $q(\Lambda(t))=\frac{\det\Lambda(t)}{\det\Lambda}$.

For $\varsigma_{D_0}(\alpha|F)$ the Zeta function of the Dedekind of the main ideals we have:

$$\varsigma''_{D_0}(\alpha|F)=\sum_{(w)}\ln^2|N(w)|\cdot|N(w)|^{-\alpha}.$$

Theorem 2. Asymptotic equality holds

$$\varsigma_H(\Lambda(t)|\alpha)=\frac{\varsigma_{D_0}(\alpha|F)\det^{\alpha}\Lambda}{R}\cdot\frac{\ln^2\det\Lambda(t)}{\det^{\alpha}\Lambda(t)}-$$

$$-\frac{\ln\det\Lambda(t)2\left(\varsigma'_{D_0}(\alpha|F)+\ln\det\Lambda\right)\det^{\alpha}\Lambda}{R\det^{\alpha}\Lambda(t)}+$$

$$+\frac{\det^{\alpha}\Lambda}{R\det^{\alpha}\Lambda(t)}\left(\begin{matrix}\varsigma''_{D_0}(\alpha|F)+2\varsigma'_{D_0}(\alpha|F)\ln\det\Lambda+\\+\varsigma_{D_0}(\alpha|F)\ln^2\det\Lambda\end{matrix}\right)+$$

$$+O\left(\frac{\ln\det\Lambda(t)}{\det^{\alpha}\Lambda(t)}\right).$$

In work [1] the estimation of a residual term which we do not give due to its bulkiness is given.

III. Conclusions

The first section presents a General asymptotic formula for the hyperbolic Zeta function of an algebraic lattice of a purely real algebraic field of degree s. This formula identifies one main term and does not evaluate the residual term because of the cumbersome nature of the possible estimate.

In the second section, in the case of quadratic fields, it is possible to significantly Refine the asymptotic formula for the hyperbolic Zeta function of the algebraic lattice of the quadratic field. It gives a more detailed view of the main member, consisting of two parts, and an estimate of the residual member.

It is clear that further research should be directed to the study of the Zeta function of the Dedekind of the main ideals of the quadratic field and its derivatives in the case of quadratic fields.

Then we obtain an asymptotic formula for the hyperbolic Zeta function of an algebraic lattice of a cubic field. The expanded view of the main member already has three component parts. The estimation of the residual term is given.

From the analysis of the proof it is seen that further refinement of the asymptotic formula is related to obtaining refined asymptotic formulas for the number of algebraic units of a purely real algebraic field of degree s in rectangular domains.

Let us briefly discuss the list of current trends in further research.

The modern version of Frolov's method of approximate integration of periodic functions on quadrature formulas with weights by means of algebraic grids is simpler than in Frolov's works, though these formulas are much more difficult than the case of parallelepipedal grids, but on them the correct order of error of approximate integration is achieved. This property manifests itself for large values of the number of nodes of the grid.

The question of good approximations of algebraic lattices by integers naturally arises. In the case of a positive solution of this question, we obtain new algorithms for constructing optimal coefficients of parallelepipedal grids and new estimates of the hyperbolic Zeta function of these integer grids.

As already mentioned earlier, the hyperbolic Zeta function of lattices is given by the Dirichlet series, and, consequently, all the problems of Dirichlet series are relevant for the hyperbolic Zeta function of lattices.

One of the Central problems for Dirichlet series is to obtain an analytical extension on the whole complex plane and to find a functional equation.

The hyperbolic Zeta function of lattices defines a whole class of Dirichlet series. On the one hand, each Dirichlet series from this class is a function of the complex variable α, but on the other hand, the hyperbolic Zeta function of the lattice itself is defined on the metric space of the lattices. In the right half-plane, there is a remarkable continuity property of the hyperbolic Zeta function of lattices on the lattice space. Namely, if there is a sequence of lattices Λ_n that converges to the lattice Λ at $n \to \infty$, then the sequence of hyperbolic Zeta functions $\zeta_H(\Lambda_n|\alpha)$ uniformly converges to the hyperbolic Zeta function $\zeta_H(\Lambda|\alpha)$ in α-half-plane $\alpha = \sigma + it$, $\sigma \geq \sigma_0 > 1$.

Set of Cartesian grids everywhere dense in a metric space lattices. For any Cartesian lattice, there is an analytical extension of the hyperbolic Zeta function to the entire complex plane. There is a functional equation for the hyperbolic Zeta function of the Cartesian lattice, but at present it has not been possible to find a form of the functional equation that would allow to pass to the limit in the left half-plane. Therefore, the problem of analytic continuation of the hyperbolic Zeta function of an arbitrary lattice remains open.

ACKNOWLEDGMENT

This article is made on the grant RFBR №16-41-710194_r_center_a .

REFERENCES

[1] Dobrovol'skii, N. M., Dobrovol'skii, N. N., Soboleva, V.N., Sobolev, D.K. & Yushina, E.I. 2015, "Hyperbolic dzeta-function of lattices of quadratic fields", Chebyshevskij sbornik, vol. 16, no. 4, pp. 100–149.

[2] Dobrovolskaya L. P., Dobrovolsky M. N., Dobrovol'skii N. M., Dobrovolsky N. N. On Hyperbolic Zeta Function of Lattices // Continuous and Distributed Systems. Solid Mechanics and Its Applications. Vol. 211. 2014. P. 23–62. doi: 10.1007/978-3-319-03146-0_2.

[3] Dobrovolskaya, L. P., Dobrovolsky, M. N., Dobrovol'skii, N. M. & Dobrovolsky, N. N. 2012, "Multidimensional Number-theoretic grid and lattice algorithms for finding the optimal coefficients." Tula: Izd-vo Tul. state PED. University n. a. L. N. Tolstoy, 283 p. (Russian)

[4] Dobrovolskaya L. P., Dobrovolsky M. N., Dobrovol'skii N. M. & Dobrovolsky N. N. 2012, "Hyperbolic Zeta-function grids and sheets the calculation of the optimal coefficients" Chebyshevskii Sb. Vol. 13, is. 4(44). pp. 4–107. (Russian)

[5] Dobrovol'skii, M. N. 2007, "A functional equation for the hyperbolic zeta function of integer lattices." *Vestnik Moskov. Univ. Ser. I Mat. Mekh.* no. 5, pp. 18–23, p. 71 (Russian); translation in Moscow Univ. Math. Bull. 62 (2007), no. 5, pp. 186–191.

[6] Dobrovol'skii N. M., Van'kova, V. S. & Kozlova, S. L. 1990, "Hyperbolic Zeta-function of an algebraic lattices." *Dep. v VINITI* 12.04.90, № 2327--B90. (Russian)

[7] Dobrovol'skii, N. M.; Roshchenya, A. L. & Rebrova, I. Yu. 1998, "Continuity of the hyperbolic zeta function of lattices." *Mat. Zametki.* Vol. 63, no. 4, pp. 522–526. (Russian); translation in Math. Notes 63 (1998), no. 3–4, pp. 460–463.

[8] Dobrovol'skii, N. M. 2005, "Multidimensional number-theoretic nets and lattices and their applications." *Tula: Publishing house of Tula state PED. Univ. L. N. Tolstoy*, – 195 p.

[9] Dobrovol'skii, N. M. 1984, "The hyperbolic Zeta function of lattices", Dep. v VINITI, no. 6090–84.

[10] Dobrovol'skii, N. M. 1984, "On quadrature formulas in classes $E_s^\alpha(c)$ and $H_s^\alpha(c)$ ", Dep. v VINITI, no. 6091–84.

[11] Yu. Rebrova, N. M.Dobrovolsky, N. N. Dobrovolsky, I. N. Balaba, A. R.Esayan, Yu. A. Basalov Theoretical–numerical method in the approximate analysis and its implementation in PODPS "TMK": Monograph. 2 p. Under. ed. N. M. Dobrovolsky. – Tula: publishing house of Tul. GOS. PED. UN-TA im. L. N. Tolstoy, 2016. – P. I. 232 p.

Моделювання технологій навчання

Безносюк Олександр
кафедри педагогіки та психології
Кременецька обласна гуманітарно-педагогічна академія ім. Тараса Шевченка
Кременець, Тернопільська обл., Україна
alexbeznosyuk57@gmail.com

Modeling of technology of teaching

Beznosyuk Olexander
Department of Pedagogy and Psychology
Kremenets Regional Humanitarian and Pedagogical Academy named after. Taras Shevchenko
Kremenets, Ternopil region, Ukraine
alexbeznosyuk57@gmail.com

Анотація **— В статті розглядається спочатку часткова модель, що описує процеси нагромадження і забування знань з певного навчального предмета за технологією навчання, яку назвемо "традиційною". Об'єм знань з певного предмета при традиційній технології навчання, орієнтованій на бездумне запам'ятовування матеріалу, виходить на насичення: нові знання надходять, а старі з тією ж швидкістю забуваються. Потім розглянута модель "інноваційна", яка властива інноваційним технологіям навчання, володіння якими підвищує ефективність самостійної роботи студента із засвоєння знань. Де зростання об'єму знань з певного предмета через великий час після початку навчання відбувається тим швидше, чим більша частка зусиль викладача, спрямована на формування „інноваційних" знань. Після завершення освіти об'єм знань виходить на горизонтальну асимптоту. Чим більша при навчанні частка зусиль, що йдуть на формування „інноваційних" знань, тим більший граничний об'єм „традиційних" знань. І якщо в випускника „інноваційні" знання відсутні взагалі, то після закінчення навчання відбувається неминуче забування нагромаджених „традиційних" знань, що призводить до практично повного їх зникнення. І навпаки, при достатньому об'ємі „інноваційних" знань знання випускника після закінчення офіційного навчання можуть навіть збільшуватися.**

Abstract— **In the article, we first consider a partial model describing the processes of accumulation and forgetting of knowledge on a particular subject on the technology of learning, which we call "traditional". The amount of knowledge on a particular subject with traditional learning technology, focused on thoughtless memorization of the material, goes to saturation: new knowledge comes in, and old ones are forgotten at the same speed. Then the "innovative" model, which is inherent in innovative learning technologies, possesses which increases the efficiency of student's independent work on learning. Where the increase in the amount of knowledge on a particular subject, after a great deal of time after the beginning of education, takes place more rapidly than the greater part of the teacher's efforts aimed at the formation of "innovative" knowledge. After completing education, the volume of knowledge goes to the horizontal asymptotic. The greater the part of the efforts that goes into the formation of "innovative" knowledge, the greater the limit of the "traditional" knowledge. And if the graduate does not have "innovative" knowledge at all, after the end of the study, the inevitable forgetting of accumulated "traditional" knowledge, which leads to almost complete disappearance. Conversely, with a sufficient amount of "innovative" knowledge, the knowledge of a graduate after the completion of formal training may even increase.**

Ключові слова— **модель, традиційні та інноваційні технології навчання, студент. нагромадження і забування знань.**

Keywords— **model, traditional and innovative technologies of teaching, student. accumulation and forgetting of knowledge.**

Як зазначають вчені, математика дає можливість не тільки кількісно уточнювати результат, що інтуїтивно передбачається, але й одержувати зовсім несподівані висновки, прийти до яких навіть на якісному рівні без математики практично неможливо. Використання математики — це своєрідне підключення до попереднього досвіду всього людства.

Розглянемо спочатку часткову модель, що описує процеси нагромадження і забування знань з певного навчального предмета за технологією навчання, яку назвемо "традиційною". Нехай, для простоти, знання, уміння і навички з деякого навчального предмета (далі для стислості викладу названі просто знаннями) засвоюються студентом із постійною швидкістю V0. Нехай уже накопичені знання розпадаються (забуваються) із швидкістю, пропорційною їхньому об'єму X. Коефіцієнт пропорційності будемо вважати сталим. Він, як і швидкість засвоєння, залежить від індивідуальних особливостей учня і від специфіки навчального матеріалу. Його зручно вибрати у вигляді $1/\tau$, де τ— характерний час забування.

Тоді процес зміни об'єму нагромаджених знань описується лінійним диференціальним рівнянням:

$$\frac{dX}{dt} = V_0 - \frac{X}{\tau}. \qquad (1)$$

Тепер спробуємо відбити в моделі особливості, властиві інноваційним технологіям навчання. Для цього введемо величину Y— об'єм „інноваційних" знань студента, володіння якими підвищує ефективність його самостійної роботи із засвоєння знань. Будемо вважати, що швидкість приросту знань з певного навчального предмета, одержуваних самостійно, пропорційна об'єму„інноваційних" знань. Коефіцієнт пропорційності f будемо вважати також сталим, де f — частота засвоєння „інноваційних" знань.

Нехай сумарна швидкість формування „традиційних" знань і „інноваційних" знань залишається такою, що дорівнює V0. Різноманітні технології навчання можуть відрізнятися одна від одної співвідношенням зусиль викладача і студента, що витрачаються на формування „інноваційних" знань і „традиційних" знань. У нашій моделі це співвідношення описується коефіцієнтом k таким чином, що швидкість формування „інноваційних" знань дорівнюватиме kV0, а „традиційних" знань — (1- k)V0.

Як зазначено вищу, що інтенсивність забування „традиційних" знань, отриманих у процесі навчання, характеризується коефіцієнтом 1/τ, забування ж „інноваційних" знань не відбувається (наприклад, у силу того, що студент постійно користується ними як інструментом самонавчання).

Сукупність описаних процесів зміни об'ємів нагромаджених „інноваційних" знань і „традиційних" знань описується диференціальними рівняннями:

$$\frac{dY}{dt} = kV_0,$$

$$\frac{dX}{dt} = (1-k)V_0 + fY - \frac{X}{\tau}. \qquad (2)$$

Нехай початкові умови, для визначеності, такі:

$$X(0)=0,\ Y(0)=0. \qquad (3)$$

Наше попереднє дослідження показало, що одержання правильних умовиводів на основі навіть такої примітивної моделі викликає значні труднощі не тільки у педагогів-практиків, але й у людей, які професійно займаються дидактикою як наукою. З іншого боку, використання математичного апарату, аналогій і комп'ютерних програм робить цю операцію посильною в деяких випадках навіть для старшокласників.

Якщо коефіцієнт *k,* що визначає частку зусиль викладача, спрямованих на формування „інноваційних" знань, не змінюється в часі, то система звичайних диференціальних рівнянь (2) при початкових умовах (3) легко розв'язується аналітично:

$$Y(t) = kV_0 t,\ X(t) = V_0\tau\left[kft + (kft - 1 + k)\left(e^{-ft} - 1\right)\right]. \qquad (4)$$

Модель традиційного навчання, у якому не враховується вплив „інноваційних" знань, відповідає умові k=0. У цьому випадку $X(t)\big|_{\alpha=0} = V_0\tau\left(1 - e^{-\frac{t}{\tau}}\right)$. Графік такої залежності на початковому етапі найкрутіший, але потім він прямує до горизонтальної асимптоти $X(\infty) = V_0\tau$. Таким чином, об'єм знань з певного предмета при традиційній технології навчання, орієнтованій на бездумне запам'ятовування матеріалу, виходить на насичення: нові знання надходять, а старі з тією ж швидкістю забуваються.

У тому випадку, коли в процесі навчання відбувається формування „інноваційних" знань (k>0), асимптота графіка залежності X(t) стає вже не горизонтальною, а похилою. У цьому можна переконатися за допомогою (4): якщо врахувати, що $e^{-\frac{t}{\tau}} \to 0$ при $t \to \infty$, то вийде вираз для лінійної функції, графік якої і є похилою асимптотою. При цьому

$$\lim_{t\to\infty}\frac{dX}{dt} = kfV_0\tau,$$

тобто чим більший параметр *α*, тим більша гранична швидкість зростання величини *X.* Це означає, що зростання об'єму знань з певного предмета через великий час після початку навчання відбувається тим швидше, чим більша частка зусиль викладача, спрямована на формування „інноваційних" знань.

На початку ж навчання, як уже вказувалося, традиційна технологія дає найбільшу швидкість зростання об'єму знань, і тут тенденція зворотна: чим більший *α,* тим нижче початкова швидкість зростання знань. Це можна зрозуміти, підставивши в (2) початкові значення *X* і *У.* і одержавши $\lim_{t\to\infty}\frac{dX}{dt} = V_0(1-k)$ (зміна об'єму знань на початку навчання визначається лише швидкістю одержання знань безпосередньо від викладача). Якщо формуються тільки „інноваційні" знання *(k*=1), то початкова швидкість нагромадження знань взагалі дорівнює нулю!

В деякий момент часу t0 об'єми знань студентів, які навчаються за технологіями з усіма можливими k, стають однаковими (це можна довести й аналітично). До моменту t0 "виграє" традиційна технологія з k=0, а після цього моменту – інноваційна з k=1.

Спробуємо знайти to(τ,f). Прирівнявши X(t0) при k=0 і k=1, отримуємо трансцендентне рівняння відносно t_0: $f\tau = \frac{\frac{t_0}{\tau}}{1 - e^{-\frac{t_0}{\tau}}} - 1$. Таким чином, аналітичного виразу для t_0 одержати неможливо. Але при відомих *f* і *τ* можна було б чисельними методами (або графічно) знайти t_0.

Цікаво простежити долю студента після завершення формальної освіти. У нашій моделі це відповідає зникненню "підкачки" „традиційними" знаннями і „інноваційних" знань "ззовні", що

виражається в тому, що після деякого моменту часу tз, швидкість V0 буде дорівнювати нулеві. Тоді рівняння (2) набудуть вигляду

$$\frac{dY}{dt} = 0\,, \qquad \frac{dX}{dt} = fY - \frac{X}{\tau}\,.$$

Після завершення освіти об'єм знань виходить на горизонтальну асимптоту, однак сталі значення X(∞) різні. Чим більша при навчанні частка зусиль, що йдуть на формування „інноваційних" знань, тим більший граничний об'єм „традиційних" знань. І якщо в випускника „інноваційні" знання відсутні взагалі (k=0), то після закінчення навчання відбувається неминуче забування нагромаджених „традиційних" знань, що призводить до практично повного їх зникнення. І навпаки, при достатньому об'ємі „інноваційних" знань знання випускника після закінчення офіційного навчання можуть навіть збільшуватися.

Відразу після закінчення офіційного навчання швидкість приросту „традиційних" знань стрибкоподібно зменшується на величину V0(1-k). І лише при k=1 (формувалися тільки „інноваційні" знання) графік буде без злому.

Якщо до моменту закінчення освіти tз, точка t0 уже пройдена, то розподіл студентів за об'ємом знань у подальшому не зміниться (тільки розрив між ними збільшиться). У цьому випадку результат випускних іспитів більш-менш адекватно відбиває успішність наступної професійної діяльності (якщо припустити, що остання визначається в першу чергу об'ємом „традиційних" знань).

Після того, як були побудовані залежності X(t) для різних сталих значень параметра k, що характеризує частку зусиль, спрямованих на формування інноваційних" знань, виявилося нескладною справою вибрати значення k, яке максимізує об'єм предметних знань на відомий момент контролю X(tк). Відповідь виявилася простою: якщо tк<t0 (момент контролю буде раніше моменту, у який всі залежності X(t) для різних постійних значень параметра k перетинаються), то найкращий результат (у розумінні максимальності X(tк)) буде при k=0 (тобто всі сподівання на бездумне запам'ятовування); якщо tк>t0, то найкращим буде варіант k=1 (усі зусилля викладача – на навчання інноваційних" знань); якщо tк=t0, то всі стратегії незмінних k дають однакові результати.

Література

[1] Beznosyuk O.O. Continuous education:mathematical model// Lifelong learning: continuous education tor sustainable development: proceedings of international cooperation. Vol. 6/ Leningrad State University n. a. A. S. Pushkin [et al.]; - Saint-Petersburg: Alter Ego, 2008. - , pp.138-142.

The order of projective Edwards curve over F_{p^n} and embedding degree of this curve in finite field

Skuratovskii R. V.
Department of computer algebra and discrete mathe-matics
University MAUP
Kiev, Ukrain
ruslcomp@mail.ru

***Abstract*—We consider algebraic affine and projective curves of Edwards over a finite field F_{p^n} . Most cryptosystems of the modern cryptography can be naturally transform into elliptic curves. We research Edwards algebraic curves over a finite field, which at the present time is one of the most promising supports of sets of points that are used for fast group operations [1, 3, 4]. We find not only a specific set of coefficients with corresponding field characteristics, for which these curves are supersingular but also a general formula by which one can determine whether a curve $E_d[F_p]$ is supersingular over this field or not.**

***Key words*— finite field, elliptic curve, Edwards curve, group of points of an elliptic curve.**

I. INTRODUCTION

The embedding degree of the supersingular curve of Edwards over F_{p^n} in a finite field is investigated, the field characteristic where this degree is minimal is found.

The criterion of supersungularity of the Edwards curves is found over F_{p^n}. Also the generator of crypto stable sequence on an elliptic curve with a deterministic lower estimate of its period is proposed.

We consider algebraic affine and projective curves of Edwards over a finite field. We find not only a specific set of coefficients with corresponding field characteristics, for which these curves are supersingular but also a general formula by which one can determine whether a curve is supersingular over this field or not. The embedding conditions of a group of supersingular curve $E_d[F_p]$ in a field F_{p^k} [5] with minimal degree k of extention were found.

II. MAIN RESULT

The twisted Edwards curve with coefficients a and d is the curve $E_{a,d}$:

$$ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in F_p^*,$$

where $ad(a-d) \neq 0,\ d \neq 1,\ p \neq 2,\ a \neq d.$

An Edwards curve is a twisted Edwards curve with $a = 1$.

We will denote by E_d Edwards curve $x^2 + y^2 = 1 + dx^2y^2,\ d \in F_p^*,$ over F_p.

Special points are (infinitely distant points) $(1,0,0)$ and $(0,1,0)$, therefore, we have singularities at infinity in the corresponding affine components $A^1 : az^2 + y^2z^2 = z^4 + dy^2$ and $A^2 :\ ax^2z^2 + z^2 = z^4 + dx^2$.

We describe the structure of the local ring at the point p_1, its elements are fractions of the functions of the form $F(x,y,z) = \dfrac{f(x,y,z)}{g(x,y,z)}$, whose denominators do not possess the value 0 at the point p_1. A local ring having singularity in 2-points has functions in which the denominators are not divisible by $(x-1)(y-1)$.

We find $\delta_p = \dim \overline{O_p} \big/ O_p$, where O_p – the local ring at a singular point p, this ring is generated by the relations of regular functions $O_p = \left\{ \dfrac{f}{g} : (g,(x-1)(y-1)) = 1 \right\}$, $\overline{O}_p$ – the whole closure of the local ring at a singular point p.

Denote $\delta_p = \dim \overline{O_p} \big/ O_p = 1$ the dimension of the factor as vector space. Since the basis of extension $\overline{O}_p$ over O_p consists of one element in each of two distinct points, then $\delta_p = 1$.

So, we calculate the genus of curve for Reed [6]

$$\rho^*(C) = \rho_\alpha(C) - \sum_{p \in E} \delta_p = \frac{(n-1)(n-2)}{2} - \sum_{p \in E} \delta_p = 3 - 2 = 1$$

because $n = 4$. where $\rho_\alpha(C)$ – the arithmetic type of the curve C, parameter $n = degC = 4$.

Since it is of genus 1, then it is isomorphic to a flat cubic curve but is not elliptic, because it has singularity in the projective part. The curve of Edwards as the twisted curve of Edwards isomorphic to some affine part of the elliptic curve. Normalization of the Edwards curve is a curve in the form of Veyreshtras proposed by Montgomery E_M [1].

In order to detect supersingular curves, according to Koblitsa's study [7,8], one can use the search for such parameters for which the curve and its corresponding curve have the same number of solutions.

As well known the transition to the torsion curve is given by the reflection $(\bar{x}, \bar{y})$ a $(x,y) = \left(\bar{x}, \dfrac{1}{\bar{y}}\right)$ [1].

Let us denote by N_{E_d} the number of points of affine Edwards curve over finite field F_p.

The following statement is criterion of the curve supersingelarity.

Theorem 1. If $p \equiv 3(mod\,4)$ and p is a prime number and $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\mathrm{mod}\, p)$ then the order of the curve $x^2 + y^2 = 1 + dx^2 y^2$ coincides with order of the curve $x^2 + y^2 = 1 + d^{-1}x^2 y^2$ over F_p and equal to $N_{E_d} = p+1$ if $p \equiv 3(\mathrm{mod}\, 8)$, and it equals to $N_E = p-3$ if $p \equiv 7(\mathrm{mod}\, 8)$. Over the extended field F_{p^n}, where $n \equiv 1(mod\, 2)$ order of this curve is $N_E = p^n + 1$, if $p \equiv 3(\mathrm{mod}\, 8)$, and it is $N_E = p^n - 3$, if $p \equiv 7(\mathrm{mod}\, 8)$.

Example. Number of points for $d = 2$ and $p = 31$ $N_{E_2} = N_{E_2^{-1}} = p - 3 = 28$.

Corollary 1. If coefficient d of E_d is such that $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\mathrm{mod}\, p)$, then E_d has $p - 1 - 2(\frac{d}{p})$ points over F_p and birational equivalent [1] curve E_M has $p+1$ points over F_p.

Corollary 2. If the coefficient of the curve satisfies the supersingularity $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\mathrm{mod}\, p)$ equation studied in Theorem 1, then E_d has $p - 1 - 2(\frac{d}{p})$ points over F_p a boundary-equivalent [1] curve with p + 1 points over F_p.

Theorem 2. The number of points of the affine Edwards curve is equal to

$$N_{E_d} = (p + 1 + (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j) \equiv$$

$$\equiv ((-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j + 1)(\mathrm{mod}\, p).$$

This sum is congruent to This result follows from the number of solutions of the equation $y^2 = (dx^2 - 1)(x^2 - 1)$ over F_p equals to $p - 1 - 2\left(\frac{d}{p}\right) + \left(1 + (\frac{d}{p})\right) = p - \left(\frac{d}{p}\right)$. Thuz we have

$$N_{E_d} = (p + 1 - (\frac{d}{p}) - (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j} C_{\frac{p-1}{2}}^{j})^2 d^j) \equiv$$

$$\equiv (p + 1 - (\frac{d}{p}) - (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j) \equiv$$

$$\equiv (1 + (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j)(\mathrm{mod}\, p).$$

Example. If $p = 31$, then $N_{E_2} = N_{E_2^{-1}} = p - 3 = 28$ over prime field F_p, that is less than $p+1$.

Theorem 3. The number of points of the projective Edwards curve is equal to

$$N_{PE_d} = (p + 1 + 2 + (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j) \equiv$$

$$\equiv ((-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j + 3)(\mathrm{mod}\, p).$$

Note that addend 2 arise due two infinite points (1,0,0) and (0,0,1).

We call the embedding degree a minimal power k of finite field extention such that C_r can embedded in multiplicative group of F_{p^k}.

Property. The embedding degree [5] of the supersingular curve E_d is equal to 2.

In fact, the order of the supersingular group $E_{1,d}$ can be equal to $p^k + 1$ divides $p^{2k} - 1$ and does not divide the lesser degrees.

III. Main result

Let us obtaine conditions of embedding the group of supersingular curve $E_d[\mathrm{F}_p]$ of order q in multiplicative group of field F_{p^k} with embedding degree $k = 12$ [5]. For this goal we use Zigmondy theorem. This theorem implies that suitable characterscstic of field F_p is an arbitrary prime q, which do not divide 12 and satisfy the condition $q | \Phi_{12}(p)$, where $\Phi_{12}(x)$ is the cyclotomic polynom. This p will satisfy the necessary conditions namely $(x^n - 1) \not\vdots p$ for an arbitrary $n = 1,...,11$.

Recall that by a cofactor of curve we call multiplier to a large prime number q in factorization of order of curve.

Theorem 4. If Edwards curve over finite field F_p where $p \equiv 7(mod 8)$ is supersingular and $p - 3 = 4q$, where $p, q \in \mathrm{P}$, then it has minimal cofactor 4.

Theorem 5. If Edwards curve over F_p, where $p \equiv 3(mod 8)$ is supersingular and $p + 1 = 4q$, where $p, q \in \mathrm{P}$, then it has minimal cofactor 4.

Example. For $p = 2^{255} - 19$ the twisted Edwards curve $E_{29,-28}$ has cofactor 4 and the twisted Edwards curve $E_{25,2}$ has cofactor 8.

The possibility of doing the reverse operation to the operation of doubling the point has not yet been fully investigated for the twisted Edwards curve, the following theorem gives an answer to this question. Under the

divisibility of the point (*X; Y*), it understands the finding of its preimages (*x*; *y*), which, when applying the point doubling formula, result in the point (*X*; *Y*) [1].

Theorem 6. An arbitrary point of a twisted Edwards curve (1), which is not a point of the 2nd or 4th order, admits divisibility if and only if $\left(\frac{1-aX^2}{p}\right) \neq -1$.

Take the elliptic curve of a given large simple order q [3], where $p \neq q$. As a one-sided, take the function: $P_i = f(P_{i-1}) = \phi(P_{i-1})G$, where

$$\phi(P_{i-1}) = \begin{cases} x, & P_{i-1} = (x, y) \\ p, & P_{i-1} = O \end{cases}.$$

Apply the generation formula $P_i = f(P_{i-1}) = \phi(P_{i-1})G$. Therefore, the complexity of the inverse of this function is equivalent to the problems of a discrete logarithm. As a hard bit of this one-way function we set the predicate $\mathrm{P}(P_{i-1}) = (\frac{\phi(P_{i-1})}{p})$ or the alternative the predicate

$$\mathrm{P}(P_{i-1}) = \begin{cases} 1, & x_i \geq \frac{p-1}{2} \\ 0, & x_i < \frac{p-1}{2} \end{cases}.$$

The complexity of computation of the product $P_i = f(P_{i-1}) = \phi(P_{i-1})G$ according to the method of doubling the addition is $O((\log_2 \phi(P) - 1)(\mathrm{W}(\phi(P) - 1)))$ [9].

To maximize the generator's operating period, we can use the cyclic group of the curve E_d not a prime order. For mapping generator G of cyclic group $E_d[\mathrm{F}_{p^k}]$ in an element which is another generator of this group we add G with itself m times, where m satisfies the condition $(m, E_d[\mathrm{F}_{p^k}]) = 1$. Viz $P_i = f(P_{i-1}) =$

$= \frac{\phi(P_{i-1})}{\left(\phi(P_{i-1}), |E_d|\right)} G = mG$, where $|E_d|$ is the order of the curve group E_d. A possible modification is the choice of the coordinate of the point P_i which gcd with $|E_d|$ is lesser. In other words, let

$t := \underset{z \in \{x,y\}}{\mathrm{Argmin}} \left(\gcd(x, |E_d|), \gcd(y, |E_d|)\right)$ and as a factor we take:

$$\phi(P_{i-1}) = \begin{cases} t, & P_{i-1} = (x, y) \\ p, & P_{i-1} = O. \end{cases}$$

In the case of a field F_{p^n} we can choose a supersingular curve whose order is known by Theorem 1 then the order of the group of points of the generator will be $\varphi(p^k + 1)$ or $\varphi(p^k - 3)$.

As a hard bit of this one-way function we take a mapping of the quadratic residue of second coordinate of point P_n viz $\left(\frac{y_n}{p}\right)$.

This one-sided function has a core similar to that used in the Kalinski generator [9], hence, according to the Goldwasser's theorem, the sequence $\{P_i\}_{i=1}^{T}$ will be unpredictable and crypt resistant [11].

REFERENCES

[1] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters. "Twisted Edwards Curves". IST Programme ECRYPT, and in part by grant ITR-0716498, PP. 1-17, 2008.

[2] Skuratovskii R. V. Modernized Pohlig-Hellman and Shanks algorithm. Vol. 1 Visnuk of KNU. Cybernetics. pp. 56., 2015.

[3] Скуратовський Р. В., Мовчан П. В., "Нормалізація скрученої кривої Едвардса та дослідження її властивостей над Fp". Збірник праць 14 Всеукраїнської науково-практичної конференції. ФТІ НТУУ "КПІ" 2016, Том 2, С. 102-104.

[4] Skuratovskii R. V., Kvashuk D. M. Vlastyvosti skruchenoyi kryvoyi Edvardsa, mozhlyvist" podilu yiyi tochky na dva i zastosuvannya// Zbirnyk naukovyx prac" "Problemy informatyzaciyi ta upravlinnya". - 2017.- № 4(60). – S. 61-72.

[5] Paulo S. L. M. Barreto Michael Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. International Workshop on Selected Areas in Cryptography SAC 2005: pp. 319-331.

[6] W. Fulton Algebraic curves. An Introduction to Algebraic Geometry - Third Preface - January, 2008. - 121 P.

[7] H. Edwards A normal form for elliptic curves. American Mathematical Society. - 2007. - Volume 44, Number 3, July - pp. 393-422.

[8] N. Koblitz, "Eliptic Curve Cryptosystems" // Mathematics of Computation, V. 48, No. 177. –Ð. pp. 203-209, 1987.

[9] Bolotov A. A., Gashkov S. B., Frolov A. B., Chasovskyh A. A. Elementarnoe vvedenye v ellyptycheskuy kryptohrafiyu – M.: KomKnyka. Tom 2., 2006. – 328 s.

[10] Deepthi P.P., Sathidevi P.S.. New stream ciphers based on elliptic curve point multiplication. Computer Communications (2009). pp 25–33

[11] Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography. Cambridge, Massachusetts, July 2008. P. 289.

The sum of consecutive fibonacci numbers

Skuratovskii R. V.
IKIT
MAUP
Kiev, Ukraine
ruslcomp@mail.ru

Rudenko D. V.
Lyceum 171
Kiev, Ukraine
dmytrorudenkoi@gmail.com

***Abstract*—New properties of the sums of linear recursive sequences were proposed in this paper. Particularly, theoretical-numerical characteristics of Fibonacci, Lucas and associated with them number sequences are being researched. For the first time necessary and sufficient conditions of periodicity of Fibonacci and Lucas sums were investigated. Also the conditions of the divisibility of any sum of the consecutive m Fibonacci numbers by their amount. Using computer calculations, we checked the corresponding values that satisfy the condition of the theorem proved by us. The relevance of the chosen topic of research is caused by numerous applications of the sequence of Fibonacci numbers and their generalizations in a variety of scientific research areas, in particular, they are widely used in mathematics, cryptography biology, geology, crystallography, medicine, psychology, astronomy, economics, computer science, art, etc. The sequences studied by us have not only a theoretical but also an applied value, so the Lucas sequence we studied in our application is used in coding and cryptography. In addition, we consider new sequences of finite sums of successive elements, which in general represent a new sequence. As well as the classical Fibonacci sequence, our linear recurrence sequences will be used in the mathematics itself, for example, Y. Matyaselevich uses the numbers of Fibonacci to solve the known 10th Hilbert problem. Another of our choices for generalization of sequences, namely the sequence of Lucas numbers, is also being investigated in our time [10]. The regularity of the change in the period of the sequence of the imposed sum of successive elements, depending on the quadraticity remainder of the number 5 in Z_p . The rigorous argumentation is given with the help of the numbers theory theorem.**

Keywords—periodicity of Fibonacci sums by modulo, linear recursive sequence, Fibonacci sequence and Lucas.

I. INTRODUCTION

In our article we study the theorem-numerical characteristics of Fibonacci numbers and related sequences. For the first time, the necessary and sufficient conditions for the periodicity of the Fibonacci sums and the conditions for the multiplicity of the sum of any successive numbers of the Fibonacci sequence by the number of its terms have been investigated. Using computer calculations, we checked the corresponding values that satisfy the condition of the theorem proved by us.

The relevance of the chosen topic of research is due to the numerous applications of the sequence of Fibonacci numbers and their generalizations in a variety of scientific research areas, in particular, they are widely used in mathematics, cryptography, coding of information, physics, philosophy, botany, biology, geology, crystallography, medicine, psychology, astronomy, economics, computer sciences, art, etc. The sequences studied by us have not only a theoretical but also an applied value, so the Luke sequence we studied in our application is used in coding and cryptography. In addition, we consider new sequences of finite sums of successive elements, which in general represent a new sequence.

The sum of the sequential Fibonacci numbers and analogously some other sequences forms new sequences.

At this item we will consider such task:

find all the natural values $m>1$ such that the divisibility is fulfilled $\sum_{k=1}^{m} f_k \vdots m$, where sequence $\{f_n\}_{n=1}^{+\infty}$ is determined by the ratio $f_{n+1} = f_n + f_{n-1}, n \geq 2$, values f_1 and f_2 – some integers that may vary.

We denote by $T(m)$ the period of mentioned above sums of consecutive Fibonacci numbers reduced by the modulo m.

Let's consider examples of calculations.

1) Let $f_1 = 1$ and $f_2 = 1$, so we consider the Fibonacci sequence. In this case we get such values m:

1, 2, 24, 48, 72, 77, 96, 120, 144, 192, 216, 240, 288, 319, 323, 336, 360, 384, 432, 480, 576, 600, 648, 672, 720, 768, 864, 960, 1008, 1080, 1104, 1152, 1200, 1224, 1296, 1320, 1344, 1368, 1440, 1517, 1536, 1680, 1728, 1800, 1920, 1944, 2016, 2064, 2160, 2208, 2304, 2352, 2400, 2448, 2592, 2640, 2688, 2736, 2880, ….

2) Let $f_1 = 2$ and $f_2 = 1$. In that case we get such values m:

1, 3, 24, 48, 72, 96, 120, 144, 192, 216, 240, 288, 336, 360, 384, 406, 432, 480, 576, 600, 648, 672, 720, 768, 864, 936, 960, 1008, 1080, 1104, 1152, 1200, 1224, 1296, 1320, 1344, 1368, 1440, 1536, 1680, 1728, 1800, 1920, 1944, 2016, 2160, 2208, 2304, 2352, 2400, 2448, 2592, 2640, 2688, 2736, 2880, 3000, 3024, 3072, 3120, 3240, 3312, 3360, 3456, 3600, 3672, 3720, 3840, 3888, 3960, 4032, 4104, ….

3) Now let's examine the initial values, which define Lucas sequence $f_1 = 1$ and $f_2 = 2$, so we get this values of m:

1, 3, 18, 24, 42, 48, 72, 96, 120, 138, 144, 192, 216, 240, 258, 264, 282, 288, 336, 360, 384, 402, 432, 480, 498, 576, 600, 618, 642, 648, 672, 714, 720, 744, 762, 768, 864, 912, 960, 978, 1002, 1008, 1080, 1104, 1152, 1200, 1224, 1296, 1320, 1338, 1344, 1362, 1368, 1440, 1536, 1578, 1584, 1680, 1698, 1728, 1800, 1842, 1920, 1938, 1944, 2016, 2082, 2160, 2202, 2208, 2280, 2298, 2304, 2352, 2394, 2400, 2448, 2592, 2640, 2658, 2688, 2736, 2778, 2802, 2880, 2922, 3000, 3018, 3024, 3072, 3138, 3240, 3282, 3312, 3360, 3378, 3456, 3480, 3522, 3600, 3642, 3648, 3672, 3720, 3840, 3858, 3882, 3888, 3960, 4032, 4098, 4104, 4224, 4320, 4362, 4368, 4416, 4458, 4464, 4512, 4554, 4608, 4674, 4704, 4722, 4800, 4896, 4920, 4938, 4962, 5040, 5178, 5184, 5280, 5298, 5322, 5376, 5400, 5442, 5472, 5520, 5682, 5688, 5760, 5802, 5832, 5898, 6000, 6042, 6048, 6120, 6144, 6378, 6384, 6480, 6498, 6522, 6600, 6618, 6624, ….

After analyzing the three cases presented above, we notice that among the numbers found there are often numbers that are divisible by 24. Therefore, in connection with this, we can express the guess that, probably, the condition of the search task "of the sum of successive Fibonacci numbers" satisfy the numbers m, which are a multiple of 24.

The criterion of divisibility of the sum of successive Fibonacci numbers by the number of terms.

Lemma. Let $f_{n+1}, f_{n+2}, ..., f_{n+m}, n \geq 0$ _ m arbitrary successive Fibonacci numbers. Then the next equality holds:

$$\sum_{k=1}^{m} f_{n+k} = f_{n+m+2} - f_{n+2}. \qquad (2.1)$$

Indeed, taking into account the equality $\sum_{k=1}^{l} f_k = f_{l+2} - 1$, for all natural numbers l, we will make the following transformations:

$\sum_{k=1}^{l} f_k = f_{l+2} - 1$, for all natural numbers l, we will make the following transformations:

$$\sum_{k=1}^{m} f_{n+k} = f_{n+1} + f_{n+2} + ... + f_{n+m} =$$
$$= (f_1 + f_2 + ... + f_{n+m}) - (f_1 + f_2 + ... + f_n) =$$
$$= \sum_{k=1}^{n+m} f_k - \sum_{k=1}^{n} f_k = (f_{n+m+2} - 1) - (f_{n+2} - 1) = f_{n+m+2} - f_{n+2}$$

what was needed.

Here was used the equality: $\sum_{k=1}^{n+m} f_k = f_{n+m+2} - 1$.

The following statement takes place.

Theorem 1. The sum of any m sequential Fibonacci numbers is multiple of m **if** and only if the numbers f_m and $f_{m+1} - 1$ are multiples of m.

Proof. The formulated theorem can be briefly reworded as follows:

$$\sum_{k=1}^{m} f_{n+k} \vdots m, \ n \geq 0 \Leftrightarrow \begin{cases} f_m \vdots m, \\ f_{m+1} - 1 \vdots m. \end{cases}$$

Necessity. Let's know that divisibility $\sum_{k=1}^{m} f_{n+k} \vdots m$ is performed for an arbitrary value $n \geq 0$. Let us prove that the conditions

$$\begin{cases} f_m \vdots m, \\ f_{m+1} - 1 \vdots m. \end{cases}$$

are fulfilled.

We put value $n = 0$ in the identity (2.1):

$$\sum_{k=1}^{m} f_k = f_{m+2} - f_2 = f_m + f_{m+1} - 1. \qquad (2.2)$$

Here we used $f_{m+2} = f_m + f_{m+1}$ and $f_2 = 1$.

Now we put value $n = 1$ in the identity (2.1):

$$\sum_{k=1}^{m} f_{k+1} = f_{m+3} - f_3 = f_{m+2} + f_{m+1} - 2 = f_m + 2(f_{m+1} - 1). \qquad (2.3)$$

We know that the left-hand sides of the equalities (2.2) and (2.3) are divisible by m, therefore the following is true:

$$\begin{cases} f_m + f_{m+1} - 1 \vdots m, \\ f_m + 2(f_{m+1} - 1) \vdots m, \end{cases} \qquad (2.4)$$

That is why the substraction $(f_m + f_{m+1} - 1) - (f_m + 2(f_{m+1} - 1))$ is also divisible by m, or $f_{m+1} - 1 \vdots m$. And so from (2.4) follows that $f_m \vdots m$.

Sufficiency. Suppose that

$$\begin{cases} f_m \vdots m, \\ f_{m+1} - 1 \vdots m. \end{cases}$$

We will prove that for any integer $n \geq 0$ the divisibility $\sum_{k=1}^{m} f_{n+k} \vdots m$ is fulfilled. The proof is carried out using the method of mathematical induction by the number $n \geq 0$.

The base of induction. Let $n = 0$. Then $\sum_{k=1}^{m} f_{n+k} = \sum_{k=1}^{m} f_k = f_{m+2} - 1 = f_m + (f_{m+1} - 1) \vdots m$, as the sum of two numbers which are divisible by m.

The assumption of induction. Suppose that for any $0 \le l \le n$ the following is true $\sum_{k=1}^{m} f_{l+k} \vdots m$. We will prove that $\sum_{k=1}^{m} f_{n+1+k} \vdots m$.

By using, in particular, the relation (2.1), we make the following transformations:

$$\sum_{k=1}^{m} f_{n+1+k} = f_{n+1+m+2} - f_{n+1+2} = f_{n+m+3} - f_{n+3} =$$

$$= (f_{n+m+2} + f_{n+m+1}) - (f_{n+2} + f_{n+1}) =$$

$$= (f_{n+m+2} - f_{n+2}) + (f_{n+m+1} - f_{n+1}) =$$

$$= \sum_{k=1}^{m} f_{n+k} + \sum_{k=1}^{m} f_{n-1+k} \vdots m,$$

because, according to the assumption of an induction, each of the sums is multiple of m. Consequently, the theorem is fully proved.

Conjecture 1. The period $T(p)$ by the modulo p is equal to $p-1$ if $(\frac{5}{p}) = 1$ and it is equal to $2p+2$ if $(\frac{5}{p}) = -1$.

Example 1. Let $(\frac{11}{5}) = 1$, because $4^2 \equiv 5 (\mathrm{mod} 11)$, then the period $T(p) = 10$. The period by the modulo 3 is equal to 8, because $(\frac{3}{5}) = -1$.

Theorem 3. The period by the module pq, where $p, q \in \mathrm{P}$ is equal to the product

$$lcm\left(T(p), T(q)\right) \qquad (1)$$

The period by the composite module 33 equals to $T(33) = lcm(8,10) = 40$.

$$T(38) = T(2 \cdot 19) = lcm\left(T(p), T(q)\right) = lcm\left(3, 18\right) = 18$$

also $T(72) = T(9 \cdot 8) = T(9) \cdot T(8) = lcm\left(8, 18\right) = 24 \cdot 3$.

The period by the composite module $m = 2 \cdot 31$ is the product $T(2) = 3$ by $T(31) = 30$. In other words $T\left(62\right) = lcm\left(T\left(2\right) T(31)\right) = 30$.

Theorem 2. The period by the modulo p^2, where $p \in \mathrm{P}$, is multiple of $T(p)$ and equals to $pT(p)$.

Example 2. The period by the module 49 is equal to $T\left(49\right) = 112 = 2^4 7 = T\left(7^2\right) = T\left(7\right)7 = \left(16\right) \cdot 7 = \left(2^4\right)7.$

Note that $T\left(7\right) = 16$.

Since additional factor to $T\left(7\right)$ is the number 7 therefore $T\left(7^2\right) = T\left(7\right)7$.

CONCLUSION

The research-numerical characteristics of Fibonacci numbers and related sequences are studied in the research work. At the same time, the following research was carried out and the following results were obtained:

1) By using the periodicity of the sequence of the remainders $\{f_n \bmod m\}_{n=1}^{+\infty}$ of Fibonacci numbers f_n on the natural numbers $m > 1$, the table of the remainders of first 30 Fibonacci numbers was compiled for $2 \le m \le 12$.

2) An appropriate theorem, which is checked by means of a computer, is proved, the problem "the sum of the successive numbers of Fibonaccis. Moreover, all the values m that satisfy the condition of this task are found.

3) For the first time the necessary and sufficient conditions for the periodicity of the Fibonacci sums and the conditions for the multiplicity of the sum of any m successive Fibonacci numbers by the number of its terms m have been investigated. The theoretical numerical substantiation of the periodicity of the differences of partial sums of the Fibonacci sequence by module p is found.

This problem is considered, in particular, for the numbers of Lucas, there is a certain similarity of the properties of the consistency of these sums.

REFERENCES

[1] 1. Vorobiev N. Fibonacci numbers. M .: Nauka, 1978. 144 p.

[2] 2. Knut D. The art of programming. Basic algorithms. T. 1 3rd ed. M .: Williams, 2006.

[3] 3. Luzhetsky V.A. Highly-mathematical Fibonacci processors. UNIVERSUM-Vinnitsa. 2000. 248 p.

[4] 4. Markushevich A.I. Return sequences. Popular lectures on mathematics. Moscow: Nauka, 1983. 48 pp.

[5] 5. Naiman E.L. Small encyclopedia of the trader. 9 th ed., Pererab. and additional. Moscow: Alpina Business Books, 2008.

[6] 6. Liddle R., Niederreiter G. Finite fields. Volume 1, Volume 2. M .: World ,. 1988. 430 p.

[7] 7. Soroko E.M. Structural harmony of systems. Minsk: Science and Technology, 1984.

[8] 8. Stakhov A.P. Metal proportions are the new mathematical constants of nature. "Academy of Trinitarianism", M., El. No. 77-6567, publ.14748, 22.03.2008.

[9] 9. Spinadel V.W. The metallic means of family and forbidden symmetries. "Academy of Trinitarianism", M., El No. 77-6567, publ. 12603, 18.11.2005.

[10] 10. Novosad M.V, Dykcha I.A. Luke's numbers. Scientific herald of Chernivtsi University. 2009. 446. pp. 11-15

Distribution of elements of the norm group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$

Pavel Varbanets
Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
Odessa, Ukraine
varb@sana.od.ua

***Abstract*—Consider the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ and prime rational number p that is an irreducible in $\mathbb{Q}(\sqrt{-d})$. We construct an asymptotic formula for the number $R(x,\varphi)$ of elements of the norm group E_n in the sectorial domain $\varphi_1 < \arg w \le \varphi_2$, $\varphi_2 - \varphi_1 = \varphi$. We construct the asymptotic formula for the summatory function, associated with $r_m(k)$, and obtain a nontrivial estimate of error term for $R(x,\varphi)$ in narrow sectors $\varphi_1 < \arg w \le \varphi_2$, where $\varphi_2 - \varphi_1 \ge x^{-s}$, $0 < s \le \frac{1}{8}$, based on such function $r_m(k)$ that is the generalization of classical function of number of representations of the natural k of the positive quadratic form $x^2 + dy^2$.**

***Index Terms*—imaginary quadratic field, norm group, Hecke zeta-function, asymptotic formula**

I. Introduction

Let d be a free-square positive integer and p be an indecomposable in $\mathbb{Q}(\sqrt{-d})$ prime rational number. Denote by K the ring of integer elements from the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Without loss generality we can suppose that $-d \equiv 3 \pmod 4$, so that

$$K = \left\{ w = u + \sqrt{-d}v \,\middle|\, u, v \in \mathbb{Z} \right\}.$$

For $w = u + \sqrt{-d}v$ we denote $N(w) = u^2 + dv^2$ and call the norm of w.

Our aim is to study the distribution of elements w from K with norm $N(w) \equiv 1 \pmod{p^m}$, where $m \ge 3$.

Denote by $K^*_{p^m}$ the multiplicative group of reduced system of residues modulo p^m, and let

$$E_n := \left\{ w \in K^*_{p^n} \,\middle|\, N(w) = 1 \pmod{p^n} \right\}$$

E_m is a cyclic subgroup in $K^*_{p^n}$ and its order equals to $(p+1)p^{n-1}$.

We will construct an asymptotic formula for the number $R(x,\varphi)$ of elements from E_n in the sectorial domain

$$S(x,\varphi) = \left\{ \begin{array}{l} \phi_1 \le \arg w < \phi_2, \\ 0 < N(w) \le x, \\ \phi_2 - \phi_1 = \phi < \frac{\pi}{2} \end{array} \right\}. \tag{1}$$

It's clear that

$$R(x,\varphi) = \sum_{\alpha \in E_n} \sum_{\substack{w \in K \\ w \equiv \alpha \pmod{p^n} \\ w' \in S(x,\varphi)}} 1.$$

First, we define the translated Hecke Z-function of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$

$$Z_m(s;\delta_0,\delta) := \sum_{-\delta_0 \ne w \in K} \frac{e^{gmi \arg(w+\delta_0)}}{N(w+\delta_0)^s} \cdot e^{2\pi i \Re(\delta w)},$$

$(\Re s > 1)$,

where w runs over a set of non-associated numbers of K, $\delta_0, \delta \in \mathbb{Q}(\sqrt{-d})$, g is the number of units in K.

We give some of the auxiliary results which have the self inclusive interests.

II. Auxiliary Results

Lemma 1. *The Hecke zeta-function $Z_m(s;\delta_0,\delta)$ of the imaginary field $\mathbb{Q}(\sqrt{-d})$ satisfies the functional equation*

$$\begin{aligned} (\pi d)^{-s}\Gamma(2|m|+s) Z_m(s;\delta_0,\delta) = \\ = (\pi d)^{-(1-s)}\Gamma(2|m|+1-s) \times \\ \times Z_{-m}(1-s;\delta_0,-\delta)\, e^{-2\pi i \Re(\delta\bar{\delta}_0)}. \end{aligned} \tag{2}$$

Moreover, $Z_m(s;\delta_0,\delta)$ is an entire function if $m \ne 0$ or $m = 0$ and δ is not a Gaussian integer. For $m = 0$ and $\delta \in G$ it is holomorphic except for the point $s = 1$, where it has a simple pole with the residue π.

To prove this assertion we use the Poisson summation formula and follow by the proof of an analogous statement for Hecke Z-function over the Gaussian field (see, [4], [2], [1]).

Lemma 2. *In the strip $\varepsilon \le \Re s \le 1+\varepsilon$, $\varepsilon > 0$ the following estimate*

$$\begin{aligned} (s-1)\cdot Z_m(s;\delta_0,\delta) \ll \left(|t|+1\right) \times \\ \times \left(t^2+m^2\right)^{\frac{(1-2\sigma)(1+\varepsilon-\sigma)}{1+2\varepsilon}} \cdot |N(\delta)|^{-\frac{\sigma+\varepsilon}{1+2\varepsilon}} \end{aligned} \tag{3}$$

holds.

To prove Lemma 2 it's enough to use estimates for $Z_m(s)$ on bounds of strip $0 \le \Re s \le 1+\varepsilon$ and then using the Phragmén-Lindelöf principle.

Lemma 3. *([5], Theorem 1) Let ℓ, q are positive integers with $(\ell, q) = 1$. Then for $q < x$ the following asymptotic formula*

$$\begin{aligned} \sum_{\substack{\alpha \in K \\ N(\alpha) \equiv \ell \,(mod\, q)}} 1 = \tfrac{x}{q} C(q,d) + \\ + O\left(x^{\frac{1}{2}} exp\left(c\tfrac{(\log)^{\frac{1}{2}}}{\log\log q} \right) \right) + O\left(\tfrac{x^{\frac{1}{2}}}{q^{\frac{1}{4}}} \tau(q) \right) \end{aligned}$$

holds,
where $q^{-\varepsilon} \ll C(q,d) \ll q^{\varepsilon}$ with the constants in symbol "$\ll$" depending only on d and ε.

The proof of this statement based on application the p-adic description of the solutions of the congruence

$u^2+dv^2 \equiv a \pmod{p^\ell}$ and the estimations of exponential sums on a curve over the finite field. Moreover, we use the Lavrik's truncated functional equation for the Hecke Z-function of the imaginary quadratic field.

Lemma 4. *Let $p \equiv 3 \pmod 4$. Then for $n = 1, 2, 3, \ldots$ the estimate*

$$\sum_{\alpha \in E_n} e^{2\pi i \Re\left(\frac{\alpha^2}{p^n}\right)} \ll p^{\frac{n}{2}} \tag{4}$$

holds.

The proof of this lemma based on the p-adic description of powers of the generative element over the norm group E_n that is multiple to $p+1$ and applying the estimate of exponential sum with an exponent of polynomials of special type.

Therefore, let give below the description of elements of the norm group E_n.

Let us denote by E_n the following subgroup of $K^*_{p^n}$, p be an indecomposable in $\mathbb{Q}(\sqrt{-d})$ prime rational number:

$$E_n := \{x \in K^*_{p^n} \ : \ N(x) \equiv 1 \pmod{p^n}\}.$$

Take into account that the multiplicative group of the field K_p is a cyclic group. It is easy to prove (as in $\mathbb{Z}^*_{p^n}$) that it exists a generating element of the group E_1, such that it will generate every group E_n, $n > 1$.

In order to find that element, we take such generating element g_0 of group K^*_p for which $g_0^{(p+1)p} = 1 + hp^2$ with $(h, p) = 1$. Taking g_0 such that its norm $N(g_0) \equiv 1 \pmod{p^n}$ we infer that g_0^{p-1} is revealed generating element of group E_n, $n = 1, 2, \ldots$.

Let $g_0^{p-1} = u + \sqrt{-d}v$. Then

$$ord(u + \sqrt{-d}v) = |E_n| = 2(p+1)p^{n-1}$$

and

$$(u + \sqrt{-d}v)^{2(p+1)} = 1 + p^2 x_0 + \sqrt{-d}py_0,$$
$$x_0 + 2dy_0^2 \equiv 0 \pmod p, \ (x_0, p) = (y_0, p) = 1,$$

and also for any $t = 4, 5, \ldots$, we have modulo p^n

$$\begin{aligned} &\Re\Big(u + \sqrt{-d}v\Big)^{2(p+1)t} = \\ &\qquad = A_0 + A_1 t + A_2 t^2 + \cdots + A_{n-1}t^{n-1}, \\ &\Im\Big(u + \sqrt{-d}v\Big)^{2(p+1)t} = \\ &\qquad = B_0 + A_1 t + B_2 t^2 + \cdots + B_{n-1}t^{n-1}, \end{aligned} \tag{5}$$

where

$$\begin{cases} A_0 \equiv 1 \pmod{p^4}, \ B_0 \equiv 0 \pmod{p^4}, \\ A_1 \equiv p^2 x_0 + \frac{1}{2}p^2 d y_0^2 \equiv 0 \pmod{p^3}, \\ B_1 \equiv p y_0 \pmod{p^3}, \\ A_2 \equiv -\frac{1}{2}p^2 d y_0^2 \pmod{p^3}, \\ B_2 \equiv 0 \pmod{p^3}, \\ A_j \equiv B_j \equiv 0 \pmod{p^3}, \ j = 3, 4, \ldots n-1. \end{cases} \tag{6}$$

Denote

$$\begin{aligned} &\Big(u + \sqrt{-d}v\Big)^{2k} = \\ &\qquad = u(k) + \sqrt{-d}v(k), \ 0 \le k \le p, \\ &\Big(u + \sqrt{-d}v\Big)^{2(p+1)t+2k} \equiv \\ &\qquad \equiv \sum_{j=0}^{n-1} \Big(A_j(k) + \sqrt{-d}B_j(k)\Big) t^j \pmod{p^n}. \end{aligned}$$

It is clear

$$A_j(k) = A_j u(k) - B_j v(k),$$
$$B_j(k) = A_j v(k) + B_j u(k).$$

For $k = 1, 2, \ldots, p$, we have

$$\begin{aligned} &u(k) \equiv u(-k), \ v(k) \equiv -v(-k) \pmod{p^n}, \\ &(u(k), p) = (v(k), p) = 1, \ if \ k \ne \frac{p+1}{2}, \\ &u(0) = 1, \ v(0) = 0, \\ &u(k) \equiv 0 \pmod p, \ (v(k), p) = 1, \ if \ k = \frac{p+1}{2}. \end{aligned}$$

Moreover, for $k \ne \frac{p+1}{2}$

$$A_0(k) \equiv u(k), \ B_0(k) \equiv v(k) \pmod p,$$
$$p||A_1(k), \ p||B_1(k), \ p^2||A_2(k), \ p^2||B_2(k);$$

and

$$\begin{aligned} &A_1(0) \equiv 0 \pmod{p^4}, \ B_1(0) \equiv py_0 \pmod{p^4}, \\ &p^2||A_2(0), \ B_2(0) \equiv 0 \pmod{p^3}, \\ &A_0(k) \equiv 0, \ B_0(k) \equiv 0 \pmod p, \\ &p||A_1(k), \ p^2||B_1(k), \ p^2||A_2(k), \\ &B_2(k) \equiv 0 \pmod{p^3} \ if \ k = \frac{p+1}{2}, \\ &A_j(k) \equiv B_j(k) \equiv 0 \pmod{p^3}, \ k = 0, 1, \ldots, p, \ j \ge 3. \end{aligned}$$

The verification of these relations is a simple exercise (in view the congruence

$$\begin{aligned} &(u + \sqrt{-d}v)^{p+1} = 1 + p^2 x_0 + \sqrt{-d}y_0, \\ &(x_0, p) = (y_0, p) = 1, \\ &2x_0 + dy_0^2 \equiv 0 \pmod p, \\ &u^2 + dv^2 \equiv +1 \pmod{p^n} \qquad), \end{aligned}$$

and we omit.

Lemma 5. *([5],Lemma 5) Let p be a prime number, u_1, u_2 be integers and let $(u_1, u_2, p^n) = p^m$. Then the following estimate*

$$\left| \sum_{l_1^2 + d l_2^2 \equiv 1 \pmod{p^n}} e^{2\pi i \frac{u_1 l_1 + u_2 l_2}{p^n}} \right| \ll p^{\frac{n+m}{2}} \tag{7}$$

holds, with an absolute constant in symbol " $\ll$ ".

Lemma 6. *(Vinogradov's "glasses") Let $r \in \mathbb{N}, \Omega > 0, 0 < \Delta < \frac{1}{2}\Omega$ and let ϕ_1, ϕ_2 be real numbers, $\Delta \le \phi_2 - \phi_1 \le \Omega - 2\Delta$. Then there exists a periodic function $f(\phi)$ with the period Ω such that:*

(i) $f(\phi) = 1$, in the segment $\phi \in [\phi_1, \phi_2]$;
$0 \le f(\phi) \le 1$ in the segments $[\phi_1 - \Delta, \phi_1]$ and

$[\phi_2, \phi_2 + \Delta]$;

$f(\phi) = 0$, *in the segment* $[\phi_2 + \Delta, \phi_1 + \Omega - \Delta]$;

(ii) $f(\phi)$ *has the expansion in a Fourier series*

$$f(\phi) = \sum_{m=-\infty}^{+\infty} a_m e^{2\pi i \frac{m\phi}{\Omega}},$$

where $a_0 = \frac{1}{\Omega}(\phi_2 - \phi_1 + \Delta)$,

$$|a_m| \leq \begin{cases} \frac{1}{\Omega}(\phi_2 - \phi_1 + \Delta), \\ \frac{2}{\pi|m|}, m \neq 0, \\ \frac{2}{\pi|m|}\left(\frac{r\Delta}{\pi|m|\Delta}\right)^2. \end{cases}$$

III. Main Results

Let us consider the function of a natural argument

$$r_m(k) = \sum_{\substack{w \in K \\ N(w)=k}} e^{gmi \arg(w)}.$$

Thus we can write the generating series for $\Re s > 1$

$$F_m(s) = \sum_{\substack{k \leq x \\ k \equiv 1 \pmod{p^n}}}^{\infty} \frac{r_m(k)}{k^s}.$$

The following theorem is valid

Theorem 1. *Let* $m \neq 0, p^n \leq x \leq p^{2n}$. *Then we have*

$$\sum_{\substack{k \leq x \\ k \equiv 1 \pmod{p^n}}} r_m(k) \ll \frac{\sqrt{x}}{p^{\frac{n}{2}}} + p^{\frac{n}{2}} \log x + p^{\frac{n}{2}} M \log M.$$

where $M = |m| + 3$.

Corollary. *Let* $q \ll x \ll q^2$, *where* q *consists only from the prime numbers that are indecomposable in* $\mathbb{Q}(\sqrt{-d})$. *Then for* $m \neq 0$ *the asymptotic bound*

$$\sum_{\substack{k \leq x \\ k \equiv 1 \pmod{q}}} r_m(k) \ll \frac{x^{\frac{1}{2}}}{q^{\frac{1}{2}}} + q^{\frac{1}{2}} \tau(q) \log x + q^{\frac{1}{2}} \tau(q) M \log M.$$

holds.

Now, applying Theorem 1, Corollary and Lemma of Vinogradov's glasses give the following statement.

Theorem 2. *Let* $p^{\frac{3}{2}n} \leq x \leq p^{2n}, 0 \leq \phi_1 < \phi_2 \leq \frac{\pi}{2}$ *and let* $0 < s \leq \frac{1}{8}$. *Then for* $\phi_2 - \phi_1 \geq x^{-s}$ *the asymptotic formula*

$$R(x;\phi) = \frac{\phi_2 - \phi_1}{2} \cdot \frac{p+1}{p} \cdot \frac{x}{p^n} + O\left(3^n \frac{x^{1-s}}{p^n} \log x\right)$$

holds.

IV. Conclusion

The group E_n is a subgroup of group $E_n^{\pm}$ which elements satisfy the congruence $N(w) \equiv \pm 1 \pmod{p^n}$ for every $w \in E_n^{\pm}$ such that $[E_n^{\pm} : E_n] = 2$. Thus the elements from E_n can be considered as squares of elements from $E_n^{\pm}$, i.e. the elements from E_n are the quadratic residues in $E_n^{\pm}$.

Our investigation is the generalization of results from [1].

References

[1] L.Balyas, P. Varbanets, *Quadratic residues of the norm group in sectorial domains*, Algebra and Discrete Mathematics, 22**2**, 2016, pp. 153-170.

[2] E.Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen I-II*, Math.Z., T.**1**, 1918, ss.357-376; T.**6**, 1920, ss.11-51.

[3] J.Kubilius, *On one problem of multidimensional analytic number theory*, Proc. Vilnius Univ., N.**4**, 1955, pp.5-41 (in Lithuanian).

[4] Elias M. Stein, Guido Weiss, *Introduction to Fourier analysis on Euclidian spaces*, Princeton, New Jersey, Princeton University Press, 1971, P.312.

[5] P.Varbanets, *Problem of circle in aritmetic progression*, Math.zametki, N.**8(6)**, 1970, pp.787-798(in Russian).

Class Fields, Riemann Surfaces and (Multiple) Zeta Values

Nikolaj Glazunov
dept. of electronics
National Aviation University
Kiev, Ukraine
glanm@yahoo.com

***Abstract*—The paper is concerned with class fields, Riemann surfaces and (multiple) zeta values in the cases of the field of rational numbers and (imaginary) quadratic fields. Results on multiple zeta values have presented by D. Zagier, by P. Deligne and A.Goncharov, by A. Goncharov and others. S. Unver have investigated p-adic multiple zeta values. Tannakian interpretation of p-adic multiple zeta values is given by Furusho. Motivic unipotent fundamental groupoid and Galois descents have investigated by C. Glanois. In these interesting papers (and in references therein) authors use powerful motivics approaches. Here we present very shortly more elementary approach to (multiple) zeta values in the cases of the field of rational numbers and (imaginary) quadratic fields. At first we present the explicit version of the Kronecker-Weber theorem in the case of imaginary quadratic fields with class number one. Next considerations concern with Riemann zeta values, Eisenstein series and modular invariants, class fields, zeta functions, Riemann surfaces, iterated integrals and (multiple) zeta values. In some cases, for instance under computer algebra computations, we have to enumerate investigated objects. Some simple parametric spaces and moduli spaces in the case of imaginary quadratic fields have been constructed by the author. Numerical examples are included.**

***Index Terms*—imaginary quadratic field, modular function, cyclotomic field, zeta function, iterated integral, zeta value**

I. Introduction

Results on multiple zeta values have presented by D. Zagier [1], by Deligne and Goncharov [2], by Goncharov [3] and others. Unver [5] have investigated p-adic multiple zeta values. Tannakian interpretation of p-adic multiple zeta values is given by Furusho [4]. Motivic unipotent fundamental groupoid and Galois descents are used in the paper by Glanois [6]. In these interesting papers (and in references therein) as well as in papers of another authors are used powerful motivics approaches .

Here we present very shortly more elementary approach to (multiple) zeta values in the cases of the field of rational numbers $\mathbb{Q}$ and (imaginary) quadratic fields. This approach is based on works [7]–[10].

Theorem 1: (The Kronecker-Weber theorem) Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

With results by Heegner, Deuring, Birch, Baker, Stark, Shafarevich we have

Proposition 1: Imaginary quadratic fields with class number one and with descriminants $-D = 4, 8, 3, 7, 11, 19, 43, 67, 163$ are contained, respectively, in cyclotomic fields

$$\begin{gathered}\mathbb{Q}(\sqrt[4]{1}), \mathbb{Q}(\sqrt[8]{1}), \mathbb{Q}(\sqrt[3]{1}), \mathbb{Q}(\sqrt[7]{1}), \mathbb{Q}(\sqrt[11]{1}),\\ \mathbb{Q}(\sqrt[19]{1}), \mathbb{Q}(\sqrt[43]{1}), \mathbb{Q}(\sqrt[67]{1}), \mathbb{Q}(\sqrt[163]{1}).\end{gathered} \tag{1}$$

In some cases, for instance under computer algebra computations, we have to enumerate investigated objects. Some simple parametric spaces and moduli spaces in the case of imaginary quadratic fields are presented in the abstract of the author [14].

II. Riemann zeta values, Eisenstein series and modular invariants

Here we follow to [7]–[10].

Let $s = \sigma + it$ be a complex number and let $\zeta(s)$ be the Riemann zeta function which is presented for $\sigma > 1$ by the series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s};$$

By Euler for $m \geq 1$

$$\zeta(2m) = (-1)^{m-1} \frac{(2\pi)^{2m}}{2(2m)!} B_{2m}$$

where B_{2m} are Bernoulli numbers; recall also that

$$\zeta(-n) = -\frac{B_{n+1}}{n+1},$$

for odd $n = 1, 3, 5, \ldots$.

Example 1: (By Euler (taken from [10])),

$$\zeta(2) = \frac{\pi^2}{6}. \ \zeta(4) = \frac{\pi^4}{90},$$
$$\zeta(-1) = -\frac{B_2}{2} = -\frac{1}{12}, \zeta(-3) = \frac{1}{120}.$$

Let τ belong to the modular figure of the modular group

$$\Gamma = \Gamma(1) = SL(2, \mathbb{Z})/\{E, -E\},$$

where E is the unit matrix.

Definition 1: In these notations with $k > 1$ the Eisenstein series is defined as

$$c_k = \sum_{m \neq 0, k>1} \frac{1}{(n + m\tau)^{2k}}.$$

Proposition 2: Eisenstein series have the representation

$$c_k = 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!} \sum_{n>0, m>0} n^{2k-1} q^{nm},$$

where $q = \exp^{2\pi i\tau} \neq 0$.

If we will use functions of the sums of divisors σ_{2k-1} we obtain

$$c_k = 2\zeta(2k) + \frac{2(-2\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

or shortly

$$c_k = 2\zeta(2k) + \frac{2(-2\pi)^{2k}}{(2k-1)!}S_{2k-1}$$

.

Put $g_2 = 60c_2$, $g_3 = 140c_3$.

Proposition 3: $\Delta = g_2^3 - 27g_3^2 \neq 0$.

As $\Delta \neq 0$ it is possible to define $J = \frac{g_2^3}{\Delta}$.

Definition 2: Modular invariant of the elliptic curve $y^2 = 4x^3 - g_2x - g_3$ is equal to $j = 2^6 3^3 J$.

Proposition 4: $j = \frac{1}{q} + u_1 q + \cdots$ where u_i are integers, $u_0 = 0$.

Define polylogarithm

$$L_m(z) = \sum_{n=1}^{\infty} z^n n^{-m}.$$

Example 2:

$$\zeta(2) = L_2(1).$$

III. Class fields and zeta functions

Here we follow to [8], [10].

Let K be an imaginary quadratic field and let Cl_K be its class group.

Definition 3: Let $N(\mathfrak{a})$ be the norm of the ideal $\mathfrak{a}$. The Dedekind ζ-function for K is defined for all $s > 1$ by the series

$$\zeta_K(s) = \sum \frac{1}{N(\mathfrak{a})^s},$$

where the sum is taken over all nonzero ideals $\mathfrak{a} \in \mathcal{O}_K$.

Let R be a subring ($R \neq \mathbf{Z}$) of the ring of integers $\mathcal{O}_K$ of the imaginary quadratic field K.

Let $M_1, \dots M_h$ be pairwise nonequivalent modules of K with the same ring of multipliers R.

Proposition 5: $j(M_1), \dots, j(M_h)$ are integer algebraic numbers which are conjugate over K.

Proposition 6: The field $K(j(M_i))/K$ is the normal field.

Definition 4: The field $K(j(M_i))/K$ is called the ring class field.

Follow to [8] it is possible to define ray class field. As in an imaginary quadratic field there is no real infinite primes so modulus of the field is an ideal of the ring of integers of the field.

Let $\mathfrak{m}$ be a modulus of the an imaginary quadratic field K, let $Cl_K^{\mathfrak{m}}$ be the ray class group, let τ be the Weber function .

Let $\mathfrak{R} \in Cl_K$ and let $\mathfrak{R}^* \in Cl_K^{\mathfrak{m}}$ be the ideal class whose image in Cl_K is equal to $(\mathfrak{m})\mathfrak{R}^{-1}$.

Proposition 7: The field $K(j(\mathfrak{R}), \tau(\mathfrak{R}^*))/K$ is the ray class field.

Let C be an ideal class.

Definition 5: The ideal class zeta function is the expression of the form

$$\zeta_C(s) = \sum_{\substack{\mathfrak{a}\in C \\ \mathfrak{a} \text{ integral}}} \frac{1}{N(\mathfrak{a})^s}$$

IV. Modular group, congruence subgroups and Riemann surfaces

Let $H = \{z | \Im z > 0\}$ be the upper halfplane, and let

$$\overline{H} = H \cup \mathbb{P}^1(\mathbb{Q}).$$

The space $\Gamma \setminus \overline{H}$ is the compact Riemann surface of the genus zero.

Let n be a positive integer.

Let $\Gamma(n)$ be the principal congruence subgroup of the level n and let $\Gamma_0(n)$, $\Gamma_1(n)$ be the Hecke congruence subgroups. By [11] we have

Proposition 8: The spaces

$$\Gamma(n) \setminus \overline{H},\ \Gamma_0(n) \setminus \overline{H},\ \Gamma_1(n) \setminus \overline{H},$$

are (compact) Riemann surfaces.

V. Multiple zeta values

Definition 6: Let $x_1, \dots x_p$ be natural numbers with $x_p \geq 2$. The multiple zeta value of the weight w and the depth p is called the expression of the form

$$\zeta(x_1, \dots x_p) = \sum_{0<n_1<\cdots<n_r} \frac{1}{n_1^{x_1} \cdots n_p^{x_p}}, w = \sum x_i.$$

Example 3:

$$\zeta(2,2) = \sum_{0<n_1<n_2} \frac{1}{n_1^2 n_2^2}, w = \sum x_i = 4.$$

Example 4:

$$\zeta(2,2) = \frac{1}{2}(\zeta(2)\zeta(2) - \zeta(4)).$$

Let μ_N be the group of roots of unity.

Definition 7: Let $x_1, \dots x_p$ be natural numbers with $x_p \geq 2$. The multiple zeta value relative to μ_N of the weight w and the depth p is called the expression of the form

$$\zeta\binom{x_1,\dots x_p}{\epsilon_1,\dots,\epsilon_p} = \sum_{0<n_1<\cdots<n_p} \frac{\epsilon_1^{n_1} \dots, \epsilon_p^{n_p}}{n_1^{x_1} \cdots n_p^{x_p}}, \epsilon_i \in \mu_N,$$

$$w = \sum x_i, (x_p, n_p) \neq (1,1).$$

VI. Iterated integrals and (multiple) zeta values

Here we follow to [12], [13].

Let $\mathbb{C}$ be the complex plane and $f_i(z)$ be the holomorphic function on $\mathbb{C}$. Let $f_i(z)dz$ be the differential of the first kind on $\mathbb{C}$. Let S be a Riemann surfaces and w be the differential of the first kind on S. Parshin has considered iterated integrals of this type on Riemann surfaces [12]. Chen [13] for smooth paths on a manifold M and respective path spaces have investegated iterated (path) integrals. For differential forms $w_1, \dots, w_r$ on M he has constructed the iterated integrals by repeating r times the integration of the path space differential forms (and their

linear combinations). Chen [13] has denoted the iterated integrals as $\int w_1 w_2 \cdots w_r$ and set $\int w_1 w_2 \cdots w_r = 1$ when $r = 0$ and $\int w_1 w_2 \cdots w_r = 0$ when $r < 0$.

Example 5:

$$\zeta(2) = \int_0^1 \frac{dt_1}{t_1} \int_0^{t1} \frac{dt_2}{1 - t_2} = \frac{\pi^2}{6}.$$

More generally iterated integrals are path space differential forms which permit further integration.

We plan to consider relations between (multiple) zeta values and iterated integrals with emphasize on (computer) algebraic aspects.

REFERENCES

[1] D. Zagier, "Periods of modular forms, traces of Hecke operators, and multiple $\zeta-$values, " Research into Automorphic Forms and $L-$functions, Kyoto, Surikaisekikenkyusho Kokyuroku 843, pp.162–170, 1993.

[2] P. Deligne , A. Goncharov , "Groupes fondamentaux motiviques de Tate mixte, "Ann. Sci. Ecole Norm. Sup., (4) 38, no. 1, pp. 1–56, 2005.

[3] A. Goncharov , "Multiple ζ-values, Galois groups, and geometry of modular varieties, " European Congress of Mathematics, vol. I, Barcelona, Progr. Math., vol. 201, Birkhauser, 2000, 361–392.

[4] H. Furusho , "P-adic multiple zeta values II. Tannakian interpretations," Am. J. Math., 129 (4), 1105–1144, 2007.

[5] S. Ünver , "Cyclotomic p-adic multi-zeta values in depth two.," Manuscr. Math., 149, no. 3-4, 405–441, 2016.

[6] C. Glanois, "Motivic unipotent fundamental groupoid of $G_m \backslash \mu_N$ for $N = 2, 3, 4, 6, 8$ and Galois descents," Journ. of Number Theory, 160, 334–384, 2016.

[7] H. Weber , Lehrbuch der Algebra, III, Braunschweig, 1908.

[8] H. Hasse, "Zum Hauptidealsatz der komplexen Multiplikation, usw," Monatshefte fur Math., 38, 315–322, 323–330, 331–344, 1931.

[9] M. Deuring, "Klassenkorper der komplexen Multiplikation, "Enzyklopadie der Math. Wiss. Bd. 12, Heft 10, Teil II, 23.

[10] Z. Borevich, I. Shafarevich, Number Theory, Pure and Applied mathematics. New York : Academic Press, 1986.

[11] R. Gunning, Lectures on modular forms, Annals of Mathematics Studies, 48, Princeton, New Jersey, Princeton University Press, 1962.

[12] A. Parshin, "A generalization of Jacobian variety, "Izv. Akad. Nauk SSSR Ser Mat., 30, 175–182, 1966.

[13] K. Chen. "Iterated path integrals, "Bull. Amer. Math. Soc. 83, 831-879, 1977.

[14] N. Glazunov, "Class groups of rings with divisor theory, L-functions and moduli spaces, "Int. conf. 'Algebraic and geometric methods of analysis'. Book of abstracts. 2018, https://www.imath.kiev.ua/ topology/conf/agma2018

Vibrations of a polyhedron

Anastasia Dudko
Department of Higher Mathematics and Statistics
South Ukrainian National Pedagogical University
Odessa, Ukraine
nastysha00301@gmail.com

Vyacheslav Pivovarchik
Department of Higher Mathematics and Statistics
South Ukrainian National Pedagogical University
Odessa, Ukraine
vpivovarchik@gmail.com

***Abstract*—A graph of truncated icosahedron is considered each edge of which is a Stieltjes string symmetric with respect to its midpoint. The spectrum of small vibrations of such a graph is described.**

***Index Terms*—Stieltjes string, Lagrange identity, adjacency matrix, eigenvalues, cyclomatic number.**

I. Introduction

A fullerene (buckyball) is any molecule composed entirely of carbon, in the form of a hollow sphere, ellipsoid, tube, and many other shapes. In our case, we will consider buckminsterfullerene C_{60}. It was prepared in 1989 by Richard Smalley and was named after Richard Buckminster Fuller, an architect who created a geodesic dome similar to a truncated icosahedron known in mathematics as one of the Archimedean solids. Buckminsterfullerene is the smallest fullerene molecule containing pentagonal and hexagonal faces in which no two pentagons share an edge. The structure of C_{60} is a truncated icosahedron (one of the semiregular or Archimedean solids), which resembles an association football ball of the type made of twenty hexagons and twelve pentagons, with a carbon atom at the vertices of each polygon and a bond along each polygon edge [8].

In this paper we consider small transverse vibrations of truncated icosahedron the edges of which are so-called Stieltjes strings, i.e. elastic threads of zero density bearing point masses. Transverse vibrations of graphs of such strings were considered in many publications [2], [3], [4].

Spectral problems describing longitudinal vibrations of a graph of springs bearing masses are reduced to the same equations [6].

We choose arbitrary orientation of the edges of the graph. Let us consider a Stieltjes string bearing $n \geq 3$ point masses $m_1, m_2, ..., m_n$ ($m_k > 0$), let $l_0, l_1, ..., l_n$ ($l_k > 0$) be the intervals into which the masses divide the total length l of the string ($\sum\limits_{k=1}^{n} l_k = l$). We enumerate the point masses m_k ($k = 1, 2, ..., n$) and subintervals l_k ($k = 0, 1, ..., n$) on an edge successively in the direction of the edge. In the sequel we consider Stieltjes strings symmetric with respect to their midpoints. This means that: 1) if n is even then: $m_k = m_{n-k+1}, \quad k = 1, ..., \frac{n}{2}$, $l_k = l_{n-k}, \quad k = 0, ..., \frac{n}{2} - 1$, 2) if n is odd then: $m_k = m_{n-k+1}, \quad k = 1, ..., \left[\frac{n}{2}\right]$, $l_k = l_{n-k}, \quad k = 0, ..., \left[\frac{n}{2}\right]$ where $[a]$ denotes the integer part of a.

We consider a fullerene graph G each edge of which is the same symmetric Stieltjes string bearing n point masses. The graph is stretched and can vibrate such that each mass moves in the direction orthogonal to the equilibrium position of the edge.

Denote by $v_i \quad (i = 1, 2, ..., 60)$ the vertices of G, by e_j ($j = 1, 2, ..., 90$) the edges of G.

We choose arbitrary orientation of the edges. For each i denote by $d(v_i) = 3$ the degree of a vertex v_i, by $d^+(v_i)$ the indegree, i.e. the number of edges incoming into v_i, by $d^-(v_i)$ the outdegree, i.e. the number of edges outgoing from v_i. Let W_i^+ be the set of numbers of edges incoming into v_i and W_i^- be the set of numbers of edges outgoing from $v_i \quad (i = 1, 2, ..., 60)$.

We assume absence of point masses at the vertices. For amplitudes $U_k^{(j)}$ of vibrations of masses we obtain the following spectral problem:

$$\frac{U_k^{(j)} - U_{k-1}^{(j)}}{l_{k-1}} + \frac{U_k^{(j)} - U_{k+1}^{(j)}}{l_k} = -m_k z U_k^{(j)}, \quad (1)$$

$$U_0^{(j_1^-)} = U_0^{(j_2^-)} = ... = U_0^{(j_{d^-(v_i)}^-)} = U_{n+1}^{(j_1^+)} =$$

$$= U_{n+1}^{(j_2^+)} = ... = U_{n+1}^{(j_{d^+(v_i)}^+)}, \quad (2)$$

$$\sum_{m=1}^{d^+(v_i)} \frac{U_{n+1}^{(j_m^+)} - U_n^{(j_m^+)}}{l_n} - \sum_{m=1}^{d^-(v_i)} \frac{U_1^{(j_m^-)} - U_0^{(j_m^-)}}{l_0} = 0 \quad (3)$$

where $k = 1, 2, .., n; \quad i = 1, 2, .., 60; \quad j_m^- \in W_i^-, \quad m = j_1^-, ..., j_{d^-(v_i)}^-; \quad j_m^+ \in W_i^+, \quad m = j_1^+, ..., j_{d^+(v_i)}^+$ and U_k^j is the amplitude of vibrations of the mass m_k located on the edge e_j, z is the spectral parameter. Here equations (1.2) are the continuity conditions and (1.3) describe the balance of forces.

Following [5] we look for a solution in the form $U_k^{(j)} = R_{2k-2}(z, c)U_1^{(j)}, \quad k = 1, 2, ..., n+1$, where $R_{2k-2}(z, c)$ is a polynomials of degree $k - 1$.

The polynomials $R_k(z, c)$ satisfy the following recurrence relations:

$$R_{2k}(z, c) = l_k R_{2k-1}(z, c) + R_{2k-2}(z, c),$$

$$R_{2k-1}(z, c) = R_{2k-3}(z, c) - m_k z R_{2k-2}(z, c)$$

with the initial conditions

$$R_{-1}(z, c) \equiv \frac{1 - c}{l_0}, \quad R_0(z, c) \equiv 1.$$

For a symmetric string

$$R_{2n-1}(z, 0) = \frac{1}{l_0} R_{2n}(z, 1) \quad (4)$$

and due to the Lagrange identity (see, e.g. [7], Lemma 3.5)

$$\frac{1}{l_0}(R_{2n}(z,1))^2 - \frac{1}{l_0} = R_{2n}(z,0)R_{2n-1}(z,1). \quad (5)$$

It is convenient to introduce the following solution of (1):

$$U_k^{(j)}(z) = \frac{B^{(j)} - A^{(j)}R_{2n}(z,1)}{R_{2n}(z,0)}R_{2k-2}(z,0) + \\ + A^{(j)}R_{2k-2}(z,1), \quad (6)$$

where $A^{(j)}, B^{(j)}$ are constants independent of k and z. These solutions exist for all z which are not zeros of $R_{2n}(z,0)$.

Continuity conditions (2) look now as

$$A^{(j_1^-)} = A^{(j_2^-)} = ... = A^{(j^-_{d^-(v_i)})} = \\ = B^{(j_1^+)} = B^{(j_2^+)} = ... = B^{(j^+_{d^+(v_i)})} := \Phi(v_i). \quad (7)$$

Balance of forces equation (3) with account of (6), (7) attains the form

$$\sum_{m=1}^{d^+(v_i)} (l_n B^{(j_m^+)} R_{2n-1}(z,0) - A^{(j_m^+)}) - \\ - \sum_{m=1}^{d^-(v_i)} (B^{(j_m^-)} - A^{(j_m^-)} R_{2n}(z,1)) = 0. \quad (8)$$

or

$$R_{2n}(z,1)d(v_i)\Phi(v_i) - \sum_{v_j \sim v_i} \Phi(v_j) = 0.$$

Here the sum is taken over all the virtices v_j adjacent with v_i.

Finally, we obtain using the notation $\zeta = 3R_{2n}(z,1)$, $F = \{\Phi(v_1), ..., \Phi(v_{60})\}^T$, and denoting by A the adjacency matrix of our graph:

$$\zeta F - AF = 0. \quad (9)$$

Let z_0 be not a zero of $R_{2n}(z,0)$, then it is an eigenvalue of problem (1)–(3) if and only if $\zeta_0 := 3R_{2n}(z_0,1)$ is an eigenvalue of matrix equation (9). This means that the spectrum of problem (1)–(3) consists of zeros of $R_{2n}(z,0)$ and of zeros of the polynomials $3R_{2n}(z,1) - \zeta_s$, where ζ_s ($s = 1, 2, ..., 60$) are the eigenvalues of (9).

This means that the characteristic polynomial of problem (1) – (3) is

$$\phi(z) = (R_{2n}(z,0))^{30} P_{60}(3R_{2n}(z,1)),$$

where

$$P_{60}(\zeta) = (\zeta-3)(\zeta^2+3\zeta+1)^3(\zeta^4-3\zeta^3-2\zeta^2+7\zeta+1)^3 * \\ *(\zeta+2)^4(\zeta^2+\zeta-4)^4(\zeta^2-\zeta-3)^5(\zeta^2+\zeta-1)^5(\zeta-1)^9.$$

Thus we obtain the following set of zeros of P_{60}: $\zeta_1 = \zeta_2 = \zeta_3 = -2.618$, $\zeta_4 = \zeta_5 = \zeta_6 = \zeta_7 = -2.562$, $\zeta_8 = \zeta_9 = \zeta_{10} = \zeta_{11} = -2$, $\zeta_{12} = \zeta_{13} = \zeta_{14} = \zeta_{15} = \zeta_{16} = -1.6818$, $\zeta_{17} = \zeta_{18} = \zeta_{19} = -1.438$, $\zeta_{20} = \zeta_{21} = \zeta_{22} = \zeta_{23} = \zeta_{24} = -1.303$, $\zeta_{25} = \zeta_{26} = \zeta_{27} = -0.382$, $\zeta_{28} = \zeta_{29} = \zeta_{30} = -0.139$, $\zeta_{31} = \zeta_{32} = \zeta_{33} = \zeta_{34} = \zeta_{35} = 0.618$, $\zeta_{36} = \zeta_{37} = \zeta_{38} = \zeta_{39} = \zeta_{40} = \zeta_{41} = \zeta_{42} = \zeta_{43} = \zeta_{44} = 1$, $\zeta_{45} = \zeta_{46} = \zeta_{47} = \zeta_{48} = 1.562$, $\zeta_{49} = \zeta_{50} = \zeta_{51} = 1.820$, $\zeta_{52} = \zeta_{53} = \zeta_{54} = \zeta_{55} = \zeta_{56} = 2.303$, $\zeta_{57} = \zeta_{58} = \zeta_{59} = 2.757$, $\zeta_{60} = 3$.

The graph C_{60} is cyclically connected (see Definition 2.3 in [1]). The maximum multiplicity of an eigenvalue of the problem on such graph is $\mu + 1$ where μ is the cyclomatic number of the graph [1], Theorem 3.2. Since $\mu = q - p + 1$, in our case $\mu + 1 = 32$. We see that in our problem the maximum possible multiplicity is 32 when the eigenvalue is a (simple) zero of $R_{2n}(z,0)$ and a double zero of $R_{2n}(z,1) - 1$.

REFERENCES

[1] O.Boyko, O.Martynyuk, V.Pivovarchik," On maximal multiplicity of eigenvalues of finite-dimensional spectral problem on a graph." Submitted to Methods of Functional Analysis and Topology.

[2] J. Genin, and J. S. Maybee, "Mechanical vibrations trees," J. Math. Anal. Appl. 45, 1974, pp 746–763.

[3] G. Gladwell," Inverse problems in vibration," Kluwer Academic Publishers, Dordrecht, 2004.

[4] G. Gladwell," Matrix inverse eigenvalue problems," In: G. Gladwell, A. Morassi, eds., Dynamical Inverse Problems: Theory and Applications. CISM Courses and Lectures 529, 2011, pp. 1–29.

[5] F.R.Gantmakher and M.G.Krein, " Oscillating matrices and kernels and vibrations of mechanical systems" (in Russian), GITTL, Moscow-Leningrad, 1950, German transl. Akademie Verlag, Berlin, 1960.

[6] V.A. Marchenko, " Introduction to the theory of inverse problems of spectral analysis" (in Russian), Acta, Kharkov, 2005.

[7] V. Pivovarchik, N. Rozhenko, C. Tretter, "Dirichlet-Neumann inverse spectral problem for a star graph of Stieltjes strings," Linear Algebra and Applications, Vol. 439, 2013, No.8, pp. 2263-2292.

[8] R. Qiao, A. Roberts, A. Mount, S. Klaine, P. C, Ke," Translocation of C60 and Its Derivatives Across a Lipid Bilayer," Nano Letters. Retrieved 4 September, 2010.

Модели обучения анализу сложности алгоритмов

Вадим Рублев
Кафедра теоретической информатики
Ярославский госуниверситет им. П.Г. Демидова
Ярославль, Россия
roublev@mail.ru

Мурад Юсуфов
Кафедра теоретической информатики
Ярославский госуниверситет им. П.Г. Демидова
Ярославль, Россия
flood4life@gmail.com

Algorithm complexity analysis teaching models

Vadim Rublev
Computer science department
Yaroslavl State University
Yaroslavl , Russia
roublev@mail.ru

Murad Yusufov
Computer science department
Yaroslavl State University
Yaroslavl , Russia
flood4life@gmail.com

***Аннотация*—Обучение студентов специальности "Фундаментальная информатика и информационные технологии" анализу вычислительной сложности алгоритмов сталкивается с трудностями недостаточного развития математического мышления, а потому требует индивидуального подхода для массы студентов. Проблема может быть решена с помощью компьютерной системы обучения, а потому требует построения управляющих моделей обучения. В основу построения такой системы положена дискретная модель таблицы символьной прокрутки с условиями последнего выполнения цикла и выхода из цикла, которые позволяют получить двусторонние оценки вычислительной сложности цикла или комбинации циклов. Применение компьютерной алгебры позволяет обучить студента приемам преобразования символьных выражений и получению асимптотических оценок, а также проконтролировать ход решения задач.**

Abstract—Teaching algorithm complexity analysis to students is often hindered by the lack of mathematical background in said students, therefore most students require a lot of individual training. This problem can be solved by introducing a computerised teaching system that in turn requires designing controlling teaching models. The core of such system is the discrete model of symbol scroll table that includes the last loop execution and loop break conditions. Those conditions can be used to estimate the computational complexity of one loop or a combination of loops. Usage of computer algebra enables teaching symbol expression transform and deriving asymptotic estimations methods to the students as well as controlling the problem solving steps.

***Ключевые слова*—сложность алгоритмов, обучение, таблица символьной прокрутки,условия выполнения цикла и выхода из цикла**

***Keywords*—algorithm complexity, teaching, symbol scroll table, last loop execution and loop break condition**

I. ВВЕДЕНИЕ

В процессе обучения студентов специальности "Фундаментальная информатика и информационные технологии" анализу вычислительной сложности алгоритмов возникают трудности, связанные с недостаточным развитием математического мышления у обучаемых. Эта проблема может быть решена с помощью компьютерной автоматизированной системы обучения (АСО). Для ее разработки необходимо построить управляющие модели обучения [1]- [3]. Эти модели можно разделить на 2 группы: модели анализа вычислительной сложности алгоритмов и модели обучения, подготавливающие студента к использованию моделей первой группы.

II. МОДЕЛИ АНАЛИЗА

A. Таблица символьной прокрутки

Целью АСО «Анализ сложности алгоритмов» является обучение студентов общим методам анализа сложности алгоритма. В заданиях используются любые комбинации вложенности и зависимости циклов, но система не рассчитана на итерации циклов любой сложности, хотя она разрабатывается с учетом возможности расширения в этой области.

Поскольку сложность алгоритма, содержащего циклы, определяется количеством выполнения этих циклов, то в основу методики получения оценок положено составление *символьной таблицы прокрутки алгоритма*. В этой таблице для каждой переменной алгоритма, кроме тех, от которых не зависят асимптотические оценки вычислительной сложности, отводится столбец, а также специальные столбцы:

— столбец с номером выполнения цикла (один столбец для каждого цикла) и символьным обозначением этого

номера при последнем выполнении цикла;
— столбец “Усл. ц.”, в котором записывается символьное условие выполнения цикла (с комментарием “п” для последнего выполнения и с комментарием “в” для выхода из цикла).

Вводится понятие “строк таблицы прокрутки”, связанных с выполнением цикла. Проверка условия выполнения цикла, которое отображается в столбце условия строки, является центральной. Если некоторые из параметров условия изменяются перед проверкой условия, то эти изменения отображаются в предыдущей строке или строке условия. Изменение тех параметров условия, которые имеют место после проверки условия, отображаются в строке следующей после проверки условия так же, как и изменение переменных тела цикла Таким образом, с выполнением условия может быть связано несколько строк, но только та из них, которая содержит проверку условия, помечается в столбце номера выполнения цикла. Если условие истинно, то совершается переход к следующему выполнению тела цикла, отображаемому в последующих строках. Рассмотрим пример 1 алгоритма с двумя невложенными, но зависимыми циклами:

```
void f (unsigned long n){
  float x = n, z = n;
  while (x > 2) { x = sqrt(x); z = z * z; }
  while (z / = 2 > 1);     }
```

Не все строки символьной прокрутки могут быть отображены в таблице. Рекомендуется обязательно отображать для цикла первые 2 строки выполнения тела цикла с номерами 1 и 2, строку последнего выполнения цикла с номером p<номер цикла>, строку выхода из цикла с номером p<номер цикла>+1.

Ниже приведена таблица символьной прокрутки этого алгоритма.

N_l	i_1	i_2	x	z	*Усл. ц.*	
			n	n		
1	1				$n > 2$	
	2		$n^{1/2}$	n^2	$x > 2$	
	3		$n^{(1/2)^2}$	n^{2^2}	$x > 2$	
	…		…	…	…	
	p_1		$n^{(1/2)^{p_1-1}}$	$n^{2^{p_1-1}}$	$x > 2$	*п*
	$p_1 + 1$		$n^{(1/2)^{p_1}}$	$n^{2^{p_1}}$	$x \not> 2$	*в*
2		1		$n^{2^{p_1}}/2$	$z > 1$	
		2		$n^{2^{p_1}}/2^2$	$z > 1$	
		…		…	…	
		p_2		$n^{2^{p_1}}/2^{p_2}$	$z > 1$	*п*
		$p_2 + 1$		$n^{2^{p_1}}/2^{p_2+1}$	$z \not> 1$	*в*

Рассмотрим теперь пример 2 алгоритма с двумя вложенными, но зависимыми циклами:

```
void f (unsigned long n){
  float x = n, z = n, y;
  while (x > 2) { x = sqrt(x); y = z = z * z;
    while (y / = 2 > 1); }    }
```

Ниже приведена таблица символьной прокрутки этого алгоритма. Процесс разработки учащимся таблицы символьной прокрутки требует контроля со стороны системы:

N	i	x	z	y	*Усл. ц.*
		n	n		
1	1				$x > 2$
		$n^{1/2}$	n^2	n^2	
2	1			$n^2/2$	$y > 1$
	2			$n^2/2^2$	$y > 1$
	…	…	…	…	…
	$p_2(1)$			$n^2/2^{p_2(1)}$	$y > 1$п
	$p_2(1) + 1$			$n^2/2^{p_2(1)+1}$	$y \not> 1$в
	…	…	…	…	…
1		$n^{(1/2)^{p_1-1}}$	$n^{2^{p_1-1}}$		
	p_1				$x > 2$п
		$n^{(1/2)^{p_1}}$	$n^{2^{p_1}}$	$n^{2^{p_1}}$	
2	1			$n^{2^{p_1}}/2$	$y > 1$
	2			$n^{2^{p_1}}/2^2$	$y > 1$
	…	…	…	…	…
	$p_2(p_1)$			$n^{2^{p_1}}/2^{p_2(p_1)}$	$y > 1$п
	$p_2(p_1) + 1$			$n^{2^{p_1}}/2^{p_2(p_1)+1}$	$y \not> 1$в
1	$p_1 + 1$				$x \not> 2$в

- во-первых, надо контролировать правильность последовательности занесения символьных значений в строки и их столбцы таблицы ;
- во-вторых, надо контролировать правильность преобразования символьного выражения при занесении в тот или иной столбец строки.

Для контроля правильности последовательности занесения символьных значений учащийся перед составлением таблицы символьной прокрутки разрабатывает на основании предложенного системой алгоритма пошаговое его описание. Это описание должно строго соответствовать порядку выполнения операторов алгоритма. Для каждого цикла сначала должны выполняться операторы, предшествующие проверке условия цикла, затем операторы самого условия, также предшествующие его выполнению (например, преинкрементные или предекрементные операции), затем оператор условия цикла и номер шага, идущего при невыполнении условия цикла, затем операторы условия цикла, последующие его проверке (например, постинкрементные или постедекрементные операции), и, наконец, операторы тела цикла (после последнего оператора тела цикла указывается номер шага следующего выполнения цикла). Номер шага stop означает конец выполнения алгоритма. Приведем пошаговое описания для примера 1.

1. x=n
2. z=n
3. x>2
4. x=$x^{1/2}$ 6
5. z=z*z 3
6. z/=2
7. z>1 stop
8. 7

Для контроля правильности преобразования вводится система элементарных алгебраических преобразований (см. [3], [4]), при которой указанное учащимся в интерфейсе преобразование выполняется для выделенных ввыражении операндов. Например, полученное в таблице примера 1 строки 2-го выполнения цикла 1 значение для столбца x $(n^{1/2})^{1/2}$ преобразуется выбором операции

умножения степеней в $n^{(1/2)^2}$.

Не всегда можно провести подобное упрощающее преобразование. Например, если параметр x целочисленный, а его итерация определяется оператором $x = 1.5 * x$, то его значение на первой итерации будет $[1.5 * x]$, но после второй итерации выражение значения $[1.5^2 * x]$ вместо $[1.5 * [1.5 * x]]$ является ошибочным. В этом случае можно ввести обозначение $x(i)$ для i-й итерации, положив $x(0) = x$ и $x(i) = [1.5 * x(i-1)]$ $(i > 0)$. При дальнейшем анализе условий цикла можно будет воспользоваться оценками сверху и снизу этого выражения для получения двусторонних оценок сложности цикла.

B. Анализ условий циклов и получение двусторонних оценок сложности циклов

Условия последнего выполнения цикла и выхода из цикла позволяют получить двусторонние оценки вычислительной сложности цикла или комбинации циклов. Для этого, в первую очередь, следует разделить в разных частях неравенства выражение с параметром количества p выполнений цикла (назовем его частью P) и выражение с параметрами алгоритма (назовем его частью N). Вслед за этим необходимо решить неравенство относительно p. Если сделать это трудно,то необходимо сначала выделить в каждой из частей ведущий аддитивный член (наиболее быстро растущий по параметру p в части P или по параметрам алгоритма в части N). Затем в меньшей части (предшествует знаку $<$ или $\leq$) отбросить все аддитивные члены со знаком "+", а остальные оценить сверху через долю ведущего аддитивного члена. В другой части – отбросить все аддитивные члены со знаком "–", а остальные оценить через ведущий аддитивный член.

Рассмотрим анализ условий примера 1.

Для цикла 1 условие последнего выполнения цикла $n^{(1/2)^{p_1-1}} > 2$ для разделения выражений от p и n преобразуем в неравенство $p_1 < \log_2 \log_2 n + 1$, а условие выхода из цикла $n^{(1/2)^{p_1}} \leq 2$ преобразуем в неравенство $\log_2 \log_2 n \leq p_1$. Учитывая целочисленность параметра p_1 получаем точное значение $p_1 = \lceil \log_2 \log_2 n \rceil$, что дает оценку вычислительной сложности цикла 1: $p_1 = \theta(\log \log n)$.

Для цикла 2 условие последнего выполнения цикла $n^{2^{p_1}}/2^{p_2} > 1$ преобразуем в неравенство $p_2 < 2\log_2^2 n$, а условие выхода из цикла 2 $n^{2^{p_1}}/2^{p_2+1} \leq 1$ дает $\log_2^2 n - 1 \leq p_2$, что вместе дает оценку вычислительной сложности цикла 2: $p_2 = \theta(\log^2 n)$. По наибольшей сложности циклов эта оценка также является оценкой вычислительной сложности алгоритма примера 1.

Рассмотрим теперь анализ условий примера 2.

Цикл 1 примера 2 отличается от цикла 1 примера 1 лишь тем, что тело цикла содержит вызов внутреннего цикла, и так как параметр x изменяется точно также и условие такое же, то вычислительная сложность цикла 1 примера 2 также определяется оценкой $p_1 = \theta(\log \log n)$.

Для определения вычислительной сложности алгоритма примера 2 необходимо определить общее количество выполнения вложенного цикла 2 при всех выполнениях цикла 1: $\sum_{i=1}^{p_1} p_2(i)$. Определим количество $p_2(i)$ выполнения цикла 2 при i-м выполнении цикла 1. Из условия последнего выполнения этого цикла $n^{2^i}/2^{p_2(i)} > 1$ следует неравенство $p_2(i) < 2^i \log_2 n$, а из условия выхода этого цикла $n^{2^i}/2^{p_2(i)+1} \leq 1$ вытекает неравенство $2^i \log_2 n - 1 \leq p_2(i)$, что, учитывая целочисленность параметра $p_2(i)$, дает его значение $2^i\lceil \log_2 n \rceil - 1$. Суммируя общее выполнение, получаем для верхней оценки суммы $\log_2 n \sum_{i=1}^{p_1} 2^i = 2^{p_1+1} \log_2 n < 2\log_2^2 n$ и для нижней оценки суммы $\log_2 n \sum_{i=1}^{p_1} 2^i - p_1 > \log_2^2 n$, что дает оценку суммарной сложности вложенного цикла 2 $\sum_{i=1}^{p_1} p_2(i) = \theta(\log^2 n)$. Это является и оценкой сложности алгоритма примера 2.

Набор элементарных преобразований компьютерной алгебры, используемый при построении таблицы символьной прокрутки, пополняется преобразованиями для неравенств анализа условий циклов, а также методами усиления оценок. Обучаемый выбирает то или иное элементарное преобразование и выполняет его, а система контролирует правильность выполнения.

При анализе вложенных зависимых циклов необходимо анализировать дискретные суммы выражений, связанных с общим количеством выполнения вложенного цикла. В примере 2 при суммировании использована формула суммы геометрической прогрессии. В случае более сложных сумм (чем арифметические или геометрические прогрессии) можно использовать формулу Эйлера-Маклорина (см. [5]), определяя асимптотику суммы интегралом. Но, во-первых, эта формула требует, чтобы функция суммирования была достаточно гладкой (что не всегда верно), а, во-вторых, она оказывается бесполезной в тех случаях, когда сумма растет настолько быстро, что соответствующий интеграл не является элементарной функцией. В этих случаях сравнительно просто ([1], [2]) выводятся двусторонние оценки скорости роста суммы негладкой функции через интеграл в первом случае, а во втором случае – через верхний предел суммирования. При необходимости эти свойства также используются для получения оценок вычислительной сложности циклов.

III. МОДЕЛИ ОБУЧЕНИЯ

Модели обучения основаны на разбиении изучаемого материала на порции (секции, темы) и контроля усвоения материала порций в виде тестов или упражнений (*тестов-упражнений*). Поскольку для полного усвоения материала обучение должно быть адаптивным, то в начале работы с каждой темой студент получает начальное количество тестов-упражнений, и если он выполняет их безошибочно, то переходит к работе со следующей темой.

Если он делает первую ошибку, то дается одна возможность ее исправить, и если ему это удается, то прежнее количество тестов или упражнений остается неизменным. Если же студент делает повторную ошибку в том же тесте-упражнении, то оно снимается с выполнения и прежнее количество тестов-упражнений для выполнения увеличивается. Тем самым студент стимулируется на внимательное изучение материала. Если же он после внимательного изучения материала выполняет безошибочно 2 или более тестов-упражнений, то остав-

шееся их количество для выполнения снижается прогрессивным образом, что также стимулирует студента.

В каждом тесте на вопрос предлагается несколько высказываний-ответов, но среди них правильными могут быть 1 или несколько высказываний-ответов, либо все высказывания-ответы, либо ни одного. Успешным считается лишь такой ответ, при котором указаны все правильные высказывания-ответы. Это направлено на углубленное изучение материала учащимся. Для того, чтобы наборы ответов не повторялись у разных обучаемых в группе, для каждого теста создается банк высказываний-ответов, из которого случайным образом выбираются высказывания-ответы при тестировании. При размере банка 20 и выборе 6 высказываний-ответов вероятность повторения будет меньше 10^{-6}.

IV. ЗАКЛЮЧЕНИЕ

Рассмотренные модели позволяют перейти к построению АСО «Анализ сложности алгоритмов».

ЛИТЕРАТУРА

[1] Rublev V.S., Ermilova A.V. “On Some Results in Computational Complexity Analysis of Integer Relation Algorithms,” 2 nd International on Computer Algebra and Information Technologies, August 21-26, 2016 Odessa, Ukraine. Abstract / Mechnikov Odessa National University. Odessa : TES, 2016. p.12 (ISBN 978 - 7337 - 43 - 9)

[2] Рублев В. С., Юсуфов М. Т. “Автоматизированная система для обучения анализу вычислительной сложности алгоритмов,” Международный научный журнал Современные информационные технологии и ИТ-образование. 2016. Т. 12, №1. С. 135–145.

[3] Рублев В. С., Юсуфов М. Т. “Автоматизированная обучающая система «Анализ вычислительной сложности алгоритмов» (исследование организации 1-ой части проекта),” Международный научный журнал Современные информационные технологии и ИТ-образование. 2017. Т. 13, № 2. С. 170–178

[4] Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра: символьные и алгебраические вычисления / Пер. с англ. - М.: Мир, 1991.

[5] Estrada R., Kanwal R. P. A distributional approach to asymptotics theory and applications, 2ed., Birkhauser, 2002. 463 p.

REFERENCES

[1] Rublev V.S., Ermilova A.V. “On Some Results in Computational Complexity Analysis of Integer Relation Algorithms,” 2 nd International on Computer Algebra and Information Technologies, August 21-26, 2016 Odessa, Ukraine. Abstract / Mechnikov Odessa National University. Odessa : TES, 2016. p.12 (ISBN 978 - 7337 - 43 - 9)

[2] Rublev V.S., Yusufov M. T. Automated system for teaching computational complexity of algoritm course, Convergent Cognitive Information Technologies (Selected Papers of the First International Sientific Conference Convergent Cognitive) Moscow, Russia, November 25-26, 2016 (http://ceur-ws.org/Vol-1763/). (ISSN 1613-0073 VOL-1763 urn.nbn.de: 0074-1763-4)

[3] Rublev V.S., Yusufov M. T., Development of the first part of the automated system for teaching computational complexity of algorithms course, International Scientific Journal “Modern Information Technologies and IT Education”. 2017. V. 13, № 2. pp. 170–178

[4] Davenport J.H., Siret Y., Tournier E. Computer algebra: systems and algorithms for algebraic computation / - Academic Press, 1988. ISBN 978-0-12-204230-0

[5] Estrada R., Kanwal R. P. A distributional approach to asymptotics theory and applications, 2ed., Birkhauser, 2002. 463 p.

About Riezs means for the coefficients of hybrid symmetric square L-functions

Olga Savastru
Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
Odessa, Ukraine
savolga777@gmail.com

***Abstract*—Let $f(z)=\sum_{n=1}^{\infty}a_f(n)e^{2\pi inz}$ be a holomorphic cusp form of even weight $k\geqslant 12$ for the full modular group $SL(2,\mathbb{Z})$, $z\in H$, $H=\{z\in\mathbb{C}|Im(z)>0\}$ is the upper half plane. We suppose that $f(z)$ is a normalized eigenfunction for the Hecke operators $T(n)(n\geqslant 1)$ with $a_f(1)=1$. We study the error term in asymptotic formula for the coefficients of hybrid symmetric square L-functions associated with f. The Voronoi type formulas for coefficients, both of the infinite series type and of the truncated type, are proved. Some other related topics are also discussed.**

***Index Terms*—holomorphic cusp forms, symmetric square L-function, functional equation, Riesz means, Voronoi type formulas**

I. Introduction

Let $f(z)=\sum_{n=1}^{\infty}a_f(n)e^{2\pi inz}$ be a holomorphic cusp form of even weight $k\geqslant 12$ for the full modular group $SL(2,\mathbb{Z})$, $z\in H$, $H=\{z\in\mathbb{C}|Im(z)>0\}$ is the upper half plane. We suppose that $f(z)$ is a normalized eigenfunction for the Hecke operators $T(n)(n\geqslant 1)$ with $a_f(1)=1$. In this case, $f(z)$ has the Fourier expansion

$$f(z)=\sum_{n=1}^{\infty}\lambda_f(n)e^{2\pi inz},$$

where

$$\lambda_f(n)=\frac{a_f(n)}{n^{\frac{k-1}{2}}},\ T(n)f=\lambda_f(n)f$$

for every $n\in\mathbb{N}$.

The Fourier coefficients of f are known to be real.

In 1974 Deligne [1] proved

$$|\lambda_f(n)|\leqslant\tau(n),$$

where $\tau(n)$ is the number of positive divisors of n. For prime p we have

$$\lambda_f(p)=\alpha_p+\overline{\alpha_p},\quad \alpha_p\cdot\overline{\alpha_p}=1.$$

The existence of α_p is implied by Deligne's result [1].

The problem of studying of coefficients $\lambda_f(n)$ on special sequences was considered by various authors. Hafner J. L., Ivić A. [4] obtained on O-estimate and $\Omega_{\pm}$-results for

$$\sum_{n}\lambda_f(n).$$

Rankin [8]- [9], Selberg [10] investigated the second moment

$$\sum_{n\leqslant x}|\lambda_f(n)|^2.$$

Rankin considered higher moments

$$\sum_{n\leqslant x}\lambda_f(n)^{2\beta},$$

where $0<\beta<1$ and $\beta>1$.

In 2011 Lau Y. K., Lü G. S., Wu J. [7] obtained estimates for

$$\sum_{n\leqslant x}\lambda_f(n)^j,$$

where $3\leqslant j\leqslant 8$.

Results for the sums $\sum_{n\leqslant x}\lambda_f(n^2)$ and $\sum_{n\leqslant x}\lambda_f^2(n^j)$, where $j=2,3,4$, can be found in [5]- [6].

The Hecke L-function attached to f is defined as

$$L(s,f)=\sum_{n=1}^{\infty}\frac{\lambda_f(n)}{n^s}$$

for $\Re s>1$. $L(s,f)$ is absolutely convergent in a certain half-plane and is continuable analytically to an entire function on the whole plane.

In [11], Shimura introduced the function $L(s,sym^2f,\chi)$. For an arbitrary primitive Dirichlet character χ mod d, the symmetric square L-function attached to f is defined as the following Euler product:

$$L(s,sym^2f,\chi):=\prod_p(1-\alpha_f^2(p)\chi(p)p^{-s})(1-\chi(p)p^{-s})^{-1}\times(1-\overline{\alpha}_f^2(p)\chi(p)p^{-s})$$

for $\Re s>1$.

We have

$$L(s,sym^2f,\chi)=L(2s,\chi^2)\sum_{n=1}^{\infty}\frac{\lambda_f(n)^2\chi(n)}{n^s}:=\sum_{n=1}^{\infty}\frac{c_n\chi(n)}{n^s},$$

where $L(2s,\chi^2)$ is the Dirichlet L-function associated with χ^2.

In this paper we investigate the distribution of coefficients of hybrid symmetric square L-function, consider the Riezs means for coefficients of $L(s,sym^2f,\chi)$. The Voronoi type formulas, both of the infinite series type and of the truncated type, are proved. Voronoi type formulas allow one to consider exponential sums connected with the $c_n\chi(n)$, can be used for evaluation of corresponding

sum over arithmetic progressions. Fomenko [2] investigated sum of coefficients of symmetric square L-function associated with a cusp form and a trivial character.

II. Auxiliary statements

In this section, we introduce some facts about hybrid symmetric square L-function.

Let χ be a primitive Dirichlet character χ mod d. The function $L(s, sym^2 f, \chi)$ is entire and satisfies the following functional equation:

$$\Lambda(s, sym^2 f, \chi) = C_\chi \Lambda(1-s, sym^2 f, \bar{\chi}),$$

where

$$\Lambda(s, sym^2 f, \chi) = \left(\frac{\pi}{d}\right)^{-\frac{3s}{2}} \Gamma\left(\frac{s}{2}+\frac{1}{2}\right)$$
$$\times\Gamma\left(\frac{s}{2}+\frac{k-1}{2}\right)\Gamma\left(\frac{s}{2}+\frac{k}{2}\right) L(s, sym^2 f, \chi)$$

and C_χ is a constant depending on χ with $|D_\chi| = 1$. Particularly, when χ is a primitive character with odd prime modulus p, $C_\chi = \frac{W(\chi)^3}{p^{\frac{3}{2}}}$ with the Gauss sum $W(\chi)$.

Lemma 1. *Let p be an odd prime and $b \in \mathbb{N}$, $(b,p)=1$. Then we have*

$$\sum_{\chi \mod p} C_\chi \chi(b) \ll \varphi(p) p^{-\frac{1}{2}},$$

where the sum running over primitive characters mod p.

From the Phragmen-Lindelof principle and functional equation, we obtain

Lemma 2.

$$L(\sigma+it, sym^2 f, \chi) \ll (d|t|+1)^{\frac{3}{2}(1-\sigma+\epsilon)}$$

uniformly for $-\epsilon \le \sigma \le 1+\epsilon$, $|t| > 10$.

Throughout this paper, ϵ is an arbitrarily small positive constant.

III. Voronoi type formulas

When χ is a primitive character, we define the Riesz mean of the coefficients of the hybrid symmetric square L-function as follows:

$$D_\rho(x, sym^2 f, \chi) = \Gamma(\rho+1)^{-1} \sum_{n \leqslant x}{}' c_n \chi(n))(x-n)^\rho,$$

where $x \ge 1$ and $\rho \ge 0$ is a real number. $\sum'$ means that if $\rho = 0$ and x is an integer, then in the sum c_x is replaced by $\frac{1}{2}c_x$.

Hafner [3] obtained the Voronoi for the Riesz mean of general L-functions with functional equations. The following Voronoi formula is obtained by applying his result to $D_\varrho(x, sym^2 f, \chi)$. In accordance with [3], we represent the Riesz mean as follows:

$$D_\rho(x, sym^2 f, \chi) = \frac{L_\rho(0, sym^2 f, \chi)}{\Gamma(\rho+1)} x^\rho + \Delta_\rho(x, sym^2 f, \chi).$$

For $\rho = 0$, we have

$$\sum_{n \leqslant x}{}' c_n \chi(n)) = L_\rho(0, sym^2 f, \chi) + \Delta_0(x, sym^2 f, \chi).$$

We can apply Theorem A, Theorem B of [3] to the function $L(s, sym^2 f, \chi)$ with (in Hafner's notation)

$$a(n) = b(n) = c_n \chi(n),\ \lambda_n = \mu_n = (\frac{\pi}{d})^{\frac{3}{2}} n,$$

$$\varphi(s) = \psi(s) = (\frac{\pi}{d})^{-\frac{3}{2}s} L(s, sym^2 f, \chi),$$

$$\Delta(s) = \Gamma\left(\frac{s}{2}+\frac{1}{2}\right)\Gamma\left(\frac{s}{2}+\frac{k-1}{2}\right)\Gamma\left(\frac{s}{2}+\frac{k}{2}\right),$$

$$\sigma_a = \sigma_a^\star = 1,\ N = 3,\ \alpha_1 = \alpha_2 = \alpha_3 = \frac{1}{2},$$

$$\alpha = \frac{3}{2},\ r = 1,\ \beta_1 = \frac{1}{2}, \beta_2 = \frac{k-1}{2}, \beta_3 = \frac{k}{2},$$

$$a = -\frac{1}{3},\ h = 6,\ \theta_\rho = \frac{2}{3}r + \frac{1}{3}.$$

We have

$$\Delta_\rho(x, sym^2 f, \chi)$$
$$= \left(\frac{\pi}{d}\right)^{\frac{3}{2}(2\rho+1)} \sum_{n=1}^{\infty} \frac{C_\chi c_n \bar{\chi}(n)}{n^{1+\rho}} f_\rho\left(\left(\frac{\pi}{d}\right)^3 nx\right)$$

for $x > 0$, where the infinite series on the right-hand side converges for $\rho > 0$ uniformly on any finite closed x-interval.

$$f_\rho(y) = \frac{1}{2\pi i}\int_L \frac{\Gamma(1-s)\Delta(s)}{\Gamma(2+\rho-s)\Delta(1-s)} y^{1+\rho-s} ds$$

$$= \frac{1}{2\pi i}\int_L \frac{\Gamma(1-s)\Gamma(\frac{s+1}{2})\Gamma(\frac{s+k-1}{2})\Gamma(\frac{s+k}{2})}{\Gamma(2+\rho-s)\Gamma(\frac{-s}{2})\Gamma(\frac{-s+k+1}{2})\Gamma(\frac{-s+k}{2})} y^{1+\rho-s} ds$$

for $y > 0$. Here L is the oriented polygonal path with vertices $a - i\infty, a - iT, b - iT, b + iT, a + iT$ and $a + i\infty$ (in that order), where b and T are real numbers satisfying $b > k$, $T > k$, and b is not an integer.

Moreover we have

$$\frac{d}{dx} f_{\rho+1}(x) = f_{\rho+1}(x)$$

and

$$f_\rho(y) = 2^\rho (3\pi)^{-\frac{1}{2}} y^{\frac{2}{3}\rho+\frac{1}{3}} cos(6y^{\frac{1}{3}} - \frac{\pi}{2}\rho) + O(y^{\frac{2}{3}\rho}) + O(y^{1+\rho-b}),$$

where $b > k$, $\rho \ge 0$ and the last term does not appear when $b > \rho + 1$ and ρ is not an integer.

Now we present the truncated Voronoi formula for $\Delta_\rho(x, sym^2 f, \chi)$.

Theorem. *Let $x > 1$, $0 \le \rho \le 1$, $N \ge d^3$ and we assume N is large enough compared with k and ρ. Then we have the following truncated Voronoi formula:*

$$\Delta_\rho(x, sym^2 f, \chi)$$
$$= C_\chi d^{\rho+\frac{1}{2}} 2^\rho \pi^{-\rho-1} 3^{-\frac{1}{2}} x^{\frac{2}{3}\rho+\frac{1}{3}} \sum_{n \le N} \frac{c_n \bar{\chi}(n)}{n^{\frac{1}{3}\rho+\frac{2}{3}}} \cos(6y^{\frac{1}{3}} - \frac{\pi}{2}\rho)$$
$$+O(x^{\frac{4\rho+1}{6}} d^{\rho+1} N^{\frac{1-2\rho}{6}+\epsilon}) + O(x^{\frac{2(1+\rho)}{3}+\epsilon} d^{1+\rho+\epsilon} N^{-\frac{1+\rho}{3}+\epsilon}),$$
$$+O(x^{\frac{1+2\rho}{3}} d^{\rho+\frac{1}{2}} N^{\frac{1-\rho}{3}+\epsilon}) + O(x^\rho d^{\frac{3}{2}}),$$

where the last term does not appear when $\frac{d^3}{6\pi^3 x} < 1$.

REFERENCES

[1] P. Deligne, "La Conjecture de Weil," Inst. Hautes Etudes Sci. Pul. Math., 43 (1974), pp. 29-39.

[2] O. M. Fomenko, "The behavior of Riesz means of the coefficients of a symmetric square L-function," Journal of Mathematical Sciences, 143 (2007), no. 3, pp. 3174–3181.

[3] J. L. Hafner, "On the representation of the summatory functions of a class of arithmetical functions," In Analytic Number Theory. M. I. Knopp (ed.), Lecture Note in Math.,vol. 899, (Springer-Verlag, 1981), pp. 148-165.

[4] J. Hafner , A. Ivić, "On sums of Fourier coefficients of cusp forms," Enseign. Math. 35 (1989), no. 3-4, pp. 375-382.

[5] H. X. Lao, A. Sankaranarayanan,"The average behavior of Fourier coefficients of cusp forms over sparse sequences," Proc. Amer. Math. Soc., 137 (2009), no. 8, pp. 2557-2565.

[6] H. X. Lao , H. Wei," Ω – result on coefficients of automorphic L–functions over sparse sequences," J. Korean Math. Soc., 52(2015), no. 5, pp. 945-954.

[7] Y. K. Lau , G. S.Lü, J. Wu, "Integral power sums of Hecke eigenvalues ," Acta Arith., 150 (2011), no. 2, pp. 193-207.

[8] R. A. Rankin," An Ω–result for the coefficients of cusp forms ,"Math. Ann.,203 (1973),pp. 239-250.

[9] R. A. Rankin,"Sums of powers of cusp form coefficients II," Math. Ann., 272 (1985), no. 4,pp. 593-600.

[10] A. Selberg ," Bemerkungen über eine Dirichletsche Reihe, die mit der Theorie der Modulformen nahe verbunden ist," Arch. Math. Naturvid, 43 (1940), pp. 47-50.

[11] G. Shimura, "On the holomorphy of certain Dirichlet series", Proc.London Math. Soc., 31 (1975), pp. 79-98.

Melody harmonization with form development in procedural music

Komarov O.V.
Information Systems Department
Odessa National Polytechnic University
Odessa, Ukraine
o.w.komarow@gmail.com

Boltenkov V.O.
Information Systems Department
Odessa National Polytechnic University
Odessa, Ukraine
vaboltenkov@gmail.com

***Abstract*—An importance of musical form development in procedural generated music has been argued. The repetition principle as an approach of form development introduced. A proposed improvement of genetic harmonization method has been described as multi-objective optimization problem using contextual genetic algorithms. It allows to harmonize similar melody sequences with similar accompaniment, and improve listener's perception.**

***Index Terms*—procedural music, harmonization, genetic algorithm, multi-objective optimization**

I. Introduction

Methods of procedural content generation, music in particular, are actively developing and applying at the present time [1]. Music generation process can be divided into few consecutive steps, one of which is the harmonization of the melody. For the automatic melody harmonization, a genetic method was proposed [2], which allows to achieve high harmoniousness values. However, this method suffers from a lack of a holistic vision of the harmonized composition, which makes it impossible for purposeful musical form development. At the same time, the form of composition is one of the most important factors of music perception [3], and its weak expression significantly reduces the quality of the generated music. To solve this problem, we propose a genetic method using the principle of repetition, which will allows to reproduce in the accompaniment a musical form stated in a melody.

II. Main part

To understand and recongize the music composition, the listener memorizes and compares similar and often repeating complexes of sounds. The most simple, accessible and reliable means of musical form development is the repeated movement or carrying out of the same musical material twice or several times [3]. The harmonization process itself is not responsible for the development of the musical form, but it makes it's own contribution, supporting the form stated in the melody. Following the principle of repetition [3], the repeated complexes of the melody sounds should be harmonized by repeated complexes of accompaniment (Fig.1).

To do this, a harmonization plan should be created, and then harmonization should be performed due to it.

A. Harmonization plan

At first, a melody should be represented as a character string, where each character represent only the pitch of each note, while durations are omitted. The pitch of the note has only 87 possible semitone values, therefore the usual byte character format is suitable for representation.

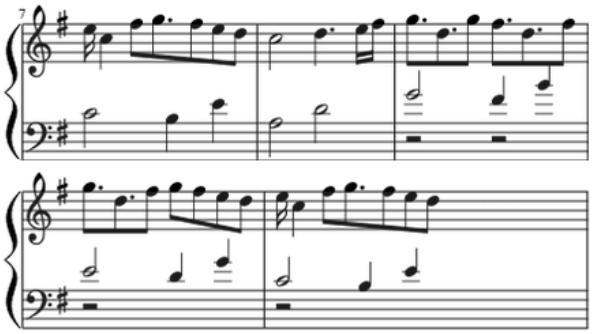


Figure 1. Melody and accompaniment repetition in first and last bars in My Chemical Romance - Welcome To The Black Parade

Then duplicate substrings of length n or longer must be found in the melody string. This can be done by constructing a suffix tree, counting the number of passes through each vertex [4].

The construction of a suffix tree allows to form a set of repetitions along with the number of occurrences in a string. The required set must exclude intersecting substrings. If a certain substring B includes a substring A, and substring A occurs more often than a substring B, then it is assumed that A splits B into independent substrings: B1 and B2 (excluding A itself between them). Each of these substrings is included in the set of repetitions, if it is not shorter than n (Fig.2).

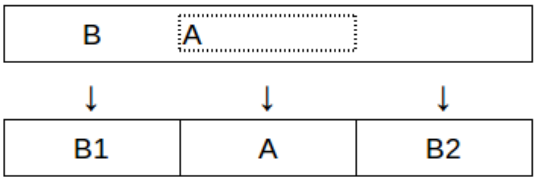


Figure 2. Replacing string B with strings B1 and B2.

After that original melody string must be divided into disjoint regions, highlighting the found substrings on it. The areas of repeating substrings are identified with labels A, B,... and free areas with labels U1, U2,... (Fig.3).

The resulting structure forms a mock-up of the future composition.

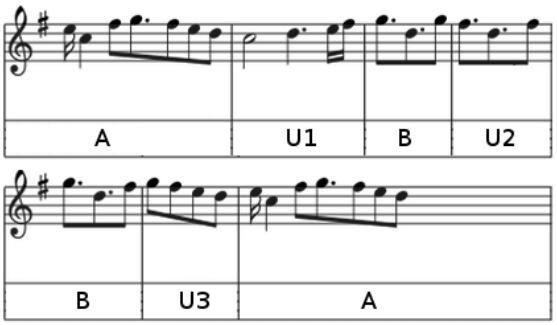


Figure 3. An example of division on form developing areas

B. Context Harmonization

Each area should be harmonized separately, sequentially, in the context of already harmonized neighboring areas. This can be done using a contextual genetic algorithm.

We call a contextual genetic algorithm a genetic algorithm in which each phenotype is evaluated only after concatenation on the left and right with a certain constant values called a context. If several contexts are specified, fitness function is used for each concatenation separately. In this case each phenotype gets a multiple ratings, and the problem can be considered as a multi-objective optimization problem, where each goal is characterized by evaluation in a separate contextes (Fig.4). After that any appropriate method for genetic multi-objective optimization can be used, for example, niched Pareto genetic algorithm [5].

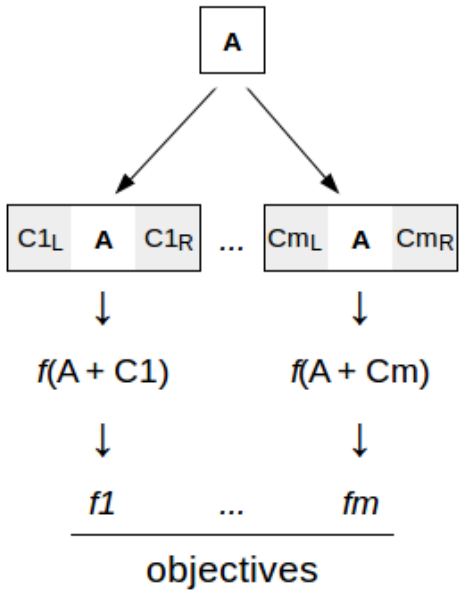


Figure 4. Fitness eveluations f1,..., fm of A in contextes C1,..., Cm

Harmonizing the area, it is necessary to take into consideration all the contexts in which the harmonized block turns out to be. Harmonization of a melody is a combinatorial problem [6]. Performing it takes significant time, especially when it includes multi-objective optimization. Therefore it is important to determine the queue of block processing.

Contexts of harmonization process are already harmonized blocks, adjusted to the current harmonizing block. The first block in the queue always has an empty context. U-blocks always have only one context.

For other blocks, the number of contexts increases depending on the number of occurrences of the block in the string and the number of blocks that are harmonized to this moment. In order to minimize the number of contexts, harmonization should be carried out in order of decreasing the number of occurrences in the composition.

C. Interval sequences

Often repetitions may occur not in absolute pitch sequences, but in relations between pitches of notes.

The difference between the two heights in the musical theory is usually called the interval. A melody can be represented as the sequence of intervals, the differences between neighboring notes. In this case, we can apply the principle of repetition in a stronger form - repeated interval sequences should be harmonized in the same way (Fig.5).

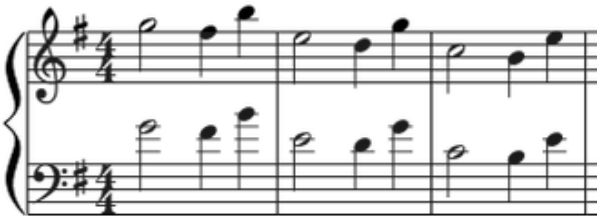


Figure 5. Three different interval repetitions in My Chemical Romance - Welcome To The Black Parade

In order to harmonize the repeated interval sequences similarly, it is necessary that the genotype of the individual in the genetic algorithm should be encoded in intervals. Absolute pitch values will be restored for the phenotype evaluation by shifting to a certain pitch.

This raises an additional problem. Some combinations of sounds after the pitch shift acquire a different harmonic value. Some combinations of such sounds are desirable, some are forbidden by rules of harmony.

In spite of the number of semitones in the scale and the number of possible repetitions of a given sequence, the number of significantly different shifts is limited to 12. This is due to the fact that the octave shift is completely harmonicaly safe, and the octave consists of 12 semitones. However, these 12 different options are worth considering, and should be harmonically evaluated in each case - separately.

First, the melody turns into an interval sequence, after which the repeated sequences are searched for by the suffix tree. Further, for each such sequence, the pitch of the first note of the sequence in specific occurency is considered as a pitch shift for this occurency. Among them, pitches that differ by a multiple of 12 are considered equivalent.

However, existence of inequivalent shifts leads to the problem of multi-objective optimization. Since we already used multi-objective optimization for context harmonization, we should combine goals of each process.

A combination of context and pitch shift will be called a harmonic situation. Each occurency of repetition in melody has its own pitch shift and context (even if context is empty).

Common process of harmonization in multiple situations can be described as follows (Fig.6). At first, identical harmonic situations should be removed from a set of optimization goals. A genotypes of genetic algorithm should be made as a sequence of intervals. We should evaluate genotype for each situation. Before each evaluation we form a phenotype due to harmonic situation's pitch shift. Then, the result concatenates with the context of situation. And after that, it is evaluated by fitness function. Evaluations in different situations are estimates of each objective.

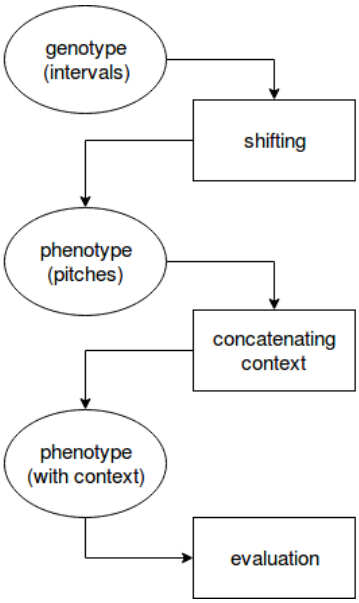


Figure 6. Genotype evaluation in harmonic solution

Conclusions

The proposed method improves musical form development in procedural generated music. This improves the listener's perception of harmonized compositions.

Proposed method can be used for repetitions both in absolute pitches and interval sequences. Method gives better harmoniousness values on abosolute pitches, however interval processing provides stronger musical forms.

References

[1] M.Hendrikx, S.Meijer, J.V.D.Velden, and A.Iosup, "Procedural content generation for games: A survey" ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 9, pp. 1-22, February 2013.

[2] S.Phon-Amnuaisuk, A.Tuson, and G.Wiggins, "Evolving Musical Harmonisation" in Artificial Neural Nets and Genetic Algorithms: Proceedings of the International Conference in Portorož, Slovenia. Vienna: Springer, 1999. pp. 229-234.

[3] B.V.Asaf'ev, "Music form as a process", Saint Petersburg, Russia: Musica, 1971 (in Russian).

[4] R.Koschke, R.Falke, and P.Frenzel "Clone Detection Using Abstract Syntax Suffix Trees" in WCRE '06 Proceedings of the 13th Working Conference on Reverse Engineering, Benevento, Italy. Washington: IEEE, 2006. pp. 253-262.

[5] J. Horn, N. Nafpliotis, and D. E. Goldberg "A niched Pareto genetic algorithm for multiobjective optimization" in Proceedings of the First IEEE Conference on Evolutionary Computation. IEEE World Congress on Computational Intelligence, Orlando, FL, USA. Washington: IEEE, 1994. pp. 82-87.

[6] F. Pachet, P. Roy. "Musical Harmonization with Constraints: A Survey", Constraints, vol. 6, pp. 7-19, January 2001.

Оберенена спектральна задача для стільтьєсівської струни з вільно ковзаючим кінцем

Ольга Мартинюк
Кафедра вищої математики та статистики
Південноукраїнський національний педагогічний
університет імені К. Д. Ушинського
Одеса, Україна
martynyuk.olga@gmail.com

Ольга Яковлєва
Кафедра вищої математики та статистики
Південноукраїнський національний педагогічний
університет імені К. Д. Ушинського
Одеса, Україна
olganik6505@gmail.com

Inverse spectral problem for Stieltjes string with freely sliding end

Olga Martynyuk
Department of Mathematics and Statistics
Southern Ukrainian National Pedagogical
University named K. D. Ushinsky
Одеса, Україна
martynyuk.olga@gmail.com

Ольга Яковлєва
Department of Mathematics and Statistics
Southern Ukrainian National Pedagogical University
named K. D. Ushinsky
Одеса, Україна
olganik6505@gmail.com

***Анотація*—У роботі розглядаються малі поперечні коливання струни Стільтьеса скінченої довжини з вільно ковзаючим лівим кінцем без тертя, правий кінець якої або закріплений, або вільно ковзає в напрямку, перпендикулярному до рівноважного положення струни. У першому випадку ми маємо задачу Неймана-Діріхле, а в другому - задачу Неймана-Неймана. Для зазначеної струни розглядаються прямі і обернена задачі. Остання є дискретним аналогом оберненої задачі, породженої рівнянням Штурма-Ліувілля, в якій два спектра крайових задач зі змішаними крайовими умовами однозначно визначають потенціал рівняння Штурма-Ліувілля. Розв'язок оберненої задачі полягає в тому, що необхідно знайти величини зосереджених мас і довжини часткових інтервалів стільтьєсівської струни за відомими частотами коливань струни при її закріпленому правом кінці і частотам коливань струни при вільному русі без тертя її правого кінця. У роботі отримано необхідну і достатню умову розв'язання даної задачі: строге чергування коренів характеристичних многочленів задач Неймана-Діріхле і Неймана-Неймана. Також використовується розклад S-функції, яка є відношенням цих многочленів, у ланцюговий дріб Стільтьєса, коефіцієнти якої і будуть шуканими величинами.**

***Ключові слова*—Стільтьєсівська струна, крайові умови Діріхле, Неймана, S-функція, спектр, власні значення**

***Abstract*—In this paper small transverse vibrations of a Stieltjes string of finite length with free sliding left end without damping and with the right end fixed or free to move in the direction orthogonal to the equilibrium position of the string are considered. In the first case we face the Neumann-Dirichlet problem, in the second case the Neumann-Neumann problem. Direct and inverse problems for such a string are considered. The last problem is a discrete analogue of the inverse problem generated by the Sturm-Liouville equation, where two spectra of boundary value problems with mixed boundary conditions uniquely determine the potential of the Sturm-Liouville equation. The solution of the inverse problem lies in finding the values of the point masses and lengths of the subintervals by known frequencies of the string vibrations with the right end free and known frequencies of the string vibrations with the right end fixed. In this paper a necessary and sufficient condition for solvability of this problem is obtained which is the strict alternation of the roots of the characteristic polynomials of the Neumann-Dirichlet and Neumann-Neumann problem. The decomposition of the S–function which is the ratio of these polynomials into a continued fraction is also used.**

***Index Terms*—Stieltjes string, Dirichlet, Neuman boundary conditions, S-function, spectrum, eigenvalues**

Відомо, що стільтьєсівською струною М. Г. Крейн (див. [2]) назвав пружну невагому ідеально гнучку нитку, яка несе на собі зосереджені маси, що можуть накопичуватися до одного з її кінців. Ми розглядаємо випадок скінченої кількості зосередженних мас.

Розглянемо струну Стільтьєса довжини l, яка натягнута між своїми закріпленими кінцями з силою натягу струни, що дорівнює 1, і містить n зосереджених мас. Позначимо через $m_1, m_2, ..., m_n$ величини зосереджених мас і через $l_0, l_1, ..., l_n$ величини часткових послі-

довних інтервалів, на які струна в положенні рівноваги розділяється зосередженими масами. Лівий кінець стільтьєсівської струни є вільно ковзаючим без тертя, правий її кінець закріплений або вільно ковзає без тертя.

Коливання такої системи можна охарактеризувати за допомогою малих поперечних зміщень зосереджених мас $V_k(t)$ у момент часу t (ми не враховуємо зміщення в напрямі лінії рівноваги струни). Зауважимо також, що при гармонічних коливаннях струни Стільтьєса з найменшою частотою струна прогинається всіма своїми частинами одночасно або в одну, або в іншу сторону; при гармонічних коливаннях, які видають k–ий обертон, стільтьєсівська струна має $k-1$ нерухомих вузлів [2]. Це твердження відповідає класичній теоремі Штурма.

Зазначимо, що аналогічні рівняння виникають при розгляді вільних коливань механічної системи, яка складається з n зосереджених мас $\{m_i\}_{i=1}^n$, вертикально підвішених між двома нерухомими опорами так, що кожна маса m_i з'єднана з найближчими сусідніми масами m_{i-1}, m_{i+1} невагомими пружинами з жорсткостями k_{i-1}, k_i відповідно. Перша m_1 і остання m_n маси прикріпленні до пружин з жорсткостями k_0, k_n відповідно, інші кінці пружин нерухомо закріплені на опорах (див. [3]).

Отже, можемо використовувати лінійне наближення, і вважати, що для кутів α, під якими розташовані часткові відрізки, виконуються умови $\alpha = \sin\alpha = tg\alpha$.

Спочатку розглянемо прямі спектральні задачі для стільтьєсівської струни з вільно ковзаючим лівим кінцем і закріпленим або вільно ковзаючим правим кінцем.

Якщо обрати деяку масу m_k і розглянути її зміщення $V_k(t)$, $(k = \{2,\dots,n\})$, то коливання цієї маси описує рівняння:

$$\frac{V_k(t)-V_{k-1}(t)}{l_{k-1}} + \frac{V_k(t)-V_{k+1}(t)}{l_k} - m_k V_k''(t) = 0). \tag{1}$$

Умови вільного ковзання обох кінців струни – умови Неймана, мають вигляд:

$$V(0) = V(1),\ \ V(n) = V(n+1). \tag{2}$$

Умови вільного ковзання лівого кінця і закріплення правого кінця струни (умови Неймана і Діріхле відповідно), такі:

$$V(0) = V(1),\ \ V(n+1) = 0. \tag{3}$$

Виконаємо в рівнянннях (1) – (3) заміну $V_k(t) = U_k e^{i\rho t}$, де U_k – амплітуда коливань маси m_k, ρ – деякий параметр. У такому випадку амплітуди малих коливань струни можна охарактеризувати за допомогою системи рівнянь

$$\frac{U_k-U_{k-1}}{l_{k-1}} + \frac{U_k-U_{k+1}}{l_k} + m_k\lambda U_k = 0,\ (k = \{2,\dots,n\}). \tag{4}$$

Крайова умова коливання першої маси струни (лівого кінця струни) має вигляд:

$$\frac{U_1-U_2}{l_1} + m_1\lambda U_1 = 0. \tag{5}$$

Зазначимо, що рівняння (5) можна отримати з першого рівняння системи (4) при $k=1$ та $l_0 \to +\infty$. Умова (5) для лівого кінця струни Стільтьєса також еквівалентна рівності

$$U_1 = U_0.$$

Якщо правий кінець струни закріплений – виконується умова

$$U_{n+1} = 0, \tag{6}$$

а якщо він вільно ковзає, – виконується умова

$$U_{n+1} = U_n. \tag{7}$$

Отже, система рівнянь (4), (5), (6) – крайова задача Неймана-Діріхле для стільтьєсівської струни; задача, що описується системою рівнянь (4), (5), (7) є крайовою задачею Неймана-Неймана для струни Стільтьєса. У цих задачах U_k – амплітуда коливань маси m_k, а число $\lambda = \rho^2$ відіграє роль спектрального параметра.

Позначимо через

$$M = diag\{m_1, m_2, \dots, m_n\},$$

$$U = \{U_1, U_2, \dots, U_n\}^T,$$

$$A = \begin{pmatrix} \frac{1}{l_1} & -\frac{1}{l_1} & 0 & \dots & 0 & 0 \\ -\frac{1}{l_1} & \frac{1}{l_2}+\frac{1}{l_1} & -\frac{1}{l_2} & \dots & 0 & 0 \\ 0 & -\frac{1}{l_2} & \frac{1}{l_3}+\frac{1}{l_2} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \frac{1}{l_{n-1}}+\frac{1}{l_{n-2}} & -\frac{1}{l_{n-1}} \\ 0 & 0 & 0 & \dots & -\frac{1}{l_{n-1}} & \frac{1}{l_n}+\frac{1}{l_{n-1}} \end{pmatrix}$$

$$\widetilde{A} = \begin{pmatrix} \frac{1}{l_1} & -\frac{1}{l_1} & 0 & \dots & 0 & 0 \\ -\frac{1}{l_1} & \frac{1}{l_2}+\frac{1}{l_1} & -\frac{1}{l_2} & 0\dots & 0 & 0 \\ 0 & -\frac{1}{l_2} & \frac{1}{l_3}+\frac{1}{l_2} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \frac{1}{l_{n-1}}+\frac{1}{l_{n-2}} & -\frac{1}{l_{n-1}} \\ 0 & 0 & 0 & \dots & -\frac{1}{l_{n-1}} & \frac{1}{l_{n-1}} \end{pmatrix}$$

Тоді спектральну задачу Неймана-Діріхле можна розглядати як задачу на знаходження власних значень лінійної в'язки

$$L(\lambda) = A - \lambda M,$$

а спектральну задачу Неймана-Неймана як задачу на знаходження власних значень лінійної в'язки

$$L(\lambda) = \widetilde{A} - \lambda M.$$

З рекурентних співвідношень (4) можна послідовно визначити амплітуди малих коливань струни U_k у вигляді:

$$U_k = Q_{2k-2}(\lambda)U_1, \quad (k = \{1,2,...,n+1\}),$$

де $Q_{2k}(\lambda)$ – деякий многочлен степеня k $\quad(k = \{0,1,...,n\})$. Запровадимо многочлени

$$Q_{2k-1}(\lambda) = \frac{Q_{2k}(\lambda) - Q_{2k-2}(\lambda)}{l_k},\ (k = \{1,2,...n\}),$$

тоді отримаємо такі рекурентні співвідношення:

$$Q_{2k}(\lambda) = l_k Q_{2k-1}(\lambda) + Q_{2k-2}(\lambda),$$

$$Q_{2k-1}(\lambda) = Q_{2k-3}(\lambda) - m_k\lambda Q_{2k-2}(\lambda) \tag{8}$$

з відповідними початковими умовами

$$Q_0(\lambda) \equiv 1, \;\; Q_{-1}(\lambda) = 0. \tag{9}$$

Корені рівняння

$$Q_{2n}(\lambda) = 0$$

є власними значеннями $\{\eta_k\}_{k=1}^n$ задачі Неймана-Діріхле, які занумеровані в порядку зростання індексів

$$\eta_1 < \eta_2 < ... < \eta_n,$$

тобто $Q_{2n}(\lambda)$ є характеристичним многочленом задачі, породженою системою рівнянь (4), (5),(6). З іншого боку, цей многочлен визначається своїми коренями $\{\eta_k\}_{k=1}^n$ з точністю до деякого ненульового сталого множника D, тому многочлен $Q_{2n}(\lambda)$ можемо записати у такому вигляді

$$Q_{2n}(\lambda) = D\prod_{k=1}^{n}\left(1-\frac{\lambda}{\eta_k}\right), \tag{10}$$

де $D \neq 0$.

Корені $\{\zeta_k\}_{k=1}^n$ рівняння

$$Q_{2n-1}(\lambda) = 0$$

є власними значеннями струни Стільтьєса при вільному русі без тертя обох кінців струни, тобто задачі Неймана-Неймана. Вони занумерованими в порядку зростання індексів і для яких виконується

$$0 = \zeta_1 < \zeta_2 < ... < \zeta_n.$$

Многочлен $Q_{2n-1}(\lambda) = 0$ також визначається своїми коренями з точністю до деякого множника $B \neq 0$

$$Q_{2n-1}(\lambda) = B\lambda\prod_{k=2}^{n}\left(1-\frac{\lambda}{\zeta_k}\right). \tag{11}$$

Для коренів многочленів $Q_{2n}(\lambda)$, $Q_{2n-1}(\lambda)$ можемо довести справедливість нерівності

$$0 = \zeta_1 < \eta_1 < \zeta_2 < \eta_2 < \zeta_3 < \eta_3 < ... < \eta_n < \zeta_n. \tag{12}$$

Використовуючи рекурентні співвідношення (8) – (9), отримаємо

$$\frac{\lambda Q_{2k}(\lambda)}{Q_{2k-1}(\lambda)} = \frac{\lambda\left(l_k Q_{2k-1}(\lambda) + Q_{2k-2}(\lambda)\right)}{Q_{2k-3}(\lambda) - m_k\lambda Q_{2k-2}(\lambda)} = l_k\lambda + \cfrac{1}{-m_k + \cfrac{1}{\lambda\cfrac{Q_{2k-2}(\lambda)}{Q_{2k-3}(\lambda)}}}. \tag{13}$$

Якщо розглянути відношення многочленів $Q_{2n}(\lambda)$ та $Q_{2n-1}(\lambda)$, які є відповідно храктеристичними многочленами задач Неймана-Діріхле та Неймана-Неймана, то, з урахуванням співвідношень (8) – (9), за індукцією матимемо

$$\frac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)} = l_n\lambda + \cfrac{1}{-m_n + \cfrac{1}{l_{n-1}\lambda + \cfrac{1}{-m_{n-1} + ... + \cfrac{1}{l_1\lambda + \cfrac{1}{-m_1}}}}} \tag{14}$$

Таким чином, враховуючи відношення (13) і (14), маємо

$$\lim_{\lambda\to 0}\frac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)} = -\frac{1}{m_1 + m_2 + ... + m_n} = -\frac{1}{M}. \tag{15}$$

З іншого боку, якщо розглянути відношення многочленів (10), (11), то згідно з (15), отримаємо

$$\frac{Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)} = -\frac{1}{M}\frac{\prod_{k=1}^{n}\left(1-\frac{\lambda}{\eta_k}\right)}{\lambda\prod_{k=2}^{n}\left(1-\frac{\lambda}{\zeta_k}\right)}. \tag{16}$$

Означення 1 (див. [1]). Функція $f(z)$ називається *невалінновою функцією*, якщо:

- $f(z)$ аналітична в півплощинах $Imz > 0$ та $Imz < 0$;
- $f(\overline{z}) = \overline{f(z)}$ $(Imz \neq 0)$;
- $ImzImf(z) \geq 0$ для $Imz \neq 0$.

Означення 2. Функцію $f(z)$, яка є аналітичною в $C\backslash[0,+\infty)$, будемо називати S-функцією, якщо

1) $f(z)$ невалінноva;
2) $f(z) \geq 0$ для $z < 0$.

Ми розглядаємо лише раціональні функції.

Розглянемо обернену задачу для стільтьєсівської струни, яка породжена малими поперечними коливаннями зосереджених мас з умовою Неймана на лівому кінці. Вона полягає в тому, що за відомою сумою мас струни M і $2n$ невід'ємними числами $\{\zeta_k\}_{k=1}^n, \{\eta_k\}_{k=1}^n$, такими що для них справедливі нерівності (12), потрібно знайти величини зосереджених мас й визначити їх розташування на струні, тобто необхідно знайти величини $\{m_k\}_{k=1}^n$ і $\{l_k\}_{k=1}^n$ за умови, що при закріпленому правому кінці власними значеннями струни є числа $\{\eta_k\}_{k=1}^n$, а при вільному русі без тертя правого кінця струни – числа $\{\zeta_k\}_{k=1}^n$.

Відомо, що для коренів многочленів $Q_{2n}(\lambda)$, $Q_{2n-1}(\lambda)$ справедливе строге чергування (12), отже ця пара многочленів не має спільних коренів. Звідси за теор.II.2.1 [1] маємо, що $\dfrac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)}$ є невалінновою функцією. З рекурентних співвідношень (8), (9) слідує те, що ця функція є додатньою при $z < 0$. Таким чином, раціональна функція $\dfrac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)}$ є S-функцією. Отже, їх можна розкласти єдиним способом у ланцюговий дріб відповідно (див. [1]):

$$\frac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)} = a_n\lambda + \tag{17}$$

$$+\cfrac{1}{-b_n+\cfrac{1}{a_{n-1}\lambda+\cfrac{1}{-b_{n-1}+...+\cfrac{1}{a_1\lambda+\cfrac{1}{-b_1}}}}},$$

де $\{a_k\}_{k=1}^n, \{b_k\}_{k=1}^n$ – додатні числа та $a_k = l_k, b_k = m_k$, $k = \{1, 2, ..., n\}$ (див. [2]).

Вочевидь, справедливе і обернене твердження: величини зосереджених мас $\{m_k\}_{k=1}^n$, і довжини часткових відрізків $\{l_k\}_{k=1}^n$, як коефіцієнти розкладу ланцюгового дробу, однозначно визначають раціональну функцію $\dfrac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)}$.

Отже, щоб розв'язати вихідну обернену задачу, необхідно побудувати раціональну функцію виду (16) за відомими величинами $\{\eta_k\}_{k=1}^n, \{\zeta_k\}_{k=1}^n$ та M. Якщо функція $\dfrac{\lambda Q_{2n}(\lambda)}{Q_{2n-1}(\lambda)}$ буде S-функцією, то зможемо розкласти її в ланцюговий дріб виду (14), коефіцієнти якого і будуть величинами зосереджених мас $\{m_k\}_{k=1}^n$, $(m_k > 0)$ та часткових інтервалів $\{l_k\}_{k=1}^n$, $(l_k > 0)$. Тобто необхідною і достатньою умовою існування розв'язку такої задачі є справедливість нерівностей $0 = \zeta_1 < \eta_1 < \zeta_2 < \eta_2 < \zeta_3 < \eta_3 < ... < \zeta_n < \eta_n$.

Вищезазначена обернена задача була розглянута Ф. Р. Гантмахером і М. Г. Крейном, авторами був запропонований метод знаходження шуканих величин [2]. Ми навели розв'язок в інших термінах.

Література

[1] Аткинсон, Ф. В. Дискретные и непрерывные граничные задачи [Текст] / пер. с англ. И. С. Иохвидова, Г. А. Каральник; Под ред. и с доп. И. С. Каца и М. Г. Крейна; [Предисловия И. С. Каца и др.]. – М.: Мир, 1968. – 749 с.

[2] Гантмахер Ф. Р. Осциляционные матрицы и ядра и малые колебания механических систем / Ф. Р. Гантмахер, М. Г. Крейн. – [2 изд.]. – М.: ГИТТЛ, 1950. – 359 с.

[3] Марченко В. А. Введение в теорию обратных задач спектрального анализа / В. А. Марченко. – Х.: АктаНУ, 2005. – 256 с.

References

[1] Atkinson, F. V. Discrete and continuous boundary problems (in Russian), Moskow, 1968.

[2] Gantmakher, F.R. and Krein, M.G. Oscillating matrices and kernels and vibrations of mechanical systems (in Russian), GITTL, Moscow-Leningrad, 1950, German transl. Akademie Verlag, Berlin, 1960.

[3] Marchenko, V.A. Introduction to the theory of inverse problems of spectral analysis (in Russian), Acta, Kharkov, 2005

Set Rewriting Semantics and Temporal Logic for User Stories

Bartosz Zieliński*, Ścibor Sobieski†, and Paweł Maślanka‡
Department of Computer Science
Faculty of Physics and Applied Informatics, University of Łódź,
Pomorska 149/153 90-236 Łódź, Poland
Email: *bzielinski@uni.lodz.pl, †scibor@scibor.org, ‡pmaslan@uni.lodz.pl

***Abstract*—User stories are a popular, human readable format for describing user requirements. We propose an executable semantics for user stories, based on set rewriting, which focuses on capturing the basic (CRUD) operations, as well as agency (who did what). Here, the state of the system is represented as a set of facts (base predicate instances). Each user story corresponds to one or more rewriting rules, each of which defines an elementary (small) step transforming a set of facts. Execution of each user story (which may consist of several small steps) is referred to as a big (business) step, and it corresponds to a single user action. Each of those big steps, executed as transactions, creates a new version of a system state. To facilitate specification of safety and liveliness conditions on sequences of versions we introduce a variant of first order linear temporal logic. We present examples of such specifications. Finally, we outline the algorithm for translating user stories (written in constrained english) into set rewriting rules, and we provide examples of such a translation. The automated user story compiler is currently being developed. The resulting set rewriting system can be executed, tested, and model checked for satisfaction of temporal formulas using Maude rewriting system.**

***Index Terms*—set rewriting, temporal logic, user stories, semantics**

I. Introduction

The two established formats for describing user requirements — *User Stories* and *Use Cases* — are intended for human consumption. They are written in a natural (though usually constrained) language, easily understandable by non-programmer stakeholders. While specifications in the form of user stories or use cases are not necessarily machine unreadable (cf. [1]), automated verification and testing requires some kind of formal semantics.

In this paper, we attempt to provide an executable semantics for user stories. which focuses on capturing the basic (CRUD) operations, as well as agency (who did what). More complex operations are abstracted away, but the semantics is still detailed enough to be useful, e.g., to test for access control violations, or to find unreachable states. The result bears some similarity to specification of artifact-centric business processes (see e.g., [2], [3]). More precisely, we first extract (from a given collection of user stories) a data model in which a state of the system is represented as a set of elementary facts (predicate instances) in the style of ORM/NIAM [4]. Each user story corresponds to one or more rewriting rules, each of which defines an elementary (small) step transforming a set of facts. The set rewriting rules we use here can be equivalently viewed as definitions of coloured Petri Nets with inhibitor edges and ability to generate fresh nominal values (cf. [5]), where identical tokens are collapsed into one. Execution of each user story (which may consist of several small steps) is referred to as a big (business) step, and it corresponds to a single user action. Each of those big steps, executed as transactions, creates a new version of a system state. The rewriting rules can be executed and tested in Maude rewriting system (see [6], [7], c.f., [8], [9]), [10]). Checking invariants through search is often sufficient to test the correctness of user stories. However, to facilitate specification of more advanced safety and liveliness conditions on sequences of versions, we introduce a variant (named US LTL) of first order linear temporal logic [11]. To enable testing for access control violations, US LTL includes testing for an agent whose action created the current version of the system. The paper presents some examples of specifications of security conditions in our temporal logic.

Currently, translation of user stories into a set rewriting system is done manually, but we are working on a "compiler" for user stories. In the paper, we outline the translation algorithm, and provide examples of such a translation (cf. [12]).

This work extends and modifies research presented in [13].

II. Facts and Set Rewriting

A. Values, variables, substitutions, and facts

We assume fixed, countably infinite, disjoint sets VAL and VAR of, respectively, *atomic values* and *variables*. Values $c \in \text{VAL}$ are purely nominal: they have no properties or operators defined for them except for equality. Because atomic values are completely interchangeable, it makes no sense for $c \in \text{VAL}$ to appear in a rule or temporal formula. Because there is infinity of them, one can always pick *fresh* $c \in \text{VAL}$ (i.e., c which was never used before).

A *substitution* $\sigma : V \to \text{VAL}$ is a function from a finite set $V \subseteq \text{VAR}$ (called the *domain* of σ, and denoted $Dom(\sigma)$) to atomic values. Substitutions can be composed: Given substitutions $\sigma : Dom(\sigma) \to \text{VAL}$ and $\sigma' : Dom(\sigma') \to \text{VAL}$ we define $\sigma\sigma' : Dom(\sigma) \cup Dom(\sigma') \to \text{VAL}$ with $(\sigma\sigma')(v) := c$ where $c := \sigma'(v)$ if $v \in Dom(\sigma')$, and $c := \sigma(v)$ if $v \in Dom(\sigma) \setminus Dom(\sigma')$. Let $a_1, \ldots, a_n \in \text{VAL}$ and $v_1, \ldots, v_n \in \text{VAR}$, where v_i's are all distinct. We denote by $\{a_1/v_1, \ldots, a_n/v_n\} =: \sigma$ a substitution with $Dom(\sigma) = \{v_1, \ldots, v_n\}$ such that $\sigma(v_i) = a_i$ for all $i \in \{1, \ldots, n\}$.

Facts are instances of base predicates (one can think of them as rows in a database table if each row stored

also a table name). A *ground* (resp. *non-ground*) *fact* $P(a_1, \ldots, a_m)$ consists of a predicate name P and a list $a_1, \ldots, a_m$ where $a_i \in$ VAL (resp. $a_i \in$ VAR), for $i \in \{1, \ldots, n\}$. Facts which encode control flow information, instead of business relevant information, are referred to as *tokens*.

Given a non-ground fact f (resp. a set of non-ground facts Γ) we denote by $\mathit{Var}(f)$ (resp. $\mathit{Var}(\Gamma)$) a set of variables occurring in f (resp. Γ). That is, $\mathit{Var}(P(v_1, \ldots, v_m)) := \{v_1, \ldots, v_m\}$, and $\mathit{Var}(\Gamma) = \bigcup\{\mathit{Var}(f) \mid f \in \Gamma\}$. Given a substitution σ such that $\mathit{Dom}(\sigma) \supseteq \mathit{Var}(f)$ (resp. $\mathit{Dom}(\sigma) \supseteq \mathit{Var}(\Gamma)$) we denote by $\sigma(f)$ (resp. $\sigma(\Gamma)$) the result of replacing all variables in a fact f (resp. in a set of facts Γ) with atomic values according to σ, i.e., $\sigma(P(v_1, \ldots, v_n)) := P(\sigma(v_1), \ldots, \sigma(v_n))$ and $\sigma(\Gamma) := \{\sigma(f) \mid f \in \Gamma\}$.

B. Set rewrite rules

The state of the system at a given moment is represented by a set of ground facts. Set rewrite rules describe transformations of ground sets of facts. *A set rewrite rule* $\lambda = (x, \Gamma, \Delta, \Delta')$ is a 4-tuple consisting of a variable x (corresponding to an agent of the action) and three sets of non-ground facts Γ, Δ and Δ' such that (1) $x \in \mathit{Var}(\Delta)$ and (2) $(\mathit{Var}(\Gamma) \setminus \mathit{Var}(\Delta)) \cap \mathit{Var}(\Delta') = \emptyset$.

We say that a ground set of facts Ψ rewrites to a ground set Ψ' with agent $a \in$ VAL, rule λ and substitution σ, which we denote by $\Psi \xrightarrow{a,\lambda,\sigma} \Psi'$, iff

1) $\mathit{Dom}(\sigma) \supseteq \{x\} \cup \mathit{Var}(\Delta) \cup \mathit{Var}(\Delta')$,
2) $\sigma(x) = a$,
3) There is no substitution σ' with $\mathit{Dom}(\sigma) = \mathit{Var}(\Gamma) \setminus \mathit{Var}(\Delta)$ such that $(\sigma\sigma')(\Gamma) \subseteq \Psi$,
4) $\sigma(\Delta) \subseteq \Psi$,
5) $\Psi' = (\Psi \setminus \sigma(\Delta)) \cup \sigma(\Delta')$,
6) for all $v \in \mathit{Var}(\Delta') \setminus \mathit{Var}(\Delta)$, $\sigma(v) \in$ VAL is fresh.

To improve readability we use an alternative syntax for rules. Namely, we write

$$\neg\vec{\alpha}, \vec{\beta} \mid \vec{\gamma} \Rightarrow_x \vec{\delta},$$

where $\neg\vec{\alpha} = \neg\alpha_1, \ldots, \neg\alpha_n$, $\vec{\beta} = \beta_1, \ldots, \beta_m$, etc., and α_i's, β_i's, γ_i's, and δ_i's are facts, to denote the rule

$$\big(x, \{\vec{\alpha}\}, \{\vec{\beta}\} \cup \{\vec{\gamma}\}, \{\vec{\beta}\} \cup \{\vec{\delta}\}\big).$$

A rewrite system $\mathcal{R}$ is a set of rewrite rules. We write $\Psi \xrightarrow{a}_{\mathcal{R}} \Psi'$ if there exists some $\lambda \in \mathcal{R}$ and a ground substitution σ such that $\Psi \xrightarrow{a,\lambda,\sigma} \Psi'$.

III. FROM USER STORIES TO SET REWRITING

We assume that each story corresponds either to some CRUD operation (creation or update of entities) or to using data to compute or view something. The latter is abstracted as creation of special facts, e.g., of the form $\mathsf{view}(x, y)$, i.e., person x viewed entity with identifier y.

The following list specifies the workflow for translating a collection of user stories into set rewrite rules:

1) We start with "informal" user stories written after requirements gathering sessions with the customer.
2) We extract (manually) from informal stories a data model in the style of ORM/NIAM [4]. This may require auxilliary domain knowledge input from the customer.
3) We rewrite stories using controlled English with vocabulary defined by the data model.
4) We specify a set $\mathcal{L}$ of safety and liveliness properties using temporal logic US LTL (see Section IV)
5) Stories are then converted (preferably through the story compiler) to a rewriting system $\mathcal{R}$. Each user story gives rise to one or more rewriting rules.
6) We verify (e.g., using Maude rewriting system) if $\mathcal{R}$ satisfies all the properties $\mathcal{L}$. In case of errors we correct the user stories and test again.

1) *As a user I want to create files and make myself their owner.*
2) *As an owner of a file I want to delete the file.*
3) *As a file owner I want to make another user owner of the file.*

Fig. 1. User stories describing a simple filesystem

1) A user $@u$ wants to **create** files $@f$ such that $@u$ is an owner of $@f$.
2) An owner $@u$ of $@f$ wants to **delete** file $@f$.
3) An owner $@u$ of $@f$ wants to *make* user $@u'$ an owner of $@f$.

Fig. 2. User stories in the format [12] describing a simple filesystem

Figure 1 present a small collection of "informal" user stories which will serve as a running example in the remainder of this paper.

A. Extracting data model and formalising stories

Any noun (and sometimes verb) used in the stories might indicate possible predicate symbol. In stories presented in Figure 1, three nouns occur: file, user and owner. Those give rise to facts of the form $\mathsf{file}(x)$ (x is a file), $\mathsf{user}(x)$ (x is a user), and $\mathsf{owner}(x, y)$ (user x owns file y). With domain knowledge and the very phrasing of stories we can infer the following constraint: If $\mathsf{owner}(x, y)$ then $\mathsf{user}(x)$ and $\mathsf{file}(y)$.

Armed with a data model and domain constraints we rewrite original stories from Figure 1 to use the syntax of [12] (see Figure 2). The format uses variables (marked with @) to disambiguate the objects sentences speak about. The main verb (typeset in bold in Figure 2) determines the kind of CRUD action is described by the story (which, in turn, determines a skeleton of rewriting implementation). In addition, the use of plural ("files") in the first story indicates that in the story a multiplicity of objects is created.

B. Translating user story into set rewrite rules

Each user story gives rise to one or more set rewriting rules. Rewriting steps corresponding to rules related to distinct stories (or distinct instantiations of the same story) do not interleave. A transformation of a system state from a set of ground facts Ψ to a set of ground facts Ψ' on behalf

1.1) $\mathsf{user}(u) \mid \#^{\text{next}} \Rightarrow_u \#^1(u)$,
1.2) $\#^1(u) \mid \Rightarrow_u \mathsf{file}(f), \mathsf{owner}(u, f)$,
1.3) $\mid \#^1(u) \Rightarrow_u \mathsf{file}(f), \mathsf{owner}(u, f), \#^{\text{next}}$,
2.1) $\mid \#^{\text{next}}, \mathsf{file}(f) \Rightarrow_u \#^2(u, f)$,
2.2) $\#^2(u, f) \mid \mathsf{owner}(u', f) \Rightarrow_u$,
2.3) $\neg\mathsf{owner}(u', f) \mid \#^2(u, f) \Rightarrow_u \#^{\text{next}}$,
3.1) $\mathsf{owner}(u, f), \mathsf{user}(u'), \#^{\text{next}} \mid \Rightarrow_u \mathsf{owner}(u', f)$.

Fig. 3. Translation of stories in Figure 2 to set rewrite rules

of an agent a, with a sequence of rewrite steps related to a single instantiation of a user story, and constituting a full execution of this story (i.e., at Δ a story instantiation is picked, and at Δ' system is ready to pick another instantiation of another story), is called *a big business step*, and denoted by $\Delta \rightsquigarrow_a \Delta'$.

Recall that tokens are facts encoding control flow information. In particular, the presence in the set of facts of a token $\#^{\text{next}}$ enables choosing a new user story instance. If the execution of a given story instance consists of a sequence of more than one rewrite steps, a first step in the sequence removes the token $\#^{\text{next}}$, and replaces it with a story's "internal" token. A typical (ground) token has a form $\#^{\lambda}(a_1, \ldots, a_n)$, where λ is a story label, and $a_1, \ldots, a_n \in \text{VAL}$ uniquely identify the instance. In particular, a_i's must include the agent. The last rewrite of a story instance execution removes internal token and replaces it with $\#^{\text{next}}$.

The stories in Figure 2 translate into set rewrite rules presented in Figure 3. Implementation of the first story consists of three rewrite rules. The first one replaces $\#^{\text{next}}$ token with $\#^1(u)$ token which stores the user performing the action. Then there are two rules which create files and make u their owner. The first one does not remove the $\#^1(u)$ token, and thus can be repeated many times during execution of a story instance. The second one replaces $\#^1(u)$ with $\#^{\text{next}}$, and thus finishes execution of the story instance.

The second story is also implemented with three rewrite rules. To delete a single file f rule's implementation must remove not only fact $\mathsf{file}(f)$ but also any fact of the form $\mathsf{owner}(u', f)$, where u' is arbitrary (a file may have many owners). The first rule for this story removes $\mathsf{file}(f)$, as well as replaces $\#^{\text{next}}$ with $\#^2(u, f)$. The second rule removes facts of the form $\mathsf{owner}(u', f)$, while keeping token $\#^2(u, f)$. Finally, the last rule which replaces $\#^2(u, f)$ with $\#^{\text{next}}$ (and thus ends execution of the story) can be applied only if there are no more facts of the form $\mathsf{owner}(u', f)$, for arbitrary u'.

Finally, the last story is implemented with a single rule. (thus, the rule does not replace $\#^{\text{next}}$). It simply adds $\mathsf{owner}(u', f)$ to the set of facts.

C. Example execution of rules

Let the initial set of facts be (where $c_1, c_2 \in \text{VAL}$):

$$\Delta_0 := \{\mathsf{user}(c_1), \mathsf{user}(c_2), \#^{\text{next}}\}.$$

Only rule 1.1 (first rule of first story) is applicable here. Of two matching substitutions we choose $\sigma_0 := \{c_1/u\}$. Then

$$\Delta_0 \xrightarrow{c_1, 1.1, \sigma_0} \Delta_1 := \{\mathsf{user}(c_1), \mathsf{user}(c_2), \#^1(c_1)\}.$$

At Δ_1 both 1.2 and 1.3 are applicable. Let us choose 1.3, and let $\sigma_1 := \{c_1/u, c_3/f\}$ (note the fresh value $c_3 \in \text{VAL}$ substituted for variable f corresponding to the new file). Then

$$\Delta_1 \xrightarrow{c_1, 1.3, \sigma_1} \Delta_2$$
$$:= \{\mathsf{user}(c_1), \mathsf{user}(c_2), \#^{\text{next}}, \mathsf{file}(c_3), \mathsf{owner}(c_1, c_3)\}.$$

At Δ_2, rules 1.1, 2.1 and 3.1 are applicable. We choose 3.1, and let $\sigma_2 := \{c_1/u, c_3/f, c_2/u'\}$. Then

$$\Delta_2 \xrightarrow{c_1, 3.1, \sigma_2} \Delta_3 := \{\mathsf{user}(c_1), \mathsf{user}(c_2),$$
$$\#^{\text{next}}, \mathsf{file}(c_3), \mathsf{owner}(c_1, c_3), \mathsf{owner}(c_2, c_3)\}.$$

Observe that in terms of big business steps we have

$$\Delta_0 \rightsquigarrow_{c_1} \Delta_2 \rightsquigarrow_{c_1} \Delta_3.$$

IV. Linear Temporal Logic of User Stories

To be able to specify expressive safety and liveliness requirements of specification based on user stories (translated into rewriting rules), we propose a restricted (quantifier-free) variant of first order linear temporal logic called *linear temporal logic of user stories* (US LTL). After restricting the set of values to an arbitrarily chosen finite subset, one can effectively translate US LTL formulas to formulas in propositional linear logic which can be model checked against the rewriting system generated from user stories by standard tools available with term rewriting system Maude.

A. Syntax of US LTL

A set of formulas of US LTL is defined inductively as follows:

- $\top$ is a US LTL formula.
- If $x \in \text{VAR}$ then $x^\flat$ is a US LTL formula.
- If f is a non-ground, non-token fact then f is a US LTL formula.
- If ϕ and ψ are formulas of US LTL then also $\neg\phi$, $\phi \vee \psi$, $\bigcirc\phi$ (next-time ϕ), and $\phi \,\mathsf{U}\, \psi$ (ϕ until ψ) are US LTL formulas.

We denote by $\mathit{Var}(\phi)$ the set of variables of US LTL formula ϕ. Thus, $\mathit{Var}(x^\flat) = \{x\}$, and $\mathit{Var}(f)$ for facts f was defined earlier in this paper. The remaining cases use easy recursion, e.g., $\mathit{Var}(\phi \,\mathsf{U}\, \psi) = \mathit{Var}(\phi) \cup \mathit{Var}(\psi)$.

In the standard way we define derived operators, e.g., $\bot :\equiv \neg\top$, $\phi \wedge \psi :\equiv \neg(\neg\phi \vee \neg\psi)$, $\Diamond\phi := \top \,\mathsf{U}\, \phi$, $\Box\phi :\equiv \neg\Diamond\neg\phi$, etc.

B. Semantics of US LTL

Models of US LTL formulas are finite or infinite runs of big steps of the form

$$\mathcal{M} := \Delta_0 \rightsquigarrow_{a_1} \Delta_1 \rightsquigarrow_{a_2} \Delta_2 \rightsquigarrow_{a_3} \cdots$$

where Δ_i's are sets of ground facts and a_i's are elements of VAL. We write $\mathcal{M}, n, \sigma \models \phi$ iff a US LTL formula ϕ is satisfied at step $n \in \mathbb{N}$ of model $\mathcal{M}$ with substitution σ such that $Dom(\sigma) \supseteq Var(\phi)$. Relation $\models$ is defined by structural induction on ϕ as follows:

- $\mathcal{M}, n, \sigma \models \top$,
- $\mathcal{M}, n, \sigma \models x^\flat$ iff $n > 0$ and $\sigma(x) = a_n$,
- Let f be a non-ground fact. $\mathcal{M}, n, \sigma \models f$ iff $\sigma(f) \in \Delta_n$.
- $\mathcal{M}, n, \sigma \models \neg\phi$ iff not $\mathcal{M}, n, \sigma \models \phi$,
- $\mathcal{M}, n, \sigma \models \phi \vee \psi$ iff $\mathcal{M}, n, \sigma \models \phi$ or $\mathcal{M}, n, \sigma \models \psi$,
- $\mathcal{M}, n, \sigma \models \bigcirc\phi$ iff $\mathcal{M}, n+1, \sigma \models \phi$ (if the run $\mathcal{M}$ is finite, and $m \in \mathbb{N}$ is the last step, then $\mathcal{M}, m, \sigma \models \bigcirc\phi$).
- $\mathcal{M}, n, \sigma \models \phi \,\mathsf{U}\, \psi$ iff there exists $m \geq n$ such that $\mathcal{M}, m, \sigma \models \psi$ and $\mathcal{M}, k, \sigma \models \phi$ for all $n \leq k < m$.

We write $\mathcal{M}, n \models \phi$ iff $\mathcal{M}, n, \sigma \models \phi$ for all substitutions $\sigma : Var(\phi) \to$ VAL (i.e., variables are implicitly universally quantified). Finally, we say that $\mathcal{M}$ satisfies ϕ (denoted $\mathcal{M} \models \phi$) iff $\mathcal{M}, 0 \models \phi$.

C. Specifying properties with US LTL

First let us note that we can express in US LTL statements such as "user u created fact f" or "user u deleted fact f". Indeed, those statements are expressed by US LTL formulas $\neg f \wedge \bigcirc (u^\flat \wedge f)$ and $f \wedge \bigcirc (u^\flat \wedge \neg f)$, respectively. Let us use this to express as an example two requirements related to access control. The first requirement, satisfied by the rewriting system in Figure 3, is "only owner of f can delete file f". Expressed in US LTL it reads

$$\Box\big(\mathsf{file}(f) \wedge \bigcirc(u^\flat \wedge \neg\mathsf{file}(f)) \Rightarrow \mathsf{owner}(u, f)\big).$$

The second requirement, which rewriting system in Figure 3 fails to satisfy, is "Only creator of the file f can make another user owner of f". Expressed in US LTL this requirement reads

$$\Diamond\big(\neg\mathsf{owner}(u', f) \wedge \bigcirc(u^\flat \wedge \mathsf{owner}(u', f))\big) \Rightarrow \Diamond\big(\neg\mathsf{file}(f) \wedge \bigcirc(u^\flat \wedge \mathsf{file}(f))\big).$$

V. ANALYSIS AND CONCLUSION

We are currently trying to apply the methodology described in this paper to the specification in the form of user stories of a system supporting national selection of candidates for study programmes at the universities in New Guinea (which has some peculiar features, like the fact that candidates do not apply to a particular university, submitting instead their applications to the Department of Higher Education, Research, Science and Technology which matches candidates with offers by higher education institutions).

Preliminary analysis shows that for majority of stories our formalism, fairly limited as it is, is nevertheless expressive enough to be useful. It is not difficult to extend our set rewriting rules format to allow for domain relations and complex terms (see e.g., [13]), which permits non-trivial representation of remaining stories. Unfortunately, introduction of fresh values becomes problematic (as does the very notion of freshness) for non-nominal data-types. Also, the use of non-nominal data types makes model checking of temporal formulas problematic. This is why in this work we preferred to use purely nominal universe of values.

Currently we are developing an automated user story compiler which we hope to develop into user-friendly tool helping to avoid introducing errors during the requirements gathering phase of software development.

REFERENCES

[1] M. Landhausser and A. Genaid, "Connecting user stories and code for test development," in *Recommendation Systems for Software Engineering (RSSE), 2012 Third International Workshop on*, June 2012, pp. 33–37.

[2] R. Hull, "Artifact-centric business process models: Brief survey of research results and challenges," in *On the Move to Meaningful Internet Systems: OTM 2008*, R. Meersman and Z. Tari, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1152–1163.

[3] P. A. Abdulla, C. Aiswarya, M. F. Atig, M. Montali, and O. Rezine, "Recency-bounded verification of dynamic database-driven systems," in *Proceedings of the 35th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems*, ser. PODS '16. New York, NY, USA: ACM, 2016, pp. 195–210.

[4] T. Halpin, *ORM/NIAM Object-Role Modeling*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 81–101. [Online]. Available: https://doi.org/10.1007/978-3-662-03526-9_4

[5] M. Montali and A. Rivkin, "Model checking Petri nets with names using data-centric dynamic systems," *Formal Aspects of Computing*, vol. 28, no. 4, pp. 615–641, 2016.

[6] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. Talcott, "The Maude 2.0 system," in *Rewriting Techniques and Applications (RTA 2003)*, ser. Lecture Notes in Computer Science, R. Nieuwenhuis, Ed., no. 2706. Springer-Verlag, June 2003, pp. 76–87.

[7] M. Clavel, F. Duran, S. Eker, P. Lincoln, N. Marti-Oliet, J. Meseguer, and C. Talcott, *Maude Manual (Version 2.6)*, 2011.

[8] Ś. Sobieski and B. Zieliński, "Using Maude rewriting system to modularize and extend SQL," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. ACM, 2013, pp. 853–858.

[9] Ś. Sobieski and B. Zieliński, "Modularisation in Maude of parametrized RBAC for row level access control," in *Advances in Databases and Information Systems*. Springer, 2011, pp. 401–414.

[10] J. Padberg and A. Schulz, "Model checking reconfigurable Petri nets with Maude," in *Graph Transformation*, R. Echahed and M. Minas, Eds. Cham: Springer International Publishing, 2016, pp. 54–70.

[11] M. Fisher, *An introduction to practical formal methods using temporal logic*. John Wiley & Sons, 2011.

[12] Ś. Sobieski and B. Zieliński, "User stories and parameterized role based access control," in *Model and Data Engineering*, L. Bellatreche and Y. Manolopoulos, Eds. Cham: Springer International Publishing, 2015, pp. 311–319.

[13] Ś. Sobieski, B. Zieliński, and P. Maślanka, "Rewriting semantics of user stories," in *Information Technologies and Computer Modelling, Yaremche, Ivanofrankivsk, 14-19 May 2018*, 2018.

The sequences of PRN's produced by inversive generators of q^{th} order.

Sergey Varbanets
Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
Odessa, Ukraine
varb@sana.od.ua

***Abstract*—For the sequences of pseudo-random numbers (PRN's) produced by inversive congruential generator of q^{th} order**

$$y_{n+1} \equiv \frac{a}{y_n y_{n-1} \dots y_{n-q+1}} + b(n) \pmod{()p^m}$$

there found the representations of elements y_n in form of polynomials of special type on index n. Also, it is obtained the conditions on the coefficients a and $b(n)$, for which the sequens of y_n hes maximal period $\tau = qp^{m-\nu_0}$, where $\nu_0 = \nu_p(b(n))$. It has been obtained the estimates of exponential sums of Gaussian and Kloosterman types over the elements of sequence $\{y_n\}$.

***Index Terms*—sequences of pseudo-random numbers, exponential sum, inversive congruential generator, polynomial representation**

I. Introduction

The equidistribution character of the sequence of pseudo-random numbers (abbreviate, PRN's) is defined by the discrepancy of this sequence. Usually the bound of discrepancy for the sequence of PRN's, that is generated by the congruential generator, is estimated by using the Turan-Erdös-Koksma inequality, the core of which is the exponential sum with elements of this sequence in exponent.

In the works of R.G. Stoneham [5] and H. Niederreiter [2]- [4] a certain exponential sums are investigated which are intimately connected with the linear congruential PRN's produced by the linear congruential recursion

$$y_{n+1} \equiv a y_n + b \pmod{M},$$
$$0 \le y_1 \le M,\ n = 0, 1, 2, \dots,$$

where $a, b, M, y_0 \in \mathbb{Z}$, $a \ge 1$, $M > 1$, $b, y_0 \ge 0$.

H. Niederreiter [4] proved the following assertion

Theorem. *Let $h \in \mathbb{Z}$, $(h, M) = 1$, $(a, M) = 1$, and assume that a belongs to the exponent ℓ modulo M. Then, for $1 \le N \le \tau$*

$$\left| \sum_{n=0}^{N-1} e^{2\pi i \frac{h y_n}{M}} \right| < \left(\frac{M\tau}{\ell} \right)^{\frac{1}{2}} \left(\frac{2}{\pi} \log \tau + \frac{3}{4} \right),$$

where τ is the least period length of the sequence $\{y_n\}$.

The well-known deficiencies of the linear congruential sequences of PRN's, such as the relatively coarse lattice structure of these sequences, and as consequence a predictability of elements of the linear congruential generators of PRN's.

Let $f(x)$ be an integral-value function and let $\{y_n\}$ be a sequence produced by the congruential recursion

$$y_{n+1} \equiv f(y_n) \pmod{M}$$

with initial value y_0.

Consider the sequence $\{x_n\}$, $x_n = \frac{y_n}{M}$, $n = 0, 1, \dots$. This sequence calls the sequence of PRN's if it is an equidistribution on $[0, 1)$, statistical independence and has "a large" period length.

In 1986 Eichenauer and Lehn [1] and then Niederreiter [2] have studied a recursive sequence generated by the recursive relation

$$y_{n+1} \equiv \begin{cases} a y_n^{-1} + b \pmod{p} & if \quad (y_n, p) = 1, \\ b \pmod{b} & if \quad y_n \equiv 0 \pmod{p} \end{cases}$$

with some coefficients $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}_p$, $(y_0, p) = 1$, y_n^{-1} is a multiplicative inverse for y_n modulo p.

Such generator of PRN's calls the inversive generator modulo p. For the case $M = p^m$, $m > 1$, we also can consider similar generator if only for all $n = 0, 1, 2, \dots$ the values y_n satisfy the condition $(y_n, p) = 1$. This condition holds if $(a, p) = 1$, $b \equiv 0 \pmod{p}$.

In the sequel we shall always assume also without of explicit mention that this condition accomplishes.

The one of our points of interest is to study some exponential sums over the sequence of inversive congruential PRN's $\{y_n\}$ produced by one congruence

$$(I) \quad y_{n+1} \equiv a y_n^{-1} + b(n) \pmod{p^m},$$
$$(II) \quad y_{n+1} \equiv a y_{n-1}^{-1} y_n^{-1} + b(n) \pmod{p^m},$$

where $b(n) = b + c_1 n + p^{\mu} F(n)$, $b = p^{\nu_0} b_0$, $\nu_0 > 0$, $(b_0, p) = 1$, $c_1 = c y_0$, $\nu_p(c) = \mu_0 > \nu_0$ (for (I)), and $c_1 = c$ (for (II)); $(a, p) = (y_0, p) = (y_1, p) = 1$, $\mu > \max(\nu_0, \mu_0)$, $F(n) \in \mathbb{Z}[n]$.

The generator of PRN's (I) (respectively, (II)) calls the inversive generator with a variable shift (respectively, the inversive generator of second order with a variable shift).

The other subject we touched upon is obtaining the non-trivial bounds for the following exponential sums

$$S_\ell^{(j)}(h; N) = \sum_{\substack{n=0 \\ y_n \in (\ell)}}^{N-1} e^{2\pi i \frac{h y_n^j}{p^m}}, \quad j = 1, 2;\ \ell = I, II;$$

$$K_{\ell}(h_1,h_2;N)=\sum_{\substack{n=0\\ y_n\in(\ell)}}^{N-1} e^{2\pi i\frac{h_1y_n+h_2y_n^{-1}}{p^m}},\ \ell=I,II;$$

Here we note that the subscription $y_n\in(\ell)$ implies the satisfaction of y_n to recursion (ℓ) $(\ell=I or II)$.

For making our aims true we will use the following auxiliary lemmas.

II. Auxiliary Results

Lemma 1 (see, [7]). *Let $\{y_n\}$ be the sequence produced by recursion (I) under its conditions. Then for $k>\left[\frac{m}{\nu_0}\right]+1$ the following representations modulo p^m*

$$\begin{cases} y_{2k}=\dfrac{A_0^{(k)}+A_1^{(k)}y_0+\cdots+A_{r-1}^{(k)}y_0^{r-1}}{B_0^{(k)}+B_1^{(k)}y_0+\cdots+B_r^{(k)}y_0^r},\\ y_{2k+1}=\dfrac{C_0^{(k)}+C_1^{(k)}y_0+\cdots+C_r^{(k)}y_0^r}{D_0^{(k)}+D_1^{(k)}y_0+\cdots+D_{r-1}^{(k)}y_0^{r-1}} \end{cases}$$

hold.
Moreover, we have

$$A_r^{(k)}=bC_r^{(k)};$$

and for $j=0,1,\ldots,r-1$

$$\begin{aligned} &A_j^{(k)}=aD_j^{(k)}+bC_j^{(k)}+F(2k+2)C_{j-1}^{(k)};\\ &C_j^{(k+1)}=aB_j^{(k+1)}+bA_j^{(k+1)}+F(2k+3)A_j^{(k+1)};\\ &C_r^{(k+1)}=bA_r^{(k+1)},\ D_j^{(k+1)}=A_j^{(k+1)}; \end{aligned}$$

for $j=0,1,\ldots,r$

$$B_j^{(k+1)}=C_j^{(k)};$$

where $F(u)=c(u+p^{\mu}F_0(u))$, $c=c_1y_0^{-1}$.

Lemma 2 (see, [6]). *Let y_n be produced by inversive generator of type (II). Then the following representations*

$$y_{3k-1}=\frac{a^k+c^{k-1}b^2\frac{k(k-1)}{2}y_0+\frac{\left(a^{k-1}bk+a^{k-1}c\Phi_1(k)\right)}{(y_0y_1)^{-1}}}{\left(\frac{k(k-1)}{2}a^{k-1}b^2+a^{k-1}c\Phi_2(k)\right)+\frac{(k-1)b+y_1}{a^{-k+1}y_0^{-1}}},$$

$$y_{3k}=\frac{ka^kb+a^ky_0+\frac{\left(\frac{k(k-1)}{2}a^{k-1}b^2+a^{k-1}c\Phi_3(k)\right)}{y_0^{-1}y_1^{-1}}}{a^k+\frac{k(k-1)}{2}a^{k-1}b^2y_0+\frac{\left(ka^{k-1}b+a^{k-1}c\Phi_1(k)\right)}{y_0^{-1}y_1^{-1}}},$$

$$y_{3k+1}=\frac{\left(\frac{k(k-1)}{2}a^kb^2+a^kc\Phi_2(k+1)\right)+\frac{ka^2b-a^ky_1}{y_0^{-1}}}{ka^kb+a^ky_0+\frac{\left(\frac{k(k-1)}{2}a^{k-1}b^2+a^{k-1}c\Phi_3(k)\right)}{y_0^{-1}y_1^{-1}}},$$

hold,
where

$$\begin{aligned} &\Phi_1(k)=F_2+F_5+\ldots+F_{3k-1},\\ &\Phi_2(k)=F_4+F_7+\ldots+F_{3k-2},\\ &\Phi_3(k)=F_3+F_6+\ldots+F_{3k},\\ &F_j=j+p^{\mu_1}F_1(j),\ F_1(n)\in\mathbb{Z}[n],\ \mu_1\geq1. \end{aligned}$$

Lemma 3 (see, [6], Lemma 2). *Let h_1, h_2, k, ℓ be positive integers and let $\nu_p(h_1+h_2)=\alpha$, $\nu_p(h_1k+h_2\ell)=\beta$, $\delta=\min(\alpha,\beta)$. Then for every $j=2,3,\ldots$ we have*

$$\nu_p(h_1k^{j-1}+h_2\ell^{j-1})\geq\delta.$$

Moreover, for every polynomial $G(u)=A_1u+A_2u^2+p^tG_1(u)\in\mathbb{Z}[u]$ we have

$$\begin{aligned} h_1G(k)+h_2G(\ell)=A_1(h_1k+h_2\ell)+A_2(h_1k^2+h_2\ell^2)+\\ +p^{t+s}G_2(k,\ell), \end{aligned}$$

where $s\geq\min(\nu_p(h_1+h_2),\nu_p(h_1k+h_2\ell))$, $h_1,h_2,k,\ell\in\mathbb{Z}$, $G_2(u,v)\in\mathbb{Z}[u,v]$.

Lemma 4 (see, [6], Lemma 3). *Let $p>2$ be a prime number, $m\geq2$ be a positive integer, $m_0=\left[\frac{m}{2}\right]$, $f(x)$, $g(x)$, $h(x)$ be polynomials over $\mathbb{Z}$*

$$\begin{aligned} &f(x)=A_1x+A_2x^2+\cdots,\\ &g(x)=B_1x+B_2x^2+\cdots,\\ &h(x)=C_\ell x+C_{\ell+1}x^{\ell+1}+\cdots,\ \ell\geq1, \end{aligned}$$

$$\nu_p(A_j)=\lambda_j,\quad \nu_p(B_j)=\mu_j,\quad \nu_p(C_j)=\nu_j,$$

and, moreover,

$$\begin{aligned} &k=\lambda_2<\lambda_3\leq\cdots,\quad 0=\mu_1<\mu_2<\mu_3\leq\cdots,\\ &\nu_p(C_\ell)=0,\ \nu_p(C_j)>0,\ j\geq\ell+1. \end{aligned}$$

Then the following bounds occur

$$\left|\sum_{x\in\mathbb{Z}_{p^m}}e_m(f(x))\right|\leq\begin{cases}2p^{\frac{m+k}{2}} & if\quad \nu_p(A_1)\geq k,\\ 0 & if\quad \nu_p(A_1)<k;\end{cases}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}}e_m(f(x)+g(x^{-1}))\right|\leq I(p^{m-m_0})p^{\frac{m}{2}}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}}e_m(h(x))\right|\leq\begin{cases}1 & if\quad \ell=1,\\ 0 & if\quad \ell>1,\end{cases}$$

where $I(p^{m-m_0})$ is a number of solutions of the congruence

$$y\cdot f'(y)\equiv g'(y^{-1})\cdot y^{-1}\pmod{p^{m-m_0}},\ y\in\mathbb{Z}^*_{p^{m-m_0}}.$$

III. Main Results

Using Lemma 1 we have

Lemma 5. *Let $\{y_n\}$ be the sequence produced by recursion (I) under its conditions. Then for $k \geq 2$ there are valid the following representations modulo p^{ν}*

$$\begin{aligned}
y_{2k} &= y_0\left(1-a^{-1}y_0^2\right)+\\
&+k\left(b\left(1-a^{-1}y_0^2\right)+(2a)^{-1}b^2y_0+cy_0\right)+\\
&+k^2\left(-a^{-1}y_0\left(1-a^{-1}y_0^2\right)b^2+a^{-1}cy_0^2\right):=\\
&:=E_0+E_1k+E_2k^2;\\
y_{2k+1} &= \left(ay_0^{-1}+b+cy_0\right)+\\
&+k\left(b\left(1-ay_0^{-2}\right)+b^2+2cy_0\right)+\\
&+k^2\left(-\left(1-ay_0^{-2}\right)b^2-\frac{1}{2}(4-a^{-1})b^2y_0^{-1}-ac\right)\\
&:=F_0+F_1k+F_2k^2;
\end{aligned}$$

Using Lemma 2 we have

Lemma 6. *Let $\{y_n\}$ be the sequence produced by recursion (II) under its conditions. Then for $k \geq 2$ the following representations modulo p^{ν}*

$$\begin{aligned}
y_{3k-1} &= ay_0^{-1}y_1^{-1}+\\
&+(k-1)b\left(\left(-ay_0^{-2}y_1^{-1}+1\right)-\right.\\
&\left.-\frac{1}{2}by_1^{-1}\left(ay_0^{-2}y_1^{-1}-1\right)\right)+\\
&+(k-1)^2b^2\frac{1}{2}y_0^{-1}\left(-1+a^{-1}y_0y_1^2\right).
\end{aligned}$$

$$\begin{aligned}
y_{3k} &= \left(y_0+a^{-1}by_0^2y_1+b^2y_0^3y_1^2+a^{-1}b^2y_0y_1\right)+\\
&+k\left(b+a^{-1}b^2y_0y_1-\frac{1}{2}a^{-1}b^2y_0^2-\right.\\
&\left.-a^{-1}by_0^2y_1-2b^2y_0^3y_1^2-\frac{1}{2}a^{-1}b^2y_0y_1\right)+\\
&+k^2\left(-a^{-1}b^2y_0y_1-\frac{1}{2}a^{-1}b^2y_0^2+\right.\\
&\left.+b^2y_0^3y_1^2+\frac{1}{2}a^{-1}b^2y_0y_1\right).
\end{aligned}$$

$$\begin{aligned}
y_{3k+1} &= \left(y_1-a^{-1}b^2y_1^2\right)+\\
&+kb\left(\frac{1}{2}b\left(y_0^{-1}-a^{-1}y_1^2\right)+1-y_0^{-1}y_1\right)+\\
&+k^2b^2\frac{1}{2}\left(-y_0^{-1}+a^{-1}b^2y_1^2\right),
\end{aligned}$$

hold.

From representations of $\{y_n\}$ obtained above for the sequences (I) and (II) we infer (by Lemma 4)

Theorem 1. *Let $\{y_n\}$ be the sequence of PRN's produced by recursion (ℓ), $\ell = I, II$, where a is a quadratic nonresidue modulo p. Then,*

$$\begin{aligned}
&S_{\ell}^{(j)}(h;N)=\sum_{\substack{n=0\\ y_n\in(\ell)}}^{N-1}e^{2\pi i\frac{hy_n^j}{p^m}}\ll p^{\frac{m+\nu_0}{2}},\\
&j\in\mathbb{Z},\ (j,p)=(h,p)=1;
\end{aligned}$$

hold.

Theorem 2. *Let h_1, h_2 be arbitrary integers with $s = \nu_p(gcd(h_1, h_2, p^m))$, $s \leq m - \nu_0$. Then for the sequence $\{y_n\}$ produced by recursion (ℓ), $\ell = I, II$ and with a maximal period length $\tau = 3p^{m-\nu_0}$ we have*

$$K_{\ell}(h_1,h_2;N)=\sum_{\substack{n=0\\ y_n\in(\ell)}}^{N-1}e^{2\pi i\frac{h_1y_n+h_2y_n^{-1}}{p^m}}\ll p^{\frac{m+\nu_0+s}{2}}.$$

To prove the estimates for above sums it is enough to split the summation over n for two parts $n \equiv 0 \pmod 2$ and $n \equiv 1 \pmod 2$ for $\ell = I$ and, respectively, for three parts $n \equiv -1 \pmod 3$, $n \equiv 0 \pmod 3$ and $n \equiv 1 \pmod 3$ for $\ell = II$, and then apply Lemma 4.

Finally note that the more complicated sums over the sequences of PRN's of type (I) and (II) may be investigated.

Moreover, in this paper we consider only inversive generator of first and second orders. But this method can be applied to study the inversive generator of q^{th} order if $q < p$. Here, if parameter a is a nonresidue of $q + 1$ order modulo p then the sequence of PRN's has a maximal period $\tau = (q + 1)p^{m-1}$.

REFERENCES

[1] **J. Eichenauer and J. Lehn,** A non-linear congruential pseudo-random number generator, *Statist. Hefte*, **27** (1986), 315–326.

[2] **H. Niederreiter,** Some new exponential sums with applications to pseudo-random numbers, *Topics in Number Theory (Debrecen, 1974), Colloq. Math. Soc. Janos Bolyai, North-Holland, Amsterdam*, **13** (1976), 209–232.

[3] **H. Niederreiter,** On the cycle structure of linear recurring sequences, *Math. Scand*, **38** (1976), 53–77.

[4] **H. Niederreiter,** On the distribution of pseudo-random numbers generated by the linear congruential method, III, *Math. Comp*, **30** (1976), 571–597.

[5] **R. G. Stoneham,** On the uniform ε-distribution of residue within the periods of rational fractions with applications to normal numbers, *Acta Arith*, **22** (1973), 371–389.

[6] **Pavel Varbanets, Sergey Varbanets,** Inversive generator of the second order with a variable shift for the sequence of PRNs, *Annales Univ. Sci. Budapest., Sect. Comp*, **46** (2017), 255-273.

[7] **Tran Kim Thanh, Tran The Vinh, and Varbanets Sergey,** Generalization of inversive congruential generator with a variable shift, 11th CHAOS 2018 International Conference Proceedings, 5-8 June 2018, Rome, Italy, 2018 (to appear).

Divisor function on the Gaussian integers with given number of prime factors.

Yakov Vorobyov
Department of Mathematics, Informatics and Information Activity
Izmail State University of Humanities
Odessa, Ukraine
varb@sana.od.ua

***Abstract*—Consider the distribution of the divisor function values over the Gaussian integers with the fixed value of the count of prime divisors of such numbers in the narrow sectors. This problem is the special case of the early studied questions of the distribution the values of arithmetic functions over the subsequences of Gaussian integers that was being investigated in the work J. Kubilijus, J.-M. De Koninck and I. Katai. It has been obtained a nontrivial estimates of the error term of asymptotic formulas for summatory functions associated with the divisor function $\tau(\alpha)$ over the set of Gaussian integers with some growing number k, $k \to \infty$ of prime divisors of Gaussian integers. Moreover, there was studied the distribution of divisor function on the mentioned sequence of Gaussian integers in the narrow sectors.**

***Index Terms*—Gaussian integer, Hecke zeta-function, narrow sector, divisor function**

I. Introduction

Let G be the ring of Gaussian integers. Denote through $\mathfrak{P}$ the class of all multiplicative functions over G such that $f(\mathfrak{p}^a)$ depends only on a for all Gaussian prime powers $\mathfrak{p}^a$. The divisor function $\tau(\alpha)$, $\alpha \in G$, belongs to this class.

Here, we study the distribution of values of divisor function $\tau(\alpha)$ on the sequence of Gaussian integers, with given number of prime divisors for α, i.e. $w(\alpha) = k$, where $w(\alpha)$ is a number of prime divisors α.

A. Selberg [] (see also, Kybilius []) developed the method of construction the asymptotic formula for summatory functions associated with the number function of prime factors of positive integers. By using this method we study the distribution of values of divisor function $\tau(\alpha)$ when $\alpha \in G$ and $w(\alpha) = k$.

II. Auxiliary Results

We will use the following notations:

- $G := \left\{ a+bi \,\middle|\, a,b \in \mathbb{Z},\ i^2 = -1 \right\}$;
- for $\alpha \in G$ we denote $N(\alpha) = |\alpha|^2$;
- $Z_m(s)$ denotes the Hecke Z-function defined for $\Re(s) > 1$ by the Dirichlet series $\sum\limits_{0 \neq \alpha \in G} e^{4mi \arg \alpha} N(\alpha)^{-s}$, $m \in \mathbb{Z}$;
- symbol $\mathfrak{p}$ denotes a prime number from G;
- for $s \in \mathbb{C}$ we denote $\sigma = \Re(s)$, $t = Im(s)$, i.e. $s = \sigma + it$.

The main tool to proof the main results are the following lemmas.

Lemma 1. *For $0 \leq \sigma \leq 1$ we have*

$$Z_m(s) \ll \left(t^2+m^2\right)^{\frac{1-\sigma}{2}} \log^2\left(m^2+t^2\right),\ |t| > 3.$$

For $\dfrac{1}{2} \leq \sigma \leq 1$

$$Z_m(s) \ll \left(t^2+m^2\right)^{\frac{1-\sigma}{3}} \log^4\left(m^2+t^2\right).$$

Indeed, the first assertion is corollary of the functional equation for $Z_m(s)$ and the Phragmén-Lindelöf principle. The second bound for $Z_m(s)$ follows from the Kaufmann estimate for $Z_m(s)$ on the line $\Re(s) = \dfrac{1}{2}$ (see, Kaufmann []).

Lemma 2. *There exist absolute constants $0 < C_0 < 1$, $C_1 > 0$ such that the Hecke Z-function $Z_m(s)$ have no zeros in the region*

$$\Re(s) > 1 - C_0(\log(T+M))^{-\frac{2}{3}}(\log\log(T+M))^{-1},$$

where $T^2 + M^2 \geq C_1$, $|t| \leq T$, $|m| + 3 = M$.

(for proof, see []).

Lemma 3. *In the region*

$$\sigma \geq 1 - \frac{C_0}{2}(\log(T+M))^{-\frac{2}{3}}(\log\log(T+M))^{-1}, |t| \leq T,$$

where C_0 is the constant from Lemma, the following estimate

$$\log[Z_m(s)] \ll (|t|+|m|)^{-\frac{2}{3}} \log\log(|t|+|m|)$$

holds.

This assertion is an analogue of the associate estimate for $\zeta(s)$ (for details, see [**?**]).

Lemma 4. *For $n \in \mathbb{N}$ we have*

$$\ell_n = \int\limits_0^1 (cos 2\pi\varphi)^n \, d\varphi = \begin{cases} 0 & if\ n \equiv 1\,(mod\,2), \\ \dfrac{n-1}{n}\ell_{n-2}\, if\, n \equiv 0\,(mod\,2). \end{cases}$$

Lemma 5. *The Hecke zeta-function $Z_m(s;\delta_0,\delta)$ of the Gaussian field $\mathbb{Q}(i)$ satisfies the functional equation*

$$\pi^{-s}\Gamma(2|m|+s)Z_m(s;\delta_0,\delta) = \\ = \pi^{-(1-s)}\Gamma(2|m|+1-s)\cdot \\ \cdot Z_{-m}(1-s;\delta_0,-\delta)\, e^{-2\pi i \Re(\delta\delta_0)}.$$

Moreover, $Z_m(s;\delta_0,\delta)$ is an entire function if $m \neq 0$ or $m = 0$ and δ is not a Gaussian integer. For $m = 0$ and $\delta \in G$ it is holomorphic except for the point $s = 1$, where it has a simple pole with the residue π.

(To prove this lemma, see [1]).

III. Main Results

Consider the Dirichlet series

$$\mathfrak{F}_m(s,z)=\sum_{0\neq\alpha\in G}\frac{z^{w(\alpha)}\tau(\alpha)e^{4mi\arg\alpha}}{N(\alpha)^s},\ (z\in\mathbb{C}).$$

This series converges absolutely for $\Re(s)>1$.

We have for $\Re(s)>1$

$$\mathfrak{F}_m(s,z)=\prod_{\mathfrak{p}}\left(1+\frac{2ze^{4mi\arg\alpha}}{N(\mathfrak{p})^s}+\frac{3ze^{8mi\arg\alpha}}{N(\mathfrak{p})^{2s}}+\cdots=\right.$$

$$=\prod_{\mathfrak{p}}\left(1+\frac{ze^{4mi\arg\mathfrak{p}}\cdot N(\mathfrak{p})^s}{\left(N(\mathfrak{p})^s-1\right)^2}\right)=$$

$$=\left(Z_m(s)\right)^{2z}h(s,z), \tag{1}$$

where

$$h(s,z)=\prod_{\mathfrak{p}}\left(1-\frac{1}{N(\mathfrak{p})^s}\right)^{2z}\left(1+\frac{zN(\mathfrak{p})^s}{\left(N(\mathfrak{p})^s-1\right)^2}\right). \tag{2}$$

Obviously, $h(s,z)$ is an analytic function of complex variable s in semifinite plane $\Re(s)>\frac{1}{2}$, and its coefficients $b_n(z)$ of the Dirichlet series $h(s,z)=\sum_{n=1}^{\infty}\frac{b_n(z)}{n^s}$ satisfies the condition $b_n(z)\ll n^{\varepsilon}$ uniformly in z, $|z|\leq 3$, and m.

For $m\in\mathbb{Z}$ we denote

$$M_m(x,z)=\sum_{N(\alpha)\leq x}z^{w(\alpha)}\tau(\alpha).$$

We proved the following main theorem.

Theorem 1. *Let z be a complex number, $|z|\leq 1$. Then we have*

$$M_0(x,z)=\sum_{N(\alpha)\leq x}z_0^{w(\alpha)}\tau(\alpha)=$$

$$=\frac{x}{(\log x)^{1-2z}}\left(\frac{2\Psi_0(z)}{\Gamma(2z)}+\frac{\Psi_1(z)}{\log x}+\frac{\psi_2(z)}{(\log x)^2}\right)+$$

$$+\boldsymbol{O}\left(x\cdots\exp\left(-a\frac{(\log x)^{\frac{3}{5}}}{\log\log x}\right)\right)$$

with an absolute constant $a>0$ and some functions $\Psi_0(z)$, $\Psi_1(z)$, $\Psi_2(z)$, which are analytical for $|z|<2$.

The analytic functions described in Theorem 1 have the following form:

$$\Psi_0(z)=\frac{1}{2}G_0(1,z)=(L_0(1,\chi_4))^z\cdot\frac{1}{2}h(1,z). \tag{3}$$

$$\Psi_1(z)=\int_0^1 e^{-u}u^{1-2z}G_1(u,z)du, \tag{4}$$

where $G_1(u,z)$ is a particular function with the period $\delta_0\log x$ and restricted by an absolute constant. The first integral in (3) is a noncomplete Euler's $\Gamma-function$.

$$\Psi_2(z)=\frac{2\sin\pi z}{\pi}(z-1)\Psi_1(z). \tag{5}$$

For the case $m\neq 0$ we can study the function

$$M_m(x,z)=\sum_{N(\alpha)\leq x}z^{w(\alpha)}\tau(\alpha)e^{4mi\arg\alpha}.$$

Using the same reasoning as in Theorem 1 and taking into account that the Hecke Z-function is an entire function for $m\neq 0$, we can obtain the following theorem.

Theorem 2. *For $m\neq 0$ the following asymptotic inequality*

$$M_m(x,z)=\sum_{N(\alpha)\leq x}z^{w(\alpha)}\tau(\alpha)e^{4mi\arg\alpha}\ll$$

$$\ll\begin{cases}x\cdot\exp\left(-a_5(\log x)^{\frac{3}{5}}(\log\log x)^{-1}\right)\\ \qquad if\ |m|\leq T\\ \\ x\cdot\exp\left(-a_5\dfrac{\log x\exp\left(c_2(\log|m|)^{\frac{1}{2}}\right)}{(\log|m|)^{-\frac{2}{3}}(\log\log|m|)^{-1}}\right)\\ \qquad if\ |m|\geq T\end{cases}$$

holds.

(Here, $a_5=\frac{1}{2}a_4>0$).

Denote

$$M(x;\varphi_1,\varphi_2;z)=\sum_{\varphi_1\leq\arg\alpha\leq\varphi_2}z^{w(\alpha)}\tau(\alpha),\ 0\leq\varphi_1<\varphi_2\leq\frac{\pi}{2}.$$

Theorem 3. *Let $0\leq\varphi_1<\varphi_2\leq\dfrac{\pi}{2}$ and*

$$\varphi_2-\varphi_1\gg(\log x)^{1-2z}\exp\left(-a\left(\log x^{\frac{3}{5}}\left(\log\log x^{-1}\right)\right)\right).$$

Then for any $z\in\mathbb{C}$, $|z|\leq 1$, we have

$$M(x;\varphi_1,\varphi_2;z)=$$

$$=\frac{2(\varphi_2-\varphi_1)}{\pi(\log x)^{1-2z}}\left(\frac{2\Psi_0(z)}{\Gamma(2z)}+\frac{\Psi_1(z)}{\log x}+\frac{\Psi_2(z)}{(\log x)^2}\right)+$$

$$+\boldsymbol{O}\left(-a\frac{(\log x)^{\frac{3}{5}}}{\log\log x}\right),\ (a>0),$$

where $\Psi_0(z)$, $\Psi_1(z)$, $\Psi_2(z)$ defined by (3),(4),(5). Constant in symbol "$\boldsymbol{O}$" is absolute.

Further, we will use the following notations:

$$A_k(x,m)=\sum_{\substack{N(\alpha)\leq x\\ w(\alpha)=k}}{}'e^{4mi\arg\alpha};$$

$$A_k(x;\varphi_1,\varphi_2)=\sum_{\substack{w(\alpha)=k\\ N(\alpha)\leq x\\ \varphi_1<\arg\alpha\leq\varphi_2}}{}'1;$$

$$A_k(x,h;m)=\sum_{\substack{x<N(\alpha)\leq x+h\\ w(\alpha)=k}}{}'e^{4mi\arg\alpha};$$

$$B_k(x,h;\varphi_1,\varphi_2)=\sum_{\substack{w(\alpha)=k\\ x<N(\alpha)\leq x+h\\ \varphi_1<\arg\alpha\leq\varphi_2}}{}'1.$$

The following theorems are valid

Theorem 4. *Let $c(x)$ be a real function, moreover $c(x) \ll o\left((\log\log x)^{\frac{1}{2}}\right)$. Then*

$$A_k(x;\varphi_1,\varphi_2) = \frac{2}{pi}x(\varphi_2-\varphi_1)\cdot\frac{(\log\log x)^{k-1}}{(k-1)!}\times \\ \times\left(\frac{\Psi_0((k-1)(\log\log x)^{-1})}{\Gamma\left(1+(k-1)(\log\log x)^{-1}\right)}+\right. \\ \left.+\boldsymbol{O}\left(k^{\frac{3}{2}}(\log\log x)^{-2}\right)\right).$$

Theorem 5. *Let $x^{\frac{2}{3}+\varepsilon} \le h \le x$. Then, within notation of previous theorem, we have*

$$B_k(x,h;\varphi_1,\varphi_2) = \frac{2}{pi}h(\varphi_2-\varphi_1)\cdot\frac{(\log\log x)^{k-1}}{(k-1)!}\times \\ \times\left(\frac{\Psi_0((k-1)(\log\log x)^{-1})}{\Gamma\left(1+(k-1)(\log\log x)^{-1}\right)}+\right. \\ \left.+\boldsymbol{O}\left(k^{\frac{3}{2}}(\log\log x)^{-2}\right)\right)+ \\ +\boldsymbol{O}\left(h(\varphi_2-\varphi_1)(\log x)^{-2}(\log\log x)^{-\frac{1}{4}}\right).$$

Proofs of theorems 4 and 5 use the Theorem on zeros density of Hecke zeta-function and the following analogous of Ramachandra theorem:

Theorem 6. *Let in region $\Re(s) > 1$ we have for Dirichlet series*

$$F_m(s) = \sum_{\alpha}\frac{a(\alpha)}{(N^s(\alpha))}\exp\left(4mi\arg\alpha\right),\ m = 0,\pm1,\pm2,$$

with representation $F_m(s) = (Z(s,m))^z A_m(s,z)$, where $z \in \mathbb{Q}[i]$, $|z| < 2$, z is not depends on m, $A_m(s,z)$ is defined by Dirichlet series that is converges absolutely on $\Re(s) > \frac{1}{2}$. Also let $N_m(\sigma,T)$ be the number of zeros of $Z(s,m)$ within rectangle $\sigma \le \Re(s) \le 1$, $|\Im(s)| \le T$, and let D_0, D be some constants that is not depended on m, such that

$$N_m(\sigma,T) \ll (TM)^{3(1-\sigma)}(\log TM)^D,\ m \ne 0,$$
$$N_0(\sigma,T) \ll T^{(}\frac{12}{5}(1-))(\log T)^{D_0}.$$

Next define

$$S(x,h;\varphi_1,\varphi_2;z) = \sum_{\substack{x<N(\alpha)\le x+h\\ \varphi_1<\arg\alpha\varphi_2}} a(\alpha);$$

$$I(x,h;z) = \frac{1}{2\pi}\int\limits_0^h\left(\int\limits_{C_0(r)} F_0(s)(v+x)^{s-1}ds\right)dv;$$

$$r = C(\log x)^{-\frac{2}{5}}(\log\log x)^{-1}.$$

Then for $0 \le \varphi_1 < \varphi_2 \le \frac{\pi}{2}$, $\varphi_2-\varphi_1 \gg \exp\left(-C(\log x)^{\frac{1}{3}}(\log\log x)^{-1}\right)$ we have

$$S(x,h;\varphi_1,\varphi_2;z) = 2(\varphi_2-\varphi_1)\pi^{-1}I(x,h;z)+ \\ +\boldsymbol{O}\left(h\exp\left(-C(\log x)^{\frac{1}{3}}(\log\log x)^{-1}\right)\right)+ \\ +\boldsymbol{O}\left(x^{\frac{2}{3}+\varepsilon}\right).$$

References

[1] Balyas L., Varbanets P., *Quadratic residues of the norm group in sectorial domains*, Algebra and Discrete Mathematics, 22**2**, 2016, pp. 153–170.

[2] Coleman M.D., *A zero-free region for the Hecke L-functions*, Mathematika, 37, 1990, pp.287–304.

[3] Dadayan Z., Radova A., *Divisor function of the Gaussian integers*, Vestnik ONU, 17**4**, 2012, pp. 34–39.

[4] Kaufman R., *Estimate of Hecke L-function on the half-line*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI), 91, 1979, pp. 40–51 (in Russian).

[5] Kubilius J., Probabilistic Methods in Theory of Numbers. AMS Monographs, 1964.

[6] Selberg A., *Note on a paper by L.G. Sathe*, J. Ind. Math. Soc., 18**3**, 1954, pp. 83–87.

[7] Vinogradov I.M., Selected works. Springer-Verlag, 1985, 401 p.

INVESTIGATION OF THE PROPERTIES OF HYBRID CRYPT-CODE CONSTRUCTIONS

Bilodid I.V., *Department of Information Systems, Simon Kuznets Kharkiv National University of Economics* Kharkiv, Ukraine, bilodid.vanya@gmail.com

Yevseiev S.P., *Department of Information Systems, Simon Kuznets Kharkiv National University of Economics* Kharkiv, Ukraine, serhii.yevseiev@hneu.net

Komyshan A.S., *Department of Information Systems, Simon Kuznets Kharkiv National University of Economics* Kharkiv, Ukraine, anton.komishan@gmail.com

Tsyhanenko O.S., *Department of Information Systems, Simon Kuznets Kharkiv National University of Economics* Kharkiv, Ukraine, oleksii.tsyhanenko@hneu.**net**

***Abstract*— Mathematical justification of the forming hybrid crypto-code system on damaged code is considered. The purpose of the research is to study the effectiveness of using crypto-code structures in modern information and communication systems.**

Keywords—hybrid, non-symmetric crypto-systems, McEliece, elliptic codes.

I. INTRODUCTION

Damaged text is the text obtained by further deformation of non-existent letter codes. Thus, a necessary and sufficient condition for the damage of text with loss of meaning is the shortening of the lengths of the code symbols of the text beyond their redundancy [1]. As a consequence, the damaged text has a length shorter than the length of the source text, and there is no sense in the source text [3].

The purpose of the work is to analyze the main threats to the use of OTP passwords, to consider the basics of building multi-channel cryptography systems on defective codes, to provide a formal description of mathematical models of hybrid crypto-code constructions on defective codes (HCCDC), and to develop encryption / decryption algorithms in the proposed HCCDC.

To achieve the goal, consider the following tasks:

- Analysis of the main threats of using OTP passwords;

- Consideration of the basics of construction and ways of using multi-channel cryptography systems on damaged codes;

- a formal description of mathematical models of hybrid crypto-code constructions on defective codes based on the modified McEliece crypto-code systems (CCS) on elliptic codes;

- Development of practical algorithms for encryption and decryption of data in the McEliece HCCDC.

The theoretical basis for building damaged texts is to remove the ordering of the symbols of the source text and, as a consequence, to reduce the redundancy of the language symbols in the damaged text. In this case, the amount of information expressing this ordering will be equal to the decrease in the entropy of the text in comparison with the maximum possible entropy value corresponding to the lack of ordering in the text in general, i.e. equiprobable appearance of any letter after any previous letter. The methods of computing information proposed by K. Shannon allow us to determine the ratio of the amount of predictable information (ie, formed according to certain rules) and the amount of that unexpected information that can not be predicted in advance.

II. DAMAGED CODES

To restore the original sequence, there is no need to know the intermediate faulty sequences. It is necessary to know only the last damaged sequence (the last damaged text after all the cycles) and all the damages with the rules for their application.

Cryptographic damaged texts are texts obtained by the following methods [3]: damage to the source text with subsequent encryption of the damaged text and / or its damage; damage to the ciphertext; damage to the cipher text of the defective text and / or ciphertext of the damage. In work [1] methods of constructing the HCCSDC based on MCCS McEliece on MEC are considered.

III. FORMING OF HYBRID CRYPTO-CODE SYSTEM ON DAMAGED CODES

The length of the information sequence (in bits) arriving at the input of the cryptosystem from the SC is determined by the following expression: for HCCSDC on shortened codes: $l_I = l_z^c + l_z^f$, where $l_z^c = K_c \times L + \frac{1}{K_f} \times s -$ length of damaged text; $l_z^f = L + u \times s -$ length of damage; $s = \left[\frac{L_0 - L_{DT}}{L_{DT}} \right] -$ number of segments of the damaged text, $K_C = 1 - K_f \approx 0,758 -$ compression ratio of the remainder (damaged text) (at u = 8, v = 3, z = 5); $K_f = \frac{2 - 2^{v-u+1}}{u} \approx 0,242$ – coefficient of compression of the flag (damage) (at u = 8, v = 3, z = 5); $z = \frac{log(u \times L) - 7}{log(1/K_C)} -$ necessary for the randomization of the cipher MV2, the number of permissible conversion rounds. For HCCSDC on extended MEC: $l_I = 1/2k \times m + l_z^c + l_z^f$.

The length of the public key (in bits) is determined by the sum of the elements of the matrix G_X^{EC} and is given by the expressions: for HCCSDC on truncated MEC: $l_K = 1/2\,k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$; for HCCSDC on

extended MEC: $l_K = 1/2\,k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$. *The length of the private key* (in bits) is determined by the sum of the matrix elements *X, P, D* (in bits) and is given by expressions: for HCCSDC on shortened codes: $l_{K_+} = 1/2\,k \left| \log_2 \left(2\sqrt{q} + q + 1\right) \right| + \left|F_u^v\right|$, where $\left|F_u^v\right| = 2^u!$ – the cardinality of the set of substitution transformations; for HCCSDC on extended codes:

$$l_{K_+} = \left(1/2\,k - 1/2\,k\right) \left| \log_2 \left(2\sqrt{q} + q + 1\right) \right| + \left|F_u^v\right|$$

Redundancy of the text is calculated by the formula

$$B(M) = B_A L_0 = \left(log\, N - \frac{H(M)}{L_0} \right) \times L_0,$$

where M – original text;

B is the redundancy of the language ($B = R - r$, R is the absolute entropy of the language ($R = \log N$, N is the power of the alphabet, r is the language entropy by one character, and $r = H(M)/L$, L is the length of the M message in the language symbols);

H (M) is the entropy (uncertainty) of the message;

L_0 - the length of the message M in the symbols of the language with meaning;

B_A is the redundancy of the language.

To obtain a defective text (FTC) and damage (DCH), the "ideal" compression method is used after completing the m cycles of the damage mechanism Cm [1, 2].

The number of cycles necessary to reduce the length of the source text is:

$$m \rangle \frac{log\, n - B_A}{log\, \eta},$$

where n is the power of representing the symbol of the source text;

B_A - redundancy of the language;

η is the number of times the original text length in MV2 decreases at each step (some constant coefficient).

A quantitative measure of the effectiveness of damage is the degree of destruction of the meaning, equal to the difference in the entropies of the defective text and the source text at different lengths of the defective text:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i) p_i, \quad \sum_{i=1}^{s} p_i = 1, \quad s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}} \right],$$

where M_i is the part of the source text corresponding to the i-th segment, p_i is its probability,

L_0 - the length of M_i is equal to the length of LFTC - the defective text, s is the number of segments.

For an ergodic source of source code characters:

$$d_{max} = log\, L_{FTC} - H(M_i).$$

In M. 1 shows the structural diagram of one step of the universal mechanism of damage.

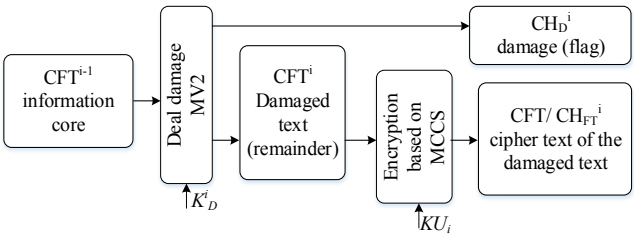


Fig. 1. Structural diagram of one step of the universal damage mechanism

Under the information core of some text is understood the damaged text of CFT, obtained by cyclic transformation of the universal mechanism of damage Cm.

Thus, as a result we have two ciphertexts (damage (CHD) and defective text (FTC)), each of which has no meaning either in the source code alphabet or in the alphabet of the ciphertext. In fact, the ciphertext of the original message (M) is represented as an aggregate of two defective ciphertexts, each of which can not individually restore the original text.

To restore the original sequence, there is no need to know the intermediate faulty sequences. It is necessary to know only the last damaged sequence (the last damaged text after all the cycles) and all the damages with the rules for their application. The main methods of damage are shown in Fig. 1. Cryptographic damaged texts are texts obtained by the following methods [2]:

damage to the source text, followed by encryption of the damaged text and / or its damage;

damage to the ciphertext;

damage to the cipher text of the defective text and / or ciphertext of the damage.

The main advantage in the proposed methods and protocols for the provision of security services based on the use of defective codes is the use of BSC, and MCCS McEliece, to ensure the cryptographic strength of damage and / or defective text.

To evaluate the cryptographic strength of the authors [1, 2], it is proposed to use the Shannon concept of the "uniqueness distance" of the cipher in the open text - the minimal natural number L, in which the corresponding message is uniquely restored by the well-known ciphertext, and the "uniqueness distance" by the key is the minimal natural number L , in which the encryption key is uniquely determined by the well-known encryption code.

The uniqueness distance for a random cipher model for which there is a probability of obtaining meaningful text with a random and equiprobable choice of the key K and an attempt to decipher the ciphertext, with

$$N_S = H(K) \frac{2^{HL}}{|I|^L} = 1$$

:

$$L = U_0 = \frac{H(K)}{log|I| - H} = \frac{H(K)}{B\, log|I|},$$

where L is the redundancy of the source text;

H is the entropy on the letter of the meaningful text in the input alphabet I, | I | > 2, 2^{HL} - an approximate value of the number of meaningful texts.

In [1, 2], under the cyclic algorithm for obtaining defective texts, we mean the universal damage-causing mechanism (Cm, where m is the number of cycles), which consists in the random replacement of the bit representation of each symbol of the source text by a tuple of a smaller or equal number of bits followed by their concatenation.

The domain of definition of the transformation in the algorithm MV2 - the set {0, 1} n - is considered as the power of the alphabet of some family of source texts, to which some probability distribution of the letters of this alphabet is related, and the symbols of the source text are the values of the discrete random element [24].

Let X be a random discrete element taking values with probabilities pi and an arbitrary fixed transformation MV2. Then for any $y \in U_{r\,n-l}$ (some binary string of a set of strings of variable length) and for any $1 \le i \le |y|$ one is fulfilled:

$$\#\left\{x \in \{0,1\}^n : c(x) = y\right\} = \#\left\{x \in \{0,1\}^n : c(x) = y^{(i)}\right\}$$

Then, regardless of the probability distribution of the random element X for the entropies of random elements FTC / FTCH (damaged ciphertext) and CHD (damage), the following equalities hold:

$$H(FTC / FT_{CH}) \le log(2^n - 2^r),$$
$$H(CHD) \le log(n - r + 1).$$

Thus, with a uniform distribution of the inputs (flags) of the MV2 algorithm

a uniform distribution of the output (residue) is formed:

$$P(c_k = 0 \,|\, 0 \le k \le \|FTC / FT_{CH}\|) = \frac{1}{2}$$

Multichannel cryptography on the basis of defective codes allows the integration of cryptographic systems, combining crypto-code constructions (MCCS McEliece) and systems on defective codes under one concept, which, complementing each other, will provide the required safety and reliability indicators, and enrich the total system with its properties .

The analysis of the methods of harming showed that, for use in the IOS, the first method is the most suitable: damage with subsequent crypto-conversion, which allows to reduce the power of the alphabet when creating a cryptogram in MCCS McEliece.

For carrying out statistical studies of the stability of the cryptosystems under study, we will use the NIST STS 822 package. The results of the studies are presented in Table.1.

Table 1 The results of the studies

Algorithm	**The number of tests in which more than 99% of the sequences have been passed**	**The number of tests in which more than 96% of the sequences have been passed**	**The number of tests in which less than 96% of the sequences have been passed**
HCCS	149 (78,83%)	189 (100%)	0 (0%)
HCCS on shortened codes	151 (79,89%)	189 (100%)	0 (0%)
HCCS on extended codes	152 (80,42%)	189 (100%)	0 (0%)
HCCSDC on shortened codes	153 (80,95%)	189 (100%)	0 (0%)
HCCSDC on extended codes	155 (82 %)	189 (100%)	0 (0%)

Table 1 demonstrated that despite the reduction in the power of the Galois field to GF (2^6) for the MNCCS and GF (2^4) for the GKKUKK, the statistical characteristics of such crypto-code structures turned out to be at least as good as the traditional McEliece MNCC on GF (2^{10}) . All cryptosystems passed 100% of NIST tests, the best result was shown by GCACC on shortened MES: 155 of 189 tests were passed at the level of 0.99, which is 82% of the total number of tests. At the same time, the traditional McEliece NKCC on the GF(2^{10}) passed 149 tests at the level of 0.99.

IV. CONCLUSIONS

Considered methods for constructing hybrid crypto-code constructions with defective codes (HCCSDC) based on the synthesis of modified non-symmetric crypto-code systems McEliece (MNCCS) on elliptic codes (EC) with multi-channel cryptographic systems on damaged codes, exchange protocols for securing confidentiality in IP networks. Theoretical bases of decrease in 2 - 3 times power capacity of MCCS McEliece with EC and hybrid structures of MCCS with damaged codes due to reduction of power of the Galois field. The required level of cryptographic strength of the hybrid cryptosystem whole is provided for their software implementation.

REFERENCES

[1] Evseev S., Korol O., Rzaev H., Smanova Z. Development of a modified asymmetric McEliece crypto-code system on shortened elliptic codes. // Eastern-European Journal of Eenterprise Technologies. – 2016. – P. 18-26

[2] Mishchenko V., Vilansky Y. Damaged texts and multichannel cryptography. // Encyclopedics. – 2007. – P. 292

[3] Evseev S., Korol O., Koc G. Building hybrid security systems based on crypto-code structures and damaged codes. // Eastern-European Journal of Eenterprise Technologies. – 2017. – P. 4-22

Исследование и модификация алгоритмов в задачах классификации и прогнозирования

Влад Кривонос
кафедра математического обеспечения компьютерных систем
Одесский национальный университет им. И.И. Мечникова
Одесса, Украина
krivonos.vladislav@stud.onu.edu.ua

Ирина Шпинарева
кафедра математического обеспечения компьютерных систем
Одесский национальный университет им. И.И. Мечникова
Одесса, Украина
ishpinareva@gmail.com

Research and modification of algorithms in classification and forecasting

Vladislav Krivonos
Department of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
krivonos.vladislav@stud.onu.edu.ua

Irina Shpinareva
Department of Mathematical Support of Computer Systems
Odessa I.I. Mechnikov National University
Odessa, Ukraine
ishpinareva@gmail.com

Аннотация – В работе ставится цель исследования и модификация алгоритмов в задачах классификации и прогнозирования. В задачах классификации рассмотрен алгоритм KNN. В качестве предметной области выступает выборка об уровне развития информационных технологий в странах мира. Результаты модификаций описывают качество реализованного алгоритма, также, для наглядности представлены графики результатов тестирования. В задачах прогнозирования рассмотрен алгоритм SLIQ. В результате проведенного анализа строится теоретическое предположение о результатах модификаций данного алгоритма.

Abstract – The aim of the research is to study and modify algorithms in problems of classification and forecasting. In the classification problems, the KNN algorithm is researched. As a subject area the level of development of information technology in the countries of the world is chosen. The results of the modifications describe the quality of the implemented algorithm, and also, for clarity, the results of the test results are presented in graphs. In the forecasting problems, the SLIQ algorithm is researched. As a result of the analysis, a theoretical assumption is made about the results of modifications of this algorithm.

Ключевые слова – исследование; модификация алгоритмов; классификация; прогнозирование; KNN; SLIQ; метрика; нормализация; выборщик; машинное обучение; метод k ближайших соседей; анализ; выборка; алгоритм;

Keywords—research; modification of algorithms; classification; forecasting; KNN; SLIQ; metrics; normalization; elector; machine learning; the nearest-neighbor method; analysis; sample; algorithm;

ВВЕДЕНИЕ

На данный момент, объемы информации накопленные человечеством достигают невероятно крупных размеров, и существует необходимость разнообразной обработки этих данных. Необходимость выявления разного рода зависимостей в больших объемах информации достаточно высока в связи с необходимостью улучшать существующие системы используя накопленные данные. Для выявления новых знаний и неочевидных зависимостей применяются разнообразные методы Data Mining. Рассмотрим задачи классификации и прогнозирования.

В задаче классификации существует определённое множество экземпляров. Каждый екземпляр относится к одному из возможных классов. Задано определенное множество экземпляров, заранее распределенных по классам. Это множество носит название «обучающая выборка». Оно служит для дальнейшего обучения алгоритма. Классы остальных экземпляров неизвестны. Задача - построить определенный алгоритм или метод, который сможет классифицировать любой экземпляр из начального множества.[1]

В задаче прогнозирования установливается функциональная зависимость между зависимыми и независимыми переменными. Прогнозирование направлено на определение тенденций динамики конкретного объекта или события на основе ретроспективных данных, т.е. анализа его состояния в прошлом и настоящем. Таким образом, решение задачи прогнозирования требует некоторой обучающей выборки данных.Задача прогнозирования подразумевает под собой выбор следующих компонент: метод прогнозирования; модель прогнозирования. Метод прогнозирования представляет собой последовательность действий, которые нужно совершить для получения модели прогнозирования. Модель прогнозирования есть функциональное представление, адекватно описывающее исследуемый процесс и являющееся основой для получения его будущих значений.

Исходя из формального определения этих двух задач, они не выглядят очень схожими, однако решаются одними и теми же алгоритмами, различаясь при этом лишь способом применения данных алгоритмов.

Целью данной работы является исследование алгоритмов и возможных модификаций этих алгоритмов в задачах классификации и прогнозирования.

I. Модифицированный алгоритм k ближайших соседей.

Рассмотрим алгоритм метрической классификации «k ближайших соседей» для задачи классификации рейтинга стран. В качестве предметной области выступает выборка об уровне развития информационных технологий в странах мира. Изначальная выборка содержит информацию о 111 странах, которые характеризуются следующими параметрами:название и код страны;количество ПК на 1000 жителей;количество пользователей Интернет на 1000 жителей; количество хостов Интернет на 100000 жителей; годовой доход от сферы телекоммуникаций и годовые инвестиции в сферу телекоммуникаций. В качестве классов выступают следующие уровни развития: Высокий (High), Средний (Medium), Низкий (Low).

Основная идея метода k ближайших соседей заключается в присвоении новому объекту класса наиболее распространенного среди ближайших соседей данного элемента.

Соседи выбираются из множества, уже классифицированных объектов, и, исходя из количественного значения k, высчитывается преобладание одного из классов среди соседей. Каждый объект имеет конечное количество атрибутов (размерностей). Предполагается, что существует определенный набор объектов с уже имеющейся классификацией.

Далее рассмотрим задачу определения дистанции. Классический вариант определения дистанции – дистанция в евклидовом пространстве. При таком способе во внимание принимается не только количество попавших в область определенных классов, но и их удаленность от нового значения.

В исходном виде модель алгоритмов kNN крайне бедна. Она имеет только свободный параметр k, да и тот дискретный с небольшим числом разумных альтернатив. Для обогащения модели необходимо вводить веса объектов и/или параметризовать способ вычисления метрики.

В работе предлагается улучшить данный алгоритм путём проведения анализа и улучшения трёх его основных блоков. Этими блоками являются: блок обработки входных данных, блок метрик и блок выборщика. Опишем возможные изменения в каждом из данных блоков.

A. *Блок обработки входных данных*

Первая фаза включает в себя нормализацию входных параметров. Реализовано два варианта нормализации. Первый вариант это стандартная нормализация – приведение всех параметров к промежутку [0,1], путем деления каждого входного параметра на максимальное значение соответствующего параметра среди всей выборки. Второй – минимаксная нормализация. Данный вариант нормализации описывается формулой.

$$MinMaxNorm(X) = \frac{(X - minX)}{(maxX - minX)},$$

Вторая фаза заключается в выборе весовых коэффициентов для параметров объектов выборки. Используется 2 метода: метод скользящего контроля; метод отжига.

B. *Блок метрик*

В данном блоке решается задача выбора метрики. Стандартной для алгоритма KNN является Евклидова метрика. Однако существует ряд других метрик конкурирующих с данной.

Манхэттенская метрика или расстояние городских кварталов. По сравнению с евклидовым расстоянием влияние отдельных больших разностей (выбросов) уменьшается, так как они не возводятся в квадрат.[2]

Расстояние Минковского (метрика Минковского) – параметрическая метрика на евклидовом пространстве, которую можно рассматривать как обобщение евклидова расстояния и расстояния городских кварталов.

C. *Блок выборщика*

Стандартный выборщик класса для контрольного объекта в алгоритме KNN пользуется принципом большинства. Модифицировать данный блок можно с помощью учёта расстояния до объектов. Название такого метода «взвешенное голосование».

Данный метод предполагает учет расстояния до нового экземпляра. Чем меньше расстояние от нового экземпляра до принимающего в голосовании участие элемента, тем более значимый голос этого элемента. Голоса подсчитываются по формуле:

$$Vote(class) = \sum_{i=1}^{n} \frac{1}{d^2(X, \mathrm{Yi})},$$

где $d^2(X, \mathrm{Yi})$ – квадрат расстояния от заранее классифицированной записи Yi до новой X, n – количество классифицированных записей класса, для которого идёт подсчёт голосов, class – имя класса.

Новому экземпляру будет присвоен класс, победивший в голосовании. При этом снижается вероятность набора одинакового количества голосов несколькими классами. Очевидно, что если k=1, то новый экземпляр по сути не проходит процесс голосования, а перенимает класс у ближайшего соседа.

D. *Результаты.*

Обучение алгоритма происходило на обучающей выборке, и результаты работы алгоритма на этой выборке представлены на рис.1. Целью обучения является отладка алгоритма и проверка его работоспособности с разными параметрами.

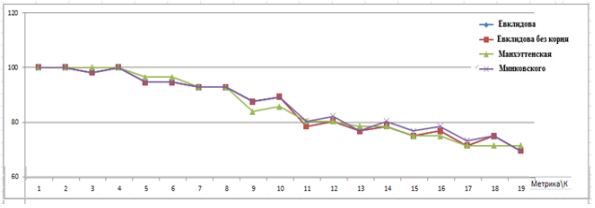


Рис 1. Обучение алгоритма на обучающей выборке с различными метриками

После отладки работы алгоритма, целью стал выбор наиболее подходящих коэффициентов и определение наиболее результативной метрики. Однако для объективной оценки данных параметров необходимо было провести ещё ряд тестов. Тесты на контрольной выборке представлены на рис. 2. Наилучшим – будем считать тот набор коэффициентов при котором k – наименьшее, а качество классификации наибольшее, т.е. если две разные метрики дали одинаковый результат классификации, но одна из них показала этот результат при меньшем k – то она считается лучшей. И по результатам данных тестов наилучшим образом себя показала Манхэттенская метрика, с коэффициентом k=5.

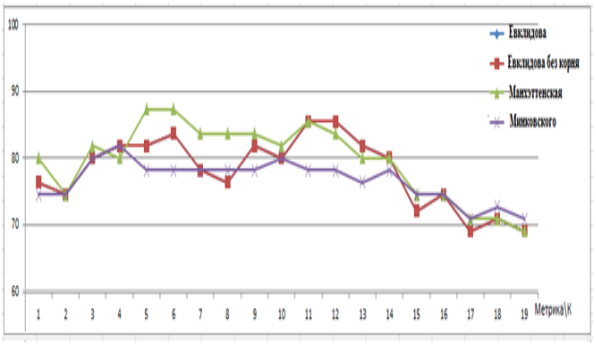


Рис.2. Результаты тестирования алгоритма на контрольной выборке с разными метриками

С учётом всех введённых модификаций, подбора коэффициентов и выбора метрик финальный вариант алгоритма показал результаты, представленные на рис. 3.

Из полученных данных следует, что на контрольной выборке введение модификаций приводит к улучшению качества и стабильности работы алгоритма при различных k. Максимальное качество классификации повысилось с 89% до 96%.

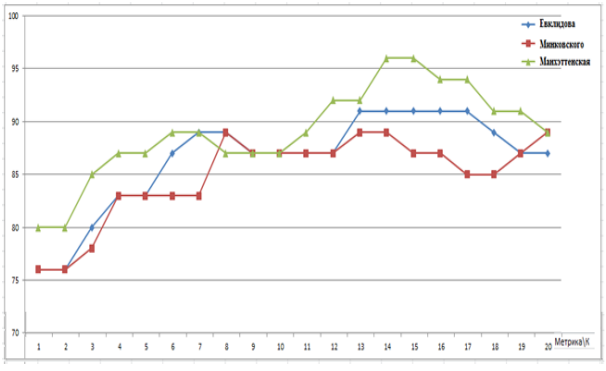


Рис. 3. Результаты тестирования финального алгоритма на контрольной выборке

Минимальное качество классификации повысилось с 65% до 76%. Среднее значение качества классификации также повысилось с 74.6833% до 86.8%. Таким образом, влияние модификаций на изначальный алгоритм привело к улучшению качества работы алгоритма в среднем на 10-12%.

II. Алгоритм SLIQ

Задачи прогнозирования и задачи классификации решают методами машинного обучения, к которым относятся алгоритмы рассматриваемые в данной работе. Модификация алгоритма к-ближайших соседей привело к улучшению результатов решения задачи классификации. Следовательно, можно предположить, что и алгоритмы используемые в задачах прогнозирования, могут быть модифицированы и улучшены.

В задачах прогнозирования рассмотрим алгоритмы построения дерева решений. Существует огромное количество методов, позволяющих создавать деревья решений. Основными считаются алгоритмы ID3, C4.5, CART, MARS. Для обработки больших данных был разработан и описан метод SLIQ.[3]

Алгоритм SLIQ обладает следующей структурой, описанной в [3]:

- предварительная сортировка данных;
- построение дерева, ветвление;
- отсечение ветвей.

На этапах построения дерева и отсечения ветвей возможен выбор в пользу тех или иных алгоритмов и методов, или их модификаций. Опишем каждый из этапов и возможные модификации к ним.

A. Этап предварительной сортировки данных

На данном этапе происходит разбиение изначальной таблицы данных обучающей выборки на компонующие её таблицы, состоящие ровно из двух столбцов, столбца атрибута и столбца индекса класса к которому он относится. При этом данные в этих компонующих таблицах должны быть отсортированы по возрастанию. В дополнение к этому строится таблица соответствий классов к листьям дерева, на начальном этапе все классы будут относиться к корню дерева, в последствии эта таблица будет модифицироваться для соответствия решающему дереву.

B. Этап построения дерева

На этапе построения дерева существуют три проблемы решение которых определяет качество работы алгоритма, а именно: выбор атрибута, выбор значения разбиения и правило остановки.

C. Проблема выбора атрибута

В проблеме выбора атрибута не существует оптимального алгоритма или метода, который бы обеспечивал максимально оптимально построенное дерево за приемлемое время. Однако, были разработаны два критерия, оба из которых следуют правилу поиска локального оптимального решения в каждом узле, обеспечивая создание дерева за приемлемое время. Такими критериями являются статистический критерий и теоретико-информационный критерий.

Критерий на основании статистики изначально использовался в алгоритме CART и носит название индекса Gini. Он создан для оценки фактического расстояния между группами классов, и описан следующей формулой:

$$\mathrm{Gini(c)} = 1 - \sum_{j=1}^{n} p_j^2 \quad (1)$$

где c – текущий узел, n – количество классов, p_j – вероятность класса j в узле c.

Теоретико-информационный критерий используется в алгоритме C4.5 и создан для выбора наиболее успешного алгоритма по следующей формуле:

$$Gain(X) = Info(T) - Info_x(T) \quad (2)$$

где Info(T) – энтропия множества, а

$$Info_x(T) = \sum_{i=1}^{n} \frac{|T_i|}{|T|} * Info(T_i) \quad (3)$$

множества T1, T2, ... Tn получены из исходного множества T, разбитого по критерию X. Выбирается атрибут, который по результату формулы (2) получил максимальное значение .[3]

D. Проблема выбора значения разбиения

Данная проблема в классических задачах решается методом перебора всех возможных значений выбранного атрибута в узле дерева, после чего, по описанным выше критериям, определяется насколько удачным было такое разбиение и берётся следующее значение атрибута. В результате выбирается наиболее удачное разбиение. В качестве модификации данного способа, предлагается использование случайных чисел для ускорения процесса нахождения максимально оптимального значения критериев в узле. Так же возможен вариант бинарного разделения множества возможных значений выбранного атрибута для поиска оптимального значения.

E. Проблема выбора правила остановки

Правило остановки должно отвечать на вопрос о том стоит ли продолжать разбиение узла или завершить разбиение для данного узла. В качестве модификации основного метода предлагаются следующие вспомогательные правила.

Метод ранней остановки (preprunning). Данный метод основывается на статистических данных для выявления необходимости дальнейшего разбиения. Таким образом, достигается уменьшение времени обучения. Однако стоит заметить, что при использовании данного подхода получаются менее точные деревья, следовательно этот метод нежелательно использовать. Признанные авторитеты в этой области Л.Брейман и Р. Куинлен советуют буквально следующее: "Вместо остановки используйте отсечение"[3].

Также можно ограничить глубину дерева. Под этим подразумевается остановка дальнейшего построения после превышения определенной глубины. Разбиение обязано быть нетривиальным. Это значит, что узлы, получившиеся в результате такого разбиения, должны группировать определенное количество экземпляров.

Каждое из данных правил является эвристическим. Следовательно, не существует такого, которое бы имело большую практическую ценность. Таким образом, стоит использовать то или иное правило в зависимости от контекста, то есть от конкретного частного случая.

F. Этап отсечения ветвей

На этапе отсечения ветвей выполняется усечение дерева путём откидывания или замены ветвей на более компактные. Необходимость данного этапа заключена в эффекте переобучения. В результате этого эффекта получается слишком ветвистое дерево. Это дерево отлично классифицирует обучающую выборку, однако является слишком большим и непригодным для использования на новых данных. Основное правило, которым руководствуются методы отсечения, звучит следующим образом: «отсекать или заменять поддеревом ветвь, если это увеличит ошибку».

Иногда, даже после процесса усечения, деревья могут быть слишком объемны и не информативны. Тогда, стоит использовать методику сбора метаданных из дерева извлекая наборы правил, описывающих представленные классы.

Метод, который извлекает правила, исследует все возможные пути из корня дерева до листа. Каждый проход сформирует правило, в котором условия будут формироваться из проверок внутри каждого узла на пути от корня до листа.[3]

Учитывая проведённый анализ алгоритма KNN, и примененные модификаций на этапах обработки входных данных, выбора метрики и определения выборщика, результатом которых является общее улучшение классификации на 10-12%. Предполагается, что введение модификаций в алгоритм SLIQ на этапах построения дерева, выбора атрибута, выбора значения разбиения и отсечения ветвей должно привести к улучшению работы алгоритма.

Литература

[1] В.О.Кривонос, І.М.Шпінарева "Автоматична класифікація об'єктів з дискретними параметрами" Інформатика, інформаційні системи та технології: XIV Всеукраїнська конференція студентів і молодих науковців. Одеса, 14 квітня 2017 р. – Одеса: ПНПУ ім. К.Д. Ушинського, ОНУ ім. І.І. Мечникова 2017. − С. 160

[2] Методы многомерных классификаций [Online]. Available: http://iopscience.iop.org/article/10.1086/376847

[3] Алгоритм SLIQ [Online]. Available: http://sci2s.ugr.es/keel/pdf/algorithm/congreso/SLIQ.pdf

REFERENCES

[1] V.Kryvonos, I. Shpynareva "Automatic classification of objects with discrete parameters " Informatics, information systems and technologies: XIV All-Ukrainian Conference of Students and Young Scientists. Odessa, 14 april 2017 y. – Odessa: PNPU KD Ushinskogo, ONU Mechnikova 2017. − C. 160

[2] Methods of multidimensional classifications [Online]. Available: http://iopscience.iop.org/article/10.1086/376847

[3] SLIQ algorithm [Online]. Available: http://sci2s.ugr.es/keel/pdf/algorithm/congreso/SLIQ.pdf

Анализ качества электронного определителя на основе унифицированного подхода

Татьяна Петрушина
Кафедра математического обеспечения компьютерных
Одесский национальный университет имени И.И.Мечникова
Одесса, Украина
tatyana.petrushina@gmail.com

Наталия Трубина
Кафедра математического обеспечения компьютерных
Одесский национальный университет имени И.И.Мечникова
Одесса, Украина
nftrubina@gmail.com

Quality analysis of the computer identifier based on a unified approach

Tatiana Petrushina
Mathematical software of computer system
Odessa National University by I.I. Mechnikov
Odessa, Ukraine
tatyana.petrushina@gmail.com

Natalia Trubina
Mathematical software of computer system
Odessa National University by I.I. Mechnikov
Odessa, Ukraine
nftrubina@gmail.com

***Аннотация*—Исследование посвящено проблемам моделирования определителя на основе унифицированного подхода к построению классификатора и повышению качества определителя путем его анализа методами Data Mining. Рассмотрены основные компоненты структуры классификатора и определителя, общепринятые подходы к диагностике - определению положения объекта в системе классификации. Сформулированы основные требования к построению унифицированной модели классификатора и определителя на его основе. Предложен подход к оценке качества определителя на основе применения методов Data Mining. На примере разнородных предметных областей получены оценки полноты набора ключевых признаков; проведен анализ оценки качества построенной иерархии признаков; проанализирован набор ключевых признаков для определения их полноты и непротиворечивости. Приведены результаты анализа определителя, построенного для такой нетрадиционной области, как стили модной одежды. Описаны некоторые новые, интересные результаты, полученные на основе этого анализа, в результате чего предложено внести изменения в структуру определителя.**

***Abstract*—The research is devoted to the problems of modeling an identifier (qualifier) on the basis of a unified approach to constructing a classifier, and improving the quality of an identification (diagnosis) by analyzing it using Data Mining methods. The main components of the structure of the classifier and identifier are considered, generally accepted approaches to determining the position of the object in the classification system. The basic requirements for the construction of a unified model of a classifier and an identifier based on it are formulated. An approach to assessing the quality of an identifier based on the application of Data Mining methods is proposed. Estimation of completeness of a set of key characteristics is obtained on the example of dissimilar subject domains; an analysis of the quality assessment of the built-in feature hierarchy is performed; a set of key characteristics is analyzed to determine their completeness and consistency. The results of the analysis of the identifier constructed for such an unconventional area as styles of fashionable clothes are presented. Some new, interesting results obtained on the base of this analysis are described, as a result, it was proposed to make changes in the structure of the identifier.**

Ключевые слова — классификатор, определитель, унифицированная модель данных, иерархическая структура, ключевые признаки, Data Mining, таксон

Keywords— classifier, identifier, unified data model, hierarchical structure, key characteristics, Data Mining, taxon

I. ВВЕДЕНИЕ

Современные информационные системы предоставляют самый широкий доступ к информации. Однако для того, чтобы эта информация была востребована и найдена – она должна быть хорошо структурирована и корректно организована. Задача адекватной структуризации информации предметной области является одной из основных задач экспертов.

Одной их основных целей структуризации информации является классификация объектов, то есть система распределения объектов по классам в соответствии с его свойствами. Классификация должна устанавливать закономерные связи между классами объектов с целью определения места объекта в системе по некоторым его признакам.

Другая задача классификации – диагностика или определение, то есть идентификация неизвестного объекта с каким-либо элементом этой системы. Для решения этой задачи применяются так называемые определители, позволяющие по набору ключевых признаков осуществлять поиск места объекта в системе. Данная задача особенно актуальна при построении определителей для различных каталогов. В

традиционных предметных областях таких, как биология, минералогия, и т.п. построение качественных определителей зачастую является основой научного исследования этой предметной области. Для новых предметных областей такая работа могла вообще ранее не выполняться, либо может быть не завершена.

При построении определителя важно использовать формальные методы оценки его качества, что не всегда может быть обеспечено экспертом. Кроме того, наличие инструментов на основе этих методов позволило бы значительно облегчить работу эксперта. Для того, чтобы предложить подобные инструменты для любых предметных областей необходим унифицированный подход к построению классификатора (каталога) и определителя.

II. УНИФИЦИРОВАННАЯ МОДЕЛЬ ОПРЕДЕЛИТЕЛЯ

Использование электронных определителей позволяет сделать процесс определения более коротким, понятным и простым за счет сокращения числа шагов определения ввиду возможности выбора на каждом шаге нескольких ключей (многовходовый ключ), каждый из которых может иметь более двух значений (политомический ключ). Такой процесс не характерен для печатных изданий определителей, где используются одновходовые дихотомические ключи. Политомические ключи упрощают процедуру сравнения таксонов, установления сходств и различий между ними, облегчают выявление синонимов и антонимов. Оптимальность применения многовходового политомического ключа для электронных определителей бала обоснована А.Л.Лобановым [1, 2].

Задача состоит в том, чтобы унифицировать подход и обеспечить возможность применения его для разнородных прикладных областей.

Как показывает проведенный авторами анализ, у разных предметных областей присутствую общие черты, такие как: иерархическая классификация (таксономия объектов) (МКБ - 10, Определитель позвоночных животных); прослеживаются общие атрибуты, такие как: наименование, синонимы, ключевые признаки, названия на разных языках; определение объекта происходит всегда по набору ключевых признаков. Некоторые свойства предметных областей представлены в таблице 1.

Таблица 1. Сравнительная характеристика предметных областей

	Наличие электронных определителей	Наличие иерархической структуры номенклатуры	Поддержка многоязычности	Тип ключа (одновходовый / многовходовый)	Число состояний признаков (2 – дихотомический ключ, 3 – политомический ключ)	Количество таксонов
Медицина						
МКБ - 10 [3]	-	+	+	1	2	21
Биология						
Определитель растений Республики Тыва [4]	-	+	+	1	2	2013
Определитель цветковых растений «Плантариум» [5]	+	+	-	N	3	69
Полевой определитель птиц фауны Украины [6]	-	+	-	1	2	416
Определитель птиц Великобритании						408
Определитель наземных моллюсков Украины [7]	-	+	-	1	2	211
Библиография						
УДК [9]	-	+	+	1	2	126441
ББК [10]	-	+	+	1	2	2000+
Минералогия						
Каталог-определитель минералов и горных пород [11]	-	+	+	1	2	130
Химия						
Определитель химических веществ: неорганическая химия [12]	-	+	+	1	2	-
Мода						
Энциклопедия моды [13]	+	-	+	-	-	56
Сайт о стилях одежды «Style She» [14]	-	-	-	-	-	25

В основу электронного определителя удобно положить использование многовходового политомического ключа с иерархической организацией. Такой ключ обладает рядом преимуществ:

- возможность расширения определителя без его перестройки;
- возможность использовать для определения признаки, имеющие перекрывающиеся состояния у изменчивых таксонов;
- значительно меньшее число поисковых ходов, позволяющих установить таксономическую принадлежность исследуемого объекта;
- высокая надежность работы определителя.

Построение определителя предполагает общий подход к моделированию данных в информационной системе, а также некоторые общие принципы организации поиска и интерпретации результатов на основе этой модели[15].

Модель данных (рисунок 1) должна состоять из таких основных объектов как номенклатура, ключевые признаки, которые имеют иерархическую структуру, а также набор значений ключевых признаков.

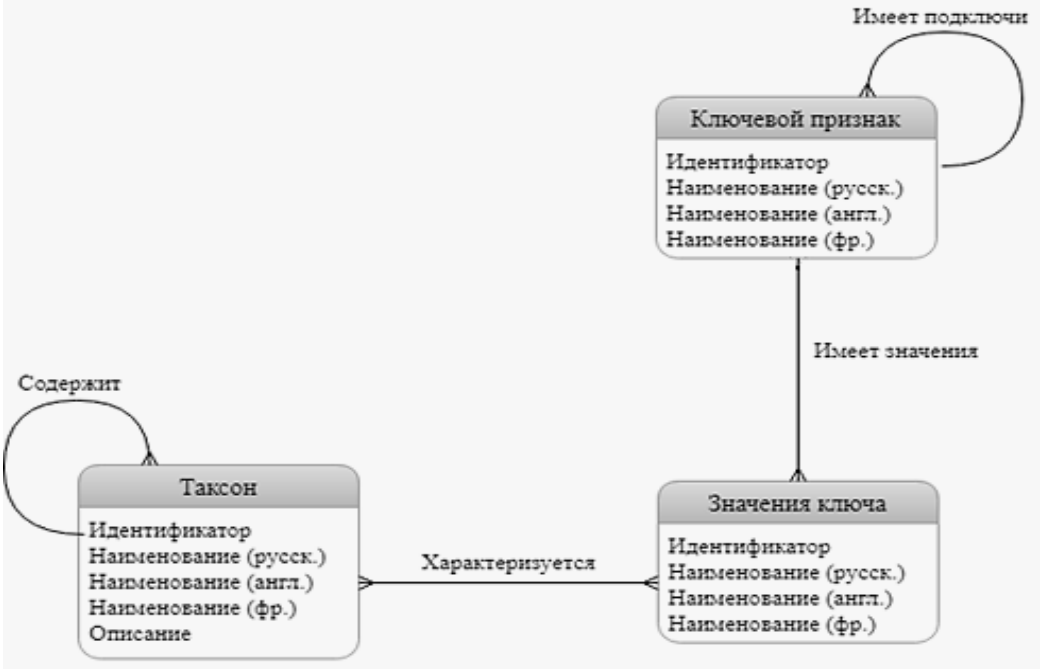


Рис. 1. Концептуальная модель данных абстрактного определителя

Объект Таксон описывает свойства таксона, такие, как его уникальный идентификатор, наименование на нескольких языках, описание таксона и др. Объект Таксон содержит в себе подтаксоны, т.е. таксоны нижнего уровня. Иерархия реализуется посредством связи «содержит» типа «один-ко-многим».

Объект «Ключевой признак» описывает характеристики ключевых признаков, такие как уникальный идентификатор и наименование на нескольких языках (русский, английский, французский). Ключевой признак имеет одно или несколько значений, однако каждое значение может принадлежать только одному ключевому признаку.

Ключевой признак может содержать подключи, т.е. ключи нижнего уровня. Иерархия реализуется посредством связи «имеет подключи» типа «один-ко-многим».

Объект «Значение ключевого признака» - описывает значения ключевых признаков, такие, как идентификатор и наименование значений на нескольких языках.

На основе унифицированной модели данных были построены определители: цветковых растений [17], минералов, птиц Украины[18], стилей одежды и др.

III. ОЦЕНКА КАЧЕСТВА ОПРЕДЕЛИТЕЛЯ

Принципы построение определителя, иерархию объектов и набор признаков определяет эксперт. Это трудоемкий процесс, который требует глубоких знаний эксперта и практического опыта в данной области. Не всегда существует возможность привлечения экспертов к построению определителя. Каждый из экспертов может иметь разные точки зрения. Кроме того, эксперт может дать оценку проведения классификации не с точки зрения общей модели, а с

точки зрения решения своих конкретных проблем. Естественно возникает задача оценки качества построенного определителя. Была поставлена задача применения формальных методов анализа данных, в том числе и методов Data Mining, для того, чтобы:

- оценить полноту набора ключевых признаков;
- провести анализ оценки качества построенной иерархии признаков;
- определение на полноту и непротиворечивость набора ключевых признаков.

Анализ качества определителей птиц Украины и стилей моды проводился в среде Microsoft SQL Server Data Tools. Для этого было необходимо построение набора данных Data Set, к которому могут быть применены стандартные методы этого инструментария. Построение такого Data Set предполагает денормализацию основных объектов системы и представление данных в виде единой таблицы. На рисунке 2 представлен фрагмент денормализованной таблицы для определителя птиц Украины.

Использование деревьев принятия решений продемонстрировано набор ключевых признаков, характерных для каждого объекта.

	TaxonId	Name_ru	Размером с	Похож на	Принадлежит к отряду	Околоводные территории	C
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: море и соленые лиманы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N
1	401	Озерная чайка	Размером с ворону	Похож на ча	Принадлежит к отряду ржанкообразн	МО: пресноводные водоемы	N

Рисунок 2. Фрагмент базы данных после денормализации

Наивный байесовский метод дал вероятностную оценку каждому ключевому признаку набора, что позволило выделить наиболее важные ключевые признаки.

Кластерный анализ позволил перегруппировать стили по восточным признакам.

IV. ВЫВОДЫ

Применение унифицированной модели данных для построения определителя себя оправдало. Это обусловлено гибкостью системы: возможность исправлять состояния признаков отдельных таксонов и вводить новые таксоны без изменения структуры определителя. С помощью унифицированной модели удалось построить некоторые определители для разнородных предметных областей.

Для определителей стилей моды и птиц Украины был проведен анализ качества методами Data Mining.

В дальнейшем предполагается расширение набора методов, применяемых для проведения оценки качества построенного определителя.

ЛИТЕРАТУРА

[1] Лобанов А.Л. Логический анализ и классификация существующих форм диагностических ключей // Энтомологическое обозрение. 1972. Т. 51,вып.3 С. 668–681

[2] Лобанов А. Л., Кирейчук А. Г., Смирнов И. С., Граничин О. Н., Вахитов А. Т., Дианов М. Б. К реализации идеального интерактивного определителя биологических объектов в Интернете // Труды Всероссийской научной конференции "Научный сервис в сети Интернет: технологии параллельного программирования". Новороссийск. 18-23 сентября 2006 г. Изд-во МГУ. 2006. С. 202–204.

[3] Международная классификация болезней 10-го пересмотра (МКБ-10) [Электронный ресурс]. – Режим доступа: http://mkb-10.com/

[4] Определитель растений Республики Тыва / Красноборов И.М., Ломоносова М.Н. Шауло Д.Н. и др. Отв. ред. Д.Н. Шауло;Рос. акад. наук, Сиб. отд-ние, Ц. сиб. бот. сад; М-во образования и науки РФ, Федеральное агенство по образованию, Тывинский гос. у-нт. - 2-е изд., испр. и доп. — Новосибирск: Изд-во СО РАН, 2007. - 706 с. Ил.587.

[5] Определитель растений "Плантариум" [Электронный ресурс]. – Режим доступа: http://www.plantarium.ru/page/find.html

[6] Фесенко Г В , Бокотей А А Птахи фауни України: польовий визначник // Київ, 2002.-416 с.

[7] Identify a bird. The RSPB bird identifier lists 408 species of birds found in the UK, including some rare overseas visitors: Available at: https://www.rspb.org.uk/birds-and-wildlife/wildlife-guides/identify-a-bird

[8] Гураль-Сверлова Н. В. Визначник наземних молюсків України / Н. В. Гураль-Сверлова, Р. І. Гураль. –Львів, 2012. – 216 с

[9] Справочник по УДК [Электронный ресурс]. – Режим доступа: https://teacode.com/online/udc/

[10] Библиотечно-библиографическая классификация. Средние таблицы. В 9 вып. Вып. 6: З Ж/О Техника. Технические науки: практическое пособие / Рос. гос. б-ка, Рос. нац. б-ка, Б-ка Рос. акад. наук. — Москва: Пашков дом, 2013. — 784 с.

[11] Каталог-определитель минералов и горных пород [Электронный ресурс]. – Режим доступа: http://vsevolodbondarev.com/html/minerals.htm

[12] Кузьменок Н.М. и др. Определитель химических веществ: неорганическая химия. Издательство: Минск, "Красико-принт", 2000. - 16 с.

[13] Энциклопедия моды [Электронный ресурс]. – Режим доступа: https://wiki.wildberries.ru/

[14] Сайт о моде и стиле [Электронный ресурс]. – Режим доступа: http://stylishe.ru/stili-odezhdy

[15] Lisitsyna I., Petrushina T., Trubina N. //A unified approach to hierarchical classifications // Abstracts 2nd International Conference COMPUTER ALGEBRA & INFORMATION TECHNOLOGIES, August 21 – 26, 2016 – c.24 – 60.

[16] Лисицына И.Н., Трубина Н.Ф. Особенности электронных систем классификации для обучения студентов-биологов //Сучасні технології вищої освіти. Збірник наукових праць VI Всеукраїнської науково–методичної конференції. Одеса, 6-8 жовтня 2010 року, - Одеса, 2010, с. 62-63

[17] Трубіна Н.Ф. Використання інформаційних електронних систем для класифікації біологічних об’єктів //IV науково-методична конференція «Досвід, проблеми та шляхи підвищення рівня підготовки випускників університету», 31 січня - 2 лютого 2011р. Збірник тез – Одеса: ОДЕКУ, 2011, с.11

[18] Кивганова Д.Д., Трубина Н.Ф., Петрушина Т.И. Построение определителя на основе унифицированной модели// Пятнадцатая всеукраинская конференция студентов и молодых ученых «Информатика, информационные системы и технологии», Одесса, 2018. – с.107 – 207

[19] Горлович А.Н., Трубина Н.Ф. Иерархическая модель стилей одежы для решения задач классификации // Тринадцатая всеукраинская конференция студентов и молодых ученых «Информатика, информационные системы и технологии», Одесса, 2016. – с.28 – 114

REFERENCES

[1] Lobanov A.L. Logicheskiy analiz i klassifikatsiya suschestvuyuschih form diagnosticheskih klyuchey // Entomologicheskoe obozrenie. 1972. T. 51,vyip.3 S. 668–681

[2] Lobanov A. L., Kireychuk A. G., Smirnov I. S., Granichin O. N., Vahitov A. T., Dianov M. B. K realizatsii idealnogo interaktivnogo opredelitelya biologicheskih ob'ektov v Internete // Trudyi Vserossiyskoy nauchnoy konferentsii "Nauchnyiy servis v seti Internet: tehnologii parallelnogo programmirovaniya". Novorossiysk. 18-23 sentyabrya 2006 g. Izd-vo MGU. 2006. S. 202–204.

[3] Mezhdunarodnaya klassifikatsiya bolezney 10-go peresmotra (MKB-10) : Available at:: http://mkb-10.com/

[4] Opredelitel rasteniy Respubliki Tyiva / Krasnoborov I.M., Lomonosova M.N. Shaulo D.N. i dr. Otv. red. D.N. Shaulo;Ros. akad. nauk, Sib. otd-nie, Ts. sib. bot. sad; M-vo obrazovaniya i nauki RF, Federalnoe agenstvo po obrazovaniyu, Tyivinskiy gos. u-nt. - 2-e izd., ispr. i dop. — Novosibirsk: Izd-vo SO RAN, 2007. - 706 s. Il.587.

[5] Opredelitel rasteniy "Plantarium" [Elektronnyiy resurs]. – Rezhim dostupa: http://www.plantarium.ru/page/find.html

[6] Fesenko G V , Bokotey A A Ptahi fauni UkraYini: poloviy viznachnik // KiYiv, 2002.-416 s.

[7] Identify a bird. The RSPB bird identifier lists 408 species of birds found in the UK, including some rare overseas visitors: Available at: https://www.rspb.org.uk/birds-and-wildlife/wildlife-guides/identify-a-bird

[8] Gural-Sverlova N. V. Viznachnik nazemnih molyuskIv UkraYini / N. V. Gural-Sverlova, R. I. Gural. –LvIv, 2012. – 216 s

[9] Spravochnik po UDK [Elektronnyiy resurs]. – Rezhim dostupa: https://teacode.com/online/udc/

[10] Bibliotechno-bibliograficheskaya klassifikatsiya. Srednie tablitsyi. V 9 vyip. Vyip. 6: 3 Zh/O Tehnika. Tehnicheskie nauki: prakticheskoe posobie / Ros. gos. b-ka, Ros. nats. b-ka, B-ka Ros. akad. nauk. — Moskva: Pashkov dom, 2013. — 784 s.

[11] Katalog-opredelitel mineralov i gornyih porod: Available at:. – Rezhim dostupa:http://vsevolodbondarev.com/html/minerals.htm

[12] Kuzmenok N.M. i dr. Opredelitel himicheskih veschestv: neorganicheskaya himiya. Izdatelstvo: Minsk, "Krasiko-print", 2000. - 16 s.

[13] Entsiklopediya modyi : Available at:https://wiki.wildberries.ru/

[14] Sayt o mode i stile : Available at:http://stylishe.ru/stili-odezhdy

[15] Lisitsyna I., Petrushina T., Trubina N. //A unified approach to hierarchical classifications // Abstracts 2nd International Conference COMPUTER ALGEBRA & INFORMATION TECHNOLOGIES, August 21 – 26, 2016 – c.24 – 60.

[16] Lisitsyina I.N., Trubina N.F. Osobennosti elektronnyih sistem klassifikatsii dlya obucheniya studentov-biologov //SuchasnI tehnologIYi vischoYi osvIti. ZbIrnik naukovih prats VI VseukraYinskoYi naukovo–metodichnoYi konferentsIYi. Odesa, 6-8 zhovtnya 2010 roku, - Odesa, 2010, s. 62-63

[17] TrubIna N.F. Vikoristannya InformatsIynih elektronnih sistem dlya klasifIkatsIYi bIologIchnih ob’EktIv //IV naukovo-metodichna konferentsIya «DosvId, problemi ta shlyahi pIdvischennya rIvnya pIdgotovki vipusknikIv unIversitetu», 31 sIchnya - 2 lyutogo 2011r. ZbIrnik tez – Odesa: ODEKU, 2011, s.11

[18] Kivganova D.D., Trubina N.F., Petrushina T.I. Postroenie opredelitelya na osnove unifitsirovannoy modeli// Pyatnadtsataya vseukrainskaya konferentsiya studentov i molodyih uchenyih «Informatika, informatsionnyie sistemyi i tehnologii», Odessa, 2018. – s.107 – 207

[19] Gorlovich A.N., Trubina N.F. Ierarhicheskaya model stiley odezhyi dlya resheniya zadach klassifikatsii // Trinadtsataya vseukrainskaya konferentsiya studentov i molodyih uchenyih «Informatika, informatsionnyie sistemyi i tehnologii», Odessa, 2016. – s.28 – 114

Hybrid Algorithm for Deep Training of the Neural Network ANFIS

O.M. Marusyk
Aviation Computer-Integrated Complexes Department, Educational & Research Institute of Information and Diagnostic Systems, National Aviation University
Kyiv, Ukraine
svm@nau.edu.ua

O.I. Chumachenko
Technical cybernetics department, Faculty of informatics and computer science NTUU "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
chumachenko@tk.kpi.ua

A.T. Kot
Technical cybernetics department, Faculty of informatics and computer science NTUU "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
svm@nau.edu.ua

***Abstract*—It is considered a fuzzy neural network ANFIS. It is shown that this neural network has disadvantages connected with its learning. Two basic methods of ANFIS learning are analyzed. It is shown, that hybrid learning algorithm of Yang has advantages before Back Propagation method. Complex algorithm of fuzzy neural network ANFIS with help of deep learning technique by preliminary learning of first hidden layer parameters membership functions parameters is developed. It is proposed a heuristic clustering method of input data that clusters characteristics respond to membership functions of input variables under their fuzzification. The improvement of neural network parameters adjustment is proved by many numerical examples.**

Keywords—artificial neural networks, deep learning, fuzzy logic, clustering of data, neural network ANFIS.

I. INTRODUCTION

In a broad sense, deep learning is a method of constructing and debugging neural networks using a multilayer topology.

Obtaining or extraction of significant hidden attributes from a large number of inputs is to solve the problems that arise for most models of artificial intelligence, including image and sound recognition, management, and so on. The methods of deep learning have the purpose of studying the hierarchy of features or characteristics of the highest level of the hierarchy constructed from the features of lower levels. In other words, rising from the lowest level to the highest, features get an increasing level of abstraction, generalized from the bottom up.

A large number of algorithms for machine learning uses shallow architectures: neural networks with one hidden layer, kernel regression, support vector machines, etc. Such algorithms obtain very simple characteristics, but they are not capable of obtaining more complex structures from a wide scope of input data. Also, such systems require a large number of well-labeled training data for debugging. On the other hand, for example, for the recognition of objects in the image, the deep neural network uses many layers of nonlinear transformations and requires a much smaller amount of labeled data.

In general, models with deep architecture [1] – [4], [6] – [8] including deep neural networks, consist of many layers of parametric nonlinear functional modules, and therefore the cost function is almost always non-convex. The existence of many local optimum or plateau in cost functions results in high complexity of optimization compared to shallow models. Local gradient optimization algorithms, such as the error-reversal algorithm, require careful initialization of the parameters, and also very often fall into the awkward local optimum. Such a phenomenon is observed in networks even with two or three layers.

In addition to the above-described problems of falling into local optimum during learning the classical method of back propagation of the signal, there are also such as the damping of the gradient with depth and the saturation of the neurons.

The problem of saturation of neurons arises during using sigmoid functions of neurons activation.

As is know, this function has a saturation property for large modulo values of x, and the derivative of such function with high values of the function is also directed to 0. In this way, the error gradient becomes too small for effective learning and says that the neuron is saturated. This phenomenon also partly leads to the problem of damping the error gradient, described below.

Since the error method for returning error to find the error gradient on the neuron of the previous layers must use a partial derivative of the error function on the parameters of the activation function, that is, according to scales according to the chain rule, then with an increase in depth, the error gradient becomes smaller after each fragmentation in the previous layers.

As you can see, each derivative of the sigmoid function in the chain of partial derivatives reduces the gradient in the lower layer at least 4 times. So, to the deepest layers, instead of a useful gradient signal, sometimes only a small part of it can reach, which colossally slows down the learning of the parameters of the deepest layers.

Since lower neurons are responsible for the extraction of elementary basic features, from which the complex signs of higher levels are further compiled, the more accurately and quickly they will be trained, the more accurate the neurons of the higher layer levels will be trained.

J. Hinton invented in 2006 an effective method for studying the deep neural network of autoencoders and a

limited Boltzmann machine, as well as new models of deep neural networks: the Deep Belief Network (DBN), the Deep Boltzmann Machine (DBM) [10] – [12].

A. Basic classes of NNDT

- Deep neural networks of direct propagation of a signal reconfigured without a teacher training.
- Convolutional neural network (CNN).
- Recurrent neural network (RNN).
- Recursive neural network (RvNN).
- Hybrid Architecture.

B. This networks include

- multilayer perceptron, trained with the help of auto-encoders, limited Boltzmann machines;
- Deep Belief Network (DBN);
- Deep Boltzmann Machine (DBM);
- Generative Adversarial Networks (GAN);
- and some else.

II. The Structure of the Neural Network ANFIS of Deep Learning

The structure of neural network ANFIS in represented on Fig. 1 [5].

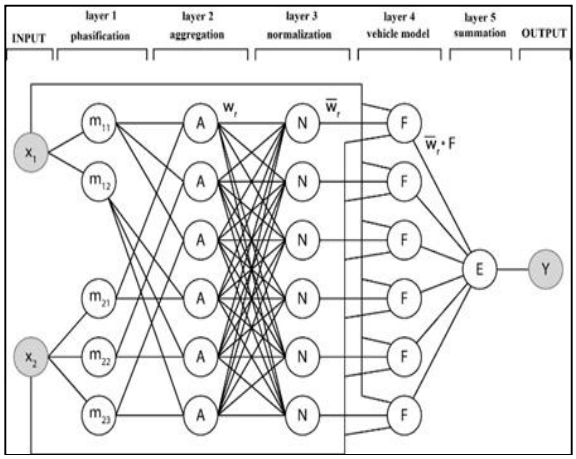


Fig. 1. An example of an TNN ANFIS structure for 2 variables with 2 and 3 belonging functions, respectively, and a complete set of logical rules of the fuzzy output of the Takagi-Sugeno type.

The first layer consists of parametrized functional neurons that execute the fuzzification of a clear input vector with the help of belonging functions $\mu_{A_{ij}}(x_j)$. In this project, Gaussian functions of the belonging type to the species

$$\mu(x,b,c) = \exp\left(-\frac{(x-b)^2}{2c^2}\right),$$

where x is the input clear variable; b is the parameter corresponding to the center of Gaussian, and c is the parameter corresponding to its magnitude (or steepness).

The second layer is not parametric, it reflects the base of the production logical rules of the generated system, and performs the function of aggregating the preconditions (antecedents) of these rules. For aggregation, multiplication operations, T-norms, T-conorms, and others can be used. The output of this layer is the so-called weight of production rules.

$$w_k = A(z_k),$$

where k is the number of rule, A is the selected aggregation function, z_k is the set of inputs rule.

The third layer is also non-parametric and performs normalization operations over the weights obtained from the second layer.

$$\bar{w}_k = \frac{w_k}{\sum_{i=1}^{M} w_i},$$

where M is the number of production rules.

Thus, the output of the third layer is the normalized weight of the logical production rules.

The fourth layer is parametric and implements the fuzzy logical output of the Takagi–Sugeno type. It consists of neurons that receive input of the initial input vector of the sample data and normalized weight of the rules and performs a linear operation on them:

$$o_k = \bar{w}_k\left(\sum_{i=1}^{N}(a_i x_i) + c\right),$$

where o_k is the output of the fourth layer neuron; a_i is the linear function parameter; x_i is the element of the input data vector; N is the size of the input vector data.

The fifth layer passes the output of the fourth layer and is also nonparametric.

All connections between neurons have a constant weight equal to 1.

The purpose of this project is to develop a comprehensive algorithm for teaching the neural network ANFIS with the use of deep learning techniques, namely, the preamble of the parameters of the first layer of the network, that is, the parameters of the functions of affiliation.

Proceeding from the nature of belonging functions in the theory of fuzzy logic, namely the objective clusterization of the field of definition of variables, it is appropriate to find a mechanism for adjusting their parameters without expert intervention.

III. The Statement of the Problem of Deep Training of the Neural Network ANFIS

Yang has proved that his hybrid learning algorithm ANFIS is effectively looking for parameters of the 4th layer of the network for a small number of training periods, but the parameters of the first layer still need to be found in a gradient way.

The task of deep learning of the ANFIS network is to find the heuristic method of clustering input data in such a way that cluster characteristics correspond to the functions of the belonging of the input variables during their reduction to fuzziness (fuzzification).

If such a method is found, one can add the parameters of the first layer in such a way as to increase the efficiency of the final stage of learning, that is, to avoid the local optimum of the target function, and achieve the necessary threshold for the accuracy of training in lesser training periods.

IV. Structure of the Algorithm

The modified hybrid algorithm of the ANFIS network consists of the following steps:

1) Determination of the statistical characteristics of the input data.

2) Selection and application of the clustering method of input data, depending on the nature of the input data.

3) Redesigning the parameters of the membership functions of the inputs in accordance with the obtained clusterization data.

4) Application of hybrid Yang algorithm training TNN ANFIS.

V. Statement of the Clustering Problem

To reconcile the parameters of the first adaptive layer of TNN ANFIS (phase of fuzzification), it is convenient to use clusterization techniques.

For this input data X^N the training dataset must be combined in pairs with the original vector **Y**. The result is a set of N2-measurable datasets, $V^N = [X^n Y | n \in N]$, which can then be clustered to find the parameters of the belonging functions of each input variable.

After that, for each set $X^n Y$ clustering is performed according to the chosen algorithm. For example, as a result of the use of the model of a mix of Gaussian distributions, a set of parameters of a mixture of distributions, which are displayed on the parameters of the function of belonging to the corresponding input variable of the network ANFIS.

Thus, the problem is reduced to the clustering of a two-dimensional space of variables, the receipt of cluster characteristics, and their mapping to the parameters of the first layer of the ANFIS network.

VI. Problem Statement of Deep Neural Network Training ANFIS

Yang has proven that his hybrid ANFIS training algorithm effectively searches for the parameters of the 4th layer of the network in a small number of training epochs, but the parameters of the first layer still need to be found in a gradient way.

Task deep learning networks ANFIS is to find a method of clustering the input data so that the characteristics of the clusters correspond to the membership functions of input variables during reduction to fuzzy data (fuzzification).

Subject to finding such a method, it is possible to transmit parameters of the first layer thus to increase the efficiency of the final stage of training, that is, the avoidance of local optimum the objective function, and to achieve the necessary level of accuracy for a training for a smaller number of training epochs.

VII. Algorithm Structure

The proposed algorithm consists of such steps:

- Definition of statistical characteristics of input data.
- Selection and application of input data clustering method, depending on the nature of the input data.
- Migration of parameters of membership functions by inputs in accordance with the obtained clustering data.
- Application of a hybrid algorithm of Yang of training the neural network ANFIS.

As algorithms of clusterization, such algorithms were considered:

- EM algorithm. Model of a mixture of Gaussian (normal) distributions;
- Algorithm of FuzzyC-Means;
- Subtractive clustering algorithm.

The choice of the method of clustering depends on the characteristics of the training set of data, as well as knowledge of the expert on the data. If an expert knows how many clusters can be effectively distinguished from data, then the algorithm for constructing Gaussian mixtures is preferred, as a more precise.

When it is not possible to determine the number of clusters a priori, it is appropriate to select a subtractive clustering method. It shows less precision than the previous one, but allows you to get the characteristics of the clusters posteriori.

VIII. Results

To compare the quality of the training of the classic ANFIS neural network and the modified ANFIS neural network, using the in-depth training, two subsequent experiments were conducted:

1) Creation of ANFIS structure and preliminary training in the first module of the software complex. Continuation of training in the second module.

2) Creating an ANFIS structure with the same structure as in the first experiment without prior learning, immediately in the second module and learning it in the same. The classical ANFIS automatically initiates the functionality of the input variables by their uniform distribution in the field of definition of variables.

From the results of the experiment it is clear that the quality of training and the classification of modified ANFIS differs significantly from the classical ANFIS:

- the error value in the first step differs by almost 8 times in favor of the modified version, that is, its

initial settings are much closer to the optimal, compared with the classic version;

- the value of the final error of classical ANFIS training is almost an order of magnitude higher than that of the modified version, which is a testimony that ANFIS without prior learning tends to fall into a non-optimal local minimum;
- the test error is also an order of magnitude higher in the classical version, as well as a low proportion of correctly classified samples makes the classic ANFIS network unsuitable for the task of classifying this type of data. On the contrary, the modified ANFIS was able to correctly classify all test samples.

CONCLUSION

It is proposed a new approach for structural-parametric synthesis neural network ANFIS. It is developed a new hybrid algorithm for its learning.

The modification of the ANFIS neural network with the use of in-depth training turned out to be qualitatively better than its classic version, and was able to accomplish the classification task that this model generally does not put into, due to the low accuracy of the unmodified version.

REFERENCES

[1] L. Deng, and D. Yu, "Deep Learning: Methods and Applications," Foundations and Trends in Signal Processing. 2014, 7 (3–4): 1–199.

[2] V. V. Borisov, V. V. Kruglov, and A. S. Fedulov, Fuzzy models and networks. 2 nd ed., The stereotype. 2012. (in Russian)

[3] Haykin Simon. Neural networks: full course, 2nd edition. 2006. (in Russian)

[4] A. P. Rotshteyn, Intelligent identification technologies: fuzzy sets, neural networks, genetic algorithms. Monograph. Vinnitsa: "Universum-Vinnitsya," 1999, 295 p. (in Russian)

[5] J.-S. R. Jang, ANFIS: Adaptive-Network-Based Fuzzy Inference Systems, IEEE Trans. Systems, Man & Cybernetics 23 (1993).

[6] Y. LeCun, Y. Bengio, and G. Hinton, Deep learning. Nature. 2015.

[7] R. Salakhutdinov, Learning Deep Generative Models. PhD Thesis. Dept. of Computer Science, University of Toronto. Sep. 2009.

[8] Y. Bengio, A. Courville, and P. Vincent, Representation Learning: A Review and New Perspectives. Department of computer science and operations research, U. Montreal. 2014.

[9] X. Glorot and Y. Bengio, Understanding the difficulty of training deep feedforward neural networks. 2010.

[10] G. Hinton, and R. Salakhutdinov, Reducing the Dimensionality of Data with Neural Networks. Science. 2006.

[11] G. Hinton, S. Osindero, and Y. The, A fast learning algorithm for deep belief nets. Neural Computation, 18:1527-1554, 2006.

[12] G. Hinton, A Practical Guide to Training Restricted Boltzmann Machines. Department of Computer Science, University of Toronto. 2010.

Odessa I.I. Mechnikov National University

3d International Conference on Computer Algebra and Information Technologies

August 20 – 25, 2018
Odessa, Ukraine

PROCEEDINGS

Одеський національний університет імені І.І. Мечникова, Одеса

ІІІ Міжнародна Конференція «Комп'ютерна Алгебра та Інформаційні Технології» CAIT-Odessa-2018

20-25 серпня 2018р.
Одеса, Україна

ПРАЦІ

Підписано до друку 14.08.2018 р.
Формат 60x84/8. Папір офсетний. Гарнітура Times New Roman.
Друк офсетний. Ум. друк. арк. 23.01. Наклад. 150 прим.
Зам. № 1408/1.

Надруковано з готового оригінал-макету у друкарні «Апрель»
ФОП Бондаренко М.О.
65045, м. Одеса, вул. В.Арнаутська, 60
тел.: +38 0482 35 79 76; www.aprel.od.ua

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців ДК № 4684 від 13.02.2014 р.