I.I. Mechnikov Odessa National University

ABSTRACTS

2nd International Conference
COMPUTER ALGEBRA & INFORMATION TECHNOLOGIES

August 21 - 26, 2016

Odessa 2016

I. I. Mechnikov Odessa National University, Odessa

2^{nd} *International Conference on Computer Algebra and Information Technologies*

August 21 – 26, 2016

Odessa, Ukraine

ABSTRACTS

Одеський національний університет імені І. І. Мечникова, Одеса

ІІ Міжнародна конференція "Комп'ютерна алгебра та інформаційні технології"

21 – 26 серпня 2016 р.

Одеса, Україна

ТЕЗИ ДОПОВІДЕЙ

Одеса — 2016

2nd International Conference on Computer Algebra and Information Technologies. August 21 – 26, 2016, Odessa, Ukraine. Abstracts. — Odessa: I. I. Mechnikov Odessa National University, 2016. — 60 p.

II Міжнародна конференція "Комп'ютерна алгебра та інформаційні технології". 21 – 26 серпня 2016 р., Одеса, Україна. Тези доповідей. — Одеса: Одеський національний університет імені І. І. Мечникова, 2016. — 60 с.

International Program Committee

C O N T E N T S

З М І С Т

Al-Jasri G.Kh.M., Boltenkov V. The study of methods for solving systems of TDOA-equations in sound source localization problems 5

Antonenko O. Semigroups generated by some classes of Mealy automata 6

Balyas L. Exponential sums with characters over the norm group 7

Chala L., Udovenko S. Adaptive strategies of mobile objects *RL*-control 8

Chumachenko O., Godny A., Synehlazov V. Information technologies of computer aided design systems based on dynamic data integration and simulation procedures 9

Dobrovolsky G., Keberle N., Todoriko O. Pronunciation quality assessment by comparison with example 11

Ermilova A., Rublev V. On some results in computational complexity analysis of integer relation algorithms 12

Filatova T., Malakhov V. Application of graphical representations for analysis criteria .. 13

Glava V., Malakhov E. Comparison of the nominal type properties of objects of different subject domains 15

Glazunov N. Computer algebra and motivic zeta functions of algebraic varieties over fields of positive characteristics 17

Granik Yu. Optimization problems and practices in microelectronic manufacturing 18

Kaman K., Lebedeva E., Zorilo V. Analysis of the digital image in terms of different types of blur tools Adobe Photoshop 19

Kosukhin N., Shpinareva I. Cryptanalysis of asymmetric algorithms using ant colony optimization 21

Kozin A., Kozina M., Papkovskaya O. Steganographic method for digital images authentication 22

Krapivnuy Yu., Kryvonos O. Model of hybrid intelligent system for image analysis 23

Lisitsyna I., Petrushina T., Trubina N. A unified approach to hierarchical classifications 24

Malakhov E., Mezhuyev V., Shchelkonogov D. Algorithms of classification of mass problems of production subject domains 25

Malakhov E., Tsariuk A. Review of methods of analysis of educational and organizational information to improve the quality of specialist training 26

Mazurok I., Zahanich D. Development of the effective vocabulary structures for the speech recognition tasks 27

Penko V., Taran Y. An analysis of the heuristic method for constructing Bayesian networks in terms of program implementation within the framework of extensible architecture 28

Petrushina T., Sviridov A. The Fibonacci Q-matrix coding method 29

Rogowski J. The comparison of the web applications development frameworks Ruby on Rails, Django and Grails 30

Rychlik A. System for the sale of intellectual property through IPTV 31

Savastru O. Divisor problem in special sets of gaussian integers 32

Shvorob I. Document-oriented graph as a way of saving semistructured medical data 33

Varbanets P. Character sums over $\mathbb{Z}[i]$ 34

Varbanets S. Sequences of PRN's produced by circular generator 35

Varbanets S., Vorobyov Ya. The Laplace transform for a pair of the Hecke Z-functions .. 37

Tran The Vinh Congruential generator of complex PRN's 38

Volkova A. Optimization techniques in implementation of linear time-invariant control systems 39

Vorobyov Ya. r-divisor over $\mathbb{Z}[i]$ 40

Waszkielewicz W., Petryshyn L. Modeling of Multiprocessor Control Systems 41

Воробьев Г., Гальмак А. Компьютерная алгебра трехмерных матриц 43

Любота В. Решение задач оптимизации на Visual Prolog 44

Огбу Д., Оксиюк А., Шестак Я. Управление производительностью сети 46

Панченко Б., Печенюк Д. Автоматизированный синтез точных альтернативных временных отрезков при коммутации дискретно-периодических сигналов 47

Сохор И. Конечные группы и компьютерная алгебра 49

Арсірій А., Арсірій О., Василевська О. Метод структурно-параметричного синтезу енергозберігаючих фізичних прототипів допоміжних елементів гідроаеродинамічної системи 50

Гунченко Ю., Ємельянов П., Шворов С. Модель функціонування тренажерних систем інтенсивної підготовки диспетчерів управління повітряним рухом 51

Зерко А., Кохановскій О., Оксіюк А. Аналіз питань доведення захищеності інформації в операційних системах 52

Левін М., Шаршаткін Д. Організаційні аспекти захисту персональних даних громадян в системах надання адміністративних послуг 53

Petryshyn L. Application of Anti-Grey Code in Digital Components Diagnosing 55

Petryshyn M. Application of vector-branching schemes in IFT processes modeling 56

The study of methods for solving systems of TDOA-equations in sound source localization problems

Al-Jasri G.Kh.M., Boltenkov V.

Odessa National Polytechnic University, Odessa, Ukraine

aljasri@gmail.com, vaboltenkov@mail.ru

The problem of determining sound source coordinates with passive acoustic sensor network (ASN) based on the TDOA-technologies has been studied. Such problems arise, in particular, in automatic localization of leaks in high pressure energetic equipment. The problem is based on the acoustic wave *time difference of arrivals* (TDOA) from sound source estimation to each pair of sensors in spatially distributed microphones system – ASN. For each sensor pair TDOA is estimated by cross-correlation function argmaximum of received signals. Each equation for the sensor pair describes a surface source position surface – isodiachron, which is a two sheet hyperboloid of revolution. One can form a system of C_N^2 equations for a N sensors network. It is assumed that TDOA estimation have errors distributed under the gauss' law. The speed of solving nonlinear equations system and the accuracy of the source coordinates estimation has been investigated. Both nonlinear approaches (maximum likelihood, nonlinear least squares) and iterative linear approaches, based on linearization (Newton–Raphson, Gauss–Newton, Levenberg-Marquardt algorithms), were studied. Problem was solved in computer algebra environment Matlab 8.1. It was established, that linearized methods for the same precision of solution require 5-8 times less computing time. However, the convergence of these methods strongly depends on the initial guess. In the context of the leak coordinates estimating in the closed technological room, the initial guess choosing is constrained by the size of the room.

Semigroups generated by some classes of Mealy automata

Antonenko O.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

antonenko@onu.edu.ua

We call an finite automaton $A = (X, Q, \pi, \lambda)$ an automaton without branches [1] if its transition function π depends only on the current state and is independent of input symbols. A state $q \in Q$ is a state without branches if and only if for all $x_1, x_2 \in X$ the equality $\pi(x_1, q) = \pi(x_2, q)$ holds. All states of an automaton without branches are states without branches. The transformation defined by an automaton without branches at some state is symbol-by-symbol one. Automata without branches always define finite semigroups independently of their output function. Let Q_1 is a subset of Q, $\Pi(Q_1) = \pi(X, Q_1) = \{\pi(x, q) \,|\, q \in Q_1, x \in X\}$, $\Pi^\infty(Q_1) = \bigcap_{k=1}^{\infty} \Pi^k(Q_1)$.

Then if $\Pi(Q)$ consists only from states without branches an automaton defines finite semigroup independently of its output function. For other examples of automata that defines finite (semi-)groups, see [2].

Let us consider finite automata $A = (X, Q, \pi, \lambda)$ over two-symbol alphabet $X = \{0, 1\}$ with the following two properties:

- for each state $q \in Q$ of an automaton, there exists not more than one symbol $x \in X$ such that $\pi(x, q) \neq q$ (slowmoving automata);
- there are no cycles except loops in the Moore diagram of an automaton (automata of the finite type), [1].

Let $p : X \to X$ be an arbitrary transformation of symbols, $x \in X$, and let $f : X^\omega \to X^\omega$ be an arbitrary transformation of infinite words. Detone by $px]f$ a transformation, which acts by p on all the symbols up to the first occurrence of the symbol x inclusive, and on the rest of the word by the transformation f. Any slowmoving transformation of the finite type can be represented in the form $f = p_1x_1]p_2x_2]\dots p_kx_k]p$, where p_i, $p : X \to X$, $x_i \in X$. Consider the family of transformations:

$$\alpha_0 = \sigma, \quad \alpha_1 = id0]\sigma, \quad \dots, \quad \alpha_n = id0]^n\sigma, \quad \dots$$
$$\beta_0 = \alpha0]id, \beta_1 = id0]\alpha0]id, \beta_2 = id0]id0]\alpha0]id, \dots, \beta_n = id0]^n\alpha0]id, \dots$$
$$\delta_0 = \alpha, \quad \delta_1 = id0]\alpha, \quad \delta_2 = id0]id0]\alpha, \quad \dots, \quad \delta_n = id0]^n\alpha, \quad \dots$$

where $\sigma(x) = 1 - x$ is the inversion, $id(x) = x$ is the identical permutation, $\alpha(x) = 0$.

We have $\alpha_i^2 = id, \beta_i^2 = \beta_i, \delta_i^2 = \delta_i$. Any invertible slowmoving transformation of finite type can be represented as composition of α_i and any slowmoving transformation of finite type can be represented as composition of $\alpha_i, \beta_i, \delta_i$.

1. Antonenko A.S., Berkovich E.L. Groups and semigroups defined by some classes of Mealy automata. Acta Cybernetica, 2007, **18**, pp. 23–46.
2. A. Akhavi, I. Klimann, S. Lombardy, J. Mairesse, M. Picantin On the finiteness problem for automaton (semi)groups. In Int. J. Algebra Comput., 2012, **vol.22**, no. 4, p.26.

Exponential sums with characters over the norm group

Balyas L.
I.I.Mechnikov Odessa National University, Odessa, Ukraine
balyas@ukr.net

Let $G := \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}, i^2 \in \mathbb{C}, i^2 = -1\}$ be the ring of Gaussian integers and G_{p^m} be the complete system of residues modulo p^m in G with $p \equiv 3(mod\ 4)$. Let $G^*_{p^m}$ be the reduced system of residues modulo p^m in G. For $p \equiv 3(mod\ 4), m \in \mathbb{N}, m \geqslant 1$ we denote as $E_m \subset G_{p^m}$ the norm group

$$E_m := \left\{x \in G^*_{p^m} | N(x) \equiv \pm 1(mod\ p^m)\right\} \tag{1}$$

It is known that this subgroup is cyclic with the order $2(p+1)p^{m-1}$ ([?]).The congruence $N(u_0 + iv_0) \equiv \pm 1(mod\ p^m)$ is true for its lead element $(u_0 + iv_0)$.

We also put $e_{p^m}(Re(z)) := e^{2\pi i Re(\frac{z}{p^m})}$, where $Spz = z + \bar{z} = 2Rez$ is a trace from $\mathbb{Q}(i)$ into $\mathbb{Q}$ for $z \in G$.

For $\alpha, \beta, \gamma, l \in G, (\alpha, p) = 1, (\beta, p) = 1, (\gamma, p) = 1, m > 1, m \in \mathbb{N}$ and non-principal character χ modulo p^m we consider the exponential sum over the norm group (1) of the following type

$$S(\alpha, \beta, \gamma; E_m) = \sum_{\substack{x,y \in E_m \\ x+y^2 \equiv 1(mod\ p^m)}} \chi(x^2) e_{p^m}(\alpha x + \beta xy + \gamma y^2) \tag{2}$$

Using the representation of the elements of group E_m ([?], [?], [?]), the properties of its coefficients in general case and in exceptional cases $\left(z = 0, z = p+1, z = \frac{p+1}{2}, z = \frac{3(p+1)}{2}\right)$; the elements of the scheme of thoughts from work [?] and Theorem 1 from the paper [?]; the generalization of Postnikov lemma ([?]) about characters ([?]); lemmas about the estimates of exponential sums with the polynomials of special forms over the ring of Gaussian integers and in rational case, we obtain the following estimate for the sum (2)

$$|S(\alpha, \beta, \gamma; E_m)| \leqslant 10 p^{\frac{m}{2}} \tag{3}$$

Exponential sums over the norm group E_m without characters were considered in [?]. These sums have no rational analogue.

1. Balyas L., Varbanets P. Twisted exponential sums over the ring of Gaussian integers. Annales Univ.Sci.Budapest, Sect.Comp., 2013, **v.40**, pp. 95–103.
2. Postnikova A.G. On sum of characters modulo of power prime. Izv.Akad.Nauk USSR, Ser. Math, 1955, **v.19**, 1, pp. 11–16 (in Russian).
3. Sergeev S. Character sums analogue of Kloosterman sums on norm group. Visnyk Odesk.Nats.Univer. Math. I Mekh, 2014, **v.19**, 22, pp. 66–74.
4. Sergeev S., Varbanets P. Exponential sums over norm group. Siauliai Math.Seminar, 2014, **9**, 17, pp. 83–92.
5. Varbanets S. General Kloosterman sums over ring of gaussian integers. Ukr.Math.J, 2007, **v.59**, 9, pp. 1179–2000.

Adaptive strategies of mobile objects RL-control

Chala L., Udovenko S.

Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

larysa.chala@nure.ua, serhii.udovenko@nure.ua

The paper considers the optimal strategies in positioning and control systems for mobile objects using machine learning methods for reinforcement. The general reinforcement learning (RL-learning) problem addresses the following: an agent must explore its environment and make decisions in different situations based on incomplete knowledge about this environment. The only feedback that the agent receives from the environment is a scalar reinforcement signal which is positive if its actions are beneficial and negative otherwise. The objective of the agent is to choose its actions so as to increase the long-term sum of the reinforcement signals [1]. The proposed approach allows to obtain high-quality approximation of the optimal strategies for evaluating functions by using multi-layer artificial neural networks. Besides the reinforcement signal, the agent also receives information on the current state of the environment (in the form of a vector of observations). Examples of the use of RL-methods developed in fuzzy control of the wheeled mobile robots. The rule base of the system of autonomous navigation of robot gets better in the process of learning with the use of reinforcement signal [2]. The examples of design of mobile robots navigation in different environments are considered. The only information available is the gain (positive or negative) generated by control decisions and this provides the reinforcement signal that drives our system. Methods are implemented in software and tested.

1. L. Chalaya, A. Hryshko, S. Udovenko Hybrid machine learning methods in dynamic objects control systems. Bionica intellecta, 2012, № 1 (78), pp. 78–84. (in Russian).
2. A. Sorokin, S. Udovenko Fuzzy control strategies for a wheeled mobile robot. Sistemi obrobki informacii, 2016, **Issue. 8**, 145, pp. 56–62. (in Russian).

Information technologies of computer aided design systems based on dynamic data integration and simulation procedures

Chumachenko O., Godny A., Synehlazov V.
National Aviation University, Kyiv, Ukraine
svm@nau.edu.ua

There are dozens of software products designed to meet the challenges of each stage of computer-aided design (Compass - 3D, Altium Designer, MatLab, Catia, Solidwork, DIALux, Anfys, Flowvision etc.). Therefore, there is no need to deal with each individual task to create new software components that can solve such problems. From an economic point of view and from the point of view of simplicity of design makes sense to combine existing software products in an integrated suite of software products for the task.

To achieve this goal it is necessary to solve the following problems:

1. Choosing N software $(W_1, W_2, W_3, \ldots, W_N)$, sharing which can solve the problem of automating the design of a product;
2. Methodology CAD design from the standpoint of redirecting information flows;
3. Integrating data in a single information process.
4. Multicriterion optimization problem.

The first stage is unique for each separate task and depends on the capabilities and preferences of the customer, hence there is no optimal algorithm for solving this problem.

Integration of multiple CAD systems using the integrating module (Application Service Bus) implies the existence of a link between all the modules via Application Service Bus. It manages all available modules of the system, and is responsible for the interaction between the modules, data conversion (if needed), and quality control of the performed work When using the Service Bus Applications we have N systems because each system is connected only to the Integrator, then the whole system is necessary to create N pairs of data transformations of the form "W_i-Integrator "Integrator-W_i".

The main principle of the objects in the system is based on operations with declarative data object. The basis of the design process is the consistent execution of commands, parameters of which are aligned with the parameters of designed objects. Considering the principles of objects and principles of the projects implemented in CAD parameterization with objects, you can establish that the object parameters and parameters performed during the design commands are separated from each other. The same parameter can be obtained by using different commands of CAD. This parameter is not only a formal representation of the object in the system. List of parameters represent object in the system. After executing a command result is stored in the parameter list of the object. Further, when performing a command parameter object will be processed with a combined command parameter. The result is stored in the parameter list of the object and so on.

Having considered of all listed above properties of CAD objects with parameterization can infer the presence of these CAD data integration. However, in such CAD object parameters and commands are separated from each other, object parameters have priority over commands and they are not only a formal representation of commands to the system. Consequently, the CAD data with the parameterization can be realized only by static data integration methods. These CAD include monitor that provides tracking status of parameters and generating automatic rebuild facilities.

For the solution of multicriterion optimization problem it is used the normed weighted sum method. The normed weighted sum method is the first method developed for solving problems of this type and it is also the simplest to employ.

Presented CAD with an integrated environment introduces a new approach to managing the design process. Used in the proposed medium scenario design can greatly simplify the work of the designer. Available in medium monitor provides the flexibility of design processes with a flexible structure description of design procedures in the scenario design.

Pronunciation quality assessment by comparison with example

Dobrovolsky G., Keberle N., Todoriko O.
Zaporizhzhya National University, Zaporizhzhya, Ukraine
gen@znu.edu.ua, kenga@znu.edu.ua, o-sun@rambler.ru

Pronunciation quality assessment method proposed in the paper is based on the following hypothesis: if a phrase spoken by a student is similar to a phrase spoken by a teacher, then the student has a good pronunciation; similarity criterion is a value of distance function, calculated on a set of features of correspondent teacher and student conditional phonemes; splitting of a spoken phrase into conditional phonemes is performed based on an assumption that in the transition from one phoneme to another the features of a sound change essentially if compared to the features of a sound within one phoneme; pauses among words are not taken in account for pronunciation quality assessment.

An audio file received from a student is transformed into a sequence of frames each of which is supported with a set of features. The sequence of frames with the help of DTW algorithm [1] is compared to the example (teacher) sequence of frames, and is split into words and conditional phonemes. The peculiarity of the comparison is the assumption that a student speaks uncertainly, and hence, slowly, with pauses. Pauses – silence fragments among words – should be excluded from the assessment. The method of distance function modification [2] on the set of features is used to detect and exclude pauses. The result of DTW algorithm with distance function modification is pair wise correspondence of teacher and student frames.

In ideal case (phrases are pronounced equivalently) the correspondence will be linear – this means the quantity and duration of all sounds. In reality, phrases differ, and the difference can be calculated.

1. Chan P., Salvador S. FastDTW: Toward Accurate Dynamic Time Warping in Linear Time and Space. Intelligent Data Analysis, 2007, **Vol. 11**, 5, pp. 561–580.
2. Glass J., Lee A. A Comparison-based Approach to Mispronunciation Detection. Spoken Language Technologies Workshop (2-5 December 2012, Miami, Florida), 2012, pp. 382–387.

On some results in computational complexity analysis of integer relation algorithms

Ermilova A., Rublev V.

P.G. Demidov Yaroslavl State University, Yaroslavl, Russia

roublev@mail.ru

The symbolic step table constitutes the basics of algorithm complexity analysis. This table consists of some specific columns for conditions of execution or exit of every loop besides the columns for each of variables. This provides the possibility to estimate the number of loop executions from above and below giving theta-estimates for the computational complexity of each loop.

When the algorithm under consideration is integer (i.e. the algorithm parameters take integer values only), the analysis of obtained expressions might be complicated. Another complication can come from the summation of sequences different from arithmetic or geometric ones. The theorems given below allow us to simplify the analysis in these cases.

Let $\mu_1(a \cdot n + b) = a \cdot n + b$ be a linear form with a natural parameter n of an algorithm and positive values of a, b.

Define by $\mu_p(a \cdot n + b)$ the iterated function $\mu_p(a \cdot n + b) = a \cdot (a \cdot \ldots (a \cdot n + b) + \ldots + b) + b$, obtained by composition of the form μ_1 with itself p times, and define by $\mu_p[a \cdot n + b] = [a \cdot [a \cdot \ldots [a \cdot n + b] + \ldots + b] + b]$ the iterated function obtained by composition of the integer part of the linear form μ_1 with itself p times (the square brackets denote here the integer part of the respective expression).

Theorem 1. *Let a, b be real coefficients of the linear form $a \cdot n + b$ with $a > 1$ and natural value of n. Then $\Theta(\ \mu_p[a \cdot n + b]\ ) = \Theta(\ \mu_p(a \cdot n + b)\ ) = \Theta(a^p n)$.*

Theorem 2. *Let the growth of the non-negative monotonically increasing function $f(x)$ $(x \geqslant 0)$ be constrained by the condition $f(x) \leqslant C \cdot f(x-1)$, where constant $C \geqslant 1$. Therefore the theta-estimates are equal:*

$$\Theta\ (\sum_{x=m}^{n} f(x)) \ = \ \Theta\ (\int_{m-1}^{n} f(x)dx) \quad (\forall m > 0).$$

Theorem 3. *For the non-negative monotonically increasing function $f(x)$ $(x \geqslant 0)$ $(x \in [0, \infty))$ let the function $g(x)$ defined by the relation $f(x)/f(x-1) = g(x)$ $(x \geqslant 1)$ be monotonically increasing and unbounded from above. Then the theta-estimates are equal:*

$$\Theta\ (\sum_{x=m}^{n} f(x)) \ = \ \Theta\ (f(n)) \quad (\forall n > m > 0).$$

Application of graphical representations for analysis criteria

Filatova T., Malakhov V.

Odessa National Polytechnic University, Odessa, Ukraine
Petro Mohyla Black Sea National University, Mykolaiv, Ukraine
filatovatatyana@mail.ru, malakhov41@mail.ru

In the process of any activity for decision making arises the necessity to improve the quality criterias. Analyzing criteria, which satisfy the requirements and have a bearing on choice of employer, deliver the desired result. For a visual representation, analysis and forecast is necessary to apply a graphical representation of using trend lines. This analysis will respond to changes of trends in the modern world and will give to the right choices in the selection of factors.

For a graphical representation of the direction of these changes in the number of data (depending on the trends) is used trend line.

Virtually none of the methods of the graphic analysis is not without trend lines, which help to determine the direction of the trend.

Construction of the trend line for the presentation and analysis of education quality criteria allows to display trends in the existing data, which influence the quality of education or forecast future data.

So we apply technical analysis - trend line to identify trends in the factors of quality education which appeal modern employer. It will allow in the collected data to detect the trend in certain factors over the years and forecast factors that affect the improvement of education. That is, which we will consider the most attention. The function to be used for the construction of trend lines may be linear, polynomial or any other depending on what we want to see in the chart, and that the original data will be used. That is possible to build multifactor model, conduct a survey and on this basis construct a graph, which will give a more complete picture of the problem [1].

Operation crossing made it possible to identify the factors $K = \{x_4, x_6, x_7\}$, with which in the future we will work, build function and schedule [1]:
x_4- "Quality of education"; properties of the object are discipline and evaluation (ie, we consider the average score in the study of subjects: x_{41} - the average score of general subjects, x_{42} - the average score of practical vocational subjects);
x_6- "Mobile activity"; properties of the object are type, characteristics, quantity, level, language (European, American etc.). Consider x_{61} - the number of students who participated in various educational and research programs, x_{62} - the number of students who speak a foreign language and x_{63} - the number of scientific publications in foreign languages.
x_7- "Practical experience"; properties of the object can be volume, type of participation in solving problems etc. Consider, for example x_{71} - the number of students which received certificates (experience with information systems) and x_{72} - number of applications for implementation after pre-graduation practice.

Based on the presented data we construct a trend line to predict. Thus, we define the trends in the existing data and we make a forecast significant factors in the future (Figure 1). As can be seen from the graph, the trend line for factor x_{72} - number of applications for adoption after pre-graduation practice is polynomial trend line of the second stage:

$$y = 0,5x^2 - 2013,5x + 2E + 06,$$
$$R^2 = 1.$$

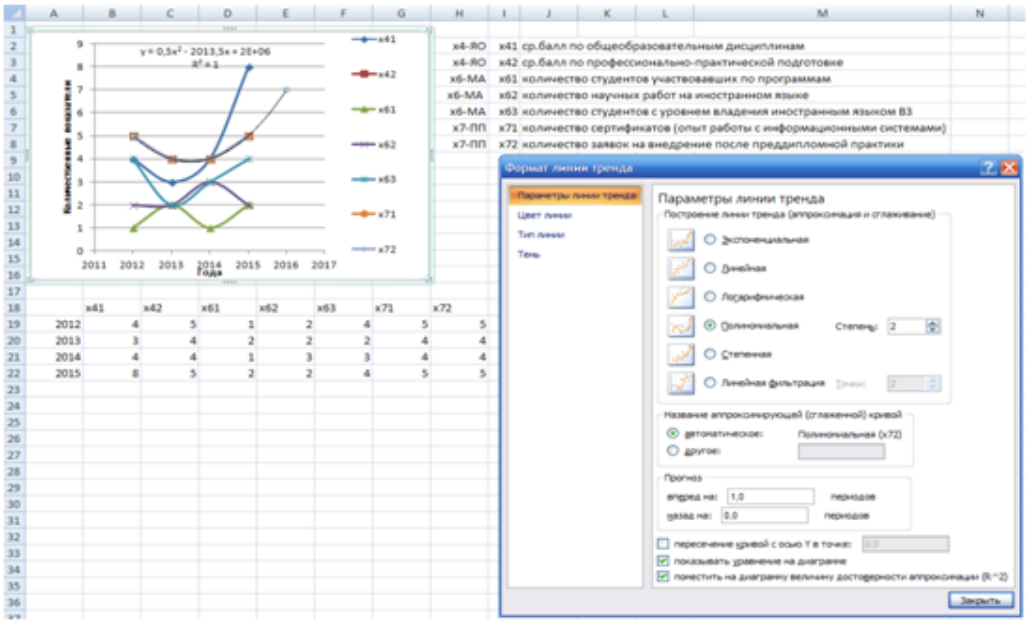

Рис 1. Рис. 1 - Диаграмма строго соответствия альтернативных программ

In our example, second-degree polynomial (a maximum) for factor x_{72} shows the dependence criteria of quality education to meet the requirements of the employer and the future of predictive value.

A polynomial trend line describes of the magnitude, which is alternately increasing and decreasing. It is useful for the analysis of a large data set of unstable value. The degree of the polynomial is determined by the number of extremes (highs and lows) of the curve. The polynomial trend line is based on the following formula:

$$y = b + c_1 \cdot x + c_2 \cdot x_2 + c_3 \cdot x_3 + \cdots + c_n \cdot x_n,$$

where b and n - constants.

As we see from the graph, the approximant $R^2 = 1$. This shows the accuracy of the graph.

From graph may conclude that in subsequent years the number of applications for implementation after pre-graduation practice will be increased. This way you can analyze other indicators of interest to employer.

1. T. Filatova, M. Glava. Mathematical Models of Information Manipulation in the Subject Field of Intellectual Production in Educational Institutions. Materials of the International conference on Electronics and Information Technology (EIT'2016), 23th–27th May, 2016. - Ukraine, Odessa, pp. 92–96.

Comparison of the nominal type properties of objects of different subject domains

Glava M., Malakhov E.
Odessa National Polytechnic University, Odessa, Ukraine
I.I. Mechnikov Odessa National University, Odessa, Ukraine
glavamaria@mail.ru, opmev@mail.ru

These days, the work of any organization in any industry is not possible without the use of information technologies. Databases and data storages can store and process the huge data stream, which simplifies the management and control activities to a considerable extent.

Taking into account the economic situation of the country and analyzing the market, which is subject to reorganization of the enterprises, we can conclude that there are problems of the integration of information systems (IS).

The any IS design starts with a description of the subject domain (SD) and with a construction of its model. The solving this problem is the merging of SD models of the analyzed IS. To excluding redundancy and inconsistency of data, it needs to determine the similar objects in different SD.

In [1] the search technology of the same SD projection (SD objects) is proposed, which is proposed to compare objects on the basis of the properties values of the tuples of these objects. The comparison algorithms differ depending on the data type of the specific property. This paper we propose the comparison algorithm of the nominal type properties.

Under the proposed technology, it needs to prepare the objects of the potentially similar subject domain for the comparison, having allocated significant properties, having ranked, having grouped by data types and having sorted the tuples [1]. It carries out manipulation of the properties of the nominal type after analysis of serial properties.

We can assume that the preceding steps brought together the rank of potentially similar objects and their properties. Implementation the comparison algorithm of the serial type properties brought together the tuples compared objects. Accordingly, values of the nominal properties compare for aligned capacities of the tuple sets.

The comparison of the values symbol-by-symbol rejected because the information on the same object or action we can represent by different nominal values.

To compare the nominal type properties we suggest creating a base of signs F, which characterize any nominal properties. These characteristics include, for example, the number of spaces in property values; the number of capital letters; the part of speech; the presence of punctuation; the presence of abbreviations, etc.

The next step is to fill in the sets of signs F, having processed the nominal values of each property of the compared SD objects.

To determine the measure of the properties similarity, we form the contingency table (or the cross-table) on the following signs:

The number of spaces = 0; 0 < The number of spaces < 3; The number of spaces ⩾ 3; The number of capital letters = 0; 0 < The number of capital letters < 4; The number of capital letters ⩾ 4; The presence of abbreviations = "yes"; The presence of abbreviations = "no"; The presence of punctuation = "yes"; The presence of punctuation = "no"; The part of speech = "noun"; The part of speech = "adjective"; The part of speech = "verb".

During next steps, we suggest to compare the nominal properties pairwise in the order that we defined in step a ranking of objects and their properties. When detecting a low level of compliance, it exclude these properties from consideration. When selection of properties with high and average similarity measure, it analyze them with help of the experts, because the software method does not guarantee that the error will be excluded in the analysis of nominal properties. Nevertheless, this method will reduce and simplify the properties processing for the experts.

The similarity measure between the properties of the nominal type on the basis of the signs complex was analyzed by the following methods: taxonomic analysis of E. S. Smirnov [2], coefficient of Pearson's mutual contingency [3], Pearson's chi-squared test [4].

The most revealing on the test data defined Pearson's chi-squared test.

1. Zabavsky B. V. Diagonal Reduction of Matrices over Rings. — Lviv: Math. Stud. Monogr. Ser., 2012, **XVI**, 251 p.
2. Maria Glava, Eugene Malakhov Searching Similar Entities in Models of Various Subject Domains Based on the Analysis of Their Tuples. 2016 International Conference on Electronics and Information Technology (EITB'16), May 23–27, 2016, Odesa, Ukraine, 2016, pp. 97–100.
3. Smirnov E.S. Taxonomic analysis. M.: Publisher Moscow University, 1969 (in Russian).
4. Gromyko G.L.: Textbook. M.: INFRA-M, 2005, p. 476 (in Russian).
5. Babich P.N., Chubenko A.B., Lapach S.N. Statistics in science and business. Kiev: Morion, 2002 (in Russian).

Computer algebra and motivic zeta functions of algebraic varieties over fields of positive characteristics

Glazunov N.

National Aviation University, Kyiv, Ukraine

glanm@yahoo.com

We investigate algebraic aspects of motivic approaches to zeta functions of algebraic varieties over fields of characteristics $p > 0$.

On the base of the investigations we develop their ontology.

We rely on the works by A. Grothendieck, P. Deligne, J. Tate, Yu. Manin, C. Soule, V. Voevodsky, F. Broun and others. At first we consider Chow and Tate motives and corresponding zeta functions. In the framework follow to P. Deligne we present motivic and computer algebra aspects of classical Riemann zeta function.

Then we consider motivic approach to zeta and $L-$ functions with emphasize on computational aspects.

Multiple zeta values are included.

Optimization problems and practices in microelectronic manufacturing

Granik Yu.
Mentor Graphics, USA
yuri_granik@mentor.com

Lithography is the key enabling technology in manufacturing of the contemporary integrated circuits. In order to achieve the best possible yield, the lithographic steps and their parameters are subjected to various optimization, tuning, and improvement procedures. Whenever possible, lithographic engineers try to formalize emerging problems, and then apply mathematical optimization theory, mainly methods of the numerical optimization. We present here a review of such problems and methods.

One dimensional optimization problems are not challenging, which can be explained by the triviality of constraints and benign computational complexity of such problems. In addition to this, often in practice simply drawing a graph of the objective function is sufficiently informative. If a numerical optimization is called for, then we offer Piyavskiy algorithm that is proven to be optimal for Lipschitz-continuous objectives.

As an example of the two-dimensional optimization problem, we present a calibration procedure for the directed self-assembly (DSA) model, and discuss application of DIRECT optimization method by Jones, Perttunen, and Stuckman.

Linear Programming (LP) belongs to the class of resolved multi-dimensional problems. Lithographic engineers, as well as physicists in general, are mostly not well acquainted with LP apparatus and its 'tricks of trades'. We show one the rare cases when LP is applicable to a physical problem.

In general, the multi-dimensional optimization problems are hard to solve in a reliable manner. The reasonable algorithms are usually gradient-based. We discuss issues with the complexity of gradient calculations. For convex optimization problems, we spotlight Nesterov's family of accelerated gradient schemas, and present results of lithographical mask optimizations.

Analysis of the digital image in terms of different types of blur tools Adobe Photoshop

Kaman K., Lebedeva E., Zorilo V.
Odessa National Polytechnic University, Odessa, Ukraine
jyzel@rambler.ru

Introduction. The use of digital images in contemporary society applies in an increasing number of spheres of human activity. If the image is used as a document, it is important to be able to ensure that it is authentic and contains no unauthorized third party interventions and changes. Sometimes to conceal some details in the photo, or, conversely, to add new images by means of image editors amenable to such manipulations as cloning and photomontage. To hide borders added from other areas (of the same) photos, often using different operations: brightness correction, retouching, blur and so on. Blur contour area after replacement photomontage or cloning, or blur in general - a very common operation processing. In addition, blurring is often used as an attack on steganography image if it contains any hidden links. In any case of blurred digital image allows a high probability to draw conclusions about unauthorized violation of his integrity. And then if that file can be used as a credible document should encourage appropriate action by the sender or recipient of the investigational Photos, Among the known methods for detecting blur today well established method that is based on the general approach to the analysis of the technology and operation of information systems [1]. This method was tested for the detection of Gaussian Blur with a radius of 1 pixel, realized in photo editor Adobe Photoshop (AP).However, in the same editor, there are many other kinds of blur, which have their own characteristics and can also be applied in that context. But so far there had been no detailed study of how this method to cope with the discovery of other types of blur.

The purpose of this study - to analyze the effectiveness of blur detection method based on the general approach to the analysis of the technology and operation of an information system in case of different types of digital image blur.

Main part. The method of digital image blur detection Gaussian analysis is singular values of its units matrix (matrix).When you blur the contours become less expressive, through which reduced the proportion of the high-frequency image signal. This reduces the growth rate of the singular values of matrix blocks in a digital image. That growth rate singular values of blurred images qualitatively different from unblurred. Was experimentally determined threshold, which allows high destiny probability to draw conclusions about the presence of a digital image blur. Research base was formed as photographs of those who received amateurish technique and those who are accepted for experiments [2].So have a digital image blur any of its brightness pixel matrix, if there are several, standard way divided into blocks of 8×88.Each unit should identify a set of singular numbers. Experimentally that have a blur with a radius of 1 pixel (the most difficult to identify situation) is the most effective use of the five smallest singular values in each block for which you want to build a linear approximation and for approximating functions define a derivative whose value (constant) is a growth rate factor these singular values. If the maximum coefficient growth rate among all the 8×88 blocks does not exceed the threshold, the image is blurred. If the average of the coefficient growth rate among all the 8×88 blocks exceeds the threshold - the image has not been blurred. In other cases, the method provides for further examination expert Table 1.

The value of the maximum and average growth rate (KGR) singular values of blocks of digital image blur during (re) blurring image.

Таблиця 1. Table 1. The experimental results

Digital image	Before blur		After Blur											
			Box blure				Blure				Blure more			
	Maximum KGR	Average KGR	Maximum KGR		Average KGR		Maximum KGR		Average KGR		Maximum KGR		Average KGR	
			first Blur	second Blur	first Blur	second Blur	first Blur	second Blur	first Blur	second Blur	first Blur	second Blur	first Blur	second Blur
1.jpg	7.53	4.93	0.20	0.16	0.16	0.13	2.65	2.48	1.74	1.63	1.17	1.00	0.69	0.67
2.jpg	7.27	3.44	0.21	0.18	0.16	0.13	0.85	0.79	0.46	0.40	1.23	1.00	0.49	0.52
3.jpg	6.04	2.90	0.19	0.18	0.15	0.13	2.55	2.38	1.21	1.13	1.27	0.95	0.55	0.48
5.jpg	10.01	6.81	0.22	0.17	0.18	0.14	2.06	1.97	1.23	1.18	1.79	1.37	0.83	0.82
6.jpg	8.19	4.24	0.12	0.11	0.07	0.06	3.24	3.00	1.47	1.40	1.69	1.35	0.78	0.69
87.jpg	4.00	2.77	0.76	0.51	0.35	0.22	1.05	1.05	0.53	0.53	2.35	1.79	1.40	1.09
94.jpg	2.45	2.18	0.16	0.09	0.10	0.05	2.58	2.41	1.60	1.51	1.60	2.48	1.07	1.49
99.jpg	3.03	2.19	0.05	0.04	0.01	0.006	0.80	0.73	0.46	0.46	1.00	0.77	0.55	0.47
104.jpg	4.59	3.62	0.17	0.13	0.12	0.08	2.21	2.14	1.53	1.46	1.37	1.09	0.93	0.80
106.jpg	6.78	5.32	0.05	0.04	0.02	0.01	1.49	1.37	0.90	0.84	0.57	0.40	0.29	0.28

If the indicators that are analyzed, will change more than twice, then the expert blur for the image is the first, otherwise it was blurry before. This threshold was determined experimentally and equals to 1.75.

In the editor, AR today, there are more than eleven types of filters to blur an image. Not all of them, we will consider due to the nature of the use of images. As already noted, the image must be blurred so that visually it was not noticeable. Some types of blur to the editor are not fundamentally able to be invisible, because they leave no footprints, and transform the image on the background (for example, the filter "Averege").However, there are many such filters that are worthy of attention in the context of the problem being solved. This work is the first step in creating a generic method of detecting blur in a digital image.

We consider in this work three types of blur: Box blur, blur and blur more.

The experiment was taken as 100 digital images, 80 of whom are from the public database of digital images [2], and 20 received non-professional photographic equipment and the latest smartphones. At the first blur of the maximum and the average value of the coefficients of the growth rate of singular values of the blocks considerably decreased compared to these same characteristics for neurosmith images. A second blur, as expected, did not significantly change these figures in comparison with the first. The results are presented in the table.

These results are quite logical and Accutane and correlate with the studies that have been conducted in relation to the Gaussian blur in [1].However, there are some differences, namely the threshold value of 1.75 cannot be considered successful to detect the blur, and blur plus, as seen from the table. As for the blur on the frame, carried out with the default settings in the graphic editor, the threshold is even greater, however, may be used.

Conclusion. Therefore, while it is impossible to say that a method developed to identify the Gaussian blur, it is quite suitable for the detection of other types of blur photo editor.It requires detailed research and adaptation of each type of blur.However, as shown by experiment, this method could be the basis for a new universal method of detecting blur in a digital image.

1. Kobozeva A. A., Zorilo V. V. Method of detection results of the blur in a digital image. Scientific and practical journal "Modern special equipment 2010, № 3 (22), C. 52–63.
2. NRCS Photo Gallery: [Electronic resource]. United States Department of Agriculture. Washington, USA. Mode of access: http://photogallery.nrcs.usda.gov (date accessed: 26.03.2016).

Cryptanalysis of asymmetric algorithms using ant colony optimization

Kosukhin N., Shpinareva I.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

ira-shpinareva@rambler.ru

One of the main goals of cryptanalysis is to assess the cryptographic algorithms safety. The asymmetric cryptographic encryption algorithms are still relevant, because the computing systems capacity grows exponentially and the digital signatures popularity is still using in electronic documents, X509 certificates. Today we have got some classical methods of cryptanalysis, such as brut-force search method, Pollard's $p-1$ Method, Pollard's ρ Method, Elliptic Curve Method, and intelligent methods. Among these methods emit bioinspired (evolutionary-genetic) algorithms. These include a genetic algorithm, swarms algorithms (ant and bee algorithms). The RSA algorithm is representing asymmetric cryptosystem. It cryptographic safety is determined laborious factorization of large numbers. The cryptanalysis and the secret key determination accomplished, by making factoring of module N into primes P and Q. In this work we analyze the ant algorithm for the decomposition of N module in the RSA algorithm. Ant colony algorithm used for decomposition of N by factorizations divider determining the number with accuracy in an interval $[n_i, n_k]$. So we have the classical problem: how to find the shortest path in the graph, solved by the ant colonies algorithm. In the algorithm the initial location of the colony established at the beginning of the work. A limited number of agents (ants) M randomly arranged at the vertices of the graph without repetition. The first pheromone level takes a small positive number for the transition probabilities values were not zero. After running the algorithm on the fast track is allocated the highest number of pheromones. The aim of the ant algorithm is to determine the route that contains m vertices and the vertex of the graph $x_j \in [n_i, n_k]$, which are divisor of N with a given accuracy, means if condition correct $F(x_j) = \left(\frac{N}{x_j}\right) - \left[\frac{N}{x_j}\right] \to \min$. To construct a suitable ant algorithm to solve a problem, it is necessary to present the problem as a set of components and transitions, to determine the value of pheromone. The determining parameters are: the number of ants, a balance between the study and the use of a combination of a greedy heuristics and torque pheromone update. The software application was developed in C# using .NET technologies in the Microsoft Visual Studio Community runtime environment. The test showed the dependence between the iterations number and number of routes in a given initial configuration algorithm, and also on parameters such as the amount of evaporation of the iteration "pheromone the accuracy of the route and the route length.

Таблиця 1. Table 1 – Algorithm testing results

N	**Multipliers**	**Initial configuration**	**Ant algorithms iterations number**	**Brute-force iterations number**
16123897	$23, 37, 18947$	$[5, 20000]$, $Q=4$, $m=6$, $M=6$	599	4015
4154963851	$3943, 1053757$	$[3000, 2000000]$, $Q=4$, $m=12$, $M=8$	2346	64459
		$[3000, 2000000]$, $Q=4$, $m=4$, $M=4$	2758	

The report reviews the composite numbers factoring by using the ant algorithm and it comparison with brute-force method.

Steganographic method for digital images authentication

Kozin A.[2], **Kozinf M.**[1], **Papkovskaya O.**[1]

Odessa National Polytechnic University, Odessa, Ukraine[1],
National University "Odesa Academy of Law Odessa, Ukraine[2]

kozindre@rambler.ru, mashaK1989@rambler.ru

Today steganography methods not only allow hidden store and transmit information, but also helps to effectively solve problems of protecting information related to unauthorized copying, search data in multimedia databases [1].

Modern scientist papers [2] proposes a solution for the authentication of information transmitted through a communication channel the implementation of a digital image authenticating mark. In paper [2, 3] for the implementation of authenticating marks authors proposed steganographic algorithm (SA) that uses a singular domain / spectral decomposition of the container matrix, which ensures the stability of the developed algorithms even in significant disturbing influences. Let selected steganography algorithm $A1(t)$, where t - selectable option.

The effectiveness of the selected SA will be evaluated standard using the peak ratio "signal to noise named PSNR. In open sources assumed that the value $PSNR > 37\ dB$ points to a perception of compliance with reliability corresponding steganographic message (Table 1).

Val. \ A(t)	**A1(10)**	**A1(20)**	**A1(30)**	**A1(40)**	**A1(50)**	**A2**
Average	70,70	70,01	69,83	69,51	69,19	52,58

Таблиця 1. Table 1. Peak ratio signal to noise for some SA

The paper presents analysis of the SA to implement authenticating mark, as well as high efficiency of modern selected SA so you can use them as part of a comprehensive three-pronged modern steganography task. The computational complexity of developed steganographic method for digital images authentication using embedding additional information thereby organizing covert communication channel and algorithms that implement them represented by polynomials of degree 2 [2,3].

1. Fridrich J. Steganography in Digital Media: Principles, Algoritms and Applications, 2010, p. 441.
2. Кобозева А.А., Козина М.А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных. Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова, 2014, №3(26), С. 93–106.
3. Кобозева А.А., Козина М. А. Метод скрытой передачи данных, обеспечивающий проверку целостности и аутентичности передаваемой информации. IMMM, 2015, **T.5**, 1, С. 57–64.

Model of hybrid intelligent system for image analysis

Krapivny Yu., Kryvonos O.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

geraclion@gmail.com

Hybrid intelligent systems are well-known instruments for combination of different artificial intelligence techniques in one system either distributed or monolithic. There are three major architecture types of hybrid intelligent systems: unified neural architecture, transformational architecture and hybrid modular architecture. Hybrid modular architecture type divides into three subtypes: loosely-coupled, tightly-coupled and fully-integrated architecture types. Hybrid intelligent system approach allows to combine advantages of artificial intelligence techniques and minimize their drawbacks. The aim of the research is to develop and implement model of fully integrated modular hybrid intelligent system which consists of two interacting modules: artificial neural network and fuzzy logic system. The constructed model is used for tasks of image analysis and object recognition. The artificial neural network module is responsible for low-level objects recognition while the fuzzy logic module is responsible for combining low-level objects into higher-level objects.

A unified approach to hierarchical classifications

Lisitsyna I., Petrushina T., Trubina N.
I.I. Mechnikov Odessa National University, Odessa, Ukraine
tatyana.petrushina@gmail.com

In the second half of the 20th century, identification theory had taken shape, principles and methods of compiling and application of keys for identification of biological objects had been developed. Hierarchical classifiers [1] have been widespread in almost all areas of human activity. Hierarchical classifiers express the taxonomy and nomenclature in biology, mineralogy, soil science, medicine, librarianship, and so on. Such classifiers presents the taxonomy and nomenclature in biology, mineralogy, soil science, medicine, librarianship, and so on. A classifier having a hierarchical structure often is called a taxonomy, and object of a classification is called a taxon [2].

The problem of finding an object position in the hierarchy, that is, assigning an object to a certain taxon by its features, is far from trivial. Moreover, these features which are used as definition keys, are also often classified according to a hierarchical basis.

Finding an object position in the classifier is often complicated by the fact that value of some features is unknown and the known values of features belong to different sets. This search strategy is proposed to provide with the help of multi-polytomous key.

The article describes a unified approach to the design of the data model for supporting a universal hierarchical classifier. The system should include the two hierarchies: one for a taxonomy nomenclature systematics and other one for a maintenance of key sets. The main characteristics of objects of the model are the same, regardless of the subject area. Implementation and tuning can be built by using inheritance mechanisms.

The stated ideas have been implemented in a prototype system, which has been used to build qualifiers of flowering plants, minerals and soils with appropriate filling of the database. This has confirmed the effectiveness of the proposed approach and its practical value.

1. Иночкин А.А, Кирейчук А.Г., Лобанов А.Л., Смирнов И.С., Степаньянц С.Д. Интернет-определители биологических объектов. 5 лет спустя Научный сервис в сети Интернет: экзафлопсное будущее. Труды Международной суперкомпьютерной конференции (19–24 сентября 2011 г., г. Новороссийск). Издательство МГУ, Москва, 2011, p. 449-–453.
2. Шаталкин А.И. Таксономия. Основания, принципы и правила. М.: Издательство: Товарищество научных изданий КМК, 2012, С. 600.

A criterion of elementary divisor domain for distributive domains

Malakhov E.[1]**, Mezhuyev V., Shchelkonogov D.**[2]
I.I. Mechnikov Odessa National University, Odessa, Ukraine
opmev@mail.ru[1]*, delis91@gmail.com*[2]

Classification of mass problems (MP) is essential for efficient control of the corresponding production subject domain (PSD) [1] and studying of MPs themselves. Three approaches of building classification algorithms are proposed: extracting, structural, and hybrid. Extracting algorithms operate on the history of functioning of the given PSD and extract the necessary information from it using operations, defined on the PSDs. Structural algorithms operate on the known structure of mass problems. Hybrid algorithms use both extracting and structural approaches. Several groups of classes of mass problems are proposed. The most generic group of classes of MPs consists of three classes: changing MPs, evaluating MPs, and target MPs. Changing MPs change the state of PSD, evaluating MPs allow rating the state of PSD, target MPs are MPs, which the given PSD is aimed to solve. Another group of classes of MPs is a subgroup of changing mass problems. Each class corresponds to the tuple (MP, attribute of the PSD or its object, marker of change). Basing on this classification it is possible to choose MPs to influence specific attributes of specific objects of the PSD to control it efficiently.

1. Malakhov E., Shchelkonogov D., Production subject domains.- International Conference on Electronics and Information Technology, Odessa, Ukraine, May 23-27.- 2016.- pp. 87-91.

Review of methods of analysis of educational and organizational information to improve the quality of specialist training

Malakhov E., Tsariuk A.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

poltavacortkx1q@mail.ru, eugene.malakhov@onu.edu.ua

The main purpose of management educational division of the University is to improve quality of specialist training produced by the university. At the level of the department one of the problems to be solved in order to achieve this goal is the choice of teachers reading the appropriate discipline and load distribution between the teachers. However, simple and direct solution to this problem is largely subjective.

Improving the efficiency of such a decision can be based on the analysis of large volumes of diverse structured and unstructured, operational and historical information. Such analysis will help identify patterns between the academic performance of students, mastery of discipline material, information characteristic of a teacher (scientific, methodical, practical etc.), the structure of the curriculum and the working program of discipline.

Performing of this analysis was decided to be done with the help of various Data Mining methods in combination of Big Data methods.

For example, dependencies between student academic performance, his grades on related subjects and the teacher is supposed to be identified by applying the clustering method. Thus it is possible to obtain information about the student's perspectives on a particular subject. If using self-learning techniques, such as EM, high speed processing of large data can be achieved, all with increasing the accuracy of calculations [1].

However, to determine the dependencies of the given example, it may be a more effective way to use a method of association rules. Answering that will be possible after conducting an appropriate studies [2].

The same method seems appropriate for solving the problem of the evaluation of the structure of the curriculum based on dependencies between disciplines and its influence on the quality of education. However, due to the large volume of unstructured information associated with the curriculum in the form of working programs of disciplines, it is suggested to create an algorithm that combines Data Mining techniques with MapReduse method [3], for a preliminary analysis of such data.

1. Hamparsum Bozdogan Statistical Data Mining and Knowledge Discovery. July 29, 2003 by Chapman and Hall/CRC Reference. – 624 p.
2. Data Mining [E-resource]. – Acces Mode: https://basegroup.ru/community/articles/data-miningin. – in Russian.
3. MapReduce or calculation out of memory and CPU capability [E-resource]. – Acces Mode: http://ng-table.comhttps://habrahabr.ru/post/103467. – in Russian.

Development of the effective vocabulary structures for the speech recognition tasks

Mazurok I., Zahanich D.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

i.e.mazurok@gmail.com, dimazaganich@yandex.ru

In recent decades mankind faced the problem of creating effective tools for data input. Today personal computers are used not only by specialists, who are capable of fast typing, but also by regular users with poor computer skills. Conventional data input methods require performing some actions by user's hands and often prohibits user from performing others tasks at the moment of data input. However, speech recognition methods doesn't have these disadvantages. It took almost half a century to improve speech recognition systems for widespread usage [**?**]. Researchers and developers of such systems had to solve a lot of problems [**?**]:

- the problem of the extraction of the desired information from an audio signal;
- the problem of the classification of the extracted information from an audio signal;
- necessity of extensive training of speech recognition systems because of a large number of words pronunciation variants;
- low overall performance of speech recognition systems.

The primary goal of this article is to develop speech recognition method, which is capable of running on the mobile device with limited computational power. We focus on reducing the size of the dictionary, which is key component of every speech recognition system.

Proposed solution to speech recognition task can be used effectively in cases where the speech recognition system has low computational resources and is not supposed to recognize complex grammatical structures. Such cases may include remote control systems with a small vocabulary of control commands.

1. Alex Acero, Hsiao-Wuen Hon, Xuedong Huang. Spoken Language Processing: A Guide to Theory, Algorithm and System Development. — Prentice Hall PTR, 2001, 480 p.
2. Zakaria Kurdi. Automatic Speech Processing and Natural Languages. — ISTE Wiley, 2016, **v.1**, 720 p.

An analysis of the heuristic method for constructing Bayesian networks in terms of program implementation within the framework of extensible architecture

Penko V., Taran Ye.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

yevgenii.taran@gmail.com

Nowadays mobile devices contain a lot of raw data. It can be collected from interaction with user, or from mobile sensors. To retrieve useful information from sensors, data mining methods have to be used. One of well suited for this situation data mining tool is Bayesian networks. To use Bayesian network at first its structure should be built.

In the article heuristic method of Bayesian network construction is described. All steps of network creation were analyzed and the way for improving quality of built Bayesian network was suggested. It consists of interaction with a user during the process of Bayesian network building. In some cases it gives positive result. The method was implemented on the mobile platform Android.

For making the idea of getting value from raw data on mobile devices more real, the architecture of expert system based on Bayesian networks is provided. It contains four modules: data processing, network structure, network building and user interaction. Each module goal is described within the framework of extensible architecture along with implementation of heuristic method. The program architecture provides possibility to expand the application with new functionality basing on developed code. Presented research provides a tool for usage of Bayesian networks on mobile devices.

The Fibonacci Q-matrix coding method

Petrushina T., Sviridov A.
I.I. Mechnikov Odessa National University, Odessa, Ukraine
tatyana.petrushina@gmail.com, laestr.path@gmail.com

The question of effective data encoding and protection in communication channels is rather important in modern IT sphere. Most of the known error detection and correction codes make it possible to restore single bits or combinations of bits; however, the types or errors become more diverse, and some unusual methods may be required. The central method discussed in this work is the Fibonacci Q-matrix coding method, which allows correcting theoretically unlimited sizes of damaged data in certain cases [1].

The aim of the research is to evolve the coding methods based on Fibonacci numbers. The following tasks were set to achieve this:

1. Study and formalize properties of the Fibonacci numeral system and the coding methods based on it.
2. Develop software libraries which implement the researched coding methods.
3. Make a comparative analysis of performance of the methods.

The standard Fibonacci Q-matrix coding method has been formalized. Its implementation was upgraded with the Fibonacci coding [2], a detailed implementation design has been introduced. A new "block Q-matrix method"has been developed, which divides the message in fixed size segments and applies the standard method on them. A software implementation of both standard and block Q-matrix methods has been done. A comparative analysis of the algorithms has been made.

The standard Fibonacci Q-matrix method makes it possible to correct unlimited sizes of damaged data, although the errors must happen only inside the predefined parts of the message; otherwise the whole message will become unreadable. The developed "block Q-matrix"method proved itself more effective in data restoring than the standard, both with single damaged bytes allocated throughout the message and series of consecutive error bytes. The undamaged parts of the message remain intact in any case.

1. Zabavsky B. V. Diagonal Reduction of Matrices over Rings. — Lviv: Math. Stud. Monogr. Ser., 2012, **XVI**, 251 p.
2. «Фибоначчиевое» кодирование [Electronic resource]. Музей Гармонии и Золотого Сечения – Access: http://goldenmuseum.com/1508FibCode_rus.html.
3. Fraenkel A.S., Klein S.T. Robust Universal Complete Codes for Transmission and Compression [Electronic resource] – Access: http://www.sciencedirect.com/science/article/pii/0166218X9300116H

The comparison of the web applications development frameworks Ruby on Rails, Django and Grails

Rogowski J.

Branch of the University of Lodz in Tomaszow Mazowiecki
Konstytucji 3 Maja str., 65/67, Tomaszow Mazowiecki, Poland
jasiorog@gmail.com

The main goal of this work is to evaluate a few of the most promising and so-called cutting-edge technology frameworks for the web application development and to find out which ones support the criteria in place for present-day services. These criteria are related to the productivity, powerful features, security, flexibility scale, performance, learning curve, and size of the community. The technologies chosen for appraising are Ruby on Rails written in Ruby, Django written in Python, and Grails written in Groovy. To achieve the stated goals, three web applications have been created in the above-specified technologies. They have the same database scheme, sample dataset and front-end interface. In order to perform the evaluation of the frameworks a comparison between frameworks is presented, showing the features, helpers, and methods in a few examples. The second phase presents benchmarks for the most popular actions in the web application. All benchmarks results have been counted by the application written in Java. This application uses HTTP requests to get access to tested applications and to trigger examined actions. The results are plotted by Gnuplot command-line driven graphing utility. Finally, a subjective evaluation considering the learning curve, IDE support, size of the community, and time needed to set up the entire environment are presented.

System for the Sale of Intellectual Property through IPTV

Rychlik A.

Instytut Informatyki Politechnika Łódzka, Łódz, Poland

andrzej.rychlik@p.lodz.pl

In this paper presents the information system managing the delivery of television programs from the headend to the set top box. Through the upstream information is transfered from which the television channel set top box sends the television program to your TV set, smartphone or computer. On this base, the system counts the fee of the subscriber and sends them to the broadcaster of chosen television program. The implementation of this system is important, because the subscriber has access cable television with 200 television channels and in satellite television with 1000 television channels. Now, the subscriber has to pay the subscription of package of television program but he watches only one. The fee was billed as a potential opportunity to watching, not his actual watching. That system was working in analog television and in digital television without upstream. When owner of broadcaster is state the subscription is quasi task and citizen has no influence for its distribution. When the market of television channels is realized via packages also subscriber has no influence which commercial broadcaster received and how much of subscription. The system is described in this work requires high level security because it may be exposed to attack from subscribers or broadcasters. Further development of the system also include television streaming on mobile devices and local programs on cable television. In the new information system will also be calculated on the remuneration payable to the organization of collective management of copyright and related rights.

Divisor problem in special sets of gaussian integers

Savastru O.
I.I. Mechnikov Odessa National University, Odessa, Ukraine
sav_olga@bk.ru

Let A_1 and A_2 be fixed sets of the Gaussian integers. $\tau_{A_1,A_2}(\omega)$ is the number of representations of ω in form $\omega = \alpha\beta$,where $\alpha \in A_1$, $\beta \in A_2$. By the $\tau_S(\omega)$ we denote the function $\tau_{A_1,A_2}(\omega)$ in case, when $A_1 = \mathbb{Z}[i]$, $A_2 = S(\varphi)$ is a fixed sector of complex plane
$S(\varphi) = \left\{\omega \in \mathbb{Z}[i] : 0 \leqslant \varphi_1 < \arg\omega \leqslant \varphi_2 \leqslant \frac{\pi}{2}, \varphi = \varphi_2 - \varphi_1\right\}$.
Let

$$T(x,\gamma,\omega_0,S(\varphi)) = \sum_{\substack{\omega\equiv\omega_0 \pmod\gamma,\\ N(\omega)\leqslant x}} \tau_S(\omega).$$

Applying the method of Vinogradov we get the asymptotic formula in case, when the norm of a difference of progression grows.

Theorem. *Let $\gamma,\omega_0 \in \mathbb{Z}[i], N(\gamma) > 1$, $(\omega_0,\gamma) = \beta, N(\beta) < N(\gamma)$. Then for every $\varepsilon > 0$, $x \geqslant N^{\frac{3}{2}}(\gamma)$ and $\varphi_2 - \varphi_1 \gg \frac{N^{\frac{3}{4}}(\gamma)}{x^{\frac{1}{2}-\epsilon}}$ the following formula holds*

$$T(x,\gamma,\omega_0,S(\varphi)) =$$

$$= \frac{2(\varphi_2-\varphi_1)}{\pi}\left(c_0(\gamma,\omega_0)\frac{x}{N(\gamma)}\log\frac{x}{N(\gamma)} + c_1(\gamma,\omega_0)\frac{x}{N(\gamma)}\right) + O\left(\frac{x^{\frac{1}{2}+\epsilon}}{N^{\frac{1}{4}}(\gamma)}\right),$$

where $c_0(\gamma,\omega_0), c_1(\gamma,\omega_0)$ are computable constants.

1. Varbanec P.D. Zarzycki P. Divisors of the Gaussian Integers in an Arithmetic Progression[text]. J.Number Theory, 1990, **V.33**, pp. 152–169.

Document-oriented graph as a way of saving semistructured medical data

Shvorob I.
Lviv Politechnic National University, Lviv, Ukraine
irka.shvorob@gmail.com

A rapid increase in the amount of information the search for new approaches to solving the problem of preservation became a necessity. It is believed that non-relational databases (NoSQL) are most suitable to preserve it semistructured data. Compared with relational databases, NoSQL databases easily scalable and provide excellent performance and solve problems for which relational model is not designed. Working with semistructured data is important to preserve as much as possible in the most quick for use form. Document-oriented graph database introduced at a higher difficulty data node graph, that is, when the count is node element with many different characteristics.

It was analyzed semistructured data processing for different types of databases: Document-based, Graph-based, Document-oriented graph. The analysis was carried out on the following parameters: number of created objects, weight database, time of record in the database, time of executing query with multiple conditions. The research found that the document-oriented graph has the greatest weight and the recording of data, but it requests are faster.

It should be noted that document-oriented database is very convenient for data processing in semistructured medical data area.

Choose between NoSQL technologies depends on many factors (problem statement, qualifications developer, features hardware requirements that the speed, etc.) so unequivocal recommendation that a database should be used cannot be given. To a large extent it depends on the project requirements.

1. NoSQL Database Couchbase. Recourse: http://www.couchbase.com/nosql-resources/what-is-no-sql.
2. Planet Cassandra. Recourse: http://www.planetcassandra.org/what-is-nosql/.

Character sums over $\mathbb{Z}[i]$

Varbanets P.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

varb@sana.od.ua

Let G_p^n be the multiplicative group of invertible of the ring $\bmod p^m$ of the Gaussian integers, $p \equiv 3 \pmod 4$ be a prime rational number.

We obtain a non-trivial estimates of the exponential sums of type

$$\sum_{S(T_1,T_2;f)} e^{2\pi i \Re(\frac{\alpha x+\beta y}{p^m})},$$

where $S(T_1, T_2; f)$ denotes that the Gaussian integers x, y run the solutions of the congruence $f(x, y) \equiv 0 \pmod{p^m}$ under the condition $N(x) \leqslant T_1$, $N(y) \leqslant T_2$, $f(x, y) \in G[x, y]$, $G = \mathbb{Z}[i]$.

Sequences of PRN's produced by circular generator

Varbanets S.
I.I. Mechnikov Odessa National University, Odessa, Ukraine
varb@sana.od.ua

The sequence of real numbers $\{a_n\}$, $0 \leqslant a_n < 1$, we call the sequence of pseudorandom numbers (arbitrary, PRN's) if it is produced by deterministic generator and being a periodical sequence has the statistical properties such that it looks like to implementation of the sequence of random numbers with independent and uniformly distributed values on $[0, 1)$. More acceptable sequences of PRN's are generated by the congruential recursion

$$y_{n+1} \equiv f(y_n, y_{n-1}, \dots, y_{n-k+1}) \pmod m$$

with some initial values $y_0, y_1, \dots, y_{k-1} \in \{0, 1, \dots, m-1\}$, where $f(u_1, \dots, u_k)$ is integer-valued function over $\mathbb{Z}_m^k$.

Our main aim here is to elucidate the motivation for constructing circular generator of the sequences of PRN's with some specific properties that be faster of its usage in cryptography. Our exposition focuses on some special measures of "randomness"with respect to which "the good"sequences have been produced by using of norm group E_m. A quantive measure of uniformity of distribution of a sequence may be the so-called discrepancy. Originated from a classical problem in Diophantine approximations this concept has found applications in the analysis of PR sequences on uniformity and unpredictability. From the well-known Turan-Erdös-Koksma inequality it is evident that the main tool in estimating discrepancy is the use of bounds on exponential sums over on elements of the sequence of PRN's.

Let p be a prime rational number, $p \equiv 3 \pmod 4$. Let us denote by E_m the following subgroup of $G_{p^m}^*$

$$E_m := \{x \in G_{p^m}^* : \ N(x) \equiv \pm 1 \pmod{p^m}\}.$$

We will make use the following sequences produced by a generating element $u + iv$ of E_m.

Denote

$$x_n^{(k)} := \Re((u+iv)^{2(p+1)n+k}),$$
$$y_n^{(k)} := \Im((u+iv)^{2(p+1)n+k}).$$

We generate the family of the sequences of congruential PRN's which associated with the sequences $\{x_n(k)\}$ and $\{y_n(k)\}$. Depending on a select $k \in \{0, 1, \dots, 2p+1\}$ we will construct the special sequences of PRN's.

Let

$$z_n^{(k)} := \frac{x_n^{(k)}}{1 + v_0(k) y_n^{(k)}} \pmod{p^m}, \tag{1}$$

where $v_0(k) = v(k) + p^2 v_1(k)$, $(v_1(k), p) = 1$.

Theorem 1. *The discrepancy of the sequence* $\left\{\frac{X_n^{(s)}}{p^{m-1}}\right\}$, $X_n^{(s)} = \left(z_n^{(k)}, \ldots, z_{n+s-1}^{(k)}\right)$, $s = 1, 2$, *has the following bound*

$$D_N^{(s)} \leqslant \frac{s}{p^{m-1}} + \frac{2p^{\frac{m-1}{2}}}{N}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^s, \ 0 < N \leqslant \tau.$$

For the lower estimate $D_N^{(2)}$ we prove the following statement.

Theorem 2. *Let p be a prime number, $p \equiv 3 \pmod 4$ and let $z_n^{(k)}$ defined by the relation (1), $k \not\equiv 0 \pmod{\frac{p+1}{2}}$. Then for the sequence $\{w_n^{(k)}\}$, $w_n^{(k)} = \frac{z_n^{(k)}}{p^m}$, $n = 0, 1, \ldots, \tau - 1$, we have*

$$D_\tau^{(2)}(W_0^{(k)}, W_1^{(k)}, \ldots, W_{\tau-1}^{(k)}) \geqslant \frac{1}{4(\pi+2)}p^{-\frac{m-1}{2}},$$

where $W_n^{(k)} = (w_n^{(k)}, w_{n+1}^{(k)})$, $n = 0, 1, \ldots, \tau - 1$.

The Laplace transform for a pair of the Hecke Z-functions

S. Varabnets, Ya. Vorobyov

I.I. Mechnikov Odessa National University, Odessa, Ukraine

varb@sana.od.ua, yashavo@mail.ru

Let Z_m Let $Z_m(s;\alpha,\beta)$ be the Hecke zeta-function defined for $\Re s > 1$ by an absolutely convergence sieve

$$Z_m(s;\alpha,\beta) := \sum_{\substack{\omega\in\mathbb{Z}[i]\\ \omega\neq-\alpha}} e^{4miarg\omega} e^{2\pi i\Re(\beta\omega)} N(\omega+\alpha)^{-s},$$

where α, β are the fixed Gaussian numbers, $N(\omega) := |\omega|^2$, the summation variable ω runs all Gaussian integers excepts $\omega = -\alpha$ if $\alpha \in \mathbb{Z}[i]$.

We proved the following theorem.

Theorem. *Let δ and γ be the Gaussian integers, $(\delta,\gamma) = 1$. Then*

$$\begin{aligned} &L_{F_m}(s;\delta,\gamma)\\ &= 4\pi^3 e^{i\frac{\pi-s}{2}}\left[\pi\prod_{\mathfrak{p}|\gamma}\left(1-\frac{1}{N(\mathfrak{p})}\right)^{-1}\left(\log N(\mathfrak{p})+\frac{\varphi(\gamma)}{\pi}b_0(\gamma)\right)-\frac{i(\pi-s)}{2}\right]\\ &+\lambda_0(s,\delta,m), \end{aligned}$$

where

$$b_0(\gamma) = \pi\prod_{\mathfrak{p}|\gamma}\left(1-\frac{1}{N(\mathfrak{p})}\right)^{-1}\left(E+\frac{L'(1,\chi_4)}{L(1,\chi_4)}+\sum_{\mathfrak{p}|\gamma}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p}-1)}\right),$$

E is the Euler constant, $L(s,\chi_4)$ is the Dirichlet L-function with non-trivial character mod4. *Moreover, the function $\lambda_0(s,\delta,m)$ is analytic for $|\sigma| < \frac{\pi}{2}$, and the estimate $|\lambda_0(s,\delta,m)| \ll (1+|s|)^{-1}$ holds for $|\sigma| \leqslant \theta$, $0 < \theta < \frac{\pi}{2}$.*

This result uses for studying the modified Mellin transform of $A_m(s,\alpha,0)Z_m(s,0,\beta)$.

Congruential generator of complex PRN's

Tran The Vinh
Hue, Vietnam
ttvinhcntt@yahoo.com.vn

The sequences of complex pseudo-random numbers (PRN's) producing by powers of generating element of the norm group E_m in the residue class ring modulo p^m (p is a rational prime) over the ring of Gaussian integers are studied.

We proved the following analogue of the Turan-Erdös-Koksma inequality (see, [1])

Theorem. *Let $M > 1$ be integer. Then for any sequence $\{y_n\}$, $y_n \in G_M$, the discrepancy D_N of points $\left\{\frac{y_n}{M}\right\}$ satisfies the inequality*

$$D_N \leqslant 2\left(1-\left(1-\frac{2\pi}{M}\right)^2\right)+ \\ +\frac{1}{M}\sum_{\substack{\gamma\in G_M\\ \gamma\neq 0}}\min\left(\frac{1}{|\sin\pi\Re(\gamma)|},\frac{1}{|\sin\pi\Im(\gamma)|}\right)\frac{1}{N}\left(|S_N|+O\left(N^{\frac{1}{2}}\right)\right),$$

where $S_N=\sum\limits_{n=0}^{N-1} e_M(\Re(\gamma y_n))$.

1. H. Niederreiter Random Number Generation and Quasi-Monte Carlo Methods. SIAM, Philadelphia, 1992.

Optimization techniques in implementation of linear time-invariant control systems

Volkova A.
Sorbonne Universités, UPMC Univ Paris 06, UMR 7606, LIP6
4, place Jussieu 75005 Paris, France
anastasia.volkova@lip6.fr

A digital filter, or a general digital signal processing system, operates on a discrete input data to produce a discrete output by means of a computational algorithm. We are interested in such algorithms that are implemented for control applications in embedded systems.

A discrete Linear Time Invariant (LTI) control system is a numerical application that transforms an input signal $\{\mathbf{u}(k)\}_{k\geqslant 0}$ into an output signal $\{\mathbf{y}(k)\}_{k\geqslant 0}$, where $k \in \mathbb{N}$ is the step time:

$$\mathcal{H}\begin{cases} \mathbf{x}(k+1) &= \mathbf{A}\mathbf{x}(k) + \mathbf{B}\mathbf{u}(k) \\ \mathbf{y}(k) &= \mathbf{C}\mathbf{x}(k) + \mathbf{D}\mathbf{u}(k) \end{cases}, \tag{1}$$

where $\mathbf{x}(k)$ is the state vector and $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ and $\mathbf{D}$ are the state-space matrices holding coefficients of the system.

Regardless of the type of embedded system, the data processed by the control system is ultimately stored in memory registers with finite capacity. Therefore, all the computations are performed in finite-precision arithmetic and thus result in an inherent limitation on the accuracy of the result.

In our work we investigate the effects of finite-precision implementation of LTI systems like (1). We apply a rigorous computer arithmetic approach to evaluate the errors due to those effects in order to provide a reliable implementation. However, the control system implementation is usually performed under various constraints.

In order to meet those constraints we have defined numerous optimization problems. These problems usually aim to minimize the errors due to the finite-precision computations, or to minimize the memory consumption, or to obtain a tradeoff between these two criteria, etc. In this work we present an overview of linear and non-linear mixed integer programming problems that arise during the reliable implementation of control systems in Fixed-Point Arithmetic.

r-DIVISOR OVER $\mathbb{Z}[i]$

Vorobyov Ya.

I.I. Mechnikov Odessa National University, Odessa, Ukraine

yashavo@mail.ru

We say that the Gaussian integer δ is an r-divisor of the Gaussian integer α fro the ring of Gaussian integers if δ divides by α for any power prime $\mathfrak{p}^a$, $\mathfrak{p}^a||\delta$, it follows that $a = r$ or $\mathfrak{p}^a||\alpha$. In our talk we study the distribution of means of the function $\tau^{(r)}(\alpha) = \sum \delta$ is r-divisor of $\alpha 1$ and prove the following theorems:

Theorem 1. *For* $x \to \infty$

$$\sum_{N(\alpha)\leqslant x} (\tau^{(r)}(\alpha))^{-1} = \begin{cases} \frac{3}{8}x\log x + A_0 x + O\left(x^{\frac{1}{2}}(\log x)^{\frac{17}{3}}\right) & if \quad r = 0, \\ 4\zeta(r+1)L(r+1,\chi_4)x + O\left(x^{\frac{1}{2}}(\log x)^2\right) & if \quad r \geqslant 1. \end{cases}$$

Theorem 2. *For any small* $\varepsilon_1 > 0$, $\varepsilon_2 > 0$ *uniformly at* x *and* h, $x^{\frac{2}{3}+\varepsilon} \leqslant h \leqslant x^{1-\delta}$, *we have*

$$\frac{1}{h}\sum_{x<N(\alpha)\leqslant x+h} \tau^{(r)}(\alpha) = \sum_{j=0}^{N} c_j(\log x)^{-j} + O((\log x)^{-N-1}) + O(exp(-(\log x)^{-\frac{1}{6}}))$$

for any positive integer N, *where* c_j *are the calculable constants and constants in symbols "*O*"depend only on* N, ε_1, ε_2.

These statements generalize the similar results over $\mathbb{N}$.

1. Lelechenko A.V., Vorobyov Ya.A. On the divisors of order r. Int. J. Pure App. Math, 2015, 98(2), pp. 181-192.

Modeling of Multiprocessor Control Systems

Waszkielewicz W., Petryshyn L.
AGH University of Science and Technology, Krakow, Poland
waszkiel@zarz.agh.edu.pl, l.b.petryshyn@gmail.com

Системы управления являются сложными и дорогими программно-техническими комплексами. Решение проблемы оптимальной диспетчеризации и обработки входного потока задач позволяет на стадии проектирования экономически обосновать архитектуру и состав технических средств систем управления и минимизировать их стоимость.

Решение проблемы увеличения производительности средств вычислительной техники заключается в распараллеливании процедур обработки информационных потоков и использовании многопроцессорных компьютеризованных систем, что предусматривает значительные инвестиции на их изготовление и требует корректного подхода к определению и анализу характеристик входных информационных потоков, а также рассчету технико-экономических параметров вычислительной системы, разработке структуры и определению процедуры обслуживания инфопотоков в вычислительной системе.

Авторами обосновано целесообразность проектирования многопроцессорных вычислительных систем управления (МПВСУ) на базе определения количества процессоров, их быстродействия, разрядности, объемов памяти в зависимости от объемов информации, подлежащей обработке с применением аппарата теории массового обслуживания.

Проанализирована аналитика моделирования систем с квазирегулярным, случайным, стационарным характером потоков данных, а также наиболее часто встречающихся на практике элементарных потоков, одновременно обладающие свойствами стационарности, ординарности и отсутствием последействия.

Аналитически определены такие параметры как:

- показатели времени обслуживания, которые характеризуют производительность МПВСУ;
- показатели механизма обслуживания, которые характеризуют пропускную способность;
- дисциплина очереди, формирование которой предполагает анализ следующих факторов: правила отбора задач, поступающих в систему обслуживания; наличие и уровни приоритетов; ограничения на размер очереди; ограничения на время ожидания в очереди.
- механизмы обслуживания приоритетов: в системе без прерывания и с прерыванием обслуживания; с несколькими альтернативными шкалами приоритетов и выбором одного из них; ограничением и без на длину очереди; со старением данных входного потока задач.

Проанализированы процессы обслуживания в следующих типовых схемах МПВСУ:

- одноканальных системах с ожиданием;

- системах с ограниченной очередью;
- системах с потерями;
- многоканальных системах с общей очередью;
- системах с ограниченной очередью ожидания;
- система с приоритетом обслуживания;
- системах с ненадежными устройствами обслуживания.

Определены критерии эффективности функционирования и показатели качества обслуживания МПВСУ: вероятности потери задачи в системах с потерями; функции распределения времени ожидания задачи; среднего времени ожидания; распределения интервала занятости; распределения величины очереди.

В материале приведены результаты анализа параметров оценки МПВСУ, основные методы и структуры распараллеленного преобразования входных потоков задач, критерии оценки эффективности функционирования и показатели качества облуживания в компьютеризованных системах управления. Разработка имеет прикладное значение при проектировании МПВСУ, позволяет построить оптимизированные математические модели обработки потоков данных и на их основе получить оптимальные технико-экономические параметры проектируемых систем управления.

Компьютерная алгебра трехмерных матриц

Воробьев Г., Гальмак А.

Могилёвский государственный университет продовольствия,
Могилёв, Республика Беларусь
halm54@mail.ru

В [1] для произвольного целого $\ell \geqslant 3$, любой подстановки σ из S_m и любой ориентации $r \in \{i, j, k\}$ на множестве всех трехмерных матриц над ассоциативным кольцом P, у которых размер, соответствующий индексу r, равен m, а два оставшихся размера могут отличаться от m, но совпадают, определяется ℓ-арная операция $[\ ]^{(r)}_{\ell,\sigma,m}$. Если подстановка $\sigma \in S_m$ удовлетворяет условию $\sigma^\ell = \sigma$, то три операции $[\ ]^{(i)}_{\ell,\sigma,m}$, $[\ ]^{(j)}_{\ell,\sigma,m}$ и $[\ ]^{(k)}_{\ell,\sigma,m}$ ассоциативны.

В данном сообщении нами решена задача компьютерного моделирования явного вида многоместной ℓ-арной операции $[\ ]_{\ell,\sigma,k}$, определенной на k-ой декартовой степени A^k полугруппы A. Разработан алгоритм и программа формирования пространственной матрицы по заданному сечению и определения её другими сечениями, а также программная модель операций $[\ ]^{(i)}_{\ell,\sigma,m}$, $[\ ]^{(j)}_{\ell,\sigma,m}$, $[\ ]^{(k)}_{\ell,\sigma,m}$.

В системе Mathcad: разработаны функции, которые по заданному сечению трехмерной матрицы находят сечения других ориентаций; на множестве $M_{m\times n\times p}(P)$ всех пространственных матриц одного и того же размера $m \times n \times p$ над полем P смоделированы операция сложения пространственных матриц и операция умножения всякой пространственной матрицы $(a_{ijk})_{m\times n\times p} \in M_{m\times n\times p}(P)$ на любой элемент λ из P. Разработана функция, моделирующая операции $[\ ]^{(r)}_{\ell,\sigma,m}$, $r \in \{i, j, k\}$.

1. Гальмак, А.М. Полиадические операции и обобщенные матрицы. —Могилёв: МГУП, 2015, 295 с.

Решение задач оптимизации на Visual Prolog

Любота В.

Одесский национальный университет им. И.И.Мечникова, Одесса, Украина

vladlubota@yandex.ua

Пролог – язык декларативного программирования. Программа на Прологе может решать не одну, а множество задач некоторой предметной области. Эти задачи мы можем извлекать несколько видоизменяя раздел целей программы.Программируется не отдельная задача а предметная среда. Такой подход существенно меняет методику применения математического аппарата и требует дальнейшего совершенствования и обобщения алгебры логики.Разумеется и выбор предметной области также вносит свои коррективы.В качестве усиления логических возможностей системы Пролог мы использовали предложенную Ю.П.Шабановым-Кушнаренко алгебру теории интеллекта, (см. [1], [2]). Для системы с хорошим языком общения не хватало лишь инструмента мышления. В качестве такового была предложена имитационная модель автомата с памятью,написанная автором на Прологе.

Рассматривались следующие предметные среды:

1. Решение логических задач (см. [3],[4]).
2. Решение задач динамического программирования (см. [5]).
3. Имитация на Пролог устройств цифровой электроники.
4. Решение задач математического программирования.
5. Решение задач динамики логических систем (см. [6],[7]).
6. Решение задач на сетях и графах (см. [8],[10]).

Рассмотрим особенности решения сетевых задач. Простейшая и имеющая многочисленные приложения - задача нахождения путей, удовлетворяющим некоторым требованиям (в частности всех путей наименьшего веса или все путей наибольшего веса).Один из подходов представляется как работа автомата с памятью, управляемая множеством условий сохранения потока (УСП). В каждом состоянии пропускается 1 ед. потока через вершины сети. Другой подход позволяет зафиксировать число управлений и откинуть множество УСП. Работа с программой при решении задачи на оптимум имеет свои особенности: необходимо временами обрывать поток выдаваемой информации и подправлять целевые требования. Входной поток информации также можно уменьшать, используя введенные автором, так называемые генераторы потоков. Это понятие оказалось важным при решении задачи получения максимальных потоков. При нахождении ядер графов, раскрасок вершин входной поток уменьшался за счет некоторых преобразований графа (см. [8]).

1. Шабанов-Кушнаренко Ю. П. Теория интеллекта.Математические средства. — Харьков.ХГУ: "Вища школа 1984.
2. Любота В. Н. Подстановочные предикаты.Теория и приложения. ДОСДМ. №13.
3. Любота В. Н. Решение логических задач с помощью алгебры подстановочных предикатов. ДОСДМ. №4.
4. Любота В. Н. О решении логических задач. ДОСДМ. №9.

5. Любота В. Н. Решение на Пролог экономических задач. ДОСДМ. №6.
6. Любота В. Н. Изучение динамики дискретных систем методами алгебры подстановочных предикатов. ДОСДМ. №11.
7. Любота В. Н. Задачи о переправе как задачи теории конечных автоматов. ДОСДМ. №15.
8. Любота В. Н. Применение алгебры конечных предикатов к решению задач теории графов. ДОСДМ. №2.
9. Любота В. Н. Сводимость задачи минимизации булевой функции к задачам теории графов и гиперграфов. ДОСДМ. №10.

Управление производительностью сети

Огбу Д.[1]**, Оксиюк А., Шестак Я.**[2]

Киевский национальный университет имени Тараса Шевченко, Киев, Украина

jamesybone@yahoo.com[1]*, lucenko.y@ukr.net*[2]

Управление производительностью сети является важной задачей на современном этапе. Решение проблем, которые не позволяют сети функционировать надлежащим образом позволят пользователям информационных сетей получать услуги в любом месте, в любое время с заданным качеством за оговоренную оплату. Чтобы быстрее реализовать требования рынка информационных услуг, стала необходимой более гибкая архитектура информационных сетей, которые представляют собой множество функционально совместимых компонентов различных поставщиков оборудования. От такой сложной инфраструктуры достаточно логично ожидать некоторых проблем, связанных с недостаточной производительностью сети. Не имеет значения, насколько хорошо были проведены работы по проектированию сети – главное понимать суть проблем, и обладать средствами для их решения. Все типы физических сред, будь то волоконно-оптический кабель или инфракрасный канал передачи, налагают определенные ограничения на производительность соединения, являющиеся в большинстве случаев функцией от покрываемого расстояния. Очень незначительное превышение этих ограничений может привести к таким проблемам производительности, как деградация данных или совсем невозможность их передачи. Проблемы, связанные с превышением ограничений физической среды, очень тяжело поддаются диагностированию; превышение рекомендуемой длины кабелей, установление не полностью совместимых повторителей или некорректное завершение шинной среды передачи очень редко заканчивается очевидным фактом не функционирования сети. Вместо этого возникают нерегулярные сбои, связанные с невозможностью своевременной и надежной доставки данных. Большинство сетевых сред передачи подвержены, по крайней мере, одному виду помех. Электромагнитные волны, используемые для передачи данных, часто служат причиной физического, механического или электрического явления, генерирующего шум и помехи, которые могут отрицательно повлиять на процедуры сетевого взаимодействия. Поэтому нужно проанализировать все потенциальные источники помех и иметь в виду при разворачивании сред передачи. В настоящее время необходимость предоставления высокого спектра услуг повлияла на повышение требований к основным параметрам сети. В связи с этим количеством передаваемой информации существенно увеличилось, что повлекло за собой снижение производительности, связанные с трафиком, возможно разделить на несколько групп: конфликты; неэффективные сетевые протоколы; перегрузка аппаратных компонентов; некорректно реализованные сетевые стеки; массовый отказ в обслуживании; проблемы при разрешении адресов; аспекты межсетевого взаимодействия. Управление производительностью сети является важной задачей на современном этапе.

1. Коузи Дж. Компьютерные сети, 1999.
2. Сейдж Э.П., Уайт Ч.С. Оптимальной управление системами. М. Радио и связь, 1982, 392 с.

Автоматизированный синтез точных альтернативных временных отрезков при коммутации дискретно-периодических сигналов

Панченко Б., Печенюк Д.

Институт кибернетики им. В.М. Глушкова НАНУ, Киев, Украина

Сумской государственный университет, Сумы, Украина

pr-bob@ukr.net

Для одной из известных задач телепроизводства – автоматизированного синтеза в режиме реального времени одним пользователем нескольких результирующих программ (альтернативных между собой) – предложено новое техническое решение [1]. Существенным требованием тут является точное (покадровое) соответствие моментов времени появления подмен (в дальнейшем - склеек) во всех альтернативных программах.

Каждая склейка (рис. 1) любого нового входящего сигнала в каждой альтернативной программе P_i ($i = \overline{1, I}$, где I – суммарное число программ) на каждом факте наступления склейки t_n должно по длительности строго покадрово соответствовать базовой программе. Это означает, что во всех итоговых программах длительность склеек $\Delta_{in} = t_n - t_n - 1$ для любого текущего i совпадают между собой вплоть до кадра. Ситуация, когда для некоторого момента времени наступления склейки t_n хотя бы одна склейка Δ_{jn} в любой j-й программе по длительности отличается хотя бы на один кадр, т.е. $\Delta_{jn} \# \Delta_{in}$, должна быть исключена. Такое отклонение в любой из I альтернативных программ исключает возможность использования этого дефектного фрагмента Δ_{jn} для дальнейшего конфигурирующего монтажа («чистки») [1]. Однако по содержанию, как показано на рис. 1, все программы полностью отличны.

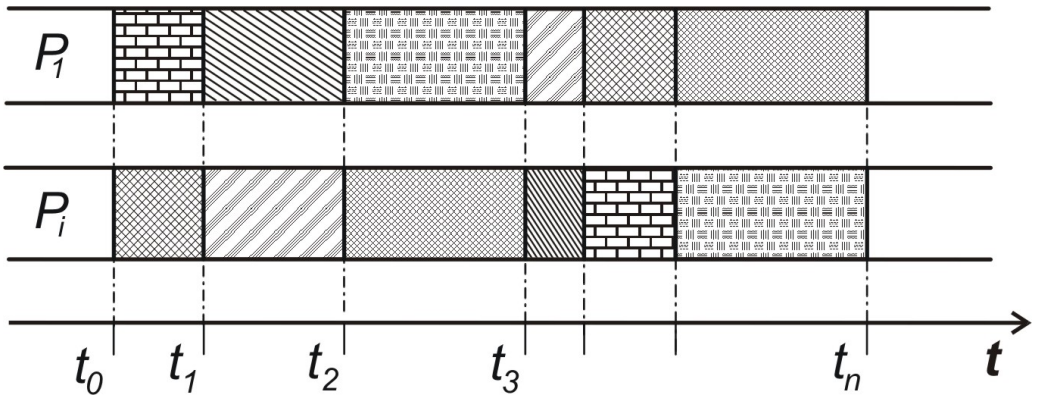

Рис 1. Рис. 1 – Диаграмма строго соответствия альтернативных программ

При ручном формировании альтернативных программ выбор решений относительно альтернативных программ как правило осуществляется ассистентами лица, принимающего решения (ЛПР). Техническая возможность совпадения временных отрезков между программами отсутствует. На выбор альтернативного сигнала накладывается следующие ограничения: запрещен выбор того же сигнала, что и у ЛПР, запрещен выбор сигнала, который был выбран ЛПР до текущего выбора, запрещен выбор некоторых заранее оговоренных сигналов - общий план, сигнал от динамической камеры (кран или тележка

и т.д.), другие ситуативные ограничения. Профессиональный набор сигналов должен строго соответствовать данным ограничениям.

Наиболее эффективно данный алгоритм может быть автоматизирован в случае, если синхронизация входящий сигналов осуществляется на уровне коммутации [2] – тут процессы сплиттирования сигналов, автоматизация их выбора, фиксация в памяти и автоматизированное сравнение номеров сигналов предусмотрены сущностью способа.

1. Panchenko B.E., Pechenjuk D.A. Method of automated digital multi-program multi-signal commutation [Text]. Publ. US 2013/0294457 A1, 11-2010.
2. Панченко Б.Е., Печенюк Д.А. Использование SDRAM для синхронизированной коммутации телевизионных сигналов [Текст]. Технологический аудит и резервы производства, Харьков, 2015, № 4/2 (24), С. 63–68.

Конечные группы и компьютерная алгебра

Сохор И.

Гомельский государственный университет имени Ф. Скорины,
Гомель, Республика Беларусь
irina.sokhor@gmail.com

GAP (Groups, Algorithms, Programming) — свободно распространяемая на условиях универсальной общественной лицензии *GPL* (General Public License) открытая, кроссплатформенная система компьютерной математики для вычислительной дискретной алгебры. Важной особенностью *GAP* является ее расширяемость либо посредством внешних пакетов и библиотек, либо с использованием паскалеподобного языка программирования *GAP*.

Подгруппа называется широкой, если каждый простой делитель порядка группы делит порядок подгруппы. Данное понятие введено В. С. Монаховым и И. Л. Сохор [1] и является новым. Для определения, является ли подгруппа H в заданной группе G широкой, в *GAP* может быть описана функция $IsWideSubgroups(G, H)$, проверяющая совпадает ли количество простых делителей порядка группы G и подгруппы H. Количество простых делителей порядка группы G вычисляется при этом с помощью встроенных функций $Size(Set(Factors(Size(G))))$. Построенная функция может в дальнейшем использоваться для вывода списка всех (максимальных, нормальных, т.п.) широких подгрупп. Анализ полученных результатов позволяет выдвигать гипотезы о свойствах группы, исходя из свойств ее широких подгрупп, или строить контрпримеры. Интересным является тот факт, что разработанный список дополнительных функций может быть оформлен в виде отдельного пакета и представлен на рецензирование в Совет *GAP* для включения пакета в приложение к дистрибутиву *GAP*.

1. Монахов В.С., Сохор И.Л. Конечные разрешимые группы с нильпотентными широкими подгруппами. Укр. мат. журн., 2016, **Т. 68**, 7, С. 957–962.

Метод структурно-параметричного синтезу енергозберігаючих фізичних прототипів допоміжних елементів гідроаеродинамічної системи

Арсірій А.[2], **Арсірій О.**[1], **Василевська О.**[1]

Одеський національний політехнічний університет, Одеса, Україна[1],
Одеський національний університет ім. І.І. Мечникова, Одеса, Україна[2]

e.arsiriy@gmail.com

Для формалізації процесу створення бази енергозберігаючих допоміжних елементів при автоматизованому проектуванні у спеціалізованому АРМ отримав подальший розвиток метод структурно-параметричного синтезу енергозберігаючих фізичних прототипів допоміжних елементів гідроаеродинамічних систем (ГАС), який полягає в урахуванні кількісної і якісних оцінок стану гідродинамічних потоків (ГП) у них [1]. Для визначення причин високих нормативних значень опорів за допомогою методу візуалізації дискретних структур потоку, що належить до класу поляризаційно-оптичних методів візуалізації прозорих робочих тіл, отримують штучні поверхні розподілу інтенсивності (кольоровості) світла, які однозначно характеризують поле градієнтів швидкостей (тисків) ГП у прототипі аналізованого допоміжного елементу [2]. Штучні поверхні фотореєструються, утворюючи множину значень інтенсивностей точок зображення - *візуальні дані* ГП. Для отримання якісної оцінки стану ГП у вигляді *інтелектуальних даних* ГП у фізичному прототипі аналізованого допоміжного елемента використовують машину нейромережевого виведення. За її допомогою на основі об'єктів нейромережевої бібліотеки створюються проекти нейронних мереж, для навчання та/або самонавчання яких, використані візуальні дані ГП і їх елементарні непохідні фрагменти – візуальні дані гідродинамічних структурних примітивів (ГСП). При цьому нейромережева бібліотека містить процедури для створення основних архітектур нейронних мереж таких як: прямого поширення сигналу (найпростіші і багатошарові персептрони, лінійні мережі), мереж зустрічного і зворотного поширення сигналу, радіально-базисних мереж, шарів і карт Кохонена, що самоорганізуються та мереж векторного квантування. Результатом виконання проектів в машині нейромережевого виведення є визначення номера класу ГСП, який відображається псевдокольором при формуванні інтелектуальних даних ГСП $Data_{IP}$ з відповідними координатами і отримання правил R_{IE}, які задають представлення інтелектуальних даних $DATA_{IE} = [R_{IE}] \bigcup_{i=1}^{X} \bigcup_{j=1}^{Y} Data_{IP_{ij}}$ де $X = Dw \cdot Rs/dw$, $X = Dh \cdot Rs/dh$, Rs просторова роздільна здатність у точках на дюйм (ppi). Симуляція створених фізично-подібного прототипів допоміжних елементів на подібному за числом Рейнольдса експериментальному стенді показала, що врахування стану ГП у вигляді інтелектуальних даних обробки візуальних поверхонь, які однозначно характеризують поле градієнтів швидкостей (тисків) потоку у прототипі, дозволяє синтезувати проектні рішення по зниженню опорів в 1,5 – 5 разів, залежно від типу енергозберігаючого допоміжного елемента.

1. Арсирий, Е.А. Разработка моделей элементов гидроаэродинамических систем на основе средств интеллектуальной визуализации. Восточ.–Европ. журн. передовых технологий. Энергосберегающие технологии и оборудование. – Харьков, 2013, №3/8(63), С. 4—8.
2. Arsiri V.A., Maisotsenko V.S. Пат. PST 5.812.423 USA Method of determining for working media motion and designing flow structures for same, Published 22.09.1998.

Модель функціонування тренажерних систем інтенсивної підготовки диспетчерів управління повітряним рухом

Гунченко Ю.[1], **Ємельянов П.**[1], **Шворов С.**[2]

Одеський національний університет ім. І.І.Мечникова, Одеса, Україна[1],
Національний університет біоресурсів і природокористування України, Одеса, Україна[2]

7996445@mail.ru

Актуальним, важливим напрямом застосування інформаційних технологій є підготовка диспетчерів управління повітряного руху (УПР) в умовах зростання інтенсивності польотів, а також у різних нестандартних та аварійних ситуаціях.

При застосуванні існуючих методик початкова підготовка диспетчерів УПР здійснюється на протязі значного часу. Аналіз наявної тренажерної бази у державах - членів EUROCONTROL, показує, що в існуючих тренажерах відсутні режими прискореної підготовки.

Метою дослідження є визначення основних завдань, складу, структури, організації функціонування тренажерних систем інтенсивної підготовки диспетчерів УПР.

Прискорена підготовка авіадиспетчерів можлива на основі використання сучасних інтенсивних технологій навчання. Найбільш суттєвим для процесу інтенсифікації навчання є активізація діяльності диспетчерів.

В основу запропонованого методичного підходу до інтенсифікації навчання покладене те, що "внутрішня переконаність"авіадиспетчерів в обмеженості часу, викликає в них стан напруженості. Загальний час тренування підрозділяється на N етапів, кожен з яких характеризується певною напруженістю роботи у нештатних ситуаціях.

Запропонована математична модель описує динаміку зміни рівня підготовки персоналу з виконання типових операцій навчальних завдань (НЗ), залежно від індивідуальних здібностей S_{0i} і кількості імітованих ситуацій (S_i). Реалізація мінімально необхідної кількості імітованих ситуацій в моделі повітряної обставини дозволяє значно скоротити часові витрати на підготовку диспетчерів до необхідних прогнозованих рівнів навчання.

Висновки. Реалізація розробленої моделі адаптивного управління процесом імітації обстановки в адаптивних тренажерних системах дозволяє при мінімальних часових (вартісних) витратах здійснювати підготовку диспетчерів УПР до необхідного рівня з виконання операцій НЗ в найскладніших умовах повітряної обстановки.

Аналіз питань доведення захищеності інформації в операційних системах

Зерко А., Кохановскій О., Оксіюк А.

Київський національний університет імені Тараса Шевченка, Київ, Україна

a.l.zerko@ukr.net

Історично склалось так, що операційні системи та програмне забезпечення розвивались як окремі продукти. Виходячи з цього питання, створення єдиного програмного середовища в ОС не розглядалось. Як наслідок – маємо дублювання гілок програмного забезпечення, надлишковість кодів тощо.

Строго математично довести рівень захищеності інформації в середовищі ОС, інформації, яка обробляється з використанням програмного забезпечення – не можливо.

Зробимо припущення:

1. програмне забезпечення ОС при розробці використовує комплекс правил, які регламентують заходи із забезпечення надійності та захисту інформації;
2. ОС вимагає від програмного забезпечення користувачів функціонування за окремим комплексом правил та настанов;
3. в середовищі ОС працює лише програмне забезпечення, яке виконує дані правила;
4. ОС має рекомендовані профілі захисту, які повинні виконуватись при встановленні та конфігуруванні ОС, програмного забезпечення користувачів, для їх подальшого використання;
5. ОС має механізми контролю, оцінювання рівня надійності та захищеності ОС та програмного забезпечення користувачів на протязі життєвого циклу.

Розробка правил, які спрямовані на виконання даного комплексу припущень надає можливість побудувати математичну модель оцінки захищеності інформації в середовищі ОС з урахуванням різноманітних факторів, що залежать від ОС та програмного забезпечення.

1. ©Державна служба спеціального зв'язку та захисту інформації України. http://www.dstszi.gov.ua/dstszi/control/uk/index.
2. Компанія "АТМНІС https://atmnis.com/files/user_files/BBOS.pdf

Організаційні аспекти захисту персональних даних громадян в системах надання адміністративних послуг

Левін М., Шаршаткін Д.

Одеський регіональній інститут державного управління
Національної академії державного управління
при Президентові України, Одеса, Україна

sharshatkin.d@ukr.net

Інтенсивний розвиток технологій надання громадянам України комплексу адміністративних онлайн-послуг в режимі "єдиного вікна"обумовлює необхідність збору, передачі, обробки та зберігання великих обсягів персональних даних. Правову базу цих процесів в цілому забезпечує закон "Про захист персональних даних"[1], однак практичне застосування його норм пов'язано з певними труднощами:

відсутністю нормативних документів, що однозначно регламентують на державному рівні міжвідомчу взаємодію установ-виробників адміністративних послуг;

недостатньою компетентністю керівників цих установ в сфері інформаційної безпеки, що не дозволяє їм адекватно оцінювати ризики, пов'язані зі створенням і експлуатацією баз персональних даних, власниками і / або розпорядниками яких вони є;

відсутністю в переважній більшості у цих установах функціональних підрозділів, що відповідають за недоторканність персональних даних одержувачів адміністративних послуг;

необхідністю використання в системах передачі персональних даних практично тих же методів (наприклад, криптографічних алгоритмів) і засобів захисту, що і в системах передачі даних, що відносяться до державної таємниці.

У зв'язку з цим досить актуальною залишається завдання захисту персональних даних громадян від несанкціонованого доступу, знищення, перекручення, блокування, копіювання, поширення та інших неправомірних дій.

Для вирішення цього завдання автори вважають за необхідне проведення наступних першочергових заходів:

- створити в обов'язковому порядку в державних установах, залучених до діяльності з надання населенню онлайн-послуг, підрозділів інформаційної безпеки і захисту інформації;
- провести первинне навчання керівників і співробітників цих підрозділів з метою ознайомлення з нормативно-правовою базою України, вимог міжнародних стандартів серії ISO 27000, дозволеними для вільного використання сучасними апаратно-програмними засобами захисту даних;
- керівникам установ-виробників адміністративних послуг звернутися до контролюючого органу (Державній службі спеціального зв'язку та захисту інформації України)

з ініціативним пропозицією розробки в найкоротші терміни єдиних вимог щодо захисту персональних даних громадян при їх передачі, зберіганні та обробці в системах, що орієнтовані на наданні адміністративних онлайн-послуг.

Виконання зазначених заходів дозволить значною мірою ліквідувати відставання України від провідних світових держав (87 позиція в рейтингу розвитку електронного уряду 2014 року [2]) в реалізації проекту "Електронний уряд".

1. Урядовий портал: офіційний сайт [Електронний ресурс] - Режим доступу: http://www.kmu.gov.ua.
2. UN E-Government Survey 2014 [Електронний ресурс] - Режим доступу: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014.

Application of Anti-Grey Code in digital components diagnosing

Petryshyn L.
AGH University of Science and Technology, Krakow, Poland
l.b.petryshyn@gmail.com

Надійність є визначальним критерієї якості функціонування інформаційних систем. Розрізняють три рівні забезпечення системної надійності: на найвищому рівні - надійність програмного коду, на проміжному рівні - завадозахищеність коду представлення даних, на найнижчому рівні - надійність апаратної складової. Якщо надійність на рівні програмного коду чи завадозащинесті коду представлення даних можна забезпечити за допомогою відомих методів, то надійність нижчого рівня апаратного забезпечення є визначальним чинником надійності системи в цілому. Сучасні інформаційні системи є достатньо складними ієрархічно розбудованими, часто розосередженими цифровими системами, що істотно ускладнює вияснення причини та локалізацію місця виходу з ладу єдиного цифрового компоненту чи розряду каналу інфообміну чи памяті, або ж цілого кола чи підсистеми. Розробка ефективних методів діагностування апаратного забезпечення цифрових систем виявляється актуальним напрямком дослідження, що вимагає опрацювання математичних, алгоритмічних і програмних моделей, імплементація яких дозволяє ідентифікувати технічний стан обєкту діагностування. Завдання діагностування полягає у своєчасному виявленні дефектів, причин та їх локалізацію з метою наступного відновлення роботоздатності системи. З систем функціонального та тестового діагностування зупинимося на останніх, в яких на обєкт дослідження подаються спеціально розроблені тестові дії. В цифрових системах не використовуються режими перехідних процесів, тільки дискретні стани, що зумовлює можливість визначення двох альтернативних станів компонентів – справний та несправний. Тому природним є застосування цифрових методів тестування апаратного забезпечення інфосистем, що базуються на побудові таблиці станів і матриці дефектів компонентів. Як показав аналіз відомих методів, тестування здійснюється із формуванням на входах діагностованого цифрового пристрою різних кодових комбінацій та контролю по виходах достовірності їх значень згідно закладеної функції перетворення, за результатами чого формується контрольна матриця дефектів. В різних джерелах різні розробники пропонують застосовувати певні алгоритми формування кодових комбінацій, в тому числі коди Грея, на які слід звернути особливу увагу, оскільки вони в повному наборі вміщують всі можливі бінарні кодові комбінації, але характеристичною особливістю є зміна логічного стану тільки в єдиному розряді кодового формату на повному періоді тестування. Така властивість дозволяє проконтролювати множину вихідних станів в кодовій статиці всіх вхідних розрядів за вийнятком одного, визначеного двома суміжними станами коду Грея. В доповіді запропоновано застосувати комплементарну процедуру тестування на базі вхідних кодів антигрея, характеристичною особливістю яких є зміна всіх, крім одного розрядів коду. Це доволяє здійснити цифрове тестування в кодовій динаміці зміни бінарних станів всіх, крім одного розрядів для довільних суміжних кодових комбінацій на повному періоді тестування. Авторами вперше розроблено математичну та алгоритмічну моделі формування кодових систем антигрея. В доповіді представлено основи та аналітику побудови кодів та кодових систем антигрея, методи їх отримання із двійкового коду та коду Грея. Новизна розробки та обмежений час її апробації зумовив необхідність винесення на обговорення аудиторії властивостей системи антигрея та потенційної можливості її застосування в діагностуванні цифрових компонентів інформаційних систем.

Application of vector-branching schemes in IFT processes modeling

Petryshyn M.
Precarpathian National University, Ivano-Frankivsk, Ukraine
inst@pu.if.ua

В основі запропонованого векторно-розгалужуючого методу моделювання процесів перетворення форми інформації (ПФІ) застосовано метод індикаторного моделювання, що базується на геометричному моделюванні, тобто визначенні довжини відрізка. Моделювання процесів ПФІ ґрунтується на ітераційному здійсненні визначених процедур порівняння. На техніці ПФІ порівняння здійснюється за допомогою компараторів, які дозволяють визначити співвідношення невідомої величини з певною «еталонною величиною», або "мірою чи "шкалою сформованою з "системи одиниць вимірювання"[1].

Векторно-розгалужуюча схема (ВРС) є повною скінченою моделлю для знаходження довільних значень діапазону перетворення шляхом прикладання до кожного з них індикаторного елементу (ІЕ). Модель ВРС будується згідно наступного алгоритму (рис. 1):

1. здійснюється прикладання ІЕ до першої точки перетворення X_j ;
2. ІЕ визначає один з двох наступних станів:
   ?? - приймає значення 0 та означає, що шукане значення знаходиться лівіше від точки X_j, розгалужуючий вектор скеровується вниз та відкладається вліво до наступної точки прикладання $X_j + 1$;
   ?? - приймає значення 1 та означає, що шукане значення знаходиться правіше від точки X_j, розгалужуючий вектор скеровується вверх та відкладається вправо до наступної точки в залежності від поточного значення ІЕ ;
3. крок 2 повторюється поки не буде визначено невідоме значення перетворення.

Рисунок 1. Векторно-розгалужуюча схема

Таким чином, процес моделювання процесів ПФІ за допомогою векторно-розгалужуючих схем, аналогічно, як на основі індикаторного моделювання, полягає в послідовному прикладанні ІЕ до визначених точок, що належать діапазону перетворення та ітераційному звуженню інтервалу невизначеності відносно невідомої точки перетворення, проте володіє розширеною функціональністю, яка дозволяє візуалізувати кожен крок перетворення та здійснити кількісну оцінку складності модельованого методу ПФІ.

Index

Арсірій А., 50
Арсірій О., 50
Гальмак А., 43
Гунченко Ю., 51
Ємельянов П., 51
Кохановскій О., 52
Левін М., 53
Любота В., 44
Огбу Д., 46
Оксиюк А., 46
Оксіюк А., 52
Панченко Б., 47
Печенюк Д., 47
Сохор И., 49
Шаршаткін Д., 53
Шестак Я., 46
Шворов С., 51
Василевська О., 50
Воробьев Г., 43
Зерко А., 52

Al-Jasri G.Kh.M., 5
Antonenko O., 6

Balyas L., 7
Boltenkov V., 5

Chala L., 8
Chumachenko O., 9

Dobrovolsky G., 11

Ermilova A., 12

Filatova T., 13

Glava M., 15
Glazunov N., 17
Godny A., 9
Granik Yu., 18

Kaman K., 19
Keberle N., 11
Kosukhin N., 21
Kozin A., 22
Kozinf M., 22
Krapivny Yu., 23
Kryvonos O., 23

Lebedeva E., 19
Lisitsyna I., 24

Malakhov E., 15, 25, 26
Malakhov V., 13
Mazurok I., 27
Mezhuyev V., 25

Papkovskaya O., 22
Penko V., 28
Petrushina T., 24, 29
Petryshyn L., 41, 55
Petryshyn M., 56

Rogowski J., 30
Rublev V., 12
Rychlik A., 31

S. Varabnets, 37
Savastru O., 32
Shchelkonogov D., 25
Shpinareva I., 21
Shvorob I., 33
Sviridov A., 29
Synehlazov V., 9

Taran Ye., 28
Todoriko O., 11
Tran The Vinh, 38
Trubina N., 24
Tsariuk A., 26

Udovenko S., 8

Varbanets P., 34
Varbanets S., 35
Volkova A., 39
Vorobyov Ya., 40

Waszkielewicz W., 41

Ya. Vorobyov, 37

Zahanich D., 27
Zorilo V., 19

For Notes:

For Notes:

I. I. Mechnikov Odessa National University, Odessa

2nd International Conference on Computer Algebra and Information Technologies

August 21 – 26, 2016

Odessa, Ukraine

ABSTRACTS

Одеський національний університет імені І. І. Мечникова, Одеса

ІІ Міжнародна конференція "Комп'ютерна алгебра та інформаційні технології"

21 – 26 серпня 2016 р.

Одеса, Україна

ТЕЗИ ДОПОВІДЕЙ

Комп'ютерна верстка та підготовка оригінал-макета
С. П. Варбанець

Підп. до друку Формат 60x90/16. Папір офс. Офс. друк. Обл. вид. арк. 21,5. Ум. друк. арк. 30,1. Зам. 58. Тираж 300 пр.

Одеський національний університет імені І. І. Мечникова