Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам’янець-Подільський національний університет
імені Івана Огієнка

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

Серія: Фізико-математичні науки

Збірник наукових праць

Випуск 15

Кам’янець-Подільський національний університет
імені Івана Огієнка
2017

УДК 519.6:519.7
ББК 22
М34

Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 14521-3492Р від 25.06.2008 р.

Збірник наукових праць включено до Переліку наукових фахових
видань ДАК Міністерства освіти і науки України з фізико-математичних наук
(наказ №1021 від 07 жовтня 2015 р.)

Друкується згідно з рішенням вченої ради Кам'янець-Подільського
національного університету імені Івана Огієнка,
протокол № 8 від 29 червня 2017 року.

М34 **Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки** : зб. наук. праць / Інститут кібернетики імені В. М. Глушкова Національної академії наук України, Кам'янець-Подільський національний університет імені Івана Огієнка ; [редкол.: О. М. Хіміч (відп. ред.) та ін.]. — Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2017. — Вип. 15. — 272 с.

У збірнику друкуються результати досліджень вітчизняних та закордонних науковців, що стосуються проблем застосування математичних моделей в різних галузях людської діяльності.

Для наукових та інженерно-технічних працівників, аспірантів, студентів.

УДК 519.6:519.7
ББК 22

ISSN 2308-5878

V. M. Glushkov Institute of Cybernetics
of National Academy of Sciences of Ukraine
Kamianets-Podilsky National Ivan Ohienko University

MATHEMATICAL AND COMPUTER MODELLING

Series: Physical and mathematical sciences

Scientific journal

ISSUE 15

Kamianets-Podilsky National Ivan Ohienko University
2017

Critics:

Editorial board:

Mathematical and computer modelling. Series: Physical and mathematical sciences : scientific journal / V. M. Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine, Kamianets-Podilsky National Ivan Ohienko University ; [Editorial Board: O. Himich (Executive Editor) and others]. — Kamianets-Podilsky : Kamianets-Podilsky National Ivan Ohienko University, 2017. — ISSUE 15. — 272 p.

There are printed results of investigation of national and foreign scientists that concern to problems of practice mathematical models in different spheres of human activity.

For scientific and technical staff, postgraduate students.

ISSN 2308-5878

UDC 519.6

K. R. Aidazade[*, **]**,** Doctor of Phys. and Mathem. Sciences, Professor, Corresponding member of the Azerbaijan National Academy of Sciences (ANAS),
S. Z. Guliyev[**, ***]**,** Cand. of Phys. and Mathem. Sciences, Associate Professor
[*]Baku State University, Azerbaijan, Baku,
[**]Institute of Control Systems (ANAS), Azerbaijan, Baku,
[***]Azerbaijan State Oil and Industry University, Azerbaijan, Baku

ON METHODS OF CONTROLLING OPTIMIZATION SOFTWARE PACKAGES WITH THE APPLICATION OF PARALLEL COMPUTING

The paper is dedicated to the analysis of methods and algorithms of controlling computational process of solving complex problems with the use of multiprocessor and/or multicore computer systems. We have developed an automatic and dialogue systems of control of unconstrained optimization process, which have a graphical user interface.

Key words: *optimization methods, parallel computations, multiprocessor and multicore systems, dialog systems.*

Introduction. It is known that in spite of a large number of methods for numerical solution to various classes of problems, the choice of the most efficient method for solving a particular problem under specific values of its parameters requires a large number of comparative experiments. As a rule, the end users tend to have difficulty both in carrying out such experiments, which requires the knowledge of domain of applicability of various numerical methods, and in proper conducting of the comparative analysis of the results, which is time consuming.

In the paper, for the class of problems of multivariate unconstrained optimization, we propose two approaches for facilitating the use of available applied software packages using modern multi-processor (multi-core) computer systems. One of the approaches involves active work of the user with the optimization program package in a dialogue mode. The other approach involves the packet control by means of a specially developed control program in automatic mode.

Problem statement. Let $P=\{p_i(x): i\in N\}$ be the class of optimization problems (tasks). Here N is a given set defining individual problems of the class; $x\in D_i\subset R^n$ are the arguments of each individual problem, which can take on values from some given admissible set D_i, defined by each specific optimization problem individually. It is assumed that for every problem $p_i(x)$ there exists a goal subset of extrema $D_i^* \subset D_i$ such that $D_i^* \neq \varnothing$. The problem $p_i(x)$ consists in finding at least one point $x^* \in D_i^*$. The set D_i^* is called a set of solutions to the problem $p_i(x)$.

To solve all the problems of the class P, there is usually a corresponding family of methods $M = \{M_j : j \in J\}$, each of which solves the problems $p_i(x)$ of the given class, i.e. they find a point $x^* \in D_i$. Moreover, each method $M_j, j \in J$, has different efficiency (in terms of time used, the accuracy of the solution, etc.) when solving the problem $p_i(x)$.

As the optimization techniques we use methods of direct search (zero-order methods), gradient-based methods (first-order methods), and Newton-type methods (second-order methods). These methods have a large number of options settings, thus providing the ability to adapt the system to any process quickly. Furthermore, the combination of direct search methods, gradient-based methods, and Newton-type methods allows us to find an optimal solution for a smaller number of steps and/or calculations of the objective function, which is important in terms of the cost of optimization process.

The report sets out the possible principles of management of optimization software package when solving a particular applied problem $p_i(x) \in P$, allowing us to increase the overall efficiency of solving the problem by combining the optimization methods in the process of solving the problem with the use of a multiprocessor (multicore) computer system.

The principle of sequential implementation on a single core (SISD) architecture is of important significance in own right, and can be considered as the basic unit for the implementation on multiprocessor or multicore architectures. Let us describe one of the principles of the possible schemes of implementation of the algorithm for solving optimization problems on such architectures.

Let $M_1, M_2, ..., M_k$ be a list of optimization methods, composed of algorithms in the software package of unconstrained optimization. It is reasonable to include in the list diverse methods, if the structure of the objective function is, generally speaking, not known.

The process of solving the problem is carried on in stages, each of which consists of training and working steps. The first of these steps is intended to identify the locally efficient algorithm from the available list of algorithms. After that, the working step is carried out, which consists in solving the problem using only the algorithm that has proven to be the most efficient in the first step. Both the training and working steps are carried out within a certain time slice. One can use two variants of the training step:

1. To determine the local efficiency of the methods, the optimization process starts from the same point x^0. In this case there is somewhat wasteful consumption of machine time, and the training step is only used to identify a locally efficient algorithm;
2. The training step is used not only to find an efficient algorithm, but also to advance to an extreme point, because instead of the original point we use the current point to train each of the following algorithm.

At the training step all the algorithms of the initial list $M_1, M_2, ..., M_k$ have the opportunity to work within the given initial time slice, with the exception of only those methods that have been the least efficient for two consecutive training steps. These methods are not allocated any time slice and are temporarily excluded from the list.

To calculate the values of the local efficiencies of the methods, we make use of the following formula:

$$E_i = | f(x^{k+1}) - f(x^k) | / (| f(x^k) | + \varepsilon) + \| x^{k+1} - x^k \| / (\| x^k \| + \varepsilon) .$$

Here E_i is the local efficiency of the i th algorithm; x^{k+1}, x^k are the final and initial points obtained using the i th algorithm; $f(x^{k+1}), f(x^k)$ are the values of the objective function at these points; $\| . \|$ is the Euclidean norm; ε is a small positive number.

The cycle criterion of the proposed procedure is the fulfillment of the exit criteria for all methods. In conclusion, the user receives the accumulated information on the search process, which includes:

- the optimal chain of methods that worked at the working steps;
- the total time of search for solutions;
- the values of the objective function, of the coordinates, and of local efficiencies of the methods obtained during the training step.

The principle of parallel implementation on a multicore architecture. The simplest implementation of a multi-threaded version of the solution to the given optimization problem seems to be an approach that involves several threads independently performing operations of the sequential algorithm described above.

The solution to an unconstrained optimization problem is carried out in stages. At each stage, the following steps are implemented:

1. At the initial step, from the list of all available algorithms $M_1, M_2, ..., M_k$ of unconstrained optimization, we randomly select several algorithms $M_{s_1}, M_{s_2}, ..., M_{s_N}$, the number N of which is chosen equal to the number of cores present on the computer system.

2. At the working step, we identify the most efficient algorithms. The duration T_i of the working step may increase if any method has proven to be the most efficient for several consecutive stages.
3. The current values of the local efficiencies E_i of the methods are calculated. From the list of working algorithms, we exclude a half of those who have exhibited the lowest efficiency.
4. To the list of working algorithms we then add as many other algorithms as were excluded in the previous step, and repeat steps 2 through 4 again.

When working with the automatic and dialogue systems, the user, in accordance with the standard requirements, formulates an optimization problem in any programming language in the form of a module (dynamic link library), and then enters it into the system by specifying the full path to the created library file; using the directives (instructions), the user runs the most appropriate (in his/her opinion) algorithms of the library of modules, and tunes their various settings. The control program will then

- organize the interaction of the modules from the package;
- manages the input of the initial and current information;
- interpret the user's directives (instructions);
- load optimization modules into the computer memory dynamically;
- output the results of computations on the display (at the same time you can get results on a printer) in a prescribed form.

Analyzing the results of the computations, the user decides on the further calculations, thus obtaining the possibility to monitor the progress of solving the problem, to intervene promptly in the computation process, to choose the working methods, and to adjust, if necessary, their parameters. The user determines how often and in what form the results should be displayed on the screen, and then, using a predefined set of directives carries out calculations.

The report will contain the protocols and results of computer-based experiments for the class of unconstrained optimization problems using different principles of management of the developed software package.

Conclusion. In the paper, we proposed an approach to control of computational process of solving complex applied problems by an example of multivariate unconstrained optimization problems using appropriate software packages on multi-processor (multi-core) computer systems. The proposed approaches essentially facilitate the end-users' work of using existing standard software packages. They require a different level of users' knowledge of methods implemented in the software packages.

References:

1. Vasilyev F. P. Optimization Methods. M.: MTsNMO, 2011. Vol. 1 and 2. (in Russian).
2. Polyak B. T. Introduction to optimization. M.: Lenand, 2014. 392 p. (in Russian).

3. Adam Freeman. Pro .NET Parallel Programming in C#. New York: Apress, 2010. 328 p.
4. Joe Duffy. Concurrent Programming on Windows. Boston, MA: Addison-Wesley Professional, 2008. 1008 p.
5. Aidazade K. R., Sidorenko N. S. An approach to the construction of combined optimization algorithms. *Technical Cybernetics.* 1982. Issue 6. P. 87–93. (in Russian)

Работа посвящена анализу методов, алгоритмов управления вычислительным процессом решения сложных задач с использованием многопроцессорных (многоядерных) компьютерных систем. Разработана автоматическая и диалоговая системы управления процессом безусловной оптимизации, имеющие графический пользовательский интерфейс.

Ключевые слова: *методы оптимизации, параллельные вычисления, многопроцессорные и многоядерные системы, диалоговые системы.*

Date received 21.02.2017

УДК 519.6:539.3

А. А. Аралова, канд. фіз.-мат. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ІДЕНТИФІКАЦІЯ ТЕРМІЧНОГО ОПОРУ ПРИ ВІДОМОМУ ЗМІЩЕННІ ДЛЯ ТЕРМОПРУЖНОГО ДЕФОРМУВАННЯ СКЛАДЕНОГО ЦИЛІНДРА

Розглянуто алгоритм розв’язання за допомогою градієнтних методів задачі ідентифікації термічного опору при відомому зміщенні для термопружного деформування довгої складеної циліндричної оболонки.

Ключові слова: *термопружний стан, градієнтні методи, циліндричні тіла.*

Вступ. У роботі [1] на основі результатів теорії оптимального керування станами різних багатокомпонентних розподілених систем [2] запропонована методологія побудови явних виразів градієнтів функціоналів-нев'язок для ідентифікації градієнтними методами [3] різних параметрів багатокомпонентних розподілених систем. У роботах [4–6] ця методологія використана для ідентифікації параметрів задач пружного, теплового та термопружного деформування довгого порожнього циліндра.

Постановка задачі. Розглянемо довгий ізотропний циліндр з порожниною. Врахувавши симетрію, виходячи з [7, 8] його термопружний стан описується рівняннями

$$-\left\{(\lambda+2\mu)\frac{d}{dr}\left(r\frac{dy}{dr}\right)-(\lambda+2\mu)\frac{y}{r}-(3\lambda+2\mu)\,\alpha r\frac{dT}{dr}\right\}=0,\ r\in\Omega;$$

$$\sigma_r\Big|_{r=r_i}=-p_i,\ \ i=1,2;\ \ -\frac{1}{r}\frac{d}{dr}\left(kr\frac{dT}{dr}\right)=\overline{f},\ \ r\in\Omega;$$

$$-k\frac{dT}{dr}\bigg|_{r=r_1}=-\alpha_1 T+\beta_1,\ k\frac{dT}{dr}\bigg|_{r=r_2}=-\alpha_2 T+\beta_2; \tag{1}$$

$$[y]=0,\ [\sigma_r(y)]=0,\ \left[k\frac{dT}{dr}\right]=0,\ \left\{k\frac{dT}{dr}\right\}^{\pm}=u[T],\ r=\xi;$$

де $\Omega=\Omega_1\cup\Omega_2$, $\Omega_1=(r_1,\xi)$, $\Omega_2=(\xi,r_2)$, $0<r_1<\xi<r_2<\infty$, $r_1, r_2=const>0$ — радіуси, відповідно, внутрішньої і зовнішньої кругових поверхонь; r — радіальна координата циліндричної системи координат; а компонента тензора напруги має вигляд $\sigma_r(y,T)=$ $=(\lambda+2\mu)\dfrac{dy}{dr}+\lambda\dfrac{y}{r}-(3\lambda+2\mu)\alpha T$, де λ, μ — постійні Ляме; $y=y(r)$ — зміщення в радіальному напрямку; $\alpha=const>0$ — коефіцієнт температурного розширення, $\alpha_{1,2}=const>0$, $\beta_{1,2}=const$, $p_{1,2}=const$; $T=T(r)$ — температура, $k=const$ — коефіцієнт теплопровідності. Перші дві умови спряження виражають неперервність радіального зміщення та нормальної напруги на поверхні контакту, а третя та четверта — наявність слаботеплопроникного прошарку з термічним опором $u=const>0$, який вважаємо невідомим, $[T]=T^{+}-T^{-}$, $T^{\pm}=\{T\}^{\pm}=T(\xi\pm 0)$.

Ідентифікація параметрів за допомогою спостережень за зміщеннями на поверхні складеного тіла. При кожному фіксованому $u\in\mathcal{U}$ замість класичного розв’язку крайової задачі (1) будемо використовувати її узагальнений розв’язок, як вектор-функцію $Y=(y,T)\in\mathcal{H}$, складові якої $\forall z=(z_1,z_2)\in\mathcal{H}$ задовольняють системі тотожностей:

$$a(y,z_1)=l(T;\,z_1), \tag{2}$$

$$a_0(u;T,z_2)=l_0(z_2), \tag{3}$$

де простір $\mathcal{H}=V\times V_0$, $V=\left\{v(r):v\big|_{\Omega_i}\in W_2^1(\Omega_i),\ i=1,\ 2;\ [v]\big|_{\xi}=0\right\}$, $V_0=\left\{v(r):v\big|_{\Omega_i}\in W_2^1(\Omega_i),\ i=1,\ 2\right\}$, $W_2^1(\Omega_i)$ — простір функцій Соболєва визначених на області $\Omega=\Omega_1\cup\Omega_2$,

$$a\left(y,w\right)=\sum_{i=1}^{2}\int_{\Omega_i} r\left(\left(\lambda+2\mu\right)\left(\frac{dy}{dr}\frac{dw}{dr}+\frac{y}{r}\frac{w}{r}\right)+\lambda\left(\frac{y}{r}\frac{dw}{dr}+\frac{dy}{dr}\frac{w}{r}\right)\right)dr,$$

$$l\left(T;w\right)=\sum_{i=1}^{2}\left(\int_{\Omega_i}\left(r\left(3\lambda+2\mu\right)\alpha T\left(\frac{dw}{dr}+\frac{w}{r}\right)\right)dr\right)+r_1p_1w\left(r_1\right)-r_2p_2w\left(r_2\right),$$

$$l\left(T;w\right)=\sum_{i=1}^{2}\left(\int_{\Omega_i}\left(r\left(3\lambda+2\mu\right)\alpha T\left(\frac{dw}{dr}+\frac{w}{r}\right)\right)dr\right)+r_1p_1w\left(r_1\right)-r_2p_2w\left(r_2\right),$$

$$a_0\left(u;T,w\right)=\sum_{i=1}^{2}\int_{\Omega_i} r\,k\frac{dT}{dr}\frac{dw}{dr}dr+u\left[T\right]\left[w\right]+\alpha_1 r_1T\left(r_1\right)w\left(r_1\right)+\alpha_2 r_2T\left(r_2\right)w\left(r_2\right),$$

$$l_0\left(w\right)=\sum_{i=1}^{2}\int_{\Omega_i} r\,\overline{f}\,wdr+\beta_1r_1w\left(r_1\right)+\beta_2r_2w\left(r_2\right).$$

Вважаємо, що в деяких точках $d_i\in\Omega,\ i=\overline{1,N}$ відомі зміщення, які задані рівностями

$$y\left(d_i\right)=f_i,\ i=\overline{1,N}\ . \tag{4}$$

Отримана задача (2), (3) полягає у визначенні додатнього дійсного числа u при якому перший компонент y розв’язку $Y=\left(y,T\right)$ задачі (2), (3) задовольняє рівності (4).

Побудуємо функціонал-нев’язку

$$J\left(u\right)=\frac{1}{2}\sum_{i=1}^{N}\left(y\left(d_i\right)-f_i\right)^2\ . \tag{5}$$

Теорема 1. При кожному фіксованому $u\in\mathcal{U}$ узагальнений розв’язок $Y=\left(y,T\right)$ крайової задачі (1) існує та єдиний в $\mathcal{H}$.

Будемо розглядати задачу (2)–(4), що полягає у визначенні елемента $u\in\mathcal{U}$ який мінімізує функціонал-нев’язки (5).

Задачу (2)–(4) будемо розв’язувати за допомогою градієнтних методів О. М. Аліфанова [3]:

$$u_{n+1}=u_n-\beta_n p_n,\ n=0,1,\ldots,n^*\ . \tag{6}$$

Напрямок спуску p_n та коефіцієнт β_n можна визначити за допомогою формул для методу мінімальних нев'язок

$$p_n=J'_{u_n},\quad \beta_n=\frac{\left\|e_n\right\|^2}{\left\|J'_{u_n}\right\|^2},\ \gamma_n=\frac{\left\|J'_{u_n}\right\|^2}{\left\|J'_{u_{n-1}}\right\|^2},\ \beta_n=\frac{(J'_{u_n},p_n)}{\left\|Ap_n\right\|^2}\ . \tag{7}$$

Виходячи з [7, 8], для знаходження (n+1)-го наближення u_{n+1} розв’язку $u\in\mathcal{U}$ задачі (2)–(4) спряжена задача має вигляд

$$-\left(\lambda+2\mu\right)\left(\frac{d}{dr}\left(r\frac{dp}{dr}\right)-\frac{p}{r}\right)=0,\ r\in\Omega_d;\ \ \sigma_r\left(p\right)\Big|_{r=r_i}=0,\ i=1,\,2\,;$$

$$-\frac{d}{dr}\left(kr\frac{d\psi}{dr}\right)-r\left(3\lambda+2\mu\right)\alpha\left(\frac{dp}{dr}+\frac{p}{r}\right)=0,\ r\in\Omega_d\,;$$

$$-k\frac{d\psi}{dr}\bigg|_{r=r_1}=-\alpha_1\psi\left(r_1\right),\quad k\frac{d\psi}{dr}\bigg|_{r=r_2}=-\alpha_2\psi\left(r_2\right);\left[p\right]\Big|_{r=\xi}=0,$$

$$\left[\sigma_r\left(p\right)\right]\Big|_{r=\xi}=0,\quad \left[k\frac{d\psi}{dr}\right]\bigg|_{r=\xi}=0,\quad \left\{k\frac{d\psi}{dr}\right\}^{\pm}=u\left[\psi\right]\Big|_{r=\xi}\,,$$

$$\left[p\right]\Big|_{r=d_i}=0,\ \left[\sigma_r\left(p\right)\right]\Big|_{r=d_i}=-\frac{1}{d_i}\left(y\left(u;d_i\right)-f_i\right),\ \ i=\overline{1,N}, \qquad (8)$$

де $u=u_n$.

Узагальненим розв’язком крайової задачі (8) називається вектор-функція $Y^*=\left(p,\psi\right)\in\mathcal{H}^*=V^*\times V_0^*$, що $\forall z=\left(z_1,z_2\right)\in\mathcal{H}^*$ задовольняє системі тотожностей:

$$a\left(p,z_1\right)=\sum_{i=1}^{N}\left(y\left(u_n;\,d_i\right)-f_i\right)z_1\left(d_i\right), \qquad (9)$$

$$a_0\left(u_n,\psi,z_2\right)-\int\limits_{\Omega_d}r(3\lambda+2\mu)\alpha\left(\frac{dp}{dr}+\frac{p}{r}\right)z_2dr=0\,, \qquad (10)$$

де $\Omega_d=\underset{\nu}{\cup}\Omega_\nu$, $\Omega_\nu=\left(r^{\nu-1},r^{\nu}\right)$, $\nu=\overline{1,\chi}\cup\overline{\chi+2,N+3}$, $r^0=r_1$, $r^\nu=d_i$ при $d_i\in\Omega_1$, $r^\chi=\xi^-$, $r^{\chi+1}=\xi^+$, $r^\nu=d_{\nu-2}$ при $d_{\nu-2}\in\Omega_2$, $r^{N+3}=r_2$, $V^*=\left\{v\left(r\right):v\big|_{\Omega_\nu}\in W_2^1\left(\Omega_\nu\right),\left[v\right]\big|_{r=\xi}=0,\quad \left[v\right]\big|_{r=d_i}=0,\,i=\overline{1,N}\right\}$ на кожному кроці визначення (n+1)-го наближення u_{n+1} розв’язку $u\in\mathcal{U}$.

Введемо до розгляду форми

$$\begin{gathered}\pi\left(u,v\right)=\left(\overline{Y}\left(u\right)-\overline{Y}\left(u_n\right),\overline{Y}\left(v\right)-\overline{Y}\left(u_n\right)\right)_d,\\ L\left(v\right)=\left(f-\overline{Y}\left(u_n\right),\,\overline{Y}\left(v\right)-\overline{Y}\left(u_n\right)\right)_d,\end{gathered} \qquad (11)$$

де $\overline{Y}\left(v\right)=\left\{y\left(v;\,d_i\right)\right\}_{i=1}^{N}$, $\left(\overline{Y}\left(v\right),\,\overline{Y}\left(w\right)\right)_d=\sum\limits_{i=1}^{N}y\left(v;\,d_i\right)y\left(w;\,d_i\right)$, $f=\left\{f_i\right\}_{i=1}^{N}$.

Легко побачити справедливість рівності

$$2J\left(v\right)=\pi\left(v,v\right)-2L\left(v\right)+\left\|\overline{Y}\left(u_n\right)-f\right\|_d^2. \qquad (12)$$

Нехай $u_n+\Delta u_n \in \mathcal{U}$. Тоді $\forall\lambda\in(0,1)$, $u_n+\lambda\Delta u_n\in\mathcal{U}$. Нехтуючи членами другого порядку малості, отримуємо

$$\begin{gathered} Y\left(u_{n+1}\right)\approx\tilde{Y}\left(u_{n+1}\right)=Y\left(u_n\right)+\theta, \\ Y\left(u_n+\lambda\Delta u_n\right)\approx Y\left(u_n\right)+\lambda\theta, \end{gathered} \tag{13}$$

де θ — розв'язок задачі (11), (12).

Врахувавши (13), отримуємо

$$\left\langle J'_{u_n},\,\Delta u_n\right\rangle=\lim_{\lambda\to0}\frac{J\left(u_n+\lambda\Delta u_n\right)-J\left(u_n\right)}{\lambda}\approx\left(\bar{Y}\left(u_n\right)-f,\;\bar{\tilde{Y}}\left(u_{n+1}\right)-\bar{Y}\left(u_n\right)\right)_d. \tag{14}$$

Врахувавши (14), отримуємо

$$\left\langle J'_{u_n},\,\Delta u_n\right\rangle\approx\sum_{i=1}^{N}\left(y\left(u_n;d_i\right)-f_i\right)\left(\tilde{y}\left(u_{n+1};d_i\right)-y\left(u_n;d_i\right)\right)=$$

$$=\sum_{i=1}^{2}\int_{\Omega_i}\frac{d}{dr}\left(r\,k\frac{dT}{dr}\right)\psi\,dr+r_1k\left.\frac{dT}{dr}\right|_{r=r_1}\psi\left(r_1\right)-r_2k\left.\frac{dT}{dr}\right|_{r=r_2}\psi\left(r_2\right)+$$

$$+\Delta u_n\left(\xi\left\{k\frac{dT}{dr}\right\}^{+}\psi^{+}-\xi\left\{k\frac{dT}{dr}\right\}^{-}\psi^{-}\right),$$

або

$$\left\langle J'_{u_n},\,\Delta u_n\right\rangle=\sum_{i=1}^{2}\int_{\Omega_i}\frac{d}{dr}\left(rk\frac{dT}{dr}\right)\psi\,dr+r_1k\left.\frac{dT}{dr}\right|_{r=r_1}\psi\left(r_1\right)-$$

$$-r_2k\left.\frac{dT}{dr}\right|_{r=r_2}\psi\left(r_2\right)+\Delta u_n\left(\xi\left\{k\frac{dT}{dr}\right\}^{+}\psi^{+}-\xi\left\{k\frac{dT}{dr}\right\}^{-}\psi^{-}\right).$$

Отже, $J'_{u_n}\approx\tilde{\psi}_n$,

де

$$\tilde{\psi}_n=\left\{\tilde{\psi}_n^i\right\}_{i=1}^2,$$

$$\tilde{\psi}_n^1=\int_{\Omega_1}\frac{d}{dr}\left(r\frac{dT}{dr}\right)\psi\,dr+\;\Delta u_n\left(r_1k\left.\frac{dT}{dr}\right|_{r=r_1}\psi\left(r_1\right)-\xi\left\{k\frac{dT}{dr}\right\}^{-}\psi^{-}\right),$$

$$\tilde{\psi}_n^2=\int_{\Omega_2}\frac{d}{dr}\left(r\frac{dT}{dr}\right)\psi\,dr+\;\Delta u_n\left(\xi\left\{k\frac{dT}{dr}\right\}^{+}\psi^{+}-r_2k\left.\frac{dT}{dr}\right|_{r=r_2}\psi\left(r_2\right)\right).$$

Запропонованою вище методологією розв'язано модельний приклад.

Нехай $r_1=\pi/4$, $r_2=\pi$, $\xi=\pi/2$. Класичний розв'язок крайової задачі (1), (4) на відрізку $\left[\pi/4,\pi/2\right]$ набуває вигляду $T=1.5\cos\left(0.5r\right)+2$,

$y = \cos(r)$, а на відрізку $\left[\pi/2, \pi\right]$ $T = 1.5\exp(-0.5r) + 1.2$, $y = 1.2\exp(-0.5r) + 1$. Також відомо $\alpha_1 = 1$, $\beta_1 = 1.02822$, $\alpha_2 = 0$; $\beta_2 = 0.574025$; $k_1 = 2$; $k_2 = 3.10176$, $\lambda_1 = 2$, $\mu_1 = 1$, $\lambda_2 = 4$, $\mu_2 = 1.053169$, $\alpha = 3$. Вважаємо, що в цій задачі $u \in \mathcal{U}$ невідоме, $f_0 = T(r_1)$.

У таблиці наведено кількість ітерацій, необхідних для досягнення значення $u_n = 0.450672$ за точністю закінчення ітераційного процесу ε.

Для наведених вхідних даних задачу розв'язано за допомогою градієнтних методів, де на кожному кроці визначення (n + 1)-го наближення u_{n+1} розв'язку $u \in \mathcal{U}$ пряма та спряжена задачі розв'язані за допомогою МСЕ з використанням кусково-квадратичних функцій шляхом мінімізації відповідного функціонала енергії. В цьому випадку похибка $O\left(h^2\right)$ в нормі простору Соболєва $W_2^1(\Omega)$, h — найбільша з довжин всіх скінченних елементів.

Таблиця

Результати обчислювального експерименту

N_1	20		50		50		30	
N_2	20		50		30		50	
ε	10^{-5}	10^{-10}	10^{-5}	10^{-10}	10^{-5}	10^{-10}	10^{-5}	10^{-10}
u_0=1	25	60	22	67	24	59	28	63
u_0=10	48	81	45	73	41	73	40	85
u_0=100	181	185	173	209	159	201	169	194

Висновки. За допомогою градієнтних методів розв'язано задачу ідентифікації щільності теплового потоку в умові спряження при відомому його зміщенні для термопружного деформування довгої складеної циліндричної оболонки. Розв'язано модельні приклади.

Список використаних джерел:

1. Сергиенко И. В., Дейнека В. С. Системный анализ много-компонентных распределенных систем. Киев: Наук. думка, 2009. 640 с.
2. Sergienko I. V., Deineka V. S. Optimal control of distributed systems with conjugation conditions. New York: Kluwer Academic Publishers, 2005. 400 p.
3. Алифанов О. М., Артюхин Е. А., Румянцев С. В. Экстремальные методы решения некорректных задач. М.: Наука, 1988. 288 с.
4. Аралова А. А., Дейнека В. С. Численное решение обратных краевых задач осесимметричного термоупругого деформирования длинного толстого полого цилиндра. *Компьютерная математика.* 2011. № 1. С 3–12.

5. Аралова А. А., Дейнека В. С. Оптимальное управление термо-напряженным состоянием полого цилиндра. *Доповіді національної академії наук України.* 2012. № 5. С. 38–42.
6. Аралова А. А. Численное решение обратных задач термо-упругости для составного цилиндра. Кибернетика и системный анализ. 2014. № 5. С. 164–172.
7. Коваленко А. Д. Термоупругость. Киев: Наук. думка, 1975. 216 с.
8. Мотовилевец И. А., Козлов В. И. Механика связанных полей в элементах конструкций. Т. 1. Термоупругость. Киев: Наук. думка, 1987. 264 с.

The consideration of algorithm of the identification, based on optimal control theory, for thermal resistance for thermoelastic deformation of long cylindrical composite shell was made.

Key words: *thermoelastic state, gradient methods, cylindrical body.*

Одержано 23.03.2017

УДК 519.85

Т. М. Барболіна, канд. фіз.-мат. наук, доцент

Полтавський національний педагогічний університет
імені В. Г. Короленка, м. Полтава

КОМБІНАТОРНА ОПТИМІЗАЦІЯ НА РОЗМІЩЕННЯХ: ОГЛЯД ОСТАННІХ РЕЗУЛЬТАТІВ

Наведений огляд останніх результатів щодо розв'язування задач комбінаторної оптимізації на розміщеннях. Висвітлено розв'язування задач як в умовах визначеності, так і зі стохастичною невизначеністю, а також моделювання детермінованими і стохастичними задачами комбінаторної оптимізації на розміщеннях.

Ключові слова: *комбінаторна оптимізація, стохастична оптимізація, оптимізаційні задачі на розміщеннях.*

Вступ. Серед оптимізаційних задач з обмеженнями комбінаторного характеру, які привертають увагу багатьох дослідників (див., наприклад, [1–23]), важливий клас становлять задачі на евклідових комбінаторних множинах, зокрема, задачі на розміщеннях. Ряд результатів щодо властивостей таких задач, зокрема, достатню умову екстремалі в лінійній безумовній задачі на розміщеннях, отримано в [4, 5] незвідну систему обмежень опуклої оболонки загальної множини розміщень, у роботах [6–8] та інших запропоновано методи розв'язування лінійних і деяких класів нелінійних задач. Низка досліджень, зокрема [3, 9, 10], присвячені дослідженню задач комбінаторної оптимізації з різними видами невизначеності (інтервальною, нечіткою).

Мета даної статті — це огляд деяких нових результатів щодо розв'язування оптимізаційних задач на розміщеннях, у тому числі, з імовірнісною невизначеністю.

Для безумовних задач комбінаторної оптимізації на розміщеннях в [11] отримано нові результати. Зокрема, отримано необхідну умову екстремалі в лінійній безумовній задачі оптимізації на розміщеннях, що разом із відомою раніше достатньою умовою формує критерій екстремалі. Встановлено, що всі екстремалі в лінійній задачі оптимізації на розміщеннях є елементами деякої множини полірозміщень. На основі критерію екстремалі лінійної функції на множині розміщень доведено критерій екстремалі в дробово-лінійній безумовній задачі комбінаторної оптимізації на розміщеннях.

Новий метод розв'язування задачі мінімізації дробово-лінійної функції на множині розміщень запропоновано в [12]. На відміну від аналітичного методу, запропонованого раніше в [7], цей метод передбачає зведення розв'язування дробово-лінійної задачі до розв'язування скінченної послідовності лінійних задач оптимізації на розміщеннях. При знаходженні мінімалей лінійної функції використовується достатня умова мінімалі, що дозволяє розробити ефективні алгоритми. Показано, що запропоновані алгоритми розв'язування задачі є поліноміальними, а отже, більш ефективними, ніж відомі раніше алгоритми розв'язування таких задач.

Як відомо, один із підходів до розв'язування лінійних та дробово-лінійних задач оптимізації на розміщеннях полягає у розбитті багатогранної множини на класи еквівалентності та наступному напрямленому переборі цих класів. Такий підхід (метод побудови лексикографічної еквівалентності) був раніше обґрунтований для розв'язування повністю комбінаторних задач [6]. Обґрунтування методу побудови лексикографічної еквівалентності для частково комбінаторних задач здійснено в [13]. Уведено в розгляд відношення лексикографічної еквівалентності точок відносно розміщень для випадку, коли кількість елементів у вибірці менше вимірності простору. Встановлено властивості класів еквівалентності, на які багатогранна множина розбивається введеним відношенням, запропоновано й обґрунтовано алгоритми розв'язування лінійних частково комбінаторних задач оптимізації на розміщеннях на основі напрямленого перебору таких класів еквівалентності.

У роботі [14] поширено застосування методу побудови лексикографічної еквівалентності на розв'язування частково комбінаторних задач оптимізації дробово-лінійної функції на розміщеннях. Показано, що розв'язування задачі лексикографічної оптимізації дробово-лінійної функції може бути здійснене в два етапи: на першому розв'язується задача лінійного програмування, а на другому — задача лексикографічної оптимізації лінійної функції. Серед запропонованих алгоритмів розв'язування задач лексикографічної комбінаторної оптимізації на розміщеннях з лінійною та дробово-лінійною цільовими функціями є як точні, так і наближений. Останній дозволяє отримувати значення цільової функції, що відрізняється від оптимуму не більше, ніж на задану величину.

Дослідженню задач комбінаторної оптимізації з імовірнісною невизначеністю присвячено роботи [15–25]. Запропоновано новий підхід до формулювання оптимізаційних задач з імовірнісною невизначеністю [15, 16], який ідейно близький до постановок задач з інтервальною та нечіткою невизначеністю [9, 10]. Підхід ґрунтується на введенні відношення лінійного порядку на скінченній множині випадкових величин. Також запропоновано постановки оптимізаційних задач на основі введення лінійного порядку на фактор-множині, яка утворюється в результаті розбиття множини дискретних випадкових величин на класи еквівалентності на основі порівняння їх числових характеристик (наприклад, моментів). Розглянуті деякі властивості запропонованих відношень порядку, зокрема, збереження упорядкування випадкових величин при додаванні до лівої і правої частини співвідношення однієї й тієї самої випадкової величини. Згадані порядки передбачають послідовне порівняння числових характеристик випадкових величин, що дає можливість більш повно враховувати специфіку задачі у порівнянні із переходом від стохастичної задачі до детермінованої шляхом заміни випадкових величин однією з їх числових характеристик (математичне сподівання, дисперсія тощо).

Властивості стохастичних задач комбінаторної оптимізації на розміщеннях у розглянутих постановках досліджено в [17–21]. Встановлено властивості розв'язку задач лінійної безумовної задачі стохастичної оптимізації на розміщеннях, у яких мінімум визначається згідно з лінійним порядком, введеним на множині дискретних випадкових величин: використовуючи критерій екстремалі в лінійній безумовній (детермінованій) задачі, обґрунтовано умову, що може бути покладена в основу пошуку розв'язку, та способи побудови розв'язку [17, 19]. Ґрунтуючись на властивостях розв'язку безумовної задачі з детермінованими коефіцієнтами цільової функції, доведено властивості розв'язку для задачі, у якій коефіцієнти цільової функції є випадковими величинами; запропоновано схему методу гілок і меж для розв'язування лінійних задач оптимізації на розміщеннях з імовірнісною невизначеністю, у якій також запропоновано правила галуження та відсікання множин [20].

Для задач, у яких мінімум визначається на фактор-множині, встановлено зв'язок зі спеціально побудованими детермінованими задачами, запропоновано редукційний метод розв'язування лінійної безумовної задачі комбінаторної стохастичної оптимізації на розміщеннях [21].

Незважаючи на значну кількість публікацій, присвячених моделюванню евклідовими задачами комбінаторної оптимізації, актуальним залишається подальше дослідження цієї проблеми.

Ряд нових математичних моделей прикладних задач як оптимізаційних задач на комбінаторних множинах розміщень та перестановок представлено в [19, 22]. Розглядаються задачі з різними цільовими функціями (лінійними та дробово-лінійними), задачі без додаткових (некомбінаторних) обмежень та з лінійними обмеженнями, як детерміновані, так і стохастичні. Врахування комбінаторного характеру обмежень та імовірнісної невизначеності вхідних даних дозволяє будувати більш точні моделі.

Також запропоновано різні підходи до формулювання задачі упакування прямокутників зі стохастичними параметрами у напівнескінченну смугу: формалізація взаємного розташування прямокутників на основі відношення порядку на множині випадкових величин [23]; модель, яка враховує ймовірність накладання прямокутників у смузі [24]; «жорстка» постановка, яка передбачає, що прямокутники не перетинаються при жодних можливих значеннях дискретних випадкових величин [25]. Задачі упакування прямокутників в умовах імовірнісної невизначеності раніше не розглядалися, а тому є новими.

Висновки. Розглянуто ряд результатів щодо розв’язування евклідових задач комбінаторної оптимізації на розміщеннях, отриманих за останні роки. Як випливає з наведеного огляду, напрямами подальших досліджень може бути продовження вивчення властивостей задач стохастичної комбінаторної оптимізації на розміщеннях, розробка й обґрунтування алгоритмів їх розв’язування.

Список використаних джерел:

1. Сергиенко И. В., Каспшицкая М. Ф. Модели и методы решения на ЭВМ комбинаторных задач оптимизации. К.: Наук. думка, 1981. 288 с.
2. Сергиенко И. В., Гуляницкий Л. Ф., Сиренко С. И. Классификация прикладных методов комбинаторной оптимизации. *Кибернетика и системный анализ.* 2009. № 5. С. 71–83.
3. Стоян Ю. Г. Романова Т. Е., Сысоева Ю. А. Оптимизационная задача размещения правильних интервальных многоугольников. *Докл. НАН Украины*. 1998. № 9. С. 114–120.
4. Стоян Ю. Г., Ємець О. О. Теорія і методи евклідової комбінаторної оптимізації. К.: Інститут системних досліджень освіти, 1993. 188 с. Режим доступу: http://dspace.puet.edu.ua/handle/123456789/487.
5. Ємець О. О., Роскладка О. В., Недобачій С. С. Незвідна система обмежень для загального многогранника розміщень. *Укр. матем. журнал*. 2003. 55, № 1. С.3–11.
6. Емец О. А., Барболина Т. Н. Комбинаторная оптимизация на размещениях. К.: Наукова думка, 2008. 159 с. Режим доступу: http://dspace.puet.edu.ua/-handle/123456789/473.
7. Емец О. А., Черненко О. А. Оптимизация дробно-линейных функций на размещениях. К. : Наукова думка, 2011. 154 с. Режим доступа: http://dspace.puet.edu.ua/handle/123456789/467.
8. Емец О. А., Барболина Т. Н., Черненко О. А. Решение задач оптимизации с дробно-линейными целевыми функциями и дополнительными ограничениями. *Кибернетика и системный анализ*. 2006. № 5. С. 79–85.

9. Ємець О. О., Ємець Ол-ра О. Розв'язування задач комбінаторної оптимізації на нечітких множинах. Полтава: ПУЕТ, 2011. 239 с. Режим доступу: http://dspace.uccu.org.ua/handle/123456789/352.
10. Сергиенко И. В., Емец О. А., Емец А. О. Задачи оптимизации с интервальной неопределенностью: метод ветвей и границ. *Кибернетика и системный анализ*. 2013. № 5. С. 38–50.
11. Емец О. А., Барболина Т. Н. Свойства комбинаторных оптимизационных безусловных задач на размещениях с линейной и дробно-линейной целевыми функциями. *Проблемы управления и информатики*. 2016. № 6. С. 46–57.
12. Ємець О. О., Барболіна Т. М. Властивості екстремалі дробово-лінійної функції на загальній множині розміщень. *Сучасні проблеми прикладної математики та інформатики: збірник наукових праць.* Львів: Львівський національний університет імені Івана Франка, 2016. С. 79–82.
13. Барболина Т. Н. Решение частично комбинаторных задач оптимизации на размещениях методом построения лексикографической эквивалентности. *Кибернетика и системный анализ*. 2013. № 6. С. 137–149.
14. Емец О. А., Барболина Т. Н. Лексикографическая эквивалентность в частично комбинаторной оптимизации дробно-линейных функций на размещениях. *Кибернетика и системный анализ*. 2017. № 2. С. 94–106.
15. Емец О. А., Барболина Т. Н. Об оптимизационных задачах с вероятностной неопределенностью. *Доповіді Національної академії наук України*. 2014. № 11. С. 40–45.
16. Барболина Т. Н. О подходе к оптимизации с вероятностной неопределенностью с использованием упорядочивания случайных величин. *Вісник Запорізького національного університету: Збірник наукових статей. Фізико-математичні науки.* 2016. № 1. С. 11–20.
17. Емец О. А., Барболина Т. Н. О свойствах линейной безусловной задачи комбинаторной оптимизации на размещениях с вероятностной неопределенностью. *Кибернетика и системный анализ.* 2016. № 2. С. 127–139.
18. Ємець О. О., Барболіна Т. М. Властивості лінійних безумовних задач оптимізації на розміщеннях з імовірнісною невизначеністю. *Доповіді НАН України*. 2016. № 2. С. 31–37.
19. Ємець О. О., Барболіна Т. М. Побудова і дослідження математичної моделі задачі директора зі стохастичними параметрами. *Вісник Черкаського університету. Серія Прикладна математика. Інформатика.* 2014. № 18 (311). С. 3–11.
20. Ємець О. О., Барболіна Т. М. Лінійні оптимізаційні задачі на разміщеннях з імовірнісною невизначеністю: властивості і розв’язання. *Системні дослідження та інформаційні технології*. 2016. № 1. С. 107–119.
21. Емец О. А., Барболина Т. Н. Решение линейных безусловных задач комбинаторной оптимизации на размещениях со стохастической неопределенностью. *Кибернетика и системный анализ*. 2016. № 3. С. 141–153.
22. Ємець О. О., Барболіна Т. М. Моделювання детермінованими і стохастичними задачами комбінаторної оптимізації. *Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки*. 2016. Вип. 14. С. 70–80.
23. Емец О. А., Барболина Т. Н. Комбинаторная оптимизационная модель упаковки прямоугольников со стохастическими параметрами. *Кибернетика и системный анализ*. 2015. № 4. С. 99–111.

24. Ємець О. О., Барболіна Т. М. Комбінаторна оптимізаційна модель упакування прямокутників з імовірнісними обмеженнями. *Наукові записки НаУКМА*. 2015. Т. 177: Комп'ютерні науки. С. 58–62.
25. Емец О. А., Барболина Т. Н. О задачах оптимизации взаимного расположения прямоугольников в условиях стохастической, интервальной или нечеткой неопределенностию. *Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки*. 2015. Вип. 12. С. 83–100.

The review of last results concerning solving of combinatorial optimization problems on arrangements is presented. The author consider solving of problems both under certainty and under probabilistic uncertainty. Also modeling by deterministic and stochastic problems of combinatorial optimization on arrangements.

Key words: *combinatorial optimization, stochastic optimization, optimization problems on arrangements.*

Одержано 15.02.2017

УДК 519.8

О. А. Березовский, канд. физ.-мат. наук

Институт кибернетики имени В. М. Глушкова НАН Украины, г. Киев

НУЛЕВОЙ РАЗРЫВ ДВОЙСТВЕННОСТИ В КВАДРАТИЧНЫХ ЭКСТРЕМАЛЬНЫХ ЗАДАЧАХ

В работе рассматривается двойственная оценка (лагранжева релаксация) для квадратичной экстремальной задачи общего вида. Сформулированы условия, при выполнении которых значение глобального экстремума квадратичной экстремальной задачи и значение ее двойственной оценки совпадают.

Ключевые слова: *квадратичная экстремальная задача, двойственная оценка, лагранжева релаксация, неотрицательно определенная матрица, точная оценка (нулевой разрыв двойственности).*

Введение. Многие задачи оптимального управления, планирования, проектирования, моделирования, анализа сетевых структур и т.д., допускают представление в виде квадратичных экстремальных задач, т.е. задач оптимизации, целевая функция и все функции ограничений которых квадратичные (англ. quadratically constrained quadratic programming):

$$f^* = f_0(x^*) = \inf_{x \in T \subseteq R^n} f_0(x), \tag{1}$$

где $T = \{x : f_i(x) \le 0, i \in I^{LQ}, f_i(x) = 0, i \in I^{EQ}; x = (x_1, x_2, ..., x_n)^T \in R^n\}$ — допустимое множество решений задачи (далее будем считать, что оно не пустое); $f_i(x) = x^T A_i x + b^T{}_i x + c_i$, $i \in \{0\} \bigcup I^{LQ} \bigcup I^{EQ}$ — квадратичные функции, определенные в n-мерном пространстве, с симметричной $n \times n$-матрицей A_i, вектором $b_i \in R^n$ и константой $c_i \in R^1$; $m = |I^{LQ}| + |I^{EQ}|$ — общее количество ограничений.

В общем случае квадратичная экстремальная задача относится к классу NP-трудных задач, в связи с чем используют выпуклые релаксации для нахождения оценок ее глобального экстремума. Двойственная оценка задачи (1) определяется как [1]:

$$\psi^* = \sup_{u \in R^m} \left(\psi(u) = \inf_{x \in R^n} L(x,u) \right) \le f^* \tag{2}$$

при ограничениях

$$A(u) \succ= 0,$$

$$u \in U^+ = \{u : u_i \ge 0, i \in I^{LQ}, u \in R^m\},$$

где $L(x,u) = x^T A(u)x + b^T(u)x + c(u)$ — функция Лагранжа для задачи (1), $A(u) = A_0 + \sum_{i=1}^m u_i A_i$, $b(u) = b_0 + \sum_{i=1}^m u_i b_i$, $c(u) = c_0 + \sum_{i=1}^m u_i c_i$, $A \succ= 0$ ($A \succ 0$) обозначает неотрицательно (положительно) определенную матрицу A.

Задачу (2) также называют лагранжевой релаксацией [2; 3] (если быть точным, она является лагранжевой релаксацией квадратичной экстремальной задачи по всем ограничениям с выписанным в явном виде условием, задающим множество двойственных переменных с точностью до граничных точек, при которых решение внутренней задачи не равно $-\infty$). Для нее можно встретить и термин SDP-релаксация Шора [4], что объясняется известным фактом взаимосвязи двойственных оценок и SDP-релаксаций. Например, в случае однородной квадратичной экстремальной задачи (т. е. когда все квадратичные формы задачи (1) не имеют линейных членов — $\forall i \in \{0\} \bigcup I^{LQ} \bigcup I^{EQ}$ $b_i = 0$) при нахождении двойственной оценки (2) решение внутренней задачи $\psi(u) = \inf_{x \in R^n} L(x,u)$ при u такое, что $A(u) \succ 0$, достигается при $x = 0$. Это позволяет переписать задачу (2) в виде задачи

$$\psi^* = \sup_{u \in R^m} (u,c) \tag{3}$$

при ограничениях

$$A_0 + \sum_{i=1}^m u_i A_i \succ= 0,$$

$$u_i \geq 0 \,,\; i \in I^{LQ} \,,$$

которая является двойственной к задаче, получаемой SDP-релаксацией исходной задачи [5], и также относится к задачам полуопределенного программирования.

Использование двойственных оценок (лагранжевых релаксаций) для решения квадратичных экстремальных задач приводит к необходимости оценки качества получаемых результатов. Если для выпуклых задач двойственный подход позволяет получить как значение, так и точку глобального экстремума, то в невыпуклом случае вопрос точности оценки достаточно сложен. Далее сформулирован ряд условий, при которых значение глобального экстремума квадратичной экстремальной задачи общего вида и значение ее двойственной оценки совпадают (т. е. когда разрыв двойственности равен нулю).

Условия получения точной двойственной оценки (нулевого разрыва двойственности). Наиболее общим и очевидным является следующее необходимое и достаточное условие того, что двойственная оценка ψ^* (2) совпадает с оптимальным значением f^* целевой функции задачи (1).

Теорема 1 [6]. Для того, чтобы двойственная оценка ψ^* (2) для квадратичной экстремальной задачи (1) с $f^* > -\infty$ была точной, необходимо и достаточно, чтобы существовал такой вектор множителей Лагранжа u^*, при котором функция $L(u^*, x) - f^*$ представима в виде суммы квадратов линейных форм:

$$\exists u^* : L(u^*, x) - f^* = \sum_{j=1}^{k} l_i^2(x) \,,\; k \leq n \,. \blacksquare$$

С помощью теоремы 2 можно упростить доказательства для некоторых известных частных случаев, а также получать новые результаты. Например, из него прямо следует [6] результат Н.З. Шора (приведенная далее теорема 2) с достаточно объемным доказательством [1] для задачи нахождения глобального минимума ограниченного снизу полинома $P^* = \min\limits_{x \in R^n} P_0(x)$, которой в соответствие поставлена квадритичная задача:

$$P^* = \min_{R} f_0(R) \tag{4}$$

при ограничениях

$$R(\alpha^{(i)})R(\alpha^{(j)}) - R(\alpha^{(k)})R(\alpha^{(l)}) = 0 \,,\; \alpha^{(i)} + \alpha^{(j)} = \alpha^{(k)} + \alpha^{(l)} \,,$$

$$0 \leq \alpha^{(r)} = (\alpha_1^{(r)}, \alpha_2^{(r)}, \ldots, \alpha_n^{(r)})^T \leq s/2 \,. \tag{5}$$

Исходная задача сводится к задаче (4)–(5) следующим образом (далее s обозначает вектор старших степеней полинома $P_0(x)$):

1) для всех $\alpha^{(i)} \le \bar{\alpha} = s/2$ вводятся новые переменные $R(\alpha^{(i)}) = R(\alpha^{(j)})R(\alpha^{(k)})$, $\alpha^{(i)} = \alpha^{(j)} + \alpha^{(k)}$, $\alpha^{(r)} = (\alpha_1^{(r)},\dots,\alpha_n^{(r)})^T \le \bar{\alpha}$, в результате чего получаем полный набор переменных, покрывающих все мономы степени $\alpha^{(i)} \le \bar{\alpha}$, а полином $P_0(x)$ представим в виде квадратичной функции $f_0(R)$;
2) к квадратичным ограничениям, определяющим новые переменные, добавляется полное семейство ограничений вида $R(\alpha^{(i)})R(\alpha^{(j)}) - R(\alpha^{(k)})R(\alpha^{(l)}) = 0$ для всех $\alpha^{(i)} + \alpha^{(j)} = \alpha^{(k)} + \alpha^{(l)}$, т. е. с помощью их линейной комбинации можно получить все представления (степени меньше или равно двух) любого монома $x_1^{\alpha_1^{(r)}} x_2^{\alpha_2^{(r)}} \dots x_n^{\alpha_n^{(r)}}$ степени $\alpha^{(r)} \le s$, а значит и полинома $P_0(x)$, в новых переменных.

Теорема 2 [1, с. 141]. Для того, чтобы двойственная оценка ψ^* квадратичной задачи (4)–(5) была точной, необходимо и достаточно, чтобы полином $P_0(x) - f^*$ был представим в виде суммы квадратов полиномов.

В ряде случаев оказывается более удобным переформулировать общее условие точности для двойственной оценки следующим образом.

Теорема 3 [7]. Для того, чтобы двойственная оценка ψ^* (2) для квадратичной экстремальной задачи (1) была точной, необходимо и достаточно, чтобы матрица $\begin{pmatrix} A_0 & b_0/2 \\ b_0^T/2 & -f^* \end{pmatrix}$ была представима в виде разности неотрицательно-определенной матрицы и линейной комбинации матриц $\bar{A}_i = \begin{pmatrix} A_i & b_i/2 \\ b_i^T/2 & c_i \end{pmatrix}$, $i = \overline{1,m}$, коэффициентами которой являются координаты вектора $u^* \in U^+$.■

Из формулировки необходимого и достаточного условия точности в виде теоремы 3 легко следует, например, следующий результат Н.З. Шора для задачи минимизации квадратичной функции на положительном ортанте.

Теорема 4 [1, с. 117]. Для задачи $f^* = \min\limits_{x \in R^n} \{(x^T A_0 x + b_0^T x) : x \ge 0\}$ в случае $f^* > -\infty$ значение двойственной оценки (2) эквивалентной квадратичной задачи

$$\min_{x \in R^n} \{(x^T A_0 x + b_0^T x) : x \ge 0,\ x_i x_j \ge 0,\ i, j = \overline{1,n}\}$$

совпадает с f^* тогда и только тогда, когда матрица $\begin{pmatrix} A_0 & b_0/2 \\ b_0^T/2 & r \end{pmatrix}$ для некоторого $r > 0$ представима в виде суммы неотрицательной и неотрицательно определенной матрицы. ■

Приведенные в виде теорем 1 и 3 условия нахождения точных оценок трудно проверить на практике, что обусловило определение достаточного условия нулевого разрыва двойственности.

Обозначим Γ^+ — множество граничных точек множества $\{u : A(u) \succ= 0, u \in R^m\}$, удовлетворяющих условию $u_i \geq 0$, $i \in I^{LQ}$. Определим для каждого $u \in \Gamma^+$ множество

$$J(u) = \{j : \lambda_j(u) = 0, j \in \{1,...,n\}\},$$

где $\lambda_j(u)$, $j \in \{1,...,n\}$ — собственные числа матрицы $A(u)$. И пусть $\xi_j(u)$ — собственные вектора, соответствующие собственным числам $\lambda_j(u)$.

Теорема 5 [8]. Если существуют такой вектор p и такое положительное число $\tilde{\varepsilon} > 0$, что для любого $\varepsilon \in (0, \tilde{\varepsilon})$

$$\forall u \in \Gamma^+ \;\; \exists j \in J(u) \text{ такое, что } \xi_j^T(u)(b_0 + \sum_{i=1}^{m} u_i b_i + \varepsilon p) \neq 0, \qquad (6)$$

то двойственная оценка ψ^* (2) для квадратичной экстремальной задачи (1) точная. Причем, если условие (6) выполняется при $p = 0$, то вектор $x^* = x(u^*) = -A^{-1}(u^*)b(u^*)/2$ решения задачи (2) является и решением задачи (1). ■

С помощью теоремы 5 были получены легко проверяемые частные случаи задачи построения шара минимального объема с заданным центром, описанного вокруг пересечения одинаково ориентированных эллипсоидов, для которых разрыв двойственности равен нулю [9]. Пример применения этой теоремы также можно найти в [8] при решении одной специальной задачи невыпуклой оптимизации, которая встречается при синтезе управления, минимизирующего область локализации инвариантного множества семейства нелинейных систем. Для решения этой задачи использовалась эквивалентная ей квадратичная постановка задачи, для нахождения нижней оценки оптимального значения целевой функции которой был применен двойственный подход. Используя теорему 5, сформулировано достаточное условие того, что данный подход дает оптимальное значение целевой функции и точку глобального экстремума исходной задачи.

Выводы. Использование релаксаций для решения квадратичных экстремальных задач приводит к необходимости оценки качества получаемых оценок. В данной работе сформулирован ряд условий, при которых оптимальное значение целевой функции квадратичной экстремальной задачи и значение ее двойственной оценки (лагранжевой релаксации) совпадают; приводятся примеры их применения.

Список использованной литературы:

1. Шор Н. З., Стеценко С. И. Квадратичные экстремальные задачи и недифференцируемая оптимизация. К.: Наук. думка, 1989. 208 с.
2. Anstreicher K., Wolkowicz H. On Lagrangian relaxation of quadratic matrix constraints. *SIAM Journal on Matrix Analysis and Applications*. 2000. 22 (1). С. 41–55.
3. Lemaréchal C. Lagrangian relaxation. *Computational combinatorial optimization*. 2001. С. 112–156.
4. Kim S., Kojima M., Waki H. Exploiting sparsity in SDP relaxation for sensor network localization. *SIAM Journal on Optimization*. 2009. Т. 20. № 1. С. 192–215.
5. Vanderberghe L., Boyd S. Semidefinite programming. *Siam Review*. 1996. № 38. Р. 49–95.
6. Березовский О. А. О точности двойственных оценок для квадратичных экстремальных задач. *Кибернетика и системный анализ*. 2012. № 1. С. 3–39.
7. Березовский О. А. Условие точности двойственных квадратичных оценок в матричном виде. *Теорія оптимальних рішень*. К.: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2015. С. 41–45.
8. Березовский О. А. О решении одной специальной оптимизационной задачи, связанной с определением инвариантных множеств динамических систем. *Проблемы управления и информатики*. 2015. № 3. С. 33–40.
9. Березовский О. А., Шулинок И. Э. Использование двойственного подхода для решения одной геометрической задачи. *Компьютерная математика*. К.: Ин-т кибернетики им. В. М. Глушкова НАН Украины, 2016. № 2. С. 94–99.

This paper discusses the dual bound (Lagrangian relaxation) for quadratically constrained quadratic programming problem in general case. The conditions are formulated under which the value of a global extremum of quadratically constrained quadratic programming problem and the value of its dual bound coincide.

Key words: *quadratically constrained quadratic programming problem, dual bound, Lagrangian relaxation, non-negative definite matrix, exact bound (zero duality gap).*

Получено 15.02.2017

УДК 681.3.06

О. Ю. Беспалов, аспірант

Національний технічний університет України «КПІ», м. Київ

УЗАГАЛЬНЕННЯ ЛЕМИ ГАУССА ПРО ХАРАКТЕРИ ПАР ЕЛЕМЕНТІВ ПРОСТОГО СКІНЧЕННОГО ПОЛЯ

У роботі доведено узагальнення леми Гаусса про характери пар елементів простого скінченного поля та наслідки з неї. Ці результати мають суттєве застосування при дослідженні властивостей еліптичних кривих.

Ключові слова: *характери скінченного поля, еліптичні криві.*

Вступ. Сучасну криптологію неможливо уявити без стійких та швидких алгоритмів цифрового підпису на еліптичних кривих. Зокрема, за останні роки з'явився новий клас еліптичних кривих, так звані криві Едвардса [1], що є рекордсменами у швидкодії операцій у групі точок кривої. Цей напрямок почав розвиватися приблизно десять років тому, але кількість робіт, йому присвячена, налічує не одну тисячу. З основними результатами цього напрямку можна ознайомитись у [2–7].

Звичайно, при дослідженні властивостей кривих Едвардса активно використовуються результати теорії чисел. Це є природнім і зрозумілим. Наприклад, одна з найголовніших для криптографії на еліптичних кривих теорем — теорема Хассе про кількість точок кривої [8, с. 196–197] теж є результатом теорії чисел.

У роботах вітчизняних авторів [5, 7] при дослідженні еліптичних кривих Едвардса неодноразово використовувався інший, менш поширений, але досить цікавий результат з теорії чисел — так звана лема Гаусса про характери пар елементів скінченного поля [9, с. 75–79]. Також певні міркування показують, що при подальших дослідженнях може виявитись необхідним більш загальне твердження, яке ми у цій роботі назвемо узагальненою лемою Гаусса про характери пар елементів скінченного поля. Зазначимо, що з узагальнення цієї леми, яке буде доведено далі у роботі, зразу випливає і сама лема, і деякі її наслідки, які використовувались, наприклад, у [5] при обчисленні кількості кривих Едвардса над простим полем, які мають певні властивості.

1. Основні позначення та терміни. Для довільного простого p позначимо $Q_p = \left\{ x \in Z_p^* \mid \exists y \in Z : \ x \equiv y^2 \left(\operatorname{mod} p \right) \right\}$ — множину зведених квадратичних лишків за модулем p. Також позначимо

$$\left(\frac{x}{p} \right) = \begin{cases} 1, & if \quad x \operatorname{mod} p \in Q_p; \\ 0, & if \quad x \,\vdots\, p; \\ -1, & if \quad x \operatorname{mod} p \in Z_p^* \setminus Q_p, \end{cases} \qquad (1)$$

символ Лежандра елемента x за модулем p.

Безпосередньо з означення випливає, що символ Лежандра (1) є характером мультиплікативної групи простого скінченного поля Z_p.

Для довільного $l \in N$, $1 \le l \le p-1$, введемо наступні множини:

$$RR_l = \left\{ \left(i, i+l\right) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\}\right) \Lambda \left(\left(\frac{i}{p}\right) = \left(\frac{i+l}{p}\right) = 1 \right) \right\},$$

$$RN_l = \left\{ \left(i, i+l\right) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\}\right) \Lambda \left(\left(\frac{i}{p}\right) = 1, \left(\frac{i+l}{p}\right) = -1 \right) \right\},$$

$$NR_l = \left\{ \left(i, i+l\right) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\}\right) \Lambda \left(\left(\frac{i}{p}\right) = -1, \left(\frac{i+l}{p}\right) = 1 \right) \right\},$$

$$NN_l = \left\{ \left(i, i+l\right) \bmod p \mid \left(i \in Z_p^* \setminus \{p-l\}\right) \Lambda \left(\left(\frac{i}{p}\right) = \left(\frac{i+l}{p}\right) = -1 \right) \right\}. \quad (2)$$

Також через

$$rr_l, rn_l, nr_l, nn_l \quad (3)$$

позначимо потужності відповідних множин з (2).

Зазначимо, що у частковому випадку, коли $l = 1$, величини (3) збігаються з величинами

(ВВ), (ВН), (НВ) та (НН), (4)

введеними в [9]. Величини (4) використовувались потім у роботі [5] (леми 2 та 3) при обчисленні точної кількості кривих Едвардса над простим скінченним полем, що мають певні властивості.

Для обчислення величин (4) в книзі [9] наведений результат Гаусса, який дозволяє обчислити ці величини. Тут і далі цей результат ми будемо називати лемою Гаусса, або лемою про характери пар елементів скінченного поля.

Лема 1 (лема Гаусса [9]): у наших позначеннях справедливі рівності:

$$(ВВ) + (ВН) = \frac{1}{2}\left(p-2-\varepsilon\right); (НВ) + (НН) = \frac{1}{2}\left(p-2+\varepsilon\right);$$

$$(ВВ) + (НВ) = \frac{1}{2}\left(p-1\right)-1; \quad (5)$$

$$(ВН) + (НН) = \frac{1}{2}\left(p-1\right); (ВВ) + (ВН) - (НВ) - (НН) = -1.$$

На основі результатів (5) у роботі [5, с. 168–169] доведені дві допоміжні леми, які в певному сенсі можна вважати частковими узагальненнями леми Гаусса. Потім, з використанням цих лем, у роботі було отримано основний результат щодо кількості кривих Едвардса.

У цій роботі буде доведено більш глобальне узагальнення леми Гаусса. Зазначимо, що з нашого результату одразу випливає як сама лема Гаусса (5), так і леми 2 та 3 з роботи [5], а також деякі інші корисні наслідки.

2. Узагальнення леми про характери пар елементів скінченного поля.

Лема 2 (про характери пар елементів скінченного поля).

Нехай p — просте, $l \in Z_p^*$. Тоді для величин (3) справедливі наступні рівності:

$$rn_l + nn_l = \frac{p-2+\left(\frac{l}{p}\right)}{2}; \; rr_l + nr_l = \frac{p-2-\left(\frac{l}{p}\right)}{2};$$

$$nr_l + nn_l = \frac{p-2+\left(\frac{-l}{p}\right)}{2}; \tag{6}$$

$$rr_l + rn_l = \frac{p-2-\left(\frac{-l}{p}\right)}{2}; \; rr_l + nn_l - rn_l - nr_l = -1 .$$

Доведення. Доводимо перше твердження з (6). Доведення інших рівностей виконуються аналогічно з певними модифікаціями. Всього кількість пар $(i, i+l)$, де $i \in Z_p^* \setminus \{p-l\}$, дорівнює $p-2$. При цьому перший елемент пари пробігає всі значення з Z_p^*, крім $p-l$, а другий — всі значення з Z_p^*, крім l (оскільки $i \neq 0$). Потрібно визначити, скільки разів другий елемент у цих парах є квадратичним нелишком, тобто скільки існує таких елементів $a \in Z_p^* \setminus \{l\}$, що $a \in Z_p^* \setminus Q_p$.

Зрозуміло, що ця кількість залежить від квадратичності елемента l. Оскільки кількість квадратичних нелишків у Z_p^* дорівнює $\frac{p-1}{2}$, то кількість квадратичних нелишків у $a \in Z_p^* \setminus \{l\}$ є $\frac{p-1}{2}$, якщо $l \in Q_p$, та $\frac{p-1}{2} - 1 = \frac{p-3}{2}$, у протилежному випадку. Звідси

$$rn_l + nn_l = \begin{cases} \frac{p-3}{2}, & if \quad \left(\frac{l}{p}\right) = -1 \\ \frac{p-1}{2}, & if \quad \left(\frac{l}{p}\right) = 1 \end{cases} = \frac{p-2+\left(\frac{l}{p}\right)}{2}.$$

Перша рівність доведена.

Для доведення рівностей з другої по четверту, зазначимо, що:

- у парах $\left(i,i+l\right)\in RR_l\cup NR_l$ перший елемент приймає значення з $Z_p^*\setminus\left\{p-l\right\}$, а другий — з $\left(Z_p^*\setminus\left\{l\right\}\right)\cap Q_p$;
- у парах $\left(i,i+l\right)\in NR_l\cup NN_l$ перший елемент приймає значення з $\left(Z_p^*\setminus\left\{p-l\right\}\right)\cap\left(Z_p^*\setminus Q_p\right)$, а другий — з $Z_p^*\setminus\left\{l\right\}$;
- у парах $\left(i,i+1\right)\in RR_l\cup RN_l$ перший елемент приймає значення з $\left(Z_p^*\setminus\left\{p-l\right\}\right)\cap Q_p$, а другий — з $Z_p^*\setminus\left\{l\right\}$.

Далі ці твердження доводяться з використанням міркувань, аналогічних до тих, що наведені при доведенні першої рівності.

Остання, п'ята рівність, доводиться інакше. Для її доведення зазначимо, що

$$rr_l+nn_l-rn_l-nr_l=\sum_{\substack{i=1\\ i\neq p-l}}^{p-1}\left(\frac{i\left(i+l\right)}{p}\right).$$

Позначимо $m=i^{-1}\bmod p$ перетворимо вираз $\left(\frac{i\left(i+l\right)}{p}\right)$ наступним чином, використовуючи властивості символа Лежандра:

$$\left(\frac{i\left(i+l\right)}{p}\right)=\left(\frac{i\left(i+l\right)i^{-2}}{p}\right)=\left(\frac{i^{-1}\left(i+l\right)}{p}\right)=\left(\frac{\left(1+lm\right)}{p}\right).$$

Оскільки $i\neq p-l$, то $m\neq\left(p-l\right)^{-1}$, або $m\neq -l^{-1}$, тому $1+lm\neq 1+l\cdot\left(-l^{-1}\right)$, тобто $1+lm\neq 0$. Крім того, оскільки $l\neq 0$, $m\neq 0$, то $1+lm\neq 1$. Покажемо, що вираз $1+lm$ приймає всі значення з $Z_p^*\setminus\left\{1\right\}$. Дійсно, нехай $a\in Z_p^*\setminus\left\{1\right\}$. Тоді

$$1+lm=a\;\Leftrightarrow\; lm=a-1\;\Leftrightarrow\; m=l^{-1}\left(a-1\right).$$

Отже,

$$rr_l+nn_l-rn_l-nr_l=\sum_{\substack{i=1\\ i\neq p-l}}^{p-1}\left(\frac{i\left(i+l\right)}{p}\right)=\sum_{i=2}^{p-1}\left(\frac{i}{p}\right)=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)-\left(\frac{1}{p}\right)=$$

$$=\left|Q_p\right|-\left|Z_p^*\setminus Q_p\right|-1=0-1=-1.$$

Лему доведено.

3. Наслідки з узагальненої леми Гаусса. Тепер наведемо ряд тверджень, що випливають з доведеної леми. Ці твердження є цікавими не тільки з математичної точки зору, але й з точки зору вирішення практичних задач криптології. Наведені далі твердження можна використовувати для обчислення кількості кривих або точок кривої, що має певні властивості або задана певними параметрами. Оскільки задача обчислення кількості точок є фактично задачею обчислення кількості розв’язків певного рівняння.

Зазначимо, що класичну лему Гаусса також можна вважати наслідком узагальненої леми при $l=1$.

Наслідок 1. Позначимо $\varepsilon_1=\left(\frac{l}{p}\right)$ та $\varepsilon_2=\left(\frac{-l}{p}\right)$. Тоді величини (3) приймають такі значення:

$$rn_l=\frac{p-1+\varepsilon_1-\varepsilon_2}{4};\ nn_l=\frac{p-3+\varepsilon_1+\varepsilon_2}{4};$$

$$rr_l=\frac{p-3-\varepsilon_1-\varepsilon_2}{4};\ nr_l=\frac{p-1-\varepsilon_1+\varepsilon_2}{4}.$$

Доведення наслідку 1 полягає у безпосередньому обчисленні значень цих величин з системи (6).

Наслідок 2. Якщо $l\in Q_p$, то

$$rn_l=\frac{p-\left(\frac{-1}{p}\right)}{4};\ nn_l=\frac{p-2+\left(\frac{-1}{p}\right)}{4};$$

$$rr_l=\frac{p-4-\left(\frac{-1}{p}\right)}{4};\ nr_l=\frac{p-2+\left(\frac{-1}{p}\right)}{4}.$$

В протилежному випадку (тобто коли $l\notin Q_p$)

$$rn_l=\frac{p-2+\left(\frac{-1}{p}\right)}{4};\ nn_l=\frac{p-4-\left(\frac{-1}{p}\right)}{4};$$

$$rr_l=\frac{p-2+\left(\frac{-1}{p}\right)}{4};\ nr_l=\frac{p-\left(\frac{-1}{p}\right)}{4}.$$

Для доведення цього наслідку скористаємось тим, що за умови $l\in Q_p$ виконується $\varepsilon_1=\left(\frac{l}{p}\right)=1$ та $\varepsilon_2=\left(\frac{-l}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{l}{p}\right)=\left(\frac{-1}{p}\right)$.

Аналогічно, за умови $l \notin Q_p$ виконується $\varepsilon_1 = \left(\frac{l}{p}\right) = -1$ та $\varepsilon_2 = \left(\frac{-l}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{l}{p}\right) = -\left(\frac{-1}{p}\right)$.

Зауважимо, що з наслідку 2 відразу випливають леми 2 та 3 з роботи [7].

Висновки. У роботі доведено узагальнення відомого результату з теорії чисел — леми Гаусса про характери пар елементів скінченного простого поля. Також отримано наслідки цієї леми. Ці результати мають практичне значення при аналізі властивостей еліптичних кривих над простим скінченним полем.

Список використаних джерел:

1. Edwards H. M. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*. 2007. Vol. 44, N. 3. P. 393–422.
2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. *IST Programme under Contract IST–2002–507932 ECRYPT,* 2007, P. 1–20.
3. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. *IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498.* 2008. P. 1–17.
4. Бессалов А. В., Дихтенко А. А., Третьяков Д. Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. *Сучасний захист інформації*. 2011. №4. С. 33–36.
5. Kovalchuk L., Bessalov A. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to EdvardsEdwards Curves Over Prime Field. *Cybernetics and Systems Analysis*. 2015. Vol. 51, issue 2. P. 165–172.
6. Ковальчук Л. В., Бессалов А. В., Беспалов А. Ю. Алгоритмы генерации базовой точки кривой Едвардса с использованием критериев делимости точки. *Кибернетика и системный анализ*. 2016. Т. 52, № 5. С. 14–24.
7. Бессалов А. В., Цыганкова О.В.. Новые свойства кривой Эдвардса над простым полем. *Радиотехника*. 2015. №180. С. 137–143.
8. Коблиц Н. Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001. 254 с.
9. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел: Пер. с англ. под редакцией Ю. В. Линника. М.: Наука, 1965. 176 с.

Generalized Gauss Lemma about characters of pair of elements of finite prime field is proved and, some corollaries are obtained. These results are useful in investigations of different properties of elliptic curves.

Key words: *characters of finite prime field, elliptic curves.*

Одержано 27.02.2017

УДК 519.6

М. В. Білоус, канд. фіз.-мат. наук
Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ОБ'ЄКТНА МОДЕЛЬ СКІНЧЕННОГО ЕЛЕМЕНТУ В РОЗВ'ЯЗУВАЧІ NADRA-3D

Розглянуто об'єктну модель скінченного елемента та її взаємодію з підсистемами породження систем лінійних алгебраїчних рівнянь програмного каркаса Nadra-3D.

Ключові слова: *метод скінченних елементів, об'єктна модель, програмний каркас.*

Вступ. Метод скінченних елементів (МСЕ) [1–3] чисельного розв'язання систем диференціальних рівнянь у частинних похідних полягає в апроксимації суцільного середовища вихідної області з нескінченною кількістю ступенів свободи скінченною кількістю підобластей (елементів). В кожному елементі вибирається вигляд апроксимуючої функції, значення якої у вузлах елемента збігаються із значенням розв'язку вихідної системи рівнянь. Розв'язання вихідної системи диференціальних рівнянь зводиться до розв'язання системи лінійних алгебраїчних рівнянь (СЛАР), побудованої за певною розрахунковою схемою. Отриманий вектор містить наближені значення шуканого розв'язку у вузлах розрахункової сітки.

У роботі [3] приведено наступне визначення скінченного елемента: скінченний елемент це трійка (ω, P, Ф), що складається з таких об'єктів:

1) ω — замкнена підмножина з ліпшицевою границею та непустою множиною внутрішніх точок;
2) P — N-мірний простір функцій, визначених на ω; зазвичай P — це простір поліномів;
3) Ф — набір лінійно незалежних лінійних функціоналів , $i = \overline{1, N}$.

Підмножина ω називається коміркою. В двовимірному випадку це трикутник (2-симплекс) або чотирикутник, в тривимірному — тетраедр (3-симплекс) або прямокутний паралелепіпед.

Лінійні функціонали φ_i називають ступенями свободи скінченного елемента, а набір функцій $p_i \in P, i = \overline{1, N}$: $\varphi_j\left(p_i\right) = \delta_{ij}$, $\forall i, j = \overline{1, N}$ — базисними функціями скінченного елемента.

Точність знайденого розв'язку вихідної системи рівнянь залежить, зокрема, від характеристик скінченних елементів: максимального розміру сторони, значень кутів між сторонами елемента, порядку поліномів базисних функцій.

Програмна реалізація обчислювальних схем МСЕ складається з перебору усіх елементів розрахункової сітки, обчислення для кожного елемента доданків матриці та вектора правої частини СЛАР МСЕ, збірки СЛАР і знаходження її розв'язку. Далі розглядається побудова ієрархії класів опису скінченних елементів при програмній реалізації таких обчислювальних схем.

Об'єктна модель скінченного елемента. В Інституті кібернетики імені В.М. Глушкова НАН України розроблено програмний каркас Nadra-3D — написаний мовою C++ набір класів та функцій для програмної реалізації обчислювальних схем МСЕ для різних класів задач. На базі цього програмного каркасу побудовано скінченно-елементний розв'язувач Nadra-3D [4] — програмний пакет для моделювання процесів фільтрації води, теплопровідності, зміни напружено-деформованого стану багатокомпонентних середовищ.

В програмному каркасі Nadra-3D запропонована наступна об'єктна модель скінченного елемента у вигляді «чорної скриньки», яка підтримує обов'язкові методи вхідного та вихідного інтерфейсів (рис. 1). Взаємодія модулів програмного каркасу з такими об'єктами (їх створення, ініціалізація, розрахунок елементарних матриць та векторів) виконується виключно за допомогою цих методів.

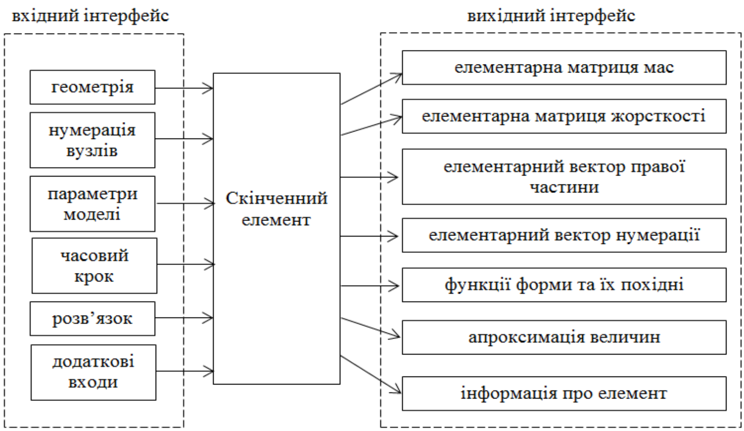


Рис. 1. *Об'єктна модель скінченного елемента*

Таким чином система може однотипно опрацьовувати скінченні елементи для різних класів задач, з різною геометрією та базисними функціями. При цьому вся логіка роботи об'єкта (реалізація математичних співвідношень для розрахунків елементарних матриць та векторів для конкретної задачі) повністю прихована всередині класу, що реалізує цей скінченний елемент. Додавання в систему нового класу скінченного елемента виконується шляхом його наслідування від одного з базових класів та наступною реєстрацією в системі породження скінченних елементів.

Методи вхідного інтерфейсу виконують наступні операції: завантаження просторових координат вузлів елементу; завантаження нумерації вузлів елемента; завантаження параметрів математичної моделі; завантаження координати часової дискретизації; завантаження значень розв’язку у вузлах елемента; завантаження інших вхідних значень (наприклад, значень температури для задач термопружності, або значень п’єзометричних напорів при моделюванні впливу фільтрації на зміну напружено-деформованого стану).

Методи вихідного інтерфейсу можна розділити на наступні групи.

1. Методи отримання інформації про скінченний елемент (тип геометрії та код скінченного елемента, тип базисних функцій, тип інтегрування, кількість ступенів свободи, здатність елемента генерувати елементарні матриці, вектори, обчислювати еталонні значення або значення на основі розрахованих розв’язків).
2. Методи виділення оперативної пам’яті для елементарних матриць та векторів. Оскільки розмір елементарних матриць залежить від кількості вузлів скінченного елемента та кількості ступенів свободи на вузол (що визначається типом розв’язуваної задачі), виділення оперативної пам’яті для них покладено на клас скінченного елемента. Система тільки відправляє запит на виділення пам’яті та отримує покажчики на відповідні структури даних.
3. Методи породження елементарних матриць та векторів (матриці мас; матриці жорсткості; векторів правої частини, точних значень розв’язку (для задач тестування); величин, розрахованих на основі вектору розв’язків).
4. Методи обчислення значень базисних функцій, їх перших та других похідних за просторовими змінними.

Ієрархія класів опису скінченних елементів в програмному каркасі Nadra-3D складається з чотирьох рівнів (рис. 2).

Базовий клас (клас нульового рівня) містить оголошення програмного інтерфейсу у вигляді чистих віртуальних функцій. Ці методи мають бути реалізовані у всіх класах опису скінченних елементів, створених для роботи з каркасом. Наслідування цьому класу забезпечує інтеграцію з усіма підсистемами програмного каркасу.

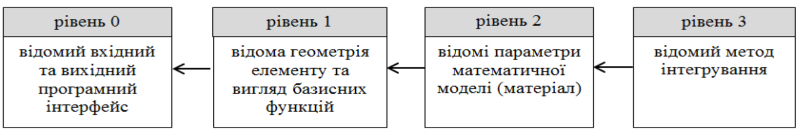


Рис. 2. *Рівні ієрархії класів опису скінченних елементів*

Класи першого рівня — нащадки базового класу. У них реалізовано методи завантаження координат та нумерації вузлів елемента, методи обчислення значень базисних функцій та їх частинних похідних за просторовими змінними. Також класи цього рівня містять статичні методи відображення довільного скінченного елемента на канонічний елемент того ж типу та навпаки. На цьому рівні, зокрема, реалізовано базові двовимірні симплекс-елементи з лінійними (рис. 3, а) та квадратичними (рис. 3, б) базисними функціями, базові тривимірні симплекс-елементи з лінійними (рис. 3, в) та квадратичними (рис. 3, г) базисними функціями, елементи з подвійною нумерацією вузлів (для врахування умов спряження) з лінійними (рис. 3, д) та квадратичними (рис. 3, є) базисними функціями.

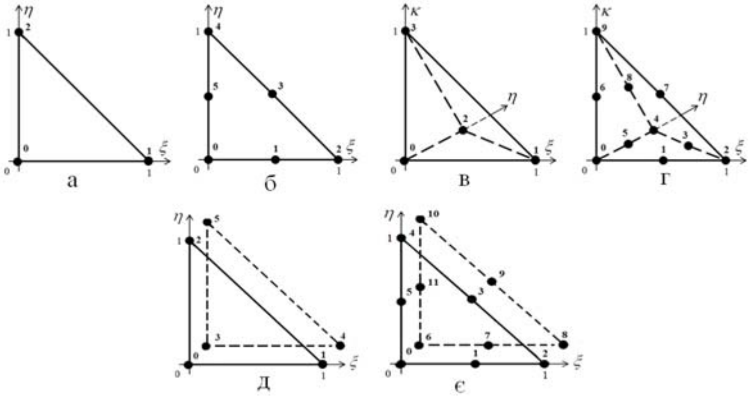


Рис. 3. *Геометрія скінченних елементів класів першого рівня*

Класи другого рівня є нащадками класів першого рівня та відповідають скінченним елементам для прикладних задач. В них реалізуються методи завантаження параметрів математичної моделі, а також визначаються характеристики скінченного елемента (кількість ступенів свободи, код елемента тощо). На цьому рівні в програмному каркасі Nadra-3D реалізовано класи опису тривимірних симплекс-елементів з лінійними та квадратичними базисними функціями для задач теорії пружності (для розв’язання систем рівнянь тривимірної лінійної теорії пружності та термопружності в декартовій системі координат); тривимірних симплекс-елементів з лінійними та квадратичними базисними функціями для задач фільтрації (постановки в декартовій системі координат).

В класах третього рівня крім визначеної в батьківських класах математичної моделі задається метод інтегрування для обчислення елементарних матриць та векторів та реалізуються методи їх розрахунку.

При використанні в цих методах чисельного інтегрування інтеграли по скінченним елементам апроксимуються скінченними сумами

$$\int_{\omega} \varphi(x)\,dx = \sum_{k=1}^{K} \alpha_k \varphi(x_k),$$

де α_k — вагові коефіцієнти, x_k — вузли інтегрування, що належать скінченному елементу ω, K — кількість вузлів інтегрування. Це призводить до того, що замість розв'язку вихідної задачі, шукається розв'язок задачі з апроксимованими функціоналом та білінійною формою. При цьому [3] для збереження порядку точності розв'язку кубатурна формула для прямолінійних скінченних елементів на симплексах має допускати точне інтегрування багаточленів степені $2(k-m)$, де k — степінь базисних функцій скінченного елемента, m — порядок розв'язуваних диференціальних рівнянь. За цих умов похибка апроксимації чисельного інтегрування порівняна з похибкою МСЕ.

Набір класів програмного каркасу Nadra-3D містить опис скінченних елементів для розв'язання рівнянь другого порядку ($m = 1$), тому кубатурні формули мають забезпечувати точне інтегрування багаточленів степені 0 для лінійних базисних функцій, та багаточленів степені 2 для квадратичних. Об'єкти, що описують скінченні елементи, параметризуються наборами вузлів інтегрування та вагових коефіцієнтів, які вони використовують при реалізації методів побудови елементарних матриць та векторів. Таким чином, для зміни використовуваної кубатурної формули достатньо завантажити до об'єкта інший набір параметрів.

Взаємодія з підсистемами програмного каркаса. Взаємодія підсистем програмного каркасу з об'єктами опису скінченних елементів відбувається за схемою, показаною на рис. 4.

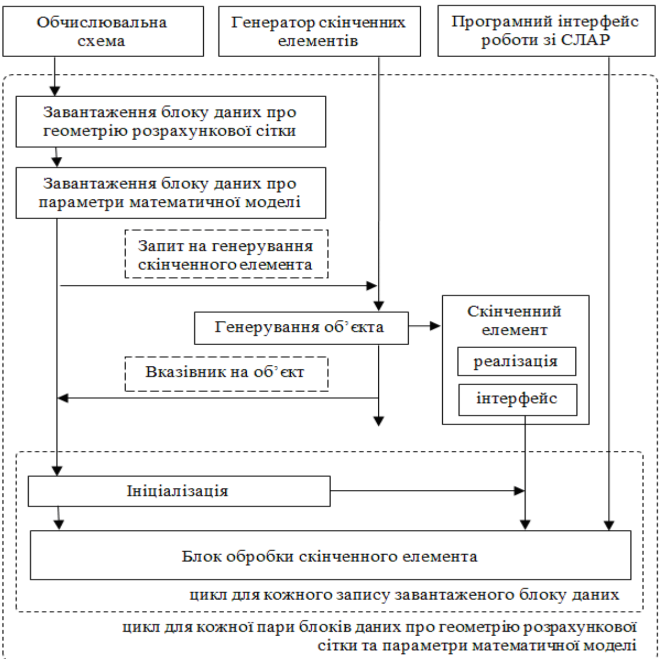


Рис. 4. *Схема роботи зі скінченними елементами*

У схемі слід відмітити розділення роботи зі збірки СЛАР між трьома підсистемами. Генератор скінченних елементів за запитом обчислювальної схеми створює об'єкт скінченного елемента та повертає вказівник на нього як вказівник на клас нульового рівня (див. рис. 2).

Об'єкт, який реалізує обчислювальну схему, відповідає за завантаження вхідних даних, ініціалізацію скінченного елемента та обробку породжених ним елементарних матриць та векторів. Наприклад, для обчислювальних схем розв'язання рівнянь параболічного типу з використанням схеми Кранка-Ніколсона для дискретизації за часом (з кроком τ) доданки розраховуються у вигляді $A = M + \frac{\tau}{2}K$, $B = \left(M - \frac{\tau}{2}K\right)\alpha^j + \frac{\tau}{2}(F^{j+1} + F^j)$, де K, M — обчислені скінченним елементом елементарні матриці жорсткості та мас, F — елементарний вектор правої частини, j — номер кроку.

Розміщення розрахованих доданків у матриці та векторі СЛАР виконується за допомогою методів програмного інтерфейсу роботи зі СЛАР, який стандартизує доступ підсистем програмного каркасу до усіх підтримуваних ним схем зберігання СЛАР в оперативній пам'яті та алгоритмів знаходження їх розв'язків.

Висновки. З використанням запропонованої об'єктної моделі скінченного елемента в програмному каркасі стало можливим реалізовувати за допомогою одного фрагмента коду обчислювальні схеми для різних типів задач. Наприклад, для стаціонарних задач лінійної фільтрації, лінійної теорії пружності у двовимірних та тривимірних постановках, з використанням лінійних або квадратичних базисних функцій обчислювальна схема збірки та розв'язання СЛАР МСЕ має однаковий вигляд. Це забезпечує, зокрема, логічне розширення програмного каркаса класами опису скінченних елементів для задач у сферичній або циліндричній системі координат з максимальним використанням вже відлагоджених модулів збірки та розв'язання СЛАР.

Список використаних джерел:

1. Сьярле Ф. Метод конечных элементов для эллиптических задач. М.: Мир, 1980. 512 с.
2. Дейнека В. С., Сергиенко И. В. Модели и методы решения задач в неоднородных средах. К.: Наук. думка., 2001. 606 с.
3. Шайдуров В. В. Многосеточные методы конечных элементов. М.: Наука. Гл. ред. физ.-мат. лит., 1989. 288 с.
4. Белоус М.В. Конечно-элементный решатель Надра-3D. *Материалы II-й международной конференции «Кластерные вычисления»*, Львов, 3-5 июня 2013. С. 40–47.

An object model of finite element and its interaction with subsystems of software framework Nadra-3D for generating of systems of linear equations are considered.

Key words: *finite element method, object model, software framework.*

Одержано 24.02.2017

УДК 517.9:519.6

А. В. Гладкий*, д-р. фіз.-мат. наук, професор,
Ю. А. Гладка,** канд. фіз.-мат. наук, доцент

*Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ,
**Київський національний торговельно-економічний університет, м. Київ

ПРО МОДЕЛЮВАННЯ ТА ФОРМУВАННЯ АКУСТИЧНИХ ПОЛІВ НА ОСНОВІ ХВИЛЬОВОГО РІВНЯННЯ ТИПУ ШРЕДІНГЕРА

Досліджуються питання чисельного моделювання та формування акустичних полів на основі параболічного хвильового рівняння в неоднорідному хвилеводі з урахуванням тонких включень. Сформульовано критерій оптимальності, досліджено диференціальні властивості функціонала якості, запропоновано чисельний метод для моделювання та оптимізації акустичних полів.

Ключові слова: *акустичне поле, рівняння типу Шредінгера, екстремальна задача, різницева схема, стійкість.*

Вступ. На сьогодні підвищений інтерес до досліджень акустичних полів в океані значною мірою обумовлений розширенням освоєння водних акваторій Світового океану, потребами дистанційного зондування та акустичного моніторингу, оскільки звукові хвилі є практично єдиними хвилями, здатними поширюватися на значні відстані [1–3].

У роботі на основі параболічних апроксимацій хвильового рівняння Гельмгольца досліджуються питання чисельного моделювання процесів поширення акустичних хвиль у неоднорідному осесиметричному хвилеводі $G=\{\ r_0<r<\infty, 0<z<L, r_0>0\ \}$, де (r,z) — циліндричні координати, і вісь z направлена вертикально вниз.

Постановка задачі. Для визначеності будемо припускати, що хвилевод двошаровий з горизонтальною межею поділу середовищ $z=\xi$, на якій виконуються умови неідеального контакту, а кусково-неперервна швидкість звука $c(r,z)$ і кусково-стала густина $\rho(z)$ мають розрив першого роду. Верхній шар G_1 заповнений середовищем зі сталою густиною ρ_1, швидкістю звуку $c_1(r,\mathrm{z})$ та коефіцієнтом поглинання $\upsilon_1(r,z)\geq 0$. Нижній шар G_2 характеризується сталою густиною ρ_2, швидкістю звуку $c_2(r,\mathrm{z})$, коефіцієнтом поглинання $\upsilon_2(r,z)\geq 0$. Крім того, верхню та нижню межі хвилеводу без обмеження загальності будемо вважати абсолютно м’якими. Таким чином, акустичні параметри можна записати співвідношеннями

$$c(r,z)=\begin{cases} c_1(r,z), & 0<z<\xi, \\ c_2(r,z), & \xi<z<L; \end{cases} \quad \upsilon(r,z)=\begin{cases} \upsilon_1(r,z), & 0<z<\xi, \\ \upsilon_2(r,z), & \xi<z<L; \end{cases}$$

$$\rho(z)=\begin{cases} \rho_1, & 0<z<\xi, \\ \rho_2, & \xi<z<L. \end{cases}$$

Комплекснозначний акустичний тиск $P(r,z)$ у хвилеводі з тонким прошарком задовольняє в області $z\in(0,\xi)\bigcup(\xi,L)$, $0<r<\infty$ рівняння Гельмгольця [1, 3]

$$\frac{1}{r}\frac{\partial}{\partial r}\left(r\frac{\partial P}{\partial r}\right)+\rho(z)\frac{\partial}{\partial z}\left(\frac{1}{\rho(z)}\frac{\partial P}{\partial z}\right)+k_0^2 n^2(r,z)P=0,$$

умови неідеального контакту

$$\left\{\frac{1}{\rho(z)}\frac{\partial P}{\partial z}\right\}^{+}=\alpha\left[P\right]\Big|_{z=\xi}, \quad \left\{\frac{1}{\rho(z)}\frac{\partial P}{\partial z}\right\}^{-}=\alpha\left[P\right]\Big|_{z=\xi},$$

граничні умови

$$P\big|_{z=0}=0, \; P\big|_{z=L}=0,$$

а також умови випромінювання на нескінченності.

Тут $P(r,z)$ — комплекснозначний розв’язок, $i=\sqrt{-1}$ — уявна одиниця, $k_0=\omega/c_0$ — хвильове число, c_0 — деяке значення швидкості звуку $c(r,z)$, ω — частота, $n^2(r,z)=(c_0/c(r,z))^2(1+i\upsilon(r,z))$ — комплекснозначний коефіцієнт заломлення, $\{f\}^{\pm}=f(r,\xi\pm 0)=f(r,\xi^{\pm})$, $\left[f(r,z)\right]\big|_{z=\xi}=f(r,\xi+0)-f(r,\xi-0)$, $\alpha>0$ — коефіцієнт, який визначається параметрами тонкого включення і враховує вплив тонкого прошарку шляхом заміни її лінією поділу γ, $\upsilon(r,z)\geq 0$ — коефіцієнт поглинання.

У рамках параболічного наближення акустичне поле можна подати при $k_0 r>>1$ у вигляді $P(r,z)=H_0^{(1)}(k_0 r)p(r,z)$, де $H_0^{(1)}(\cdot)$ — функція Ханкеля першого роду нульового порядку, а плавна амплітуда $p(r,z)$

описується початково-крайовою задачею для рівняння типу Шредінгера з комплекснозначним несамоспряженим оператором [3]

$$2ik_0 \frac{\partial p}{\partial r} + \rho(z)\frac{\partial}{\partial z}\left(\frac{1}{\rho(z)}\frac{\partial p}{\partial z}\right) + k_0^2(n^2(r,z)-1)p = 0\,, \qquad (1)$$

$$\left\{\frac{1}{\rho(z)}\frac{\partial p}{\partial z}\right\}^{+} = \alpha\left[p\right]\Big|_{z=\xi}\,,\quad \left\{\frac{1}{\rho(z)}\frac{\partial p}{\partial z}\right\}^{-} = \alpha\left[p\right]\Big|_{z=\xi}\,, \qquad (2)$$

$$p\Big|_{z=0} = 0\,,\ p\Big|_{z=L} = 0, \qquad (3)$$

$$p\Big|_{r=r_0} = u(z)\,. \qquad (4)$$

Математичну постановку оптимізаційної задачі сформулюємо як задачу мінімізації функціоналу

$$J_{\varepsilon}(u) = \int_0^L \frac{1}{\rho(z)}\beta(z)\left|p(R,z)-p_0(z)\right|^2 dz + \frac{1}{\varepsilon^2}\int_0^L \frac{1}{\rho(z)}\left|u(z)\right|^2 dz \qquad (5)$$

за умови, що $p(r,z;u)$ — розв'язок крайової задачі (1)–(4). Тут $p(R,z) = p(R,z;u)$ — розв'язок задачі (1)–(4) при $r = R, r_0 < R < \infty$, що відповідає керуванню $u(z)$; $\beta(z) > 0$ — задана дійсна функція; $p_0(z)$ — задана комплекснозначна функція; $u(z)$ — комплекснозначне керування із деякої опуклої замкнутої множини

$$U = \left\{\, u(z) \in L_{2,1/\rho}(\Omega),\ \Omega = \left(0,\xi\right)\cup\left(\xi,L\right)\right\},$$

де $L_{2,1/\rho}(\Omega)$ — простір комплекснозначних функцій, інтегрованих з квадратом відносно ваги $1/\rho$ в області Ω. Скалярний добуток і норма в $L_{2,1/\rho}(\Omega)$ визначаються за формулами

$$\left(u,v\right) = \int_{\Omega} \frac{1}{\rho(z)} u(z)\bar{v}(z)dz\,,\ \left\|u\right\| = \left(u,u\right)^{1/2} = \left(\int_{\Omega} \frac{1}{\rho(z)}\left|u(z)\right|^2 dz\right)^{1/2},$$

де риска означає комплексне спряження.

Зазначимо, що для отримання обмеженого розв'язку у функціонал якості (5) додано стабілізуючий функціонал $\frac{1}{\varepsilon^2}\left\|u\right\|^2$ при деякому заданому $\varepsilon > 0$.

Таким чином, екстремальна задача полягає у визначенні комплекснозначного керування $u \in U$, для якого функціонал (5) досягає своєї нижньої грані.

Чисельні алгоритми для моделювання та формування акустичних полів. Для чисельного розв'язання диференціальної задачі

(1)–(4) введемо рівномірну сітку, враховуючи, що сіткова функція $y = y(r,z)$, яка апроксимує $p(r,z)$, має у вузлах $(r,\xi^{\pm})$ два значення $y^{\pm} = y(r_m,\xi \pm 0) = y(r_m,\xi^{\pm})$:

$$\overline{\omega}_{\tau h} = \overline{\omega}_{\tau} \times \overline{\omega}_{h} = \left\{(r,z), r \in \overline{\omega}_{\tau}, z \in \overline{\omega}_{h}\right\} \quad , \omega_h = \left\{z \in \overline{\omega}_h,\ z \neq 0, z \neq L\right\},$$

$$\overline{\omega}_{\tau} = \{r = r_m = r_0 + m\tau, m = 0,1,2,...,\},\ \omega_{\tau} = \{r = r_m \in \overline{\omega}_{\tau}, m \geq 1\},$$

$$\overline{\omega}_h = \{z = 0, h, ..., (n_1 - 1)h, \xi^-, \xi^+, (n_1+1)h, ..., L, h = \xi / n_1 = L / N\},$$

$$\omega_h = \left\{z \in \overline{\omega}_h,\ z \neq 0, z \neq L\right\}.$$

У гільбертовому просторі H_h комплекснозначних функцій, заданих на сітці $\overline{\omega}_h$, що приймають нульове значення в граничних вузлах і задовольняють різницеві умови спряження, визначимо скалярний добуток і норму за формулами

$$(\phi,\varphi) = (\phi,\varphi)_1 + (\phi,\varphi)_2 + \frac{h}{2}\phi(\xi^-)\overline{\varphi}(\xi^-) + \frac{h}{2}\phi(\xi^+)\overline{\varphi}(\xi^+), \|\phi\| = (\phi,\phi)^{1/2},$$

$$(\phi,\varphi)_1 = \sum_{k=1}^{n_1-1} h\phi_k\overline{\varphi}_k,\ (\phi,\varphi)_2 = \sum_{k=n_1+1}^{N-1} h\phi_k\overline{\varphi}_k.$$

Використовуючи інтегро-інтерполяційний метод та загальноприйняті позначення теорії різницевих схем [4, 5], задачі (1)–(4) поставимо у відповідність двошарову неявну різницеву схему в операторній формі

$$4ik_0\, By_r + A(\widehat{y} + y) + C(\widehat{y} + y) = 0,\ r \in \overline{\omega}_{\tau}, \tag{6}$$

$$y^0 \text{ задано,} \tag{7}$$

де y^0, $y \in H_h$, $y^0 = \left\{u(z), z \in \omega_h\right\}, y = y(r) = \left\{y(r,z), z \in \omega_h\right\}$, ..,

де E — тотожній оператор, $a(z), d(r,z)$ — коефіцієнти, а лінійний комплекснозначний оператор A діє у просторі H_h і визначається співвідношеннями

$$Ay = \begin{cases} (ay_{\bar{z}})_z,\ z \in \omega_h, z \neq \xi^{\pm}, \\ \dfrac{2}{h}\Big[\ \alpha(y^+ - y^-) - a(z)y_{\bar{z}}\ \Big], z = \xi^-, \\ \dfrac{2}{h}\Big[-\alpha(y^+ - y^-) + a(z)y_z\Big], z = \xi^+. \end{cases}$$

Поступаючи аналогічно [6], можна встановити єдиність та рівномірну стійкість різницевої схеми (6), (7) за початковими даними у нормі енергетичного простору комплекснозначних функцій H_B. Зокрема справедлива наступна теорема.

Теорема 1. Різницева схема (6), (7) рівномірно стійка за початковими даними у нормі H_B, і для її розв'язку має місце апріорна оцінка

$$\left\| y^m \right\|_B \le \left\| y^0 \right\|_B, \ m = 0,1,2,\dots .$$

З метою використання градієнтних методів оптимізації потрібно дослідити диференціальні властивості критерія якості (5). Покажемо, що функціонал (5) диференційовний у довільній точці $u(z) \in U$ в комплексному просторі зі скалярним добутком

$$< u, v > = \operatorname{Re}(u, v) . \qquad (8)$$

Для цього оцінимо головну лінійну частину приросту функціонала $\Delta J_\varepsilon(u) = J_\varepsilon(u+h) - J_\varepsilon(u)$ в залежності від приросту керування h. Враховуючи комплекснозначність керування $u \in U$ та використовуючи спряжену до (1)–(4) задачу, для випадку амплітудно-фазового керування можна встановити наступну теорему [7].

Теорема 2. Функціонал (5) диференційовний за Фреше у просторі $L_2^2(\Omega, 1/\rho)$ дійсних пар $\{ \operatorname{Re} u, \operatorname{Im} u \}$. Градієнт функціонала визначається виразом

$$J_\varepsilon'(u) = 2\left\{ \psi_1(r_0, z; u) + \frac{1}{\varepsilon^2} u_1, \psi_2(r_0, z; u) + \frac{1}{\varepsilon^2} u_2 \right\},$$

де $\psi = \psi_1 + i\psi_2$ — розв'язок спряженої задачі, $u = u_1(z) + iu_2(z)$.

Розв'язок задачі оптимального керування (1)–(5) можна отримати, використовуючи градієнтні методи [4], а також запропоновану для чисельного розв'язання прямої задачі (1)–(4) різницеву схему (6), (7). Зазначимо, що ця схема може бути використана і для чисельного розв'язання спряженої задачі.

Висновки. У статті запропоновано підхід для чисельного моделювання та формування акустичних полів у неоднорідних хвилеводах з умовами неідеального контакту на основі параболічного хвильового рівняння типу Шредінгера. Отримані результати можуть бути використані при розробці засобів математичного моделювання та формування акустичних полів для широкого кола задач амплітудно-фазового керування.

Список використаних джерел:

1. Тапперт Ф. Д. Метод параболического уравнения. *Распространение волн в подводной акустике*. М.: Мир, 1980. С. 180–226.
2. Завадский В. Ю. Моделирование волновых процессов. М.: Наука, 1991. 368 с.
3. Гладкий А. В., Сергиенко И. В., Скопецкий В. В. Численно-аналитические методы исследования волновых процессов. К.: Наук. думка, 2001. 452 с.
4. Самарский А. А., Вабищевич П. Н. Вычислительная теплопередача. М.: Едиториал УРСС, 2003. 784 с.

5. Самарский А. А., Вабищевич П. Н. Численные методы решения обратных задач математической физики. М.: Едиториал УРСС, 2004. 480 с.
6. Гладкий А. В. Исследование и оптимизация волновых процессов в неоднородных средах с импедансной границей. *Кибернетика и системный анализ*. 2013. № 2. С. 94–105.
7. Гладкий А. В., Гладкая Ю. А. Об одной задаче управления в средах с условиями неидеального сопряжения. *Компьютерная математика*. 2016. № 1. С. 3–9.

The problems of numerical modeling and formation of acoustic fields on the basis of parabolic wave equation in an inhomogeneous waveguide with subtle inclusions is considered. Criterion of optimality is formulated. Differential properties of the proposed quality functional are investigated. A numerical method for modelling and optimization of acoustic fields is proposed.

Key words: *acoustic field, Schrödinger-type equation, extremal problem, difference scheme, stability.*

Одержано 20.02.2017

УДК 004.728:004.728.3,004.056.055

І. Д. Горбенко, д-р. техн. наук, професор,
О. А. Замула, д-р. техн. наук

Харківський національний університет імені В. Н. Каразіна, м. Харків

МОДЕЛІ ТА МЕТОДИ СИНТЕЗУ КРИПТОГРАФІЧНИХ СИГНАЛІВ ТА ЇХ ОПТИМІЗАЦІЯ ЗА КРИТЕРІЄМ ЧАСОВОЇ СКЛАДНОСТІ

Сформульована в загальному вигляді і вирішена задача синтезу та аналізу криптографічних дискретних сигналів методом «гілок і меж», зроблені пропозиції з оптимізації.

Ключові слова: *складений сигнал, структурна та інформаційна скритності, імітостійкість.*

Вступ. Множинний доступ з кодовим поділом абонентів в багатокористувацьких телекомунікаційних системах (ТКС) здійснюється за допомогою використання при розширенні спектру специфічних дискретних послідовностей. При цьому властивості ТКС залежать від кореляційних, структурних, ансамблевих та енергетичних властивостей дискретних сигналів [1–3].

Метою цієї статі є викладення основних теоретичних та практичних положень та проблемних питань побудови дискретних послідовностей, що названі криптографічними дискретними сигналами (КДС), які повинні мати задані кореляційні, структурні та ансамблеві властивості, будуватися за допомогою ключових даних.

1. Моделі дискретних криптографічних сигналів. Під криптографічними дискретними сигналами (КДС) пропонується розуміти сукупності послідовностей (векторів) символів певного алфавіту, які обов'язково мають необхідні (задані) структурні, ансамблеві та кореляційні властивості, часову та просторову складності та можливості формування на основі ключів [1]. Правила побудови КДС грунтуються на використанні випадкових чи псевдовипадкові процесів, вони повинні відповідати вимогам випадковості, незворотності, непомітності та непередбачуваності [4–7].

Сформулюємо в загальному вигляді задачу синтезу КДС. Під задачею побудування (синтезу) КДС будемо розуміти задачу побудови підмножин дискретних послідовностей $(W_l^q), q=\overline{1,N}, l=\overline{1,L}$, сукупність яких утворює систему дискретних сигналів заданого алфавіту розмірності $M_k = N \times L$, таких, що в кожній із підмножин (словнику) виконуються умови, що висуваються до підмножини КДС в частині структурних, ансамблевих, кореляційних властивостей, просторової та часової складності їх генерування [1–3].

Побудова КДС грунтується на основі аналізу та використанні періодичних та аперіодичних функцій кореляції та зводиться до наступних етапів.

1. Забезпечення умов виконання вимог до структурних та ансамблевих властивостей, можливостей формування підмножини КДС з допустимою часовою та просторовою складністю, в тому числі з використанням ключів.
2. Побудова КДС W^q, періодична функція автокореляції (ПФАК) кожного з яких, задовольняє системі нелінійних параметричних нерівностей (НПН):

$$R_{a_1}^q(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R_{a_2}^q(l), \;\; l=\overline{1,L-1},\; q=\overline{1,N}, \tag{1}$$

де $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ — задані значення реалізації ПФАК, а індекси обчислюються по модулю $(i + l)$ mod$L$.

При $l = L$ для усіх $q=\overline{1,N}$ (1а) дає згортку зі значенням L

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N}. \tag{2}$$

3. Побудова пар КДС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН:

$$R_{b_{1,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l); \tag{3}$$

$$R^{qp}_{b_{1,2}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,2}}(l); \qquad (4)$$

$$R^{qp}_{b_{1,3}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,3}}(l); \qquad (5)$$

$$R^{qp}_{b_{1,4}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,4}}(l); \qquad (6)$$

$$R^{qp}_{b_{1,5}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,5}}(l)\,, \qquad (7)$$

причому $l = \overline{1, L-1}$ для будь-яких поєднань q і p, $q = \overline{1, N}$, $p = \overline{1, N}$, $q \ne p$, де $R^{qp}_{b_{1,j}}(l)$ і $R^{qp}_{b_{2,j}}(l)$, задані (необхідні) реалізації ПФВК і СФВК відповідно, $j = \overline{1,5}$, а також задовольняють вимогам до стикових функцій взаємної кореляції (СФВК) пар КДС W^q та W^p зі стиковими дискретними словами W^{qp} і W^{pq}.

В системах нелінійних параметричних нерівностей (1), (2) та (3)–(7) W_i^q та W_i^p є невідомими значеннями випадкових чи псевдовипадкових символів КДС W^q та W^p, $q = \overline{1, N}$, що належать визначенню в процесі їх побудови.

Проведемо аналіз систем нелінійних параметричних квадратичних нерівностей (далі систем) (1), (2) та (3)–(7), використовуючи введену модель.

Системи (4) та (6) при $l = L$ для усіх $q = \overline{1, N}$ мають дати повну згортку зі значенням L, тобто (4):

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q = \overline{1, N}, \qquad (8)$$

а (2d) дає

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^p = \sum_{i=1}^{L} W_i^p W_i^p = L, p = \overline{1, N}, \qquad (9)$$

Системи (3), (5) та (7) при $l = L$ для усіх пар W^q та W^p дають значення функції взаємної кореляції при нульовому значенні зсуву відповідно вигляду:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0); q, p = \overline{1, N}, \qquad (10)$$

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), q, p = \overline{1, N}, \qquad (11)$$

$$\sum_{i=1}^{L} W_i^{\,p} W_{i+L}^{\,q} = \sum_{i=1}^{L} W_i^{\,p} W_i^{q} = R^{pq}(0), p, q = \overline{1, N}\,. \qquad (12)$$

В подальшому системи (1), (2), (3)–(7) та квадратичне рівняння (10) будемо називати моделлю підмножини (словника) КДС.

Проведемо аналіз систем (1), (2) на предмет існування рішень та незалежності. Безпосередньо із (1) маємо, що щодо кожного із q КДС W^q є L невідомих — $W_1^{\,q}, W_2^{\,q} \cdots W_L^{\,q}$. Для їх знаходження згідно (1) можна скласти систему із $L-1$ незалежних НПН. Далі, використовуючи (2), отримуємо ще один вираз, але уже рівняння.

Особливістю системи (1), (2) є те, що вона дає згортку кожного із КДС зі значенням L. На основі (1) та (2) при побудові кожної N підмножини КДС можна скласти N незалежних систем квадратичних НПН, кожна з яких буде містити $L-1$ квадратичних нерівностей вигляду (1) і формально одне рівняння, так що всього їх буде L.

Також проведемо аналіз сукупності систем параметричних нерівностей (3)–(7), з урахуванням (8)–(12), на предмет існування рішень та незалежності систем та окремих рівнянь. Системи (3)–(7) визначають допустимі взаємнокореляційні властивості щодо ПФВК та СФВК кожної пари КДС — W^q та W^p. Вони визначають вимоги щодо ПФВК та СФВК конкретно тільки двох КДС — W^q та W^p. При побудові трьох КДС будемо мати 3!/2 систем вигляду (3)–(7), а при N КДС відповідно — N!/2 таких систем. Таким чином, з ростом N число систем вигляду (3)–(7) збільшується експоненційно (по факторіалу).

Для $N = 2$ серед (8)–(12) систем НПН є збиткові нелінійні квадратичні рівняння. Рівняння (2) збігається з (8) та (9), тому останні два уже входять у систему (2), є залежними, тому не можуть бути використані. Далі, рівняння (10) та (11) збігаються, а, рівняння (12) є симетричним в частині кореляційної функції щодо рівнянь (10) та (11). Тому для кожної пари p та q незалежним є (10).

На основі детального аналізу маємо, що усі (3)–(7) системи НПН визначають різні реалізації ПФВК та СФВК конкретно тільки двох КДС — W^q та W^p. Тому математична модель побудови двох КДС W^q та W^p однозначно визначається п’ятьма системами НПН у вигляді (3)–(7), та, як уже було обґрунтовано, рівнянням (10).

Наведені вище результати аналізу дозволяють визначити складність моделі та на її основі складність побудування підмножини із N КДС.

1. При побудові одного КДС необхідно, у залежності від допустимих значень $R_{a_1}^{q}(l)$ і $R_{a_2}^{q}(l)$, що визначаються межами щільної упаковки, розглянути $v \geq k$ систем вигляду (1), (2).

2. При побудові двох КДС необхідно розглянути $v_2 \geq K_2$ систем вигляду (3)–(7), де K_2 визначається $R_{b_{1,j}}^{qp}(l)$ та $R_{b_{2,j}}^{qp}(l)$.
3. При побудові N КДС необхідно розглянути $v_N \geq K_N$ систем вигляду (3)–(7), де K_N визначається $R_{a_1}^{q}(l)$ і $R_{a_2}^{q}(l)$ та $R_{b_{1,j}}^{qp}(l)$ і $R_{b_{2,j}}^{qp}(l)$ допустимими значеннями.

Таким чином, на основі врахування меж фізичної упаковки підмножини КДС [1] існують можливості побудови підмножин КДС згідно (1), (2) та (3)–(7).

У постановці, що наведена вище, можна формулювати та вирішувати в межах «щільної» упаковки і задачу побудови розмитих підмножин КДС. В певній мірі вона розглянута в [1, 2].

Аналогічно (1), (2) та (3)–(7) задається модель підмножини (словника) КДС через аперіодичні функції автокореляції (АФАК). В даному випадку можливі спрощення. Так систему (1), (2) по аналогії можна подати у вигляді системи НПН на основі аперіодичних функцій кореляції, тобто

$$r_{a_1}^{q}(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{a_2}^{q}(l)\,,\ l=\overline{1,L},\ \ m=\overline{1,L}, \tag{13}$$

де $r_{a_1}^{q}(l)$ і $r_{a_2}^{q}(l)$ — задані, але допустимі реалізації з точки зору щільної упаковки. Далі системи (1), (2) та (3)–(7) також можна подати через аперіодичні функції взаємної кореляції (АФВК) у вигляді системи нелінійних параметричних нерівностей

$$r_{b_{1,1}}^{qp}(l) \leq \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{b_{1,2}}^{qp}(l);\ \ l=\overline{1,L},\ \ m=\overline{1,L}, \tag{14}$$

$$r_{b_{2,1}}^{qp}(l) \leq \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \leq r_{b_{2,2}}^{pq}(l);\ \ l=\overline{1,L},\ \ m=\overline{1,L}, \tag{15}$$

де $r_{b_{1,1}}^{qp}, rr_{b_{1,1}}^{qp}, r_{b_{2,1}}^{qp}, r_{b_{2,2}}^{qp}$ допустимі з точки зору щільної упаковки АФАК та АФВК.

2. Розв'язання задачі побудови (синтезу) підмножин КДС. Побудова (синтез) підмножини КДС ґрунтується на застосуванні ключових даних та використанні випадкових чи псевдовипадкових дискретних послідовностей.

Дослідження показали [1, 2], що вказаний клас задач може розв'язуватись при застосуванні методу «гілок і меж», наприклад, зведений до таких етапів.

1. Формування випадкових чи псевдовипадкових дискретних послідовностей з використанням ключових даних.

2. Оцінка статистичних властивостей потенційних КДС [4, 8].
3. Побудова необхідного числа потенційних КДС W^q згідно системи (1) та ключових даних.
4. Знаходження пар чи підмножин КДС W^q та W^p, які задовольняють вимогам (3)–(7), застосовуючи метод «гілок та меж».
5. Побудова матриці станів взаємно-кореляційних функцій всіх можливих пар потенційних КДС, які пройшли відбір за результатами попереднього кроку та мають усі необхідні властивості.
6. Аналіз матриці станів та формування необхідного числа підмножин чи пар КДС згідно (1), (2) та (3)–(7) та відбір у підмножину лише тих, що задовольняють вимогам.

З урахуванням необхідності забезпечення криптографічної стійкості та структурної скритності пар чи підмножин КДС як джерело дискретних послідовностей застосовується алгоритм блокового симетричного перетворення ДСТУ 7624:2014, що є стійким у пост квантовий період.

У роботах [1, 2] наведено приклади пар та підмножин КДС.

3 Оптимізація методу синтезу криптографічних сигналів. В ході досліджень запропоновано вдосконалений метод побудування КДС, що заснований на використанні властивості та взаємного зв’язку АФАК та ПФАК, а також методу «великих» та «малих» кроків.

Перше прискорення грунтується на симетрії ПФАК [1, 2].

Вирішення задачі подальшої оптимізації грунтується на використанні методу «великих» та «малих» кроків (теорема 1 та наслідок теореми 1).

Теорема 1. Нехай максимальні (мінімальні) значення реалізацій функцій $Ra_1^1(l)$ і $Ra_2^1(l)$ в (1) є такими, що величина δ, визначена як

$$\delta = \left| Ra_1'(l) - Ra_1(l) \right| \text{ або } \delta = \left| Ra_2'(l) - Ra_2(l) \right|, \tag{16}$$

$\delta \neq 0,1,2,...P-1,P$ більше P, а W^j — сигнал, який визначений над полем $GF(P)$ або над кільцем чисел по модулю P, тоді безліч значень циклічної згортки (функції автокореляції (ФАК)) $Ra^Z(l)$ може належати інтервалу

$$(\min Ra_1(l), \max Ra_2(l)), \tag{17}$$

крайньою мірою, при «відкиданні» r останніх і «додаванні» r перших символів сигналу W, де $r = \dfrac{\delta}{P}$, якщо $\delta \mid P$ і $r = \dfrac{\delta + t}{P}$, якщо $\delta \neq P$.

Доведення теореми наведено в [1, 2].

Наслідок теореми 1. Якщо $W_i \in GF(P)$, то $r = \dfrac{\delta}{2}$, якщо δ парне і $r = \dfrac{\delta + 1}{2}$, якщо δ — не парне.

Аналіз результатів досліджень показав, що прискорення в побудуванні підмножин КДС з використанням запропонованих методів залежить від обмежень на кореляційні властивості, розмірів підмножин , довжин КДС та джерела КДС і розмірів ключів.

Висновки. В роботі сформульована в загальному вигляді і вирішена задача синтезу підмножин КДС, ансамблеві, кореляційні властивості яких можуть бути встановлені в залежності від вимог, що пред'являються до завадозахищеності та інформаційної безпеки ТКС.

Список використаних джерел:

1. Gorbenko I. D., Zamula A. A., Semenko Ye. A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications. *Telecommunications and Radio Engineering*. 2016. Vol. 75, Issue 2. P. 169–178.
2. Горбенко И. Д., Замула А. А. Криптографические сигналы: требования, методы синтеза, свойства, применение в телекоммуникационных системах. *Радиотехника: Всеукр. межвед. науч.-техн. сб.* Харьков: ХНУРЭ, 2016. Вып. 186. С. 7–24.
3. Замула А. А. Ансамбли дискретных сигналов с минимальными значениями боковых лепестков функций. *Системи обробки інформації*. Х.: ХУПС, 2015. Вип. 10 (135). С. 35–39.
4. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем: Монографія / За загальною редакцією Професора Горбенко Івана Дмитровича. Харків: Форт, 2015. 959 с.
5. Варакин Л. Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
6. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Введ. 01–07–2015. К.: Мінекономрозвитку України, 2015.
7. Sarvate D. V., Pursley M. V. Crosleration Properties of Pseudorandom and Related Sequences. *IEEE Trans. Commun*. 1980. Vol. 68. P. 59 -90.
8. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Formulated in general view and solved problem of synthesis nonlinear discrete complex cryptographic signals, by branch and bounds method, presented proposal for synthesis methods optimization.

Key words: *complex signal, structural and information secrecy, imitation resistance.*

Одержано 20.02.2017

УДК 519.272.2

А. М. Гупал, д-р физ.-мат. наук, член-кор. НАН Украины,
Н. А. Гупал, научный сотрудник
Институт кибернетики имени В. М. Глушкова НАН Украины, г. Киев

СИММЕТРИЯ В ДНК. СИММЕТРИЧНЫЙ КОД

Из симметрии в ДНК построен симметричный код относительно полярности аминокислот при мутациях в нуклеотидах. Исследована помехоустойчивость генетических кодов относительно полярности аминокислот. На основе баз данных генетических заболеваний показано, что симметричный код во многих случаях исправляет нарушение полярности при мутациях.

Ключевые слова: *генетический код, мутации, аминокислота, нуклеотид.*

Введение. Первые публикации по симметрии в ДНК относятся к 90-м годам XX в. после появления новой технологии секвенирования, которую использовали в проекте «Геном человека». В работах зарубежных авторов в виде эмпирических таблиц было показано, что в одной цепочке ДНК количество коротких последовательностей нуклеотидов примерно равно количеству обратно комплементарных последовательностей. В результате такого представления компьютерных расчетов в этих работах феномен симметрии не был объяснен.

ДНК имеет форму двойной спирали, информация записана в четырехбуквенном алфавите нуклеотидов (оснований) аденин (A), цитозин (C), гуанин (G), тимин (T). Известно, что C–G, A–T — комплементарные пары оснований, связывающие две цепи. Запись и считывание оснований у первой нити хромосомы ДНК в модели Уотсона-Крика выполняется слева направо, а у комплементарной второй нити — справа налево.

Симметриия оснований. Вычисления на компьютере получили, что количества оснований A и T, а также C и G, подсчитанные по одной нити ДНК, примерно совпадают и ошибка составляет сотые доли процента.

В работе [1] симметрия в ДНК представлена в виде математических формул, что значительно упрощает восприятие этого феномена, а также является основой построения математического аппарата для получения новых результатов.

Симметрия пар оснований. В результате расчетов получили, что для пар оснований выполняются соотношения в виде формулы

$$n(ij) = n(\overline{ji}\,), \tag{1}$$

где $i, j \in \{A, C, G, T\}$, $\overline{A} = T$, $\overline{C} = G$, $\overline{T} = A$, $\overline{G} = C$. Отметим, что пары AT, TA, CG и GC не присутствуют в (1), поскольку они приводят к тавтологии.

Формулы симметрии (1) определяют шесть дополнительных связывающих ограничений в записи генетической информации по одной нити ДНК, и поэтому они воспринимаются как совершенно необязательные требования. Возможно поэтому, феномен симметрии не изложен в учебниках и монографиях по биологии и биоинформатике.

Отметим, что длина участков генов составляет несколько тысяч нуклеотидов. Они расположены на двух нитях ДНК и для них симметрия также выполняется. Это означает, что оценки переходных вероятностей для однородных цепей Маркова, подсчитанные на двух противоположных нитях ДНК, совпадают. Поэтому для решения задач распознавания генов и белков можно использовать модели Маркова определенных порядков, в том числе и со скрытыми состояниями. При отсутствии симметрии применять такие модели было бы невозможно. Не удивительно, что модели Маркова рассматривают во многих работах, посвященных распознаванию аминокислотных и нуклеотидных последовательностей.

С помощью формул вида (1) выведено правило понижения симметрии: показано, что из симметрии последовательности оснований определенной длины вытекает симметрия для последовательностей, имеющих меньшую длину, вплоть до отдельных оснований.

Из условия Маркова, которое было сформулировано при анализе литературных текстов, следует правило повышения симметрии: из симметрии пар оснований вытекает симметрия коротких последовательностей оснований.

Отметим, что длина участков генов составляет несколько тысяч нуклеотидов. Они расположены на двух нитях ДНК и для них симметрия также выполняется. Это означает, что оценки переходных вероятностей для однородных цепей Маркова, подсчитанные на двух противоположных нитях ДНК, совпадают. Поэтому для решения задач распознавания генов и белков можно использовать модели Маркова определенных порядков, в том числе и со скрытыми состояниями. При отсутствии симметрии применять такие модели было бы невозможно. В зарубежных публикациях они составляют примерно половину статей в биоинформатике.

Легко видеть, что для коротких слов модель с одинаковой полярностью имеет больше связывающих ограничений, чем модель с противоположной полярностью нитей. Поэтому ДНК с противоположной полярностью нитей имеет больше степеней свободы, чем ДНК с одинаковой полярностью, т. е. с точки зрения теории информации модель Уотсона-Крика более эффективна.

Серьезный аргумент в пользу феномена симметрии — исследование устойчивости стандартного генетического кода при случайных мутациях нуклеотидов в кодоне.

Стандартный генетический код, согласно которому в живых организмах происходит синтез белков на основе информации, содержащейся в ДНК, был открыт в 60-х годах XX в. Одним из основных факторов, которые могли влиять на эволюцию кода, являлось повышение его устойчивости по отношению к мутациям — искажениям генетической информации, возникающим в клетках любого организма. Мутации проистекают из-за ошибок в репликации в ДНК, или разрушительных воздействий мутагенов, таких как химические агенты и радиация, которые реагируют с ДНК и изменяют структуру отдельных нуклеотидов (оснований).

Аминокислоты различаются по взаимодействию с молекулами воды. Неполярные аминокислоты более гидрофобны, они отталкивают молекулы воды и слипаются друг с другом. Полярные аминокислоты гидрофильны и взаимодействуют с водой, в результате чего образуется сложная форма, которая соответствует выполняемой белком функции. Если при мутации полярный остаток в белке сменится на неполярный (или наоборот), то форма молекулы может измениться настолько, что белок не сможет выполнять свою функцию.

Стандартный генетический код сопоставляет каждой тройке нуклеотидов одну из двадцати аминокислот. Помехоустойчивость такого кода при точечных мутациях в нуклеотидах относительно полярности аминокислот составляет 69,20 %.

С помощью восьми парных перестановок построен симметричный код в табл. с помехоустойчивостью 77,86 %, в котором кодон и антикодон определяют аминокислоты с разной полярностью.

В стандартном коде в клетке C первой строки содержатся четыре полярные аминокислоты серин; а в клетке G — цистеин, цистеин, стоп и триптофан; в клетке C третьей строки содержатся четыре полярные аминокислоты треонин; а в клетке G четвертой строки — четыре неполярные аминокислоты глицин.

Стандартный код в таком смысле на 3/4 соответствует симметричному коду. Симметричный код оптимален, поскольку не существует способов повышения его помехоустойчивости, сохраняя при этом характеристики стандартного кода [2, 3].

В таблице неполярные аминокислоты выделены жирным шрифтом. Первые два столбца построенного кода содержат неполярные аминокислоты, третий и четвертый — полярные аминокислоты.

Таблица

Симметричный код

Первое осно-вание	Второе основание				Третье осно-вание
	T	C	A	G	
T	фенилаланин фенилаланин лейцин лейцин	стоп триптофан цистеин цистеин	тирозин тирозин стоп стоп	серин серин серин серин	T C A G
C	лейцин лейцин лейцин лейцин	пролин пролин пролин пролин	гистидин гистидин глутамин глутамин	аргинин аргинин аргинин аргинин	T C A G
A	изолейцин изолейцин изолейцин метионин	глицин глицин глицин глицин	аспарагин аспарагин лизин лизин	серин серин аргинин аргинин	T C A G
G	валин валин валин валин	аланин аланин аланин аланин	асп. к-та асп. к-та глут. к-та глут. к-та	треонин треонин треонин треонин	T C A G

Компьютерные расчеты получили, что помехоустойчивость кода — важный фактор для эволюции кода: устойчивость к помехам стандартного кода значительно выше, чем у случайных кодов, что свидетельствует о неслучайном выборе стандартного кода.

На основе баз данных генетических заболеваний стандартным кодом было проверено триста мутаций для различных типов заболеваний. Примерно половина из них привела к нарушению полярности или к мутациям третьего нуклеотида. Симметричный код в 80 % случаев исправил нарушение полярности при мутациях кодона. Рассмотрено два варианта несимметричных кодов, помехоустойчивость которых такая же, как у симметричного оптимального кода. Однако эти коды дали плохие результаты по сравнению со стандартным кодом.

Выводы. Таким образом, показано, что помехоустойчивость кода имеет большое влияние на нарушение полярности аминокислот при точечных мутациях нуклеотидов.

Список использованной литературы:

1. Гупал А. М., Гупал Н. А., Островский А.В. Симметрия и свойства записи генетической информации в ДНК. *Проблемы управления и информатики*. 2011. № 3. С. 120–127.
2. Сергиенко И. В., Гупал А. М., Вагис А. А. Симметричный код и генетические мутации. *Кибернетика и системный анализ*. 2016. № 2. С. 73–80.

3. Гупал А. М., Сергиенко И. В. Симметрия в ДНК. Методы распознавания дискретных последовательностей. К.: Наукова думка, 2016. 228 с.

The symmetric code concerning polarity of amino acids at mutations in nucleotides is constructed of symmetry in DNA. The noise immunity of genetic code against polarity is analyzed. On the basis of databases of genetic diseases it is shown that the symmetric code in most cases corrects violation of polarity at mutations.

Key words: *genetic code, mutations, amino acid, nucleotide.*

Получено 9.03.2017

УДК 517.988

С. В. Денисов, ассистент,
В. В. Семёнов, д-р физ.-мат. наук, профессор

Киевский национальный университет имени Т. Шевченко, г. Киев

МОДИФИЦИРОВАННЫЙ ЭКСТРАГРАДИЕНТНЫЙ МЕТОД ДЛЯ ВАРИАЦИОННЫХ НЕРАВЕНСТВ

Предложен модифицированный экстраградиентный метод с динамической регулировкой величины шага для решения вариационных неравенств с монотонными операторами, действующими в гильбертовом пространстве. Доказана слабая сходимость метода без предположения о липшицевости операторов.

Ключевые слова: *вариационное неравенство, монотонный оператор, экстраградиентный метод, слабая сходимость.*

Введение. Многие задачи исследования операций и математической физики могут быть записаны в форме вариационных неравенств вида:

$$\text{найти } x \in C : \left(Ax, y - x \right) \geq 0 \quad \forall y \in C,$$

где C — непустое выпуклое подмножество гильбертового пространства H, A — монотонный оператор, действующий в H [1, 2]. Решение вариационных неравенств является активно развивающимся направлением прикладного нелинейного анализа. К настоящему времени предложено большое количество методов, в частности, методов проекционного типа (использующих операцию метрического проектирования на допустимое множество C).

Известно, что в случае неоптимизационных постановок (поиск седловой точки или равновесия Нэша) для сходимости наиболее простого проекционного метода (аналога метода проекции градиента) необходимо выполнение усиленных условий монотонности.

Для преодоления этой трудности существует несколько подходов. Один из них состоит в регуляризации исходной задачи с целью придать ей требуемое свойство [3]. Сходимость без модификации задачи обеспечивается в итерационных методах экстраградиентного типа, впервые предложенных Г. М. Корпелевич [4]. Экстраградиентный алгоритм Корпелевич для липшицевого оператора A имеет вид:

$$\begin{cases} x_0 \in C, \\ y_n = P_C\left(x_n - \lambda A x_n\right), \\ x_{n+1} = P_C\left(x_n - \lambda A y_n\right), \end{cases}$$

где $\lambda \in \left(0, 1/L\right)$ — постоянная Липшица оператора A, P_C — оператор метрического проектирования на множество C. Обобщению и исследованию этого алгоритма посвящено большое количество публикаций.

Недавно для вариационных неравенств и задач равновесного программирования были предложены модификации алгоритма Корпелевич с одним метрическим проектированием на допустимое множество [5, 6]. В этих, так называемых, субградиентных экстраградиентных алгоритмах первый этап итерации совпадает с первым этапом итерации в алгоритме Корпелевич, а далее для получения x_{n+1} вместо проектирования точки $x_n - \lambda A y_n$ на допустимое множество C, точку $x_n - \lambda A y_n$ проектируют на некоторое опорное для C полупространство. Субградиентный экстраградиентный алгоритм имеет вид:

$$\begin{cases} x_0 \in H, \\ y_n = P_C\left(x_n - \lambda A x_n\right), \\ T_n = \left\{z \in H : \left(x_n - \lambda A x_n - y_n, z - y_n\right) \le 0\right\}, \\ x_{n+1} = P_{T_n}\left(x_n - \lambda A y_n\right), \end{cases}$$

где $\lambda \in \left(0, 1/L\right)$ — постоянная Липшица оператора A. В работах [5, 6] доказана слабая сходимость порожденных этим алгоритмом последовательностей $\left(x_n\right)$ и $\left(y_n\right)$ к некоторому решению вариационного неравенства.

Очевидным недостатком субградиентного экстраградиентного алгоритма, затрудняющим его широкое использование, является предположение о том, что константа Липшица L оператора A известна или допускает простую оценку. Кроме того, во многих задачах операторы могут не удовлетворять условию Липшица. Заметим, что в большинстве работ по алгоритмам решения вариационных неравенств рассматриваются именно липшицевые операторы.

В данной работе предлагается модификация субградиентного экстраградиентного алгоритма с динамической регулировкой величины шага для вариационных неравенств с монотонным нелипшицевым оператором и доказыватся его сходимость.

Исследование выполнено при поддержке МОН Украины (проект «Розробка алгоритмів моделювання та оптимізації динамічних систем для оборони, медицини та екології», 0116U004777).

Постановка задачи и вспомогательные сведения. Всюду далее H — действительное гильбертово пространство со скалярным произведением $(\cdot,\cdot)$ и порожденной нормой $\|\cdot\|$. Пусть C — непустое подмножество пространства H, A — оператор, действующий в H. Будем рассматривать вариационное неравенство:

$$\text{найти } x \in C : \left(Ax, y-x\right) \geq 0 \quad \forall y \in C . \tag{1}$$

Множество решений вариационного неравенства (1) обозначим $VI\left(A,C\right)$. Будем предполагать выполненными следующие условия: множество $C \subseteq H$ — выпуклое и замкнутое; оператор $A: H \to H$ — монотонный, равномерно непрерывный на ограниченных множествах и отображающий ограниченные множества в ограниченные; $VI\left(A,C\right) \neq \varnothing$. Пусть P_C — оператор метрического проектирования на множество C, то есть $P_C x$ — единственный элемент множества C со свойством

$$\left\|P_C x - x\right\| = \min_{z \in C} \left\|z - x\right\| .$$

Рассмотрим функцию $t \mapsto \left\|x - P_C\left(x - tAx\right)\right\|$, ... Она обладает следующим полезным свойством.

Лемма 1. Для $x \in H$ и $\alpha \geq \beta > 0$ имеют место неравенства

$$\frac{\left\|x - P_C\left(x - \alpha Ax\right)\right\|}{\alpha} \leq \frac{\left\|x - P_C\left(x - \beta Ax\right)\right\|}{\beta} ,$$

$$\left\|x - P_C\left(x - \beta Ax\right)\right\| \leq \left\|x - P_C\left(x - \alpha Ax\right)\right\| .$$

Модифицированный экстраградиентный алгоритм. Для решения неравенства (1) предлагаем следующий итерационный алгоритм.

Алгоритм 1.

Инициализация.

Задаем числовые параметры $\sigma > 0$, $\tau \in \left(0,1\right)$, $\theta \in \left(0,1\right)$ и элемент $x_0 \in H$.

Итерационный шаг.

Для $x_n \in H$ вычисляем

$$y_n = P_C\left(x_n - \lambda_n A x_n\right),$$

где λ_n получаем из условия

$$\begin{cases} j(n) = \min\left\{ j \ge 0 :\ \sigma\tau^j \left\| AP_C\left(x_n - \sigma\tau^j Ax_n\right) - Ax_n \right\| \le \theta \left\| P_C\left(x_n - \sigma\tau^j Ax_n\right) - x_n \right\| \right\}, \\ \lambda_n = \sigma\tau^{j(n)}. \end{cases}$$

Если $y_n = x_n$, то заканчиваем, иначе вычисляем

$$x_{n+1} = P_{T_n}\left(x_n - \lambda_n A y_n\right),$$

где

$$T_n = \left\{ z \in H : \left(x_n - \lambda_n A x_n - y_n, z - y_n\right) \le 0 \right\}.$$

Имеет место.

Лемма 2. Правило выбора параметра λ_n корректно, то есть

$$j(n) < +\infty.$$

Слабая сходимость алгоритма 1. Имеет место важное неравенство.

Лемма 3. Для последовательностей (x_n), (y_n), порожденных алгоритмом, имеет место неравенство

$$\left\|x_{n+1} - z\right\|^2 \le \left\|x_n - z\right\|^2 - \left(1 - \theta^2\right)\left\|x_n - y_n\right\|^2,$$

где $z \in VI(A, C)$.

Из леммы 3 следует фейеровское свойство последовательности (x_n) относительно множества $VI(A, C)$. Это позволяет получить следующий результат относительно сходимости предлагаемого итерационного алгоритма.

Теорема 1. Последовательности (x_n) и (y_n), порожденные алгоритмом 1, слабо сходятся к некоторой точке $z \in VI(A, C)$.

Выводы. Предложен модифицированный экстраградиентный метод с динамической регулировкой величины шага для решения вариационных неравенств с монотонными операторами, действующими в гильбертовом пространстве. Относительно операторов не предполагается их липшицевость. Основной теоретический результат — теорема о слабой сходимости методов. Сильно сходящийся вариант предложенного метода можно получить, используя метод итеративной регуляризации [3, 7] или гибридный метод из [8, 9].

Список использованной литературы:

1. Киндерлерер Д., Стампаккья Г. Введение в вариационные неравенства и их приложения. М.: Мир, 1983. 256 с.

2. Nagurney A. Network economics: A variational inequality approach. Dordrecht: Kluwer Academic Publishers, 1999. 325 p.
3. Бакушинский А. Б., Гончарский А. В. Некорректные задачи. Численные методы и приложения. М.: Изд-во МГУ, 1989. 200 с.
4. Корпелевич Г. М. Экстраградиентный метод для отыскания седловых точек и других задач. *Экономика и математические методы*. 1976. Т. 12, № 4. С. 747–756.
5. Censor Y., Gibali A., Reich S. The subgradient extragradient method for solving variational inequalities in Hilbert space. *Journal of Optimization Theory and Applications*. 2011. Vol. 148. P. 318–335.
6. Ляшко С. И., Семенов В. В., Войтова Т. А. Экономичная модификация метода Корпелевич для монотонных задач о равновесии. *Кибернетика и системный анализ*. 2011. № 4. С. 146–154.
7. Апостол Р. Я., Гриненко А. А., Семенов В. В. Ітераційні алгоритми для монотонних дворівневих варіаційних нерівностей. *Журнал обчислювальної та прикладної математики*. 2012. № 1 (107). С. 3–14.
8. Семенов В. В. Гибридные методы расщепления для системы операторных включений с монотонными операторами. *Кибернетика и системный анализ*. 2014. № 5. С. 104–112.
9. Nakajo K., Takahashi W. Strong convergence theorems for nonexpansive mappings and nonexpansive semigroups. *J. Math. Anal. Appl.* 2003. 279. P. 372–379.

We present a modified extragradient method with dynamic rule for finding the stepsize for solving variational inequalities with monotone operators acting in a Hilbert space. We establish weak convergence of method without any Lipschitzian continuity assumption on operators.

Key words: *variational inequality, monotone operator, extra-gradient method, weak convergence.*

Получено 05.03.2017

УДК 519.6

В. В. Драгун, аспірант

Українська інженерно-педагогічна академія, м. Харків

МЕТОД ЗНАХОДЖЕННЯ РОЗПОДІЛУ ПОВІЛЬНОСТІ В ШАХТНІЙ СЕЙСМІЧНІЙ ТОМОГРАФІЇ ДЛЯ ВИПАДКУ РОЗРИВНОГО ПЛАСТА

У статті запропоновано знаходити розподіл повільності в шахтній сейсмічній томографії за допомогою перших часів прибуття сейсмічного сигналу від системи джерел до системи приймачів розміщених на горизонтальній площині, яка має розрив першого роду. Цей розподіл повільності на площині отримуються за допомогою обчислення значення суми Фур'є, коефіцієнти якої обчислюють за допомогою проекцій вздовж деякої системи ліній, що лежать на цій горизонтальній площині.

Ключові слова: *шахтна сейсмічна томографія, коефіцієнти сум Фур'є.*

Вступ. Сейсмічна томографія — один з актуальних напрямків сучасної геофізики, ґрунтується на побудові зображень об'єкта за допомогою дослідження траєкторій розповсюдження сейсмічних сигналів.

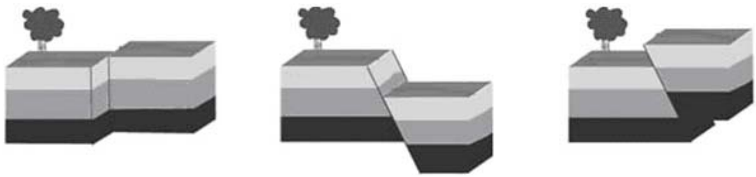
Сутність методів шахтних сейсморозвідувальних робіт в цілому полягає у збудженні і реєстрації пружних коливань в межах вугільного пласта, виділенні і аналізі динамічних і кінематичних параметрів хвиль різних типів, і відновленні внутрішньої структури пласта за цими параметрами.

Дана робота присвячена узагальненню результатів роботи [1] на більш реальний випадок, коли на досліджуваній горизонтальній площині є розрив пласта. Результатом роботи є побудова математичної моделі, опису повільності розповсюдження сейсмічних хвиль на основі відомих перших часів прибуття сейсмічного сигналу в точки спостереження. При цьому використовується метод описаний в роботах [1–3] для обчислення функції $f(x, y)$ — повільності розповсюдження сейсмічної хвилі за допомогою проекцій, у певній площині, вздовж деякої системи ліній, що перетинають об'єкт дослідження. Важливою особливістю вказаного методу є заміна тригонометричних функцій кусково-сталими сплайнами найкращого рівномірного наближення, що дозволяє знаходити коефіцієнти Фур'є не через значення функції $f(x, y)$ (які нам невідомі), а через інтеграли від цих функцій вздовж вибраної системи прямих, які можна обчислити за допомогою перших часів прибуття сейсмічного сигналу в точку спостереження.

Як відомо, дані сейсмічного зондування лежать в основі методів шахтної сейсмічної томографії при відновленні внутрішньої структури кори в досліджуваній області.

1. Огляд робіт. У роботі О. М. Литвина [2] запропоновано і досліджено новий метод розв’язання плоскої задачі радонівської комп’ютерної томографії. В основі методу лежать оригінальні формули обчислення коефіцієнтів Фур’є функцій двох змінних за допомогою проекцій (даних Радона) — інтегралів від наближуваної функції вздовж деякої системи ліній, що перетинають об’єкт дослідження. Однією з важливих особливостей вказаного методу є заміна тригонометричних функцій кусково-сталими сплайнами найкращого рівномірного наближення.

В роботах авторів [1, 4] досліджувався метод побудови просторової моделі пласта в шахтній сейсмічній томографії для випадку, якщо експериментальні даними, які використовуються, для побудови математичної моделі, є перші часи прибуття сейсмічного сигналу від системи джерел до системи приймачів розміщених в одній і тій же площині, або на системі горизонтальних площин. Просторовий розподіл використовував припущення, що в заданій площині (або в заданих площинах) пласт, зокрема вугільний, не має розривів. Це припущення дозволяло пропонувати для побудови математичної моделі ряди Фур’є, із спеціальним методом обчислення коефіцієнтів Фур’є, який використовує тільки вказані експериментальні дані. На практиці не рідко зустрічаються випадки, коли пласт має тектонічні порушення. В природі відомі 3 типи геологічних розломів: скиди, підкиди (насуви) та зсуви (рис. 1).



а *б* *в*

Рис. 1. *Види геологічних розломів: а — зсуви; б — скиди; в — підкиди (насуви)*

В цій статті вважаємо, що ми досліджуємо пласт корисних копалин, який піддався дії підкиду і тепер на досліджуваній горизонтальній площині має розрив. Підкид міг утворитися нахилом зміщувача в бік піднятого крила або переміщенням висячого крила вгору [5]. Така ситуація могла виникнути у випадку зштовхування тектонічних плит, які спричинили процес горизонтального стиснення.

2. Використання сум Фейера та Валле-Пуссена для підвищення достовірності результатів при візуалізації інформації. В даній статті, задача відновлення розподілу повільності в шахтній сейсмічній томографії горизонтальній площині полягає у відновленні функції за відомими проекційними даними — інтегралів вздовж ліній паралельних прямим $kx + ly = t$ які перетинають досліджуваний об'єкт.

Для вирішення задачі знаходження розподілу повільності в шахтній сейсмічній томографії, будемо використовувати метод запропонований у роботі [1]. Відповідно до цього методу, вирішення задачі може бути отримане у вигляді суми Фур'є:

$$F\left(x,y\right)=\sum_{k=-N}^{N}\sum_{l=-N}^{N}F_{k,l}e^{i2\pi\left(kx+ly\right)},$$

де $F_{kl}=\int_0^1\int_0^1 f(x,y)e^{-i2\pi(kx+ly)}dxdy$ — коефіцієнти Фур'є невідомої функції $f(x, y)$, що описує структуру тіла, яку пропонується обчислювати за допомогою часів пробігу сейсмічних хвиль від системи джерел до системи приймачів. У роботах [2, 3] наведені формули для їх обчислення, які використовуються в даній роботі для випадку, коли невідома функція $f(x, y)$ є повільністю $W(x,y)=1/V(x,y)$ і нам відомі лише часи прибуття.

Особливістю і перевагою розробленого методу є явні формули для наближеного обчислення коефіцієнтів Фур'є функції двох змінних часів пробігу сейсмічних хвиль від системи джерел до системи приймачів. Це звело рішення задачі до задачі обчислення коефіцієнтів Фур'є. Вибір системи прямих, уздовж яких задаються проекційні дані, а отже, і від інтегралів, і від формул для їх обчислення, обумовлений значеннями індексів k і l в сумі Фур'є.

Необхідно зазначити, що якщо функція $f(x, y)$ має розриви, то метод дозволяє використовувати також скінчену суму Фейєра у вигляді

$$S\left(x,y,N\right)=\sum_{k=-N}^{N}\sum_{l=-N}^{N}\left(1-\frac{|k|}{N+1}\right)\left(1-\frac{|l|}{N+1}\right)F_{k,l}e^{i2\pi\left(kx+ly\right)},$$

що обумовлено впливом явища Гіббса на результати дослідження. Як відомо, використання сум Фур'є, внаслідок явища Гіббса, не дозволяє отримати достовірні результати при візуалізації інформації за допомогою розривних функцій навіть тоді, коли коефіцієнти Фур'є обчислені точно. Ще однією перевагою сум Фейера в порівнянні з сумами Фур'є є те, що ядро суми Фейера є завжди позитивним і умови збіжності виписуються простіше.

Ще один важливий негативний факт стосовно сум Фур'є описаний у теоремі дю-Буа Реймонда [6, с. 152]. Існує неперервна і періодична функція $f(x)$, ряд Фур'є якої розбігається принаймні в одній точці. Водночас, як суми Фейера та Валле-Пуссена рівномірно збігаються до $f(x)$, якою б не була неперервною і періодичною функція $f(x)$ [6, с. 152].

Описаний у роботах [1–4] метод дозволяє використовувати також мішаний оператор Валле-Пуссена у вигляді

$$BV_{m,n,p,q}f\left(x,y\right)=V_{1,m,p}f\left(x,y\right)+V_{2,n,q}f\left(x,y\right)-V_{1,m,p}f\left(x,y\right)\cdot V_{2,n,q}f\left(x,y\right),$$

$$V_{1,m,p} f(x,y) = \frac{1}{p+1} \sum_{k=m-p}^{m} F_{1,k}(f;x),$$

$$V_{2,n,q} f(x,y) = \frac{1}{p+1} \sum_{l=n-q}^{n} F_{2,l}(f;y),$$

$$F_{1,m}(f;x) = \sum_{\mu=-m}^{m} a_{1,\mu}(f;y) \cdot e^{i\cdot\mu\cdot x},$$

$$a_{1,\mu}(f;y) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \left(f(x,y) e^{-i\cdot\mu\cdot x} \right) dx,$$

$$F_{2,n}(f;y) = \sum_{\nu=-n}^{n} a_{2,\nu}(f;x) \cdot e^{i\cdot\nu\cdot y}, \quad a_{2,\nu}(f;x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \left(f(x,y) e^{-i\cdot\nu\cdot y} \right) dy,$$

$$\mu = 0, \pm 1, \pm 2, ..., \pm m, \quad \nu = 0, \pm 1, \pm 2, ..., \pm n.$$

3. Наближення сумами Фур'є функцій двох змінних для визначення просторового розподілу повільності на основі першого наближення в шахтній сейсмічній томографії на основі методу описаного в [1–3]. В реальних умовах в шахтній сейсмічній томографії, на відміну від комп'ютерної томографії, промені лише в окремих випадках є прямими лініями, що обмежує використання методу описаного в роботах [2, 3]. В роботі [7, с. 37–38] написано, що при більш точному наближенні можна розглянути нев'язку часів прибуття променя

$$\delta T(p,\varphi) = \int_{L} \delta u(x) ds, \tag{2}$$

де $T = T_0 + \delta T$ і $u = u_0 + \delta u$. Опорні часи пробігу $T_0(p,\varphi) = \int_{L_0} \delta u_0(x) ds$ обчислюються для променів, відповідних повільності опорної моделі $u_0(x)$, і при інтерпретації нев'язок (2) промені вважаються прямолінійними, тобто можна використовувати метод, описаний у роботах [2, 3], в якому для обчислення коефіцієнтів Фур'є функції від двох змінних використані явні формули, для підстановки в них значень базових проекцій, аналог кубатурної формули, на той випадок коли експериментальні дані про функцію $f(x, y)$ задаються не значеннями, а проекціями вздовж заданої системи прямих.

Проведемо обчислювальний експеримент по наближеному обчисленню значень розподілу повільності на ділянці дослідження, яка має розрив першого роду. Вважаємо, що нам задані наближено знайдені розподіли повільності $f(x, y)$ на ділянці $[0, 1]^2$.

При підраховуванні сум коефіцієнтів Фур'є ми скористаємося сумами Фейера, оскільки вони мають кращу збіжність ніж суми Фур'є, а також мають похибку у два рази меншу ніж суми Валле-Пуссена [8, с. 72].

Приклад 1. Нехай нам задані розподіли повільності на досліджуваній площині $f(x, y)$.

$$f\left(x,y\right)=\begin{cases}0,54, \text{ якщо } x^2+\dfrac{y^2}{2}>0,36\cup\dfrac{x^2}{3}+y^2\le 1,\\ 0,45 \text{ інакше}.\end{cases}$$

Вхідні дані та отриманий результат, для значення N=8 (порядок суми Фур'є) і кількості джерел та приймачів по 10 на кожній зі сторін, див. рис. 2.

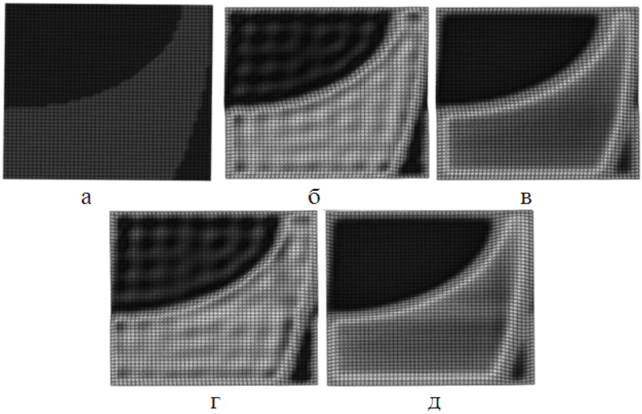


Рис. 2. *Вхідні дані та отриманий результат тестової задачі: а — вхідні дані; б — результати обчислень за допомогою сум Фур'є; в — результати обчислень за допомогою сум Фейера; г — результати обчислень методом в [1–3] та сумою Фур'є; д — результати обчислень методом в [1–3] та сумою Фейера*

Результати розв'язку задачі, для різного порядку суми Фур'є (N), представлені у таблиці.

Таблиця

Результати розв'язку прикладу 1 для різних N

Порядок суми Фур'є	Кількість джерел та приймачів	Похибка значень, обчислених за допомогою точних значень коефіцієнтів Фур'є				Похибка значень, обчислених методом в [1–3]			
		сумою Фур'є		сумою Фейера		сумою Фур'є		сумою Фейера	
		абсолютна похибка	відносна похибка	абсолютна похибка	відносна похибка	абсолютна похибка	відносна похибка	абсолютна похибка	відносна похибка
4	10, 10	0,064	0,118	0,057	0,127	0,063	0,117	0,057	0,128
4	20, 20	0,064	0,118	0,057	0,127	0,063	0,117	0,057	0,126
8	10, 10	0,055	0,106	0,053	0,112	0,056	0,121	0,053	0,117
8	20, 20	0,055	0,106	0,053	0,112	0,055	0,103	0,053	0,11

Висновки. Таким чином, запропонований підхід може розглядатися для покращення значень математичної моделі для знаходження розподілу повільності розповсюдження сейсмічних хвиль у заданій області кори Землі, у випадку коли досліджувана ділянка має розрив першого роду. При цьому інформація, яка використовувалася для наближеного обчислення вказаних коефіцієнтів сум Фейера, являє собою перші часи прибуття сейсмічного сигналу в точки спостережень від джерел сейсмічного сигналу, які пропонується наближено знаходити скориставшись твердженнями робіт [2, 3].

Список використаних джерел:

1. Литвин О. М., Драгун В. В. Метод знаходження першого наближення для розв'язання задачі шахтної сейсмічної томографії в неоднорідному середовищі. *Управляющие системы и машины*. 2016. № 3.
2. Литвин О. М. Періодичні сплайни і новий метод розв'язання плоскої задачі рентгенівської комп'ютерної . *Системний аналіз, управління і інформаційні технології*: Вісник Харківського держ. політех. ун-ту. Збірка наукових праць. Харків: ХДПУ, 2000. № 125. С. 27–35.
3. Кулик С. І. Математичне моделювання в комп'ютерній томографії з використанням вейвлетів : дис. канд. фіз.-мат. наук: «Математичне моделювання та обчислювальні методи». Харків, 2008. 192 с.
4. Литвин О. М., Драгун В. В. Метод знаходження просторового розподілу повільності на основі першого наближення в шахтній сейсмічній томографії. *Управляющие системы и машины*. Прийнято до друку.
5. Розломи [Електронний ресурс]. 2016. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Розломи.
6. Коровкин П. П. Линейные операторы и теория приближений. М.: Гос. издательство физ.-мат. литературы, 1959. 211 с.
7. Чепмен К. Преобразование Радона и сейсмическая томография. *Сейсмическая томография*. Под ред. Г. Нолетта. М.: Мир, 1990. С. 34–60.
8. Литвин О. М. Інтерлінація функцій та деякі її застосування. Харків: Основа, 2002. 544 с.

In the article suggested finding the spatial distribution of the slowness in the mine seismic tomography by using first arrival times of the seismic signal from the sources system into the receivers system located on discontinuous horizontal plane. These slowness distributions in horizontal plane are obtained by calculating the values of the Fourier sums whose coefficients are calculated using the projection system along a certain line, located in this horizontal plane.

Key words: *mine seismic tomography, the coefficients of Fourier sums.*

Одержано 16.02.2017

УДК 519.8

Н. Г. Журбенко, канд. физ.-мат. наук

Институт кибернетики имени В. М. Глушкова НАН Украины, г. Киев

ОБ ОДНОМ СЕМЕЙСТВЕ МОДИФИКАЦИЙ *R*-АЛГОРИТМА

Рассматривается семейство модификаций *r*-алгоритма — субградиентного алгоритма с преобразованием пространства. В отличие от *r*-алгоритма в предлагаемых модификациях значения коэффициентов растяжения пространства вычисляются в процессе работы алгоритма. Алгоритмы могут использоваться с постоянным шаговым множителем. Приводится результат исследования численной эффективности одного алгоритма рассматриваемого семейства.

Ключевые слова: *негладкая оптимизация, субградиент, преобразование пространства, численная эффективность.*

Введение. Более 40 лет назад был разработан субградиентный алгоритм минимизации с растяжением пространства в направлении разности двух последовательных градиентов — *r*-алгоритм [1]. Практика использования *r*-алгоритма показывает, что до настоящего времени он является одним из наиболее эффективных алгоритмов негладкой оптимизации. Однако теоретическое исследование эффективности алгоритма далеко не закончено. Основная проблема теоретического обоснования *r*-алгоритм состоит в согласованном выборе значений коэффициента растяжения пространства и шагового множителя. В работе приводится описание семейства модификаций *r*-алгоритма — $r(\sigma)$-алгоритмы. Величины коэффициентов растяжения пространства на итерациях $r(\sigma)$-алгоритмов не постоянны, они вычисляются в процессе его работы. Алгоритмы не требуют использования процедуры одномерного спуска по направлению.

Численная схема r-алгоритма. Рассматривается задача безусловной минимизации субдифференцируемой функции $f(x)$ в R^n. Будем обозначать $\partial f(x)$ множество субградиентов функции $f(x)$ в точке x.

В r-алгоритме используется оператор растяжения пространства [2] $R(\eta) = (\alpha - 1)\eta\eta^T + I$, где $\eta \in R^n$. α — направление и коэффициент растяжения пространства, $|\eta| = 1$, $\alpha \geq 0$. Вычислительная схема r-алгоритма применительно к задаче отыскания безусловного минимума функции $f(x)$ состоит в следующем.

0-ый шаг алгоритма (инициализация). Выбираем начальное приближение x_0 и невырожденное линейное преобразование B_0. Вычисляем: $g(x_0) \in \partial f(x_0)$; $g_0^* = B_0^* g(x_0)$ (субградиент в преобразованном пространстве $Y_0 = B_0^{-1} X \equiv A_0 X$, X — исходное пространство). Пусть на шаге k алгоритма ($k = 0,1,2,\ldots$) получены определенные значения векторов x_k, g_k^* (субградиент в преобразованном пространстве) и матрицы B_k. ($A_k = B_k^{-1}$ — матрица преобразования пространства).

$(k+1)$**-ый шаг алгоритма** ($k = 0,1,2,\ldots$).

Вычисляем:

1) h_{k+1} — шаговый множитель, $h_{k+1} \ge 0$.
2) $x_{k+1} = x_k - h_{k+1} B_k g_k^* / | g_k^* |$;
3) $g(x_{k+1}) \in \partial f(x_k)$. (субградиент в точке x_{k+1});
4) $\tilde{g}_{k+1}^* = B_k^* g(x_{k+1})$ (субградиент в преобразованном пространстве $Y_k = A_k X$);
5) $\eta_{k+1} = (\tilde{g}_{k+1}^* - g_k^*) / | \tilde{g}_{k+1}^* - g_k^* |$ (направление растяжения пространства Y_k);
6) $\alpha_{k+1} \ge 1, \beta_{k+1} = 1/\alpha_{k+1}$ (α_k коэффициент растяжения пространства Y_k);
7) $B_{k+1} = B_k R_{\beta_{k+1}}(\eta_k)$, (обратный оператор преобразования пространства $Y_{k+1} = A_{k+1} X = B_{k+1}^{-1} X$);
8) $g_{k+1}^* = R_{\beta_{k+1}}(\eta_{k+1}) \tilde{g}_{k+1}$ ($g_{k+1}^* = B_{k+1}^* g(x_k)$. (субградиент в преобразованном пространстве $Y_{k+1} = A_{k+1} X = B_{k+1}^{-1} X$).

Переходим к $(k+2)$-му шагу алгоритма, или прекращаем работу при выполнении критерия останова.

В r-алгоритме значения коэффициентов растяжения пространства (параметр r-алгоритма) выбираются одинаковыми на всех итерациях: $\alpha_k = \alpha > 1$. На практике рекомендуется это значение выбирать порядка 2.0. Величина шагового множителя определяется процедурой минимизации («спуска») по направлению $-B_k g_k^* / | g_k^* |$. Обычно применяемые процедуры «спуска» являются достаточно грубой реализацией алгоритма локализации минимума по направлению. Наиболее часто используется процедура адаптивной регулировки шаговых множителей [1]. Эта процедура определяется параметрами $0 < q_1 \le 1$, $q_2 \ge 1$ и целым числом $L \ge 2$. Эти величины являются параметрами (константами) алгоритма.

Вычислительная схема $r(\sigma)$-алгоритмов. Вычислительная схема предлагаемых алгоритмов соответствует приведенной схеме

r-алгоритма. Отличие состоит лишь в следующем. Вместо оператора растяжения $R_\alpha(\eta)$ будет использоваться следующий оператор

$$\tilde{R}(\tilde{\eta}) = (\alpha - 1)\tilde{\eta}\tilde{\eta}^T + I, \tag{1}$$

где $\tilde{\eta} \in R^n$, σ — нормирующий множитель, $\sigma \in R^1$, $\sigma > 0$. В отличие от оператора $R_\alpha(\eta)$, вектор $\tilde{\eta}$ не нормирован, то есть выполнение условия $|\tilde{\eta}| = 1$ не требуется. Различные варианты алгоритма будут определяться выбором нормирующего множителя σ.

Остановимся на простейших свойствах оператора $\tilde{R}_\sigma(\tilde{\eta})$: $\tilde{R}^* = \tilde{R}$; $\tilde{R}^{-1}(\tilde{\eta}) = -\left(\sigma / (1 + \sigma\tilde{\eta}^2)\right)\tilde{\eta}\tilde{\eta}^T + I$; $\tilde{R}_\sigma(0) = I$.

Пусть $|\tilde{\eta}| \neq 0$ и $\eta = \tilde{\eta} / |\tilde{\eta}|$. Тогда $\tilde{R}(\tilde{\eta}) = R_\alpha(\eta) + I$, где

$$\alpha = 1 + \sigma |\tilde{\eta}|^2 . \tag{2}$$

Таким образом, если $\tilde{\eta} \neq 0$, то оператор $\tilde{R}_\sigma(\tilde{\eta})$ является оператором растяжения по направлению $\tilde{\eta} / |\tilde{\eta}|$. Значение коэффициента растяжения определяется (2). Значение нормирующего множителя σ будет определяться на основании субградиентов $\tilde{g}^*_{k+1}, g^*_k$: $\sigma_{k+1} = \sigma(\tilde{g}^*_{k+1}, g^*_k)$. Естественным требованием на функцию $\sigma(g_1, g_2)$ будет выполнение условия (условия «однородности») $\sigma(\mu g_1, \mu g_2) = \sigma(g_1, g_2) / \mu^2$, где $\mu \in R^1, \mu > 0$. Это условие обеспечивает независимость работы алгоритма от множителя на целевую функцию.

Легко видеть, что алгоритм $r(\sigma_0)$: $\sigma_0(g_1, g_2) = 1 / |g_2 - g_1|^2$ фактически является r-алгоритмом с коэффициентом растяжения равным 2. Отметим, что именно это значение рекомендуется на практике использования r-алгоритм.

Выбирая различные нормирующие множители σ, мы будем получать различные алгоритмы рассматриваемого класса. В данной работе рассматривается $r(\sigma_1)$-алгоритм с нормирующим множителем $\sigma_1(g_1, g_2) = 1 / |(g_2 |*| g_1|)$.

Численная эффективность $r(\sigma)$-алгоритмов. Приведем результаты численных исследований эффективности алгоритма $r(\sigma_1)$ в сравнении с r-алгоритмом. Результаты численных исследований эффективности других вариантов алгоритм $r(\sigma)$ приведены в [3, 4]. В качестве тестовых задач рассматривались задачи минимизации функций: $f(x) = \sum_{i=1}^{n} \rho_n^{i-1} |x_i|$, где параметр ρ_n выбирался в зависимости от размерности задачи n по формуле $\rho_n = 10^{6/(n-1)}$. Начальная точка $x_i = 1.0$, $i = 1,2,...n$. Критерий останова: $f_k \le 10^{-6}$, где f_k — значение функции на итерации останова k.

Результаты решения тестовых задач минимизации функций $f(x)$ приведены в таблице, где приняты следующие обозначения: n — размерность пространства переменных; k — номер итерации, на которой алгоритм прекратил работу; kg — количество вычислений субградиента; $\alpha_{\max}$ — максимальное значение коэффициента растяжения; α_{avrg} — среднее значение коэффициента растяжения; r — результаты работы r-алгоритма с параметрами $q_1 = q_2 = 1$. В алгоритмах отмеченных символом «*» используется постоянная величина шага (в преобразованном пространстве). В алгоритмах, не отмеченных символом «*», используется адаптивная регулировка шаговых множителей r-алгоритма.

Таблица

Минимизация функции $f(x)$

Параметры / Алгоритм	n	k	k_g	$\alpha_{\max}$	α_{avrg}
r_1	100	1536	1554	5.38	4.49
r_1^*	100	1540	1541	5.76	4.49
r	100	3256	3264	2.00	2.00
r_1	500	7847	7873	5.19	4.58
r_1^*	500	7850	7851	5.19	4.58
r	500	16850	16864	2.00	2.00

Выводы. $r(\sigma)$-алгоритмы являются модификациями r-алгоритма. Вычислительная схема $r(\sigma)$-алгоритмов с постоянным шагом существенно проще схемы r-алгоритма. Величины коэффициентов растяжения пространства на итерациях $r(\sigma)$-алгоритмов не постоянны, они вычисляются в процессе его работы. Алгоритмы могут использоваться с постоянным шаговым множителем. Численные эксперименты показали достаточно высокую эффективность $r(\sigma)$-алгоритмов. Их эффективность не уступает эффективности r-алгоритма

Список использованной литературы:

1. Шор Н. З., Журбенко Н. Г. Метод минимизации, использующий операцию растяжения пространства в направлении разности двух последовательных градиентов. *Кибернетика*. 1971. № 3. С. 51-59.

2. Шор Н. З. Методы минимизации недифференцируемых функций и их применение. К.: Наук. думка, 1979. 208 с.
3. Журбенко Н. Г.Об одной модификации *r*-алгоритма. Материалы III Международной конференции *Математическое моделирование, оптимизация и информационные технологии*. Кишинеу: Эврика, 2012. С. 355–361.
4. Журбенко Н. Г., Чумаков Б. М. Программное управление коэффициентами растяжения *r*-алгоритма. *Теорія оптимальних рішень*. Київ: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2012. С. 113–118.

Is considered the family of minimization algorithms using space dilation operation along the direction of the difference of two successive subgradients. In contrast to r-algorithm, in the proposed modifications the values of dilation coefficients are calculated in the process of algorithm. The algorithms can be used with a constant step size. Is the result of the study of the numerical efficiency of the algorithm considered family.

Key words: *nonsmooth optimization, subgradient, the transformation of the space, numerical efficiency.*

Получено 15.03.2017

УДК 681.3.06:006.354

Л. В. Ковальчук*, д-р техн. наук,
Н. В. Кучинська,** канд. техн. наук

*Інститут СЗР України, м. Київ,
**Національний технічний університет України «КПІ», м. Київ

ОЦІНКИ ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКАЦІЙ НОВИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ ВІДНОСНО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Отримані науково обґрунтовані оцінки практичної стійкості до цілочисельного різницевого криптоаналізу ГОСТ-подібних та «Калина»-подібних блокових шифрів, проведено статистичний порівняльний аналіз отриманих значень з відповідними параметрами для випадкових вузлів заміни.

Ключові слова: *різницевий, диференціальний криптоаналіз, блокові шифри, стійкість, s-блоки, вузли заміни.*

Вступ. Сьогодні симетричні блокові алгоритми шифрування є основним криптографічним засобом забезпечення конфіденційності при обробці інформації у сучасних інформаційно-телекомунікаційних системах. За останні кілька років у країнах СНД прийнято низку власних стандартів блокових шифрів, а саме СТБ 34.101.31-2011 (Білорусь), ГОСТ Р 34.12 2015 (РФ) та ДСТУ 7624:2014 «Калина» (Україна). Варто зауважити, що в стандарті ГОСТ Р 34.12 2015 визначено два алгоритми блокового шифрування для довжини блока 128 біт («Кузнєчик») та 64 біт («Магма»). Другий алгоритм є за своєю суттю аналогічним алгоритму, визначеному в ГОСТ 28147-89. Крім того український («Калина») та російський («Кузнєчик») стандарти схожі за своєю будовою. Тому ГОСТ Р 34.12 2015 «Кузнєчик» можна вважати «Калина»-подібним алгоритмом.

Починаючи з 90-х років минулого століття, цілочисельні диференціали використовувались, в перше чергу, для побудови колізій геш-функцій. Пізніше, за останні 5–7 років, з’явились перші роботи, присвячені аналізу стійкості раундових функцій до цілочисельного різницевого криптоаналізу (наприклод, [1–3]). Запропонований у цих роботах підхід може бути застосований для дослідження блокових алгоритмів, які містять додаткове нелінійне перетворення — суматор за модулем 2^{32} або 2^{64}.

1. Побудова оцінок практичної стійкості ГОСТ-подібного алгоритму. Розглянемо $\Im$ — r-раундовий блоковий шифр, який перетворює відкритий текст $x \in V_n$ в шифрований текст $y \in V_n$ при ключі шифрування $k = (k_1, k_2,\ldots, k_r) \in (V_m)^r$ за наступним правилом:

$$y = \Im_k(x) = f_{k_r} \circ f_{k_{r-1}} \circ \cdots \circ f_{k_1}(x), \qquad (1)$$

де $k_i \in V_m$, $i = \overline{1, r}$ — раундові ключі, $f_\lambda(\cdot) : V_n \to V_n$, $\lambda \in V_m$ — раундова функція шифрування.

Означення 1. Будемо називати блоковий алгоритм шифрування (1) *модифікованим ГОСТ-подібним алгоритмом*, якщо його раундова функція має наступний вигляд:

$$f_k(u,v) = (v, u + \varphi(v + k)), \qquad (2)$$

де $x = (u,v) \in V_n$, $n = 2m$, $u,v,k \in V_m$, k — раундовий ключ, $\varphi : V_m \times V_m \to V_m$ — раундове перетворення алгоритму (2), а + є додаванням за модулем 2^m.

Довжина блоку алгоритму визначається як $n = pu,\ p \ge 2$, а блок підстановок — набором: $\forall x \in V_n : S(x) = (s^{(p)}(x^{(p)}),\ldots, s^{(1)}(x^{(1)}))$, $x^{(i)} \in V_u$, $i = \overline{1, p}$, де s-блоки $s^{(i)} : V_u \to V_u$, $i = \overline{1, p}$ — бієктивні відображення. Відображення зсуву вліво t біт вектора з V_m позначено $L_t : V_m \to V_m$. Раундове перетворення $\varphi : V_m \times V_m \to V_m$, яке задано в (2), у введених позначеннях можна представити:

$$\varphi(x,k) = L_t\left(S(x+k)\right). \qquad (3)$$

Справедливим є наступний результат.

Теорема 1. Для модифікованого ГОСТ-подібного алгоритму з r раундами справедлива оцінка практичної стійкості:

$$\max_{\Omega} EDP(\Omega) \le \left(\max_{\alpha,\beta \in V_n \setminus \{0\}} d_{+}^{\varphi}(\alpha,\beta) \right)^{\left[2r/3 \right]}.$$

Для доведення теореми використовуються отримані в [2, с. 72–73; 3, с. 27] наукові результати, які, зокрема, дозволяють оцінити величину $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d_{+}^{\varphi}(\alpha,\beta)$ в даному випадку.

В такому випадку, якщо 4-бітові вузли заміни обрані з рекомендованих до використання, але з найменшими значеннями параметрів (dke2 або dke7) оцінкою буде $\max\limits_{\Omega} EDP(\Omega) \le 0{,}0024 \approx 2^{-9}$.

Але таку оцінку можна покращити, якщо обрати вузли заміни з $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}(\omega_i,\omega_{i+1}) \le 2 \cdot 0{,}1875$, тоді

$$\max_{\Omega} EDP(\Omega) \le 1{,}13 \cdot 10^{-9} \approx 2^{-29}.$$

Якщо модифікувати ГОСТ до використання 8-бітових вузлів заміни і обрати їх так, щоб $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}(\omega_i,\omega_{i+1}) \le 2 \cdot 0{,}0195$, то $\max\limits_{\Omega} EDP(\Omega) \le 2{,}58 \cdot 10^{-30} \approx 2^{-98}$.

Побудова оцінок практичної стійкості «Калина»-подібних алгоритмів. Введемо лінійний (над кільцем Z_{2^u}) оператор $A:(V_u)^p \to (V_u)^p$, який задамо за допомогою матриці $A = \left(a_{ij}\right)_{i,j=1}^{p}$, $a_{ij} \in V_u$, де $\forall x = (x^{(p)},...,x^{(1)}) \in V_n$: $A\,x^T = y^T = \left(y^{(p)},...,y^{(1)}\right)^T$, $y^{(i)} = \sum\limits_{j=1}^{p} a_{ij} x^{(j)}$, а операції множення та додавання виконуються у кільці Z_{2^u}. Позначимо $A_i = \left(a_{ip},...,a_{i1}\right)$. Тоді, в наших позначеннях, $y^{(i)} = A_i x^T$, тобто $A\,x^T = \left(A_p x^T,...,A_1 x^T\right)^T$.

Аналогічно позначимо для оберненого оператора $A^{-1} = \left(A_p',...,A_1'\right)$, і $A^{-1}x^T = \left(A_p' x^T,...,A_1' x^T\right)^T$. Надалі розглядається лише такий оператор A, що $wt\left(A_j'\right) \le l,\ j = \overline{1,p}$.

Означення 2. В наших позначеннях будемо називати блоковий алгоритм шифрування (1) *модифікованим «Калина»-подібним алгоритмом,* якщо його раундова функція має вигляд:

$$f_k(x) = A \circ S(x * k), \tag{4}$$

де $x \in V_n$ — відкритий текст, $n = pu,\ p \geq 2$, $x = (x_p, ..., x_1)$, $x_i : V_u \to V_u$, $i = \overline{1, p}$, $k \in V_n$ — раундовий ключ, — операція побітового або модульного додавання, $S : V_n \to V_n$ — блок підстановки такий, що $S = (s^{(p)}, ..., s^{(1)})$, де $s^{(i)} : V_u \to V_u$.

У введених позначеннях для модифікованого раундового перетворення (4) алгоритмів «Калина» та «Кузнєчик» справедливим є наступна теорема, яка встановлює оцінки практичної стійкості алгоритмів відносно цілочисельного різницевого криптоаналізу.

Теорема 2.

1) для модифікованого «Калина»-подібного алгоритму верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму визначаються як:

$$EDP(\Omega) \leq \max_{\alpha, \beta \in V_n \setminus \{0\}} d^f_{+,+}(\alpha, \beta) \cdot (\max_{\alpha, \beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta))^{N-1},$$

де N — кількість раундів блокового алгоритму;

2) для модифікованого алгоритму «Кузнєчик» верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму з N раундами за шифрування визначаються як:

$$EDP(\Omega) \leq \max_{\alpha, \beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta)^{N-1}.$$

Для доведення теореми використовуються отримані в [1, с. 36–39] наукові результати та дозволяють оцінити величину $\max\limits_{\alpha, \beta \in V_n \setminus \{0\}} d^{\varphi}_{+}(\alpha, \beta)$ в даному випадку.

У такому випадку, якщо вузли заміни обрані з рекомендованих в стандарті ДСТУ7624:2014, тоді $\max\limits_{\alpha, \beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta) \leq 0{,}09375$ і $\max\limits_{\alpha, \beta \in V_n \setminus \{0\}} d^f_{+,+}(\alpha, \beta) \leq 0{,}10546875$. Звідки, для 10 раундів зашифрування $EDP(\Omega) \leq 5{,}9 \cdot 10^{-11} \approx 2^{-34}$, для 14 раундів зашифрування, $EDP(\Omega) \leq$ $\leq 4{,}578 \cdot 10^{-15} \approx 2^{-48}$, для 18 раундів зашифрування $EDP(\Omega) \leq$ $\leq 3{,}521 \cdot 10^{-19} \approx 2^{-61}$.

Якщо обрати вузли заміни таким чином, щоб вони відповідали найменшим значенням параметрів $\max\limits_{\alpha, \beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta) \leq 0{,}08203125$ і

$\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta) \le 0{,}08203125$, то для 10 раундів зашифрування отримали б $EDP(\Omega) \le 1{,}38 \cdot 10^{-11} \approx 2^{-36}$ для 14 раундів зашифрування $EDP(\Omega) \le 6{,}248 \cdot 10^{-16} \approx 2^{-51}$ і для 18 раундів зашифрування $EDP(\Omega) \le 2{,}829 \cdot 10^{-20} \approx 2^{-65}$.

Для модифікованого алгоритму (з модульним ключовим суматором), при оптимальному виборі значень параметрів справедлива аналогічна оцінка.

У випадку, якщо використано вузол заміни із стандарту ГОСТ Р 34.12 2015, тоді для модифікованого алгоритму із побітовим додаванням у ключовому суматорі $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{\oplus,+}(\alpha,\beta) \le 0{,}09375$, звідки за теоремою 3 для 10 раундів зашифрування (враховуючи, що останній раунд не використовує нелінійну заміну, а лише побітове додавання ключа), отримаємо $EDP(\Omega) \le 3{,}814 \cdot 10^{-10} \approx 2^{-31}$.

Висновки. Наведені результати дозволили оцінити практичну стійкість алгоритмів блокового шифрування визначених ув стандартах України та Росії відносно цілочисельного різницевого криптоаналізу. Отримано оцінки верхніх меж практичної стійкості модифікованого ГОСТ-подібного алгоритму до цілочисельного різницевого криптоаналізу. Отримано оцінки верхніх меж практичної стійкості модифікованих алгоритмів «Кузнєчик» та «Калина» до цілочисельного різницевого криптоаналізу у двох випадках: коли в ключовому суматорі реалізована операція модульного додавання або побітового додавання. Порівняння отриманих значень зі статистичними розподілами цих параметрів дає привід припускати, що при проектуванні шифру «Кузнєчик», окрім стійкості до класичного побітового різницевого криптоаналізу, могла бути врахована необхідність практичної стійкості і до цілочисельного різницевого криптоаналізу. Неможливо стверджувати напевно, чи був такий тип атаки розглянутий авторами шифру при проектуванні його *S*-блоку. Варто зазначити, щодо інших сучасних алгоритмів, стійкість до цілочисельного різницевого криптоаналізу не розглядалася ні при побудові шифру AES, ні шифру «Калина». Якщо припущення правильне, то «Кузнєчик» стає першим алгоритмом шифрування, який би використовував нелінійні вузли заміни за замовчуванням із близькими до практично досяжних найменших значень параметрів, тобто тих, що забезпечують йому практичну стійкість раундових перетворень до цілочисельного різницевого криптоаналізу.

Список використаних джерел:

1. Ковальчук Л. В., Кучинська Н. В., Скрипник Л. В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій клю-

чового суматора, блока підстановки та лінійного (над деяким кільцем) оператора. Науково-технічний збірник «*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*». 2015. № 1 (29). С. 33–45.

2. Ковальчук Л. В., Кучинська Н. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. *Кибернетика и системный анализ.* 2012. № 5. С. 71–81.
3. Кучинская Н. В., Скрипник Л. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига *Спеціальні телекомунікаційні системи та захист інформації*. 2013. Вип. 2(24). С. 26–32.

Practical estimates are obtained for cryptographic security of GOST-like and Kalyna-like block cipher statistical comparative analysis is conducted of the relevant parameters values for random nodes replacement.

Key words: *difference, differential cryptanalysis, block ciphers, s-blocks.*

Одержано 28.02.2017

УДК 519.8

И. В. Козин, д-р физ.-мат. наук, профессор,
С. Е. Батовский, аспирант,
В. И. Сардак, аспирантка

Запорожский национальный университет, г. Запорожье

ФРАГМЕНТАРНАЯ МОДЕЛЬ И ЭВОЛЮЦИОННЫЙ АЛГОРИТМ 2D УПАКОВКИ ОБЪЕКТОВ

Рассмотрена задача двумерной упаковки в прямоугольник объектов сложной формы. Показано, что задача упаковки имеет фрагментарную структуру. Для поиска приближенного решения задачи предложена модификация эволюционного алгоритма на перестановках с геометрическим оператором кроссовера. Приводятся результаты численного эксперимента.

Ключевые слова: *фрагментарная модель, задача размещения, 2d-упаковка, эволюционный алгоритм, геометрический кроссовер*

Введение. Задача плоского размещения или двумерной упаковки возникает в многочисленных инженерных и экономических приложениях. Решение проблемы упаковки требуется для таких отраслей, как транспорт, обработка дерева, стекла, кожи, при поиске оптимальных размещений механических и электромеханических узлов агрегатов, при загрузке автомобилей, железнодорожных платформ, танкеров и т. д. Большое количество дополнительных условий в конкретных постановках приводит к необходимости использовать вероятностные методы и эвристические процедуры [1–4].

Постановка задачи. Рассмотрим наиболее распространенную постановку задачи двумерной упаковки, когда требуется разместить заданное конечное множество плоских объектов в контейнере, который представляет собой прямоугольник заданных размеров. Объекты могут иметь достаточно сложную форму, могут быть как выпуклыми, так и невыпуклыми, неодносвязными. Однако будем предполагать, что все объекты являются связными, то есть не распадаются на отдельные части. При размещении в контейнере объекты не должны пересекаться и не могут выходить за границы контейнера. Задача разместить в контейнере по возможности большее по площади подмножество объектов. Целевой функцией в данном случае является плотность упаковки или величина неиспользованной площади в контейнере. Объекты сложной формы заменим их дискретной клеточной аппроксимацией. То есть будем представлять объекты как объединение множества квадратных ячеек достаточно малого размера. Пример такой аппроксимации показан на рис. 1.

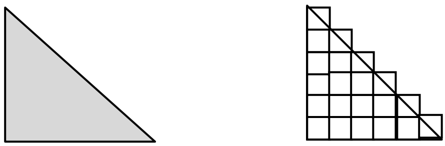


Рис. 1. *Плоский объект и его дискретная аппроксимация*

Такой подход применим к объектам произвольной формы. При размещении в контейнере будем заменять объекты их дискретной аппроксимацией с условием, что аппроксимация содержит исходный объект в качестве собственного подмножества.

Фрагментарная структура. Фрагментарной структурой [5] (X, E) на конечном множестве X называется семейство его подмножеств $E = \{E_1, E_2, ..., E_n\}$ такое, что $\forall E_i \in E$, $E \neq \varnothing$ $\exists e \in E_i : E_i \setminus \{e\} \in E$.

Элементы из множества E будем называть допустимыми фрагментами. Таким образом, для любого допустимого фрагмента E_i существует нумерация его элементов $E_i = \{e_{i1}, e_{i2}, ...e_{is_i}\}$ такая, что $\forall k = 1, 2, ...s_i$ $\{e_{i1}, e_{i2}, ...e_{ik}\} \in E$. Элементарным фрагментом будем называть допустимый фрагмент, состоящий из одного элемента. Максимальный фрагмент — допустимый фрагмент, который не является подмножеством никакого другого фрагмента.

Максимальный фрагмент может быть построен с помощью следующего «жадного» алгоритма:

а) элементы множества X линейно упорядочиваются;

б) на начальном шаге выбирается пустое множество $X_0 = \varnothing$;

в) на шаге с номером $k + 1$ выбирается первый по порядку элемент $x \in X \setminus X_k$, такой, что $X_k \bigcup \{x\} \in E$;

г) алгоритм заканчивает работу, если на очередном шаге не удалось найти элемент $x \in X \setminus X_k$ с требуемым свойством.

Результат работы алгоритма определяется заданным линейным порядком на множестве X. Таким образом, любой максимальный фрагмент может быть описан некоторой перестановкой элементов множества X. Пусть $A \in E$. Условие для элемента $x \in X$, при котором $A \bigcup \{x\} \in E$, будем называть условием присоединения элемента x.

Пусть теперь каждому фрагменту приписан вес, то есть задана функция $\rho : E \to R^1$. Будем предполагать, что функция ρ монотонна по включению (возрастающая или убывающая). Если $A, B \in E$ и $A \subseteq B$, то $\rho(A) \le (\ge) \rho(B)$. Задача оптимизации на фрагментарной структуре, это задача отыскания допустимого фрагмента максимального (минимального) веса. Очевидно, что для монотонных весов оптимальное решение будет являться максимальным фрагментом.

Фрагментарная модель. Покажем, что задача 2d-упаковки может быть представлена как задача оптимизации на фрагментарной структуре. В качестве множества элементарных фрагментов рассмотрим заданный набор объектов, точнее их дискретных аппроксимаций. Каждый допустимый фрагмент будем строить, соблюдая следующее условие присоединения. Очередной объекта размещается в заданном прямоугольном контейнере без выхода за границы контейнера и без пересечений с уже уложенными объектами. Причем при укладке объекта будем руководствоваться правилом Top-Left (северо-западный угол), а именно: объект размещается как можно выше и как можно левее с соблюдением вышеуказанных условий. Если очередной объект разместить не удается, то переходим к следующему по порядку объекту. Множества объектов, которые будут построены в результате работы такого алгоритма (множество E), образуют фрагментарную структуру. Максимальный фрагмент в данном случае определяет некоторое размещение объектов в контейнере, в которое уже нельзя добавить никакой из оставшихся объектов без нарушения условий размещения. Целевая функция задачи $F : E \to R^1$ — это площадь свободного места контейнера, то есть не площадь не занятая размещаемыми объектами. Очевидно, целевая функция является монотонной.

Любой максимальный фрагмент определяется заданным линейным порядком просмотра элементарных фрагментов. Этот порядок определяет результат работы фрагментарного алгоритма, который и построит требуемый максимальный фрагмент.

Каждый линейный порядок определяется некоторой перестановкой $s \in S_n$ укладываемых объектов (n — число объектов). Сопоставим каждой перестановке максимальный фрагмент, который ей порождается. Обозначим это отображение $\varphi : S_n \to E$. Таким образом, имеет место естественная коммутативная диаграмма отображений

$$\begin{array}{ccc} S_n & & \\ \varphi \downarrow & \searrow F \circ \varphi, & \\ E \to R^1 & & \end{array}$$

которая превращает задачу оптимизации на фрагментарной структуре в задачу оптимизации на множестве перестановок. Причем любая перестановка является допустимой. Для больших значений n задача поиска оптимальной перестановки, как правило, является трудной. Предлагается использовать для поиска приближенных решений этой задачи эволюционный алгоритм на перестановках определенного вида [6].

Эволюционный алгоритм. Базовое множество X эволюционной модели — это множество $S_n = \{i_1, i_2 ..., i_n\}$ всех перестановок чисел $1, 2, \ldots, n$. Оператор построения начальной популяции выделяет произвольное подмножество заданной мощности Q из множества X.

Правило вычисления критерия селекции устроено следующим образом: по заданной перестановке фрагментов с помощью фрагментарного алгоритма строится максимальный допустимый фрагмент и вычисляется значение целевой функции задачи для этого фрагмента.

Опишем теперь оператор кроссовера. Пусть $U = (u_1, u_2, ..., u_n)$ и $V = (v_1, v_2, ..., v_n)$ — две произвольные перестановки. Перестановка-потомок строится следующим образом: последовательности U и V просматриваются в порядке следования элементов. На k-м шаге выбирается наименьший из первых элементов последовательностей и добавляется в новую перестановку-потомок. Затем этот элемент удаляется из двух последовательностей-родителей. Например, результатом кроссовера перестановок (4, 1, 6, 3, 7, 8, 2, 5) и (2, 6, 7, 3, 1, 4, 8, 5) будет перестановка (2, 4, 1, 6, 3, 7, 8, 5). В работе [6] показано, что определенный таким образом оператор кроссовера является геометрическим в инверсной метрике на перестановках [7].

Оператор мутации M выполняет случайную транспозицию в перестановке.

Оператор селекции выбирает случайным образом набор пар из текущей популяции для последующего скрещивания.

Оператор эволюции упорядочивает элементы промежуточной популяции в последовательность по убыванию значения критерия селекции. В качестве новой текущей популяции выбираются первые Q элементов последовательности.

Обычное правило остановки — количество поколений достигло предельного значения. Лучшая по значению критерия селекции перестановка из последней построенной популяции определяет приближенное решение задачи.

Результаты работы. Для проверки качества предлагаемой метаэвристики была разработана компьютерная оценка качества эволюционно-фрагментарных алгоритмов (ЭВФ — алгоритмов). Некоторые результаты работы этой программы приводятся далее.

Примеры 1, 2. Рассматривались большие наборы одинаковых объектов Т-образного (пример 1) и Г-образного (пример 2) вида. Результаты работы алгоритма показаны соответственно на рис. 2 и рис. 3.

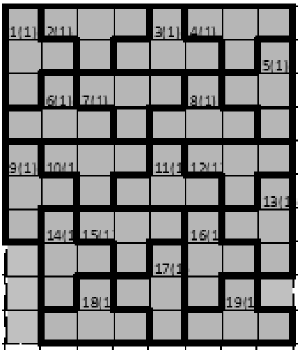


Рис. 2. *Т-образные объекты*

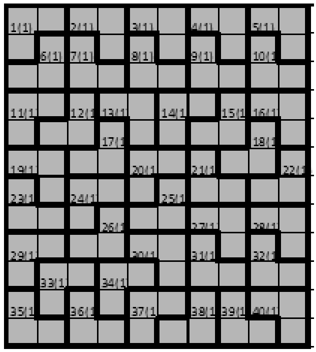


Рис. 3. *Г-образные объекты*

Пример 3. В качестве примера была взята 2d-упаковка объектов из статьи [8], полученная путем применения генетического алгоритма определенного вида (рис. 4). На рис. 5 показан результат работы ЭВФ-алгоритма для того же набора объектов в том же контейнере.

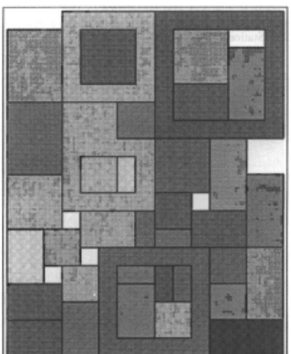


Рис. 4. *Упаковка из [8]*

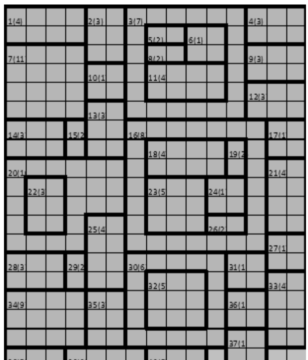


Рис. 5. *Упаковка ЭВФ алгоритмом*

Выводы. Теоретические результаты и результаты численных экспериментов показывали достаточно высокую эффективность ЭВФ алгоритма при решении различных типов задач плоского размещения и 2d-упаковки. Учитывая простоту реализации и возможность учета дополнительных ограничений, рассматриваемый в статье подход может быть предложен для практического решения задач упаковки в различных областях техники, экономики, производства.

Список использованной литературы:

1. Kierkosz I., Luczak M. A hybrid evolutionary algorithm for the two-dimensional packing problem. *Central European Journal of Operations Research*. [Berlin]: Springer, 2014. Vol. 22. P. 729–753.
2. Кривий Р. З., Лобур М. М., Ткаченко С. П. Застосування генетичного алгоритму прямокутного розміщення для гільйотинного розкрою. Вісник Національного університету «Львівська політехніка». *Комп'ютерні системи проектування. Теорія і практика*. 2010. № 685. С. 138–142. Режим доступу: http://ena.lp.edu.ua:8080/handle/ntb/7414 **.**
3. Мухачева Э. А., Мухачева А. С., Чиглинцев А. В. Генетический алгоритм блочной структуры в задачах двумерной упаковки. *Информационные технологии*. 1999. № 11. С. 12–17.
4. Gonçalves J. F. A hybrid genetic algorithm-heuristic for a two-dimensional orthogonal packing problem. *European Journal of Operational Research*. 2007. Vol. 183 (3) P. 1212–1229.
5. Козин И. В., Полюга С. И. Использование ЭВФ-алгоритмов для решения задачи прямоугольного раскроя. *Питання прикладної математики і математичного моделювання*: зб. наук. праць ; [ред. кол. … О. М. Кисельова (голов. ред.) та ін.]. Д.: Вид-во Дніпропетр. нац. ун-ту ім. Олеся Гончара. Дніпропетровськ, 2009. С. 199–208.
6. Козин И. В. Фрагментарные структуры и эволюционные алгоритмы. *Питання прикладної математики і математичного моделювання* : зб. наук. праць ; [ред. кол.: О. М. Кисельова (головний редактор) та ін.]. 2008. С. 138–146.
7. Moraglio A., Poli R. Inbreeding Properties of Geometric Crossover and Non-geometric Recombinations. *Foundations of Genetic Algorithms*. 2007. P. 1–14
8. Sakait Jain and Hae Chang Gea Two-Dimensional Packing Problems Using Genetic Algorithms. *Engineering with Computers*. 1998 14: P. 206–213.

The problem of two-dimensional packing in rectangle of objects of complex shape. It is shown that the packing problem has fragmentary structure. To find an approximate solution proposed modification of the evolutionary algorithm on permutations with geometric crossover operator. The results of numerical experiment.

Key words: *fragmented model, the layout problem, the 2d-packing problem, evolutionary algorithm, geometric crossover.*

Получено 13.02.2017

УДК 519.9

О. М. Коломис, канд. фіз.-мат. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ОЦІНКА ПОХИБКИ ЗАОКРУГЛЕННЯ АЛГОРИТМУ ОБЧИСЛЕННЯ ПЕРВИННОЇ ОЦІНКИ СПЕКТРАЛЬНОЇ ЩІЛЬНОСТІ

Наведена оцінка похибки заокруглення алгоритму обчислення первинної оцінки спектральної щільності.

Ключові слова: *первинна оцінка спектральної щільності, похибка заокруглення, швидке перетворення Фур’є.*

Вступ. Із появою алгоритму швидкого перетворення Фур’є (ШПФ) було розроблено ряд обчислювальних алгоритмів прискореного розв'язання деяких задач спектрального і кореляційного аналізу випадкових процесів [1, 2]. Зокрема, побудовані ефективні за швидкодією алгоритми обчислення таких оцінок імовірнісних характеристик об’єктів керування, як оцінок згорток, кореляційних функцій, спектральних щільностей стаціонарних і деяких типів нестаціонарних випадкових процесів [2, 3].

Розглянемо ефективні за швидкодією алгоритми обчислення оцінок спектральних щільностей стаціонарних ергодичних випадкових процесів із нульовим середнім значенням. Найчастіше для їх обчислення використовують метод прямого перетворення Фур’є з використанням алгоритму ШПФ [2, 3]. Дана стаття продовжує дослідження і обґрунтування цього методу в напрямку отримання більш якісних оцінок похибок заокруглення.

Постановка задачі та алгоритм розв’язання. Нехай $x(t)$ — випадковий стаціонарний ергодичний процес з нульовим середнім значенням і задана вибірка $x_\nu = x(t_\nu),\ \nu = \overline{0, N-1}.$ Оцінка спектральної щільності визначається співвідношенням [2]

$$S_x(k) = S_x(\omega_k) = \frac{h}{N}\left|\widehat{X}_k\right|^2,\ k = \overline{0, N-1}, \tag{1}$$

де h — крок за часом, $\widehat{X}_k = \widehat{X}(\omega_k)$ — дискретне перетворення Фур’є (ДПФ) початкового сигналу $x(t)$, $\omega_k = k/(Nh)$, $k = \overline{0, N-1}$.

Для обчислення $\widehat{X}_k$, $k = \overline{0, N-1}$ будемо використовувати алгоритм ШПФ

$$\widehat{X}_k = \widehat{X}(\omega_k) = \sum_{\nu=0}^{N-1} x_\nu W_N^{\nu k}, \tag{2}$$

де $k,\nu=\overline{0,N-1}$, $W_N=e^{-i\frac{2\pi}{N}}$.

Евклідова норма оцінки похибки заокруглення алгоритму ШПФ обчислення ДПФ $\widehat{X}=\left\{\widehat{X}_k\right\}_0^{N-1}$ сигналу $x=\left\{x_\nu\right\}_0^{N-1}$, для $N=2^\gamma$, де $\gamma>0$ — ціле, для класичного правила заокруглення має вигляд [2]:

$$\left\|E_{\widehat{X}}\right\|_E<8\cdot 1{,}06\cdot\gamma\cdot 2^{-\tau}\cdot\left\|\widehat{X}\right\|_E, \tag{3}$$

де τ — кількість двійкових розрядів у мантисі числа для обчислень на комп'ютері в режимі з плаваючою комою.

Величину $S_x(k)$, $k=\overline{0,N-1}$, що визначається у вигляді співвідношення (1), називають первинною оцінкою спектральної щільності.

У роботі [4] наведено покроковий опис алгоритму, який дозволяє обчислювати (за відповідними ознаками) оцінки спектральної щільності $S_x(k)$, або $S_x^*(k)$, або $\widehat{S}_x^*(k)$, або $\widehat{S}_x(k)$, $k=\overline{0,N-1}$, згідно відповідних співвідношень [4], причому в ньому можуть бути використані вікна як для даних, так і для частот. Для оцінки точності запропонованого алгоритму обчислення оцінок спектральних щільностей дослідимо оцінку похибки заокруглення первинної оцінки спектральної щільності, що виникає при реалізації обчислювального алгоритму на комп'ютері для класичного правила заокруглення, для обчислень у режимі плаваючої коми з τ розрядами в мантисі числа.

Оцінка похибки заокруглення алгоритму обчислення $S_x(k)$, $k=\overline{0,N-1}$. Нехай $N=2^\gamma$, $\gamma>0$ — ціле, $x_\nu=x(t_\nu)$, $\nu=\overline{0,N-1}$ — вибірка стаціонарного ергодичного випадкового процесу $x(t)$ з нульовим середнім значенням, $fl(*)$ — результат обчислення виразу, який стоїть у дужках в режимі з плаваючою комою з τ розрядами у мантисі числа, $\|*\|_E$ — евклідова норма. Справедлива наступна теорема.

Теорема. Нехай $N=2^\gamma$, $\gamma>0$ — ціле, $x_\nu=x(t_\nu)$, $\nu=\overline{0,N-1}$ — вибірка стаціонарного ергодичного випадкового процесу $x(t)$ з нульовим середнім значенням. Оцінка евклідової норми похибки заокруглення обчислення первинної оцінки спектральної щільності, згідно співвідношення (1) за допомогою алгоритму ШПФ для режиму з плаваючою комою з τ розрядами у мантисі числа має вигляд

$$\left\|E_{3,S_x}\right\|_E\sim 8\cdot 1{,}06\cdot\gamma\cdot 2^{-\tau}\cdot h\cdot\|x\|_E^2\left[1+1{,}06\cdot 2^{-\tau}(16\gamma+\sqrt{N})\right]. \tag{4}$$

Доведення. Фактичним значенням оцінки спектральної щільності $S_x(k)$, $k=\overline{0,N-1}$, що визначається співвідношенням (1), при обчисленні його на комп'ютері в режимі з плаваючою комою з τ розрядами у мантисі числа буде вираз

$$fl(S_x(k)) = fl\left(\frac{h}{N}\left|\widehat{X}_k\right|^2\right) = \frac{h}{N}\left|\widehat{X}_k + E_{\widehat{X}}(k)\right|^2(1+\varepsilon_1(k)) \le \frac{h}{N}\left(\left|\widehat{X}_k\right|^2 + E_1(k)\right), \quad (5)$$

де $E_{\widehat{X}}(k)$ — похибка заокруглення обчислення $\widehat{X}_k$ алгоритмом ШПФ, $\varepsilon_1(k)$ — похибка заокруглення, що виникає при множенні двох чисел [5]. З точністю до величини другого порядку малості відносно $\varepsilon_1(k)$ та $E_{\widehat{X}}(k)$ отримаємо:

$$E_1(k) = 2\left|\widehat{X}_k\right|\cdot\left|E_{\widehat{X}}(k)\right| + \left|\widehat{X}_k\right|^2 \varepsilon_1(k). \quad (6)$$

Позначимо $\widehat{Z}(k) = \dfrac{h}{N}[\widehat{X}_k^2 + E_1(k)]$.

Визначимо оцінку $\left\| E_{3,S_x} \right\|_E$ — похибки заокруглення обчислення $S_x(k)$, $k = \overline{0, N-1}$, з використанням алгоритму ШПФ, згідно (3)

$$\left\| E_{3,S_x} \right\|_E < 8\cdot 1{,}06\cdot\gamma\cdot 2^{-\tau}\cdot\left\|\widehat{Z}\right\|_E. \quad (7)$$

Для оцінки $\left\|\widehat{Z}\right\|_E$ під векторами $E_{\widehat{X}}$, $\widehat{X}$, x, ε_1 будемо розуміти ($N\times N$)-матриці, перші рядки яких збігаються відповідно з компонентами вказаних векторів, а решта елементів дорівнюють нулю. Тоді [5] $\left\|\widehat{Z}\right\|_E \le \dfrac{h}{N}\left(\left\|\widehat{X}\right\|_E^2 + \left\|E_1\right\|_E\right)$, де $\left\|E_1\right\|_E \le 2\left\|\widehat{X}\right\|_E\cdot\left\|E_{\widehat{X}}\right\|_E + \left\|\widehat{X}\right\|_E^2\cdot\left\|\varepsilon_1\right\|_E$.

Враховуючи, що $\left|\varepsilon_1\right| \le 1{,}06\cdot 2^{-\tau}$ і $\left\|\varepsilon_1\right\|_E \le 1{,}06\cdot 2^{-\tau}\sqrt{N}$, та використовуючи (3) і той факт, що

$$\left\|\widehat{X}\right\|_E = \sqrt{N}\cdot\left\|x\right\|_E, \quad (8)$$

остаточно отримуємо

$$\left\|E_1\right\|_E < 1{,}06\cdot 2^{-\tau}(16\gamma + \sqrt{N})\left\|x\right\|_E^2$$

та

$$\left\|Z\right\|_E \cong h[1 + 1{,}06\cdot 2^{-\tau}(16\gamma + \sqrt{N})]\left\|x\right\|_E^2. \quad (9)$$

Підставивши (9) у співвідношення (7), отримуємо оцінку (4).

Теорема доведена.

Наслідок. З точністю до величини другого порядку малості відносно $2^{-\tau}$ виконується співвідношення

$$\left\| E_{3,S_x} \right\|_E < \cdot 8\cdot 1{,}06\cdot\gamma\cdot h\cdot 2^{-\tau}\cdot\left\|x\right\|_E^2. \quad (10)$$

Зауваження. Для обчислення ДПФ $\widehat{X}_k = \widehat{X}(\omega_k)$, $k = \overline{0, N-1}$, доцільно використовувати алгоритм ШПФ дійсного сигналу із попередньою заготовкою матриці перетворення [2, 3]. В цьому випадку немає необхідності обчислювати всі N значень ДПФ, достатньо обчислити лише перші $N/2$ значень. Для цього значення x_ν розбивають на дві послідовності $y_\nu = x_{2\nu}$, $z_\nu = x_{2\nu+1}$, $\nu = \overline{0, N/2-1}$ і створюють комплексний сигнал $V(\nu) = y_\nu + z_\nu$. Мають місце співвідношення [2]

$$I(k) = \widehat{Y}(k) + W_N^k \widehat{Z}(k),\ k = \overline{0, N/2-1},\ I(N/2) = \widehat{Y}(0) - \widehat{Z}(0),$$

де

$$\widehat{Y}(k) = \frac{1}{2}\left(\widehat{V}(k) + \widehat{V}^*(N/2 - k)\right),\ \widehat{Z}(k) = \frac{1}{2i}\left(\widehat{V}(k) + \widehat{V}^*(N/2 - k)\right),$$

де $V^*(N/2 - k)$ величина комплексно спряжена з $V(N/2 - k)$. Застосувавши алгоритм ШПФ для обчислення $\widehat{V}(k)$, $k = \overline{0, N/2-1}$ і вказані співвідношення, отримаємо $N/2$ необхідних коефіцієнтів ДПФ $I(k)$, оскільки $I(k) = I^*\left(N-k\right)$. Такий підхід дозволяє майже вдвічі зменшити обсяг обчислювальних затрат та похибку заокруглень при обчисленні ДПФ.

Із більш детального аналізу алгоритму ШПФ випливає, що виграш за кількістю арифметичних операцій у порівнянні зі стандартним способом виходить ще більшим, оскільки багато множників вигляду W_N^{kr} мають в «метеликах» значення $\pm 1, \pm i$, завдяки чому виключаються відповідні операції множення.

Доведено, що при $N = 2^\gamma$ оцінка знизу (серед всіх алгоритмів обчислення ДПФ) кількості операцій додавання рівна $\dfrac{N}{2}\log_2 N$. Існують також алгоритми і програми обчислення багатовимірного ДПФ за допомогою ШПФ.

Список використаних джерел:

1. Cooley J. W., Tukey J. W. An algorithm for the machine calculation of complex Fourier Series. *Math. Comput.*, 1965, Apr., P. 257–301.
2. Задирака В. К. Теория вычисления преобразования Фурье. Киев: Наук. думка, 1983. 216 с.
3. Сергієнко І. В., Задірака В. К., Литвин О. М., Мельникова С. С., Нечуйвітер О. П. Оптимальні алгоритми обчислення інтегралів від швидкоосцилюючих функцій та їх застосування. Т. 2. Застосування. Київ: Наук. думка, 2011. 348 с.

4. Коломис О. М., Луц Л. В. Алгоритм обчислення оцінок спектральної щільності. *Питання оптимізації обчислень (ПОО-XLII)* : праці міжнар. наук. школи-семінару, присвяченої 85-річчю від дня народження академіка В. С. Михалевича (21-25 вересня 2015 р.). Київ: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2015. С. 45–46.
5. Уилкинсон Дж. Х. Алгебраическая проблема собственных чисел. М.: Наука, 1970. 564 с.

The estimation of the rounding error of the algorithm for calculating the primary estimate of the spectral density are developed. are obtained.

Key words: *the primary estimate of the spectral density, rounding error, fast Fourier Transform.*

Одержано 17.02.2017

УДК 519.685.3

Г. І. Кудін, канд. фіз.-мат. наук, доцент

Київський національний університет імені Тараса Шевченка, м. Київ

ОПТИМІЗАЦІЯ ЛІНІЙНОЇ КЛАСИФІКАЦІЇ СИГНАЛІВ ЗАСОБАМИ ЗБУРЕННЯ ПСЕВДООБЕРНЕНИХ МАТРИЦЬ

З використанням засобів збурення псевдообернених матриць запропонована схема оптимізації лінійної класифікації сигналів. Алгоритми оптимального перетворення окремих компонент векторів простору ознак у ряді випадків дозволяють розв'язувати задачу класифікації залишаючись у рамках лінійної моделі. При невдачі такого підходу приводиться алгоритм кусково лінійної класифікації.

Ключові слова: *синтез систем класифікації, псевдо обернені та проекційні матриці.*

Вступ. Протягом останніх двадцяти років в України за участю наукових співробітників Інституту кібернетики імені В.М. Глушкова НАН України розв'язано ряд вагомих як теоретичних, так і прикладних проблем з використанням засобів псевдообернення. У значній мірі це визначається теретичними результатами стосовно обчислень псевдообернених матриць при різнотипних збуреннях вихідних матриць. З використанням властивостей псевдообернених матриць були запропоновані [1, 2] ефективні алгоритми для розв'язування задач лінійної класифікації та кластеризації — в аналітичному вигляді були подані умови лінійної роздільності скінчених множин в евклідовому просторі, віддалі відповідності елементів скінчених множин до відповідних гіперплощин — лінійних кластерів. За умов великої розмірності просторів ознак, значних об'ємів навчальних множин лінійна класифікація може виявитись найбільш прийнятною, тому доцільно шукати в рамках інформації про об'єкти дослідження можливості зменшувати розмірності матриць, які використовуються в процесі необхідних обчислень. У різних областях потреб класифікації ці питання не залишаються поза увагою математиків, досягається прогрес, як правило, за рахунок нелінійних деформацій простору ознак або ігноруванням деяких елементів виборок. Водночас постановка задачі може вимагати оцінку впливу тієї чи іншої компоненти вектора ознак або конкретного елемента виборки на результат (або не результат) процесу класифікації. Далі пропонується оптимізувати лінійну роздільність множин лінійною комбінацією лінійно незалежних компонент векторів ознак навчальної виборки, яка при потребі доповнюється елементами схеми кусково лінійної класифікації.

1. Математичний апарат псевдообернених матриць. Вводяться представлення матриці $A \in R^{m \times n}$ з елементами a_{ij} :

$$A = \left(a(1) \vdots \ldots \vdots a(n)\right) \equiv \left(a_{(1)} \vdots \ldots \vdots a_{(m)}\right)^T \in R^{m \times n} ,$$

де $a(j) \in R^m$ — вектори стовпчиків, а $a_{(i)} \in R^n$ — вектори рядків матриці A , $i = \overline{1,m}$, $j = \overline{1,n}$.

Для матриці $A \in R^{m \times n}$ псевдообернену матрицю $A^+ \in R^{n \times m}$ можна визначити згідно умови:

$$\forall b \in R^m ,\ A^+ b = \arg\min_{x \in \Omega_A(b)} \|x\|^2 ,$$

де $\Omega_A(b) = Arg \min\limits_{x \in R^n} \|Ax - b\|^2$.

В практиці застосування псевдообернення важливими є матриці, які визначаються з використанням матриць A и A^+ : проекційна матриця $Z(A) = I_n - A^+ A$, а також матриця $R(A) = A^+ (A^+)^T$.

1.1. Залежність псевдообернених матриць від приєднання довільних вектор-рядків до вихідної матриці [3]. Якщо передбачити, що до матриці A добавляється новий рядок $a^T \in R^n$ після $(i-1)$ -го рядка ($i = \overline{2,\ m+1}$), тобто утворюється матриця

$$A_{i,a} = (a_{(1)} \vdots \ldots \vdots a_{(i-1)} \vdots a \vdots a_{(i)} \vdots \ldots \vdots a_{(m)})^T \in R^{(m+1)n} ,$$

то при відомій псевдооберненій матриці $A^+ \in R^{n \times m}$ для рекурентного обчислення псевдооберненої матриці $A_{i,a}^+ \in R^{n \times (m+1)}$ мають місце співвідношення — прямі формули Гревіля – Кириченка.

1.2. Залежність псевдообернених матриць від видалення довільних вектор-рядків з вихідної матриці [3]. Якщо передбачити, що для матриці $A_{i,a} \in R^{(m+1)\times n}$ (після $(i-1)$-го рядка ($i=\overline{2,\ m+1}$) матриці A стоїть вектор-рядок a^T), відома псевдообернена матриця $A_{i,a}^{+} \in R^{n\times(m+1)}$, то для обчислення псевдооберненої матриці $A^{+} \in R^{n\times m}$ (рядок a^T з матриці $A_{i,a}$ видаляється) мають місце обернені формули Гревіля – Кириченка.

2. Алгоритм лінійної класифікації сигналів [1, 2]. Нехай для точок $x(j) \in R^m$, $j=\overline{1,n}$ (додаткова компонента $x_m(j)=1$) відомо, що точки $x(i_k) \in R^m$, $k=\overline{1,\ n_1}$ знаходяться в першому класі Ω_{x1}, $\Omega_{x1}=\{x:\ x=x(i_1),...,x(i_{n_1-1}),x(i_{n_1})\}$, точки $x(i_s)= \in R^m$, $s=\overline{1,\ n_2}$ — в другому, тобто $x(j_s) \in \Omega_{x2}$.

Необхідна і достатня умова лінійної роздільності цих класів така:

$$\min_{y\in\Omega_y} y^T Z\begin{pmatrix} X^T & \cdots & J_n \end{pmatrix}^T y = y_*^T Z\begin{pmatrix} X^T & \cdots & J_n \end{pmatrix}^T y_* = 0,$$

де $X=\left(x(1)\vdots\ldots\vdots x(n)\right)\in R^{m\times n}$, $\Omega_y=\{y:\ y=(y(1),...,y(n))^T,\ \ y(i_k)\geq 1$, $k=\overline{1,\ n_1}$, $y(j_s)\leq -1$, $s=\overline{1,\ n_2}\}$, $J_n=(1,1,\ ...\ ,1)^T \in R^n$, а сам вектор $a\in R^{m+1}$, який задовольняє умові приймає значення

$$a=\begin{pmatrix} X^T & \cdots & J_n \end{pmatrix}^{+} y_*.$$

Відстань між гіперплощинами визначається виразом

$$h=2(\|a\|^2-a_{m+1}^2)^{-1/2},\ e(m+1)=(0,0,...,0,1)^T \in R^{m+1}.$$

3. Оптимізація простору векторів ознак. Якщо умова лінійної роздільності не виконується, тобто розділяючих гіперплощин між множинами $x(i_k)\in R^m$, $k=\overline{1,\ n_1}$ та $x(j_s)\in R^m$, $s=\overline{1,\ n_2}$ не виявлено, то подальший пошук розділяючих гіперплощин доцільно здійснювати за допомогою засобів збурення псевдообернених і проекційних матриць. У роботі [2] введено поняття найменш інформативної координати x_{i^*} з простору ознак, яка визначається згідно умови

$$y_*^T Z(X_{i^*}^T) y_* = \min_{i=\overline{1,n}} y_*^T Z(X_i^T) y_*,$$

$$X_i=\begin{pmatrix} x_{(1)} & \cdots & x_{(i-1)} & x_{(i+1)} & \cdots & x_{(m)} \end{pmatrix}.$$

Отже, можна чекати, що заміна найменш інформативної (чи взагалі неінформативної) компоненти x_{i^*} у векторі ознак $x=(x_1,\dots,x_m)^T$

деякою новою лінійно незалежною компонентою x_0, тобто утворення і розгляд нового вектора ознак $\left(x_1, \ldots, x_{i^*-1}, x_0, x_{i^*+1}, \ldots, x_m\right)^T$, дозволить поліпшити умову роздільності множин.

З наведеного вище, варіантом дій з поліпшенням умови лінійної роздільності множин є здійснення таких кроків:

1) серед рядків матриці X визначається найменш інформативний;
2) з усіх або частини лінійно незалежних рядків матриці X формується лінійна оболонка: P_x, $x_{(0)}^T \in P_x$, $x_{(0)}^T = \sum\limits_{\kappa \in Q} \alpha_\kappa x_{(\kappa)}^T$,

де Q — множина індексів лінійно незалежних рядків вихідної матриці X, α_κ — невизначені коефіцієнти;

3) в матриці $\begin{pmatrix} X^T & \cdots & J_n \end{pmatrix}^T$ найменш інформативний рядок заміняється рядком з оболонки P_x;
4) невизначені коефіцієнти α_κ, вектор y_* визначаються згідно наступної умови оптимальності — розширеної умову роздільності множин
$$y_*^T Z(X_{(i^*, x_{(0)})}) y_* \to \min_{x_0 \in P_x, y \in \Omega_y}.$$

При негативному результаті описаних вище дій залишається можливість побудови кусково-лінійної полоси роздільності.

4. Фільтрація роздільних підмножин до властивості кусково-лінійної класифікації сигналів [3]**.** Суть технології полягає у послідовному видаленні з навчальної вибірки таких елементів, які обумовлюють найбільше зменшення величини
$$y_*^T Z\begin{pmatrix} X^T & \cdots & J_n \end{pmatrix}^T y_*.$$

Якщо лінійна роздільність відфільтрованої підмножини Ω_x виникає за рахунок послідовного вилучення з вихідної множини декількох її членів, тобто підмножина $\Omega_x \setminus \Omega_x(1)$, де $\Omega_x(1) = \Omega_{x1}(1) \cup \Omega_{x2}(1)$, — лінійно роздільна підмножина (для неї встановлюється своя полоса роздільності), то відносно підмножини $\Omega_x(1)$ проводяться дії з забезпечення її роздільності. Процес у подальшому може здійснюватись в рамках s-кусково-лінійно роздільної множин [3]. Якщо множина Ω_x є s-кусково-лінійно роздільною, тоді підмножини $\Omega_x \setminus \Omega_x(1)$,..., $\Omega_x(s-2) \setminus \Omega_x(s-1)$, $\Omega_x(s-1)$ кусково-лінійно роздільні, будуть визначені вектори $a(1)$, ... , $a(s)$ — вектори-нормалі відповідних їм розділяючих гіперплощин, а також величини h_i, $i = \overline{1, s}$ — відстані між знайденими гіперплощинами. Для покращення якості кусково-лінійно розділення множини Ω_x є можливість збільшити міру s-кусково-лінійної роздільності $h = \min\limits_{i=\overline{1,\ s}}\{h_i\}$.

Висновки. Методи псевдообернення, теорія збурення псевдообернених і проекційних матриць, дозволяють побудувати конструктивні схеми засобів виділення у скінченому просторі дискретних точок роздільних підмножин, дозволяють оптимізувати такі процеси, використовуючи аналітичні вирази умов лінійної роздільності множин, визначити оцінки інформативності компонент векторів простору ознак, при потребі організувати перебір елементів підмножин у процесі кусково-лінійної класифікації.

Список використаних джерел:

1. Кириченко Н. Ф., Кривонос Ю. Г., Лепеха Н. П. Оптимизация синтеза гиперплоскостных кластеров и нейрофункциональных преобразований в системах классификации сигналов. *Кибернетика и системный анализ*. 2008. № 6. С. 107–124.
2. Кириченко Н. Ф., Кривонос Ю. Г., Лепеха Н. П. Синтез систем нейрофункциональных преобразователей в решении задач классификации. *Кибернетика и системный анализ*. 2007. № 3. С. 47–57.
3. Кириченко Н. Ф., Кудин Г. И. Анализ и синтез систем классификации сигналов средствами возмущений псевдобратных и проекционных операций. *Кибернетика и системный анализ*. 2009. № 3. С. 47–57.

With the use of facilities of indignation pseudoinverse matrices the offered chart of optimization of linear classification of signals. Thealgorithms of optimal transformation of separatecomponents of vectors of space of signs in a number of cases allow to decide the task of classification, remaining within the framework of linear model. At the failure of such approach an algorithm over is brought cobbed linear classification.

Key words: *synthesis of the systems of the classification, pseudoreverse and projection matrixes.*

Одержано 06.03.2017

УДК 519.8

Ю. П. Лаптин, д-р физ.-мат. наук

Институт кибернетики имени В. М. Глушкова НАН Украины, г. Киев

ИСПОЛЬЗОВАНИЕ КОНИЧЕСКОЙ РЕГУЛЯРИЗАЦИИ В ЗАДАЧАХ КВАДРАТИЧНОЙ ОПТИМИЗАЦИИ

Описывается новый подход к решению плохо обусловленных задач вычисления оценки оптимального значения невыпуклых задач квадратичной оптимизации.

Ключевые слова: *квадратичная оптимизация, Лагранжевая релаксация, оценочные задачи.*

Введение. К невыпуклым задачам квадратичной оптимизации (максимизации квадратичной формы при квадратичных ограничениях) могут быть сведены самые разные многоэкстремальные задачи. Для вычисления оценок оптимальных значений таких задач применяются Лагранжевые релаксации (см., например, [1, 2]) и SDP-релаксации (релаксации к задачам полуопределенного программирования) [3], которые в определенном смысле эквивалентны. При использовании Лагранжевых релаксаций формируются оценочные параметрические матричные задачи в пространстве двойственных переменных. Функции оценочных задач непрерывно дифференцируемы и принимают конечные значения в областях отрицательной определенности матриц функций Лагранжа исходных квадратичных задач. На границе области отрицательной определенности эти функции могут быть разрывны (в области положительной определенности принимают значения $+\infty$), а вблизи границы матрицы плохо обусловлены (причем количество близких к нулю собственных чисел может приближаться к размерности пространства), что приводит к необходимости учета этих особенностей при разработке вычислительных алгоритмов решения оценочных задач.

В работе приводятся новые подходы преодоления указанных проблем, основанные на использовании конических регуляризаций выпуклых задач оптимизации [4].

1. Квадратичные оптимизационные задачи и оценки их оптимальных значений. Постановка задачи

$$K^* = \sup K_0(x),\ x \in R^n \tag{1}$$

при ограничениях

$$K_i(x) \le 0,\ i = 1,...,m_1;\ K_j(x) = 0,\ j = m_1+1,...,N,\ m_1 < N, \tag{2}$$

где $K_i(x) = \langle A_i x, x\rangle + \langle l_i, x\rangle + c_i$, A_i — симметричные матрицы, l_i — векторы соответствующих размерностей, $c_i \in R$, $i \in \{0,1,...,N\}$.

Задача (1)–(2) — многоэкстремальная в общем случае, для вычисления оценки оптимального значения в [1] предложено использовать Лагранжеву релаксацию этой задачи. Обозначим

$$U^{-} = \left\{u = (u_1,...,u_N) : u_i \le 0,\ i = 1,...,m_1\right\}.$$

$$\psi(u) = \sup_{x \in R^n} L(x,u), \qquad (3)$$

где $L(x,u) = K_0(x) + \sum_{i=1}^{N} u_i K_i(x) = \left\langle A(u)x, x\right\rangle + \left\langle l(u), x\right\rangle + c(u)$,

$$A(u) = A_0 + \sum_{i=1}^{N} u_i A_i,\ l(u) = l_0 + \sum_{i=1}^{N} u_i l_i,\ c(u) = c_0 + \sum_{i=1}^{N} u_i c_i. \qquad (4)$$

Пусть T — множество допустимых решений задачи (1)–(2), $u \in U^{-}$, тогда

$$\psi(u) = \sup_{x \in R^n} L(x,u) \ge \sup_{x \in T} L(x,u) \ge \sup_{x \in T} K_0(x) = K^*.$$

Положим D $(\bar{D})$ — подмножества R^N, состоящие из таких $u \in U^{-}$, что $A(u)$ — отрицательно определенная (соответственно — неположительно определенная) матрица. Если $u \notin \bar{D}$, то $\psi(u) = +\infty$.

Справедливо соотношение [2]

$$\psi^* = \inf_{u \in U^{-}} \psi(u) = \inf_{u \in \bar{D}} \psi(u). \qquad (5)$$

Пусть $u \in D$, $x(u)$ — решение задачи (3). Вектор $x(u)$ — решение системы уравнений [1]

$$2A(u)x + l(u) = 0. \qquad (6)$$

Во внутренних точках множества $\bar{D}$ функция $\psi(u)$ непрерывно дифференцируема и принимает конечные значения, на границе множества $\bar{D}$ функция $\psi(u)$ может принимать как конечные значения, так и значения $+\infty$. Особенности поведения функции $\psi(u)$ вблизи границы множества $\bar{D}$ приводит к существенным проблемам при практическом решении задачи (5).

2. Коническая регуляризация задач оптимизации. В данном пункте рассматривается подход, в котором для задачи выпуклого программирования с ограничениями формируется эквивалентная задача безусловной оптимизации, целевая функция которой принимает конечные значения при любых значениях переменных. Целевая функция исходной задачи может быть не определена на границе и вне допустимой области. Предлагаемый подход обобщает результаты, изложенные в [5], и позволяет преодолевать проблемы, возникающие при решении задачи (5).

Рассмотрим задачу выпуклого программирования: найти

$$\psi^* = \inf \left\{ \psi(u) : h(u) \le 0,\, u \in R^n \right\}, \tag{7}$$

где $\psi, h : R^n \to R \cup \{+\infty\}$ — выпуклые замкнутые функции.

Обозначим $C = \left\{ u \in R^n :\ h(u) \le 0 \right\}$.

Предположение 1. $\operatorname{int} C \subseteq \operatorname{dom} \psi$, если u принадлежит границе множества C, то $h(u) = 0$.

Предположение 2. Задана точка $u^0 \in C$ такая, что $h(u^0) < 0$.

На границе множества C функция ψ может быть не определена (значение функции ψ может быть равно $+\infty$).

Из замкнутости функции ψ следует, что если $\overline{u}$ принадлежит границе множества C и для любой последовательности $u^k \in \operatorname{int} C,\ k = 1, \dots$, такой, что $u^k \to \overline{u}$ при $k \to +\infty$, выполняется $\lim\limits_{k \to \infty} \psi(u^k) < +\infty$, тогда $\overline{u} \in \operatorname{dom} \psi$.

Полученные в [5] результаты непосредственно обобщаются на рассматриваемый случай. Пусть задано некоторое число $E < \psi(u^0)$. Обозначим F надграфик функции ψ на множестве C $F = \left\{ (\lambda, u) \in R \times C : \lambda \ge \psi(u) \right\}$.

Положим $z = (\lambda, u),\ z \in R \times R^n$. Рассмотрим коническую оболочку $\mathrm{K}(E)$ надграфика F с вершиной в точке $z_E^0 = (E, u^0)$

$$\mathrm{K}(E) = \left\{ v : v \in R \times R^n,\, v = z_E^0 + \alpha(z - z_E^0), \alpha \ge 0, z \in F \right\}. \tag{8}$$

Обозначим $\overline{\mathrm{K}}(E)$ замыкание множества $\mathrm{K}(E)$. Множество $\overline{\mathrm{K}}(E)$ может рассматриваться как надграфик некоторой выпуклой функции. Эту функцию обозначим $\gamma_E(u)$ и будем называть конической аппроксимацией функции ψ на множестве C. Функция $\gamma_E(u)$ определена на всем пространстве R^n и принимает конечные значения при любых u. Пример конической аппроксимации функции показан на рисунке.

Утверждение 1. Пусть множество C ограничено. Тогда для произвольной точки $u \in R^n$, $u \ne u^0$, на луче, выходящем из точки u^0 и проходящем через u, найдется точка $\overline{u}$, $\overline{u} \in C$ (возможно не одна), такая, что $\psi(\overline{u}) = \gamma_E(\overline{u})$.

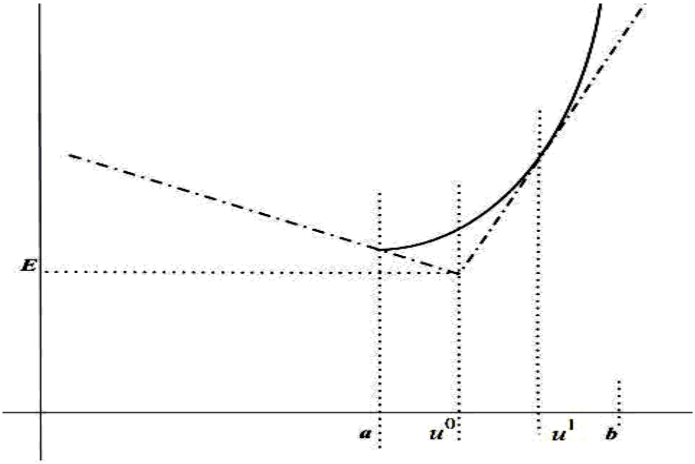


Рисунок. *Сплошной линией показана функция* $\psi(u)$, *штрихпунктирной —* $\gamma_E(u)$, *в точках* a, u^1 *значения этих функций совпадают, множество* C *— отрезок* $[a, b]$

Обозначим $\mu_E(u)$ такую точку, ближайшую к u^0. Положим

$$\eta_E(u) = \begin{cases} \left\|\mu_E(u) - u^0\right\|, & \text{если точка } \mu_E(u) \text{ существует,} \\ +\infty, & \text{в противном случае,} \end{cases}$$

$$\varphi_E(u) = \begin{cases} \psi(u), & \text{если } \left\|u - u^0\right\| \le \eta_E(u), \\ \gamma_E(u), & \text{если } \left\|u - u^0\right\| > \eta_E(u). \end{cases} \tag{9}$$

Лемма 1. Пусть для точки $u \in R^n$, $u \ne u^0$, существует точка $\mu_E(u)$, тогда

$$\gamma_E(u) = E + (\psi(\mu_E(u)) - E)\frac{\left\|u - u^0\right\|}{\left\|\mu_E(u) - u^0\right\|}. \tag{10}$$

Рассмотрим задачу: найти

$$\varphi_E^* = \inf\left\{\varphi_E(u) : u \in R^n\right\}. \tag{11}$$

Теорема 1. Пусть выполняются предположения 1, 2 и $E < \psi(x^0)$. Тогда $\varphi_E : R^n \to R$ — выпуклая функция. Если $E \le \psi^*$ то $\varphi_E^* = \psi^*$.

Задачу (11) будем называть конической регуляризацией исходной задачи (7).

Обозначим $\psi'(u,p)$ производную функции ψ в точке $u \in C$ по направлению p. Пусть зафиксирована некоторая точка u^1, положим $p = \left(u^1 - u^0\right) \Big/ \left\| u^1 - u^0 \right\|$, $t^* = \left\| \mu_E(u^1) - u^0 \right\|$, если точка $\mu_E(u^1)$ не существует, полагаем $t^* = +\infty$.

Лемма 2.

$$t^* = \sup\left\{ t : \frac{\psi(u^0 + tp) - E}{t} > -\psi'(u^0 + tp, -p), t \ge 0, u^0 + tp \in \operatorname{int} C \right\}. \quad (12)$$

Теорема 2. Пусть точка u^1 такая, что $\overline{u} = \mu_E(u^1)$ — внутренняя точка множества C. Тогда в точке $\overline{u}$ существует субградиент $\overline{g}$ функции ψ, для которого выполняется

$$\psi(\overline{u}) - E = \left\langle \overline{g}, \overline{u} - u^0 \right\rangle, \quad (13)$$

и вектор $\overline{g}$ есть субградиент функции γ_E в точке u^1 (в точке $\overline{u}$).

Теорема 3. Пусть выполняются предположения 1, 2, точка u^1, такая, что $\overline{u} = \mu_E(u^1)$ принадлежит границе множества C, тогда

1) $\overline{u} \in \operatorname{dom} \psi$,

2) $\left\langle g_h(\overline{u}), u^0 - \overline{u} \right\rangle \ne 0$ и вектор

$$g = g_\psi(\overline{u}) + \frac{E - \psi(\overline{u}) - \left\langle g_\psi(\overline{u}), u^0 - \overline{u} \right\rangle}{\left\langle g_h(\overline{u}), u^0 - \overline{u} \right\rangle} g_h(\overline{u}) \quad (14)$$

есть субградиент функции $\gamma_E(u)$ в точке u^1 (в точке $\overline{u}$), где $g_\psi(\overline{u})$, $g_h(\overline{u})$ — субградиенты функций ψ и h в точке $\overline{u}$.

При использовании предлагаемого подхода значение ψ^* обычно неизвестно. Учитывая это, величина E уточняется по ходу решения задачи (11).

Необходимо отметить, что для вычисления значения функции φ_E в произвольной точке u должна решаться задача одномерного поиска (12), что в случае общей задачи выпуклого программирования существенно увеличивает трудоемкость по сравнению с вычислением значения функции ψ в допустимой точке.

Однако для задачи, которая формируется при использовании Лагранжевой релаксации для вычисления оценки оптимального значения квадратичной задачи (1)–(2), в работе [4] был предложен подход, позволяющий решать задачу одномерного поиска (12) за время, соизмеримое с вычислением значения функции ψ в допустимой точке.

Выводы. В работе для вычисления оценки оптимального значения задачи квадратичной оптимизации предложено использовать коническую регуляризацию оценочной задачи. Такой подход позволяет построить эквивалентную задачу безусловной оптимизации, целевая функция которой определена на всем пространстве переменных задачи и удовлетворяет условию Липшица. Показано, что особенностью рассмотренного класса задач является возможность построения эффективных алгоритмов поиска по направлению. Такие алгоритмы являются существенными для использования конической регуляризации. Трудоемкость вычисления функций и субградиентов регуляризованной задачи оказывается соизмеримой с трудоемкостью вычисления функций исходной оценочной задачи. Полученные результаты будут полезны при разработке эффективных методов решения оценочных задач квадратичной оптимизации. Автор выражает глубокую благодарность Березовскому О.А. за ценные замечания и советы по данной работе.

Список использованной литературы:

1. Шор Н. З., Стеценко С. И. Квадратичные экстремальные задачи и недифференцируемая оптимизация. Киев: Наук. думка, 1989. 204 с.
2. Березовский О. А., Стецюк П. И. Об одном способе нахождения двойственных квадратичных оценок Шора. *Кибернетика и системный анализ.* 2008. № 2. С. 89–99.
3. Boyd S., Vandenberghe L. Semidefinite programming relaxations of non-convex problems in control and combinatorial optimization. *Communications, Computation, Control, and Signal Processing.* Springer US, 1997. C. 279–287.
4. Лаптин Ю. П. Коническая регуляризация в задачах квадратичной оптимизации. *Компьютерная математика.* 2016. № 2. С. 129–141.
5. Лаптин Ю. П., Бардадым Т. А. Некоторые подходы к регуляризации нелинейных задач оптимизации. *Проблемы управления и информатики.* 2011. № 3. С. 57–68.

It describes a new approach to solving the ill conditioned computational task for estimating the optimal value of non-convex quadratic optimization problems.

Key words: *quadratic optimization, Lagrange relaxation, estimating problems.*

Получено 15.02.2017

УДК 519.6

О. М. Литвин, д-р фіз.-мат. наук, професор,
О. В. Ярмош, канд. фіз.-мат. наук, доцент,
Т. І. Чорна, старший викладач

Українська інженерно-педагогічна академія, м. Харків

МЕТОД СПЛАЙН-ІНТЕРЛІНАЦІЇ ФУНКЦІЇ 4-Х ЗМІННИХ ПРИ ЗНАХОДЖЕННІ НАЙБІЛЬШОГО (НАЙМЕНШОГО) ЇЇ ЗНАЧЕННЯ В $[0,1]^4$

Представлено оператори сплайн-інтерлінації на системі взаємно перпендикулярних прямих, побудовані за допомогою операторів сплайн-інтерфлетації функції 4-х змінних, для розв'язання задачі знаходження найбільшого та найменшого значень неперервної функції 4-х змінних в замкнутій області $D \in [0,1]^4$.

Ключові слова: *оператори сплайн-інтерлінації, оператори сплайн-інтерфлетації, сліди функції, система взаємно перпендикулярних прямих.*

Вступ. Задача знаходження найбільшого (найменшого) значення функції 4-х змінних в замкнутій області $D \in [0,1]^4$ є однією з важливих задач теорії і практики. Для її розв'язання широко використовуються класичні методи, такі як симплекс-метод, метод покоординатного спуску, метод яру, метод Монте-Карло тощо [1, 2]. Як відомо, в деяких ітераційних методах наближення збігається до екстремальної точки повільно, інколи «перескакуючи» цю точку.

Базуючись на результатах, описаних у [3, 4], а також у [5], в даній роботі пропонується метод розв'язання заданої задачі, який має однакові обчислювальні властивості у віддалених точках від точки максимуму (мінімуму) і при цьому асимптотично гарантує отримання екстремальної точки з потрібною точністю.

Виклад основного матеріалу. Метод полягає в наступному. Розбиваємо область $[0,1]^4$ на m гіперпаралелепіпедів площинами $x_i = X_{i,k_i} = \dfrac{k_i}{m_i},\ k_i = \overline{0, m_i},\ i = \overline{1,4}$. Ці площини розбивають куб $[0,1]^4$ на паралелепіпеди вигляду

$$\Pi_{k_1,k_2,k_3,k_4} = \left\{ x_i \left[\frac{k_i}{m_i}, \frac{k_i+1}{m_i} \right], 0 \le k_i m_i - 1,\ k_i = \overline{0, m_i},\ i = \overline{1,4} \right\}.$$

Ребрами цих гіперпаралелепіпедів будуть прямі вигляду

$$\Gamma^{(1)}_{k^{(1)}} = \left\{ x \in D : 0 \le x_1 1,\ x_2 = X_{2,k_2},\ x_3 = X_{3,k_3},\ x_4 = X_{4,k_4} \right\};$$

$$\Gamma^{(2)}_{k^{(2)}} = \left\{ x \in D : x_1 = X_{1,k_1},\ 0 \le x_2 1,\ x_3 = X_{3,k_3},\ x_4 = X_{4,k_4} \right\};$$

$$\Gamma^{(3)}_{k^{(3)}} = \left\{ x \in D : x_1 = X_{1,k_1},\ x_2 = X_{2,k_2},\ 0 \le x_3 1,\ x_4 = X_{4,k_4} \right\};$$

$$\Gamma^{(4)}_{k^{(4)}} = \left\{ x \in D : x_1 = X_{1,k_1},\ x_2 = X_{2,k_2},\ x_3 = X_{3,k_3},\ 0 \le x_4 \le 1 \right\}.$$

Розглядаємо функції $f(x) \in C^r \left[0,1\right]^4$, $0 \le r \le r'$, $r' \ge 0$, $x = (x_1,...,x_4)$, які є неперервними разом із всіма частинними похідними до порядку r включно в області $\left[0,1\right]^4$. Для цієї функції вважаємо відомими сліди: $F_{i,k^{(i)}}(x_i) = f(x)|_{x\in\Gamma^{(i)}_{k^{(i)}}}$, де $k^{(i)} = (k_1^{(i)},...,k_{i-1}^{(i)},k_{i+1}^{(i)},...,k_4^{(i)}),\ i = \overline{1,4},\ k^{(i)} = \overline{0,m}$.

Таким чином, кожна змінна x приймає $(m_i + 1)$ різних значень $X_{i,k_i} = \dfrac{k_i}{m_i},\ 0 \le k_i m_i,\ i = \overline{1,4}$. Перпендикулярно до граней $x_4 = 0$ або $x_4 = 1$ будуть проходити (перетинати 4-вимірний куб) рівно $(m_1 + 1)\times(m_2 + 1)\times(m_3 + 1)$ прямих, ортогональних цим граням.

Аналогічно перпендикулярно до граней $x_3 = 0$ або $x_3 = 1$ область D буде перетинати $(m_1 + 1)\times(m_2 + 1)\times(m_4 + 1)$ прямих, перпендикулярно до граней $x_2 = 0$ або $x_2 = 1$ — $(m_1 + 1)\times(m_3 + 1)\times(m_4 + 1)$ прямих, перпендикулярно до граней $x_1 = 0$ або $x_1 = 1$ — $(m_2 + 1)\times(m_3 + 1)\times(m_4 + 1)$ прямих. Тобто загальна кількість таких прямих визначається числом $Q(m_1, m_2, m_3, m_4) = \sum\limits_{i=1}^{4} \prod\limits_{j=1,\, j\ne i}^{4} (m_j + 1)$.

Метод наближеного знаходження найбільшого (найменшого) значень функції $f(x)$ в 4-вимірному кубі полягає у знаходженні координат точок, в яких сліди $F(x) = f(x)|_{x\in \Gamma^{(i)}_{k^{(i)}}}$ досягають свого найбільшого (найменшого) значення для $0 \le x_i \le 1,\ i = \overline{1,4}$, і з подальшим знаходженням найбільших (найменших) значень на всій сукупності знайдених найбільших (найменших) значень при кожному i.

Для обґрунтування досліджуваного методу пропонується застосовувати оператори сплайн-інтерлінації з використанням допоміжних функцій у вигляді сплайнів першого степеня функції $f(x)|_{x\in \Gamma^{(i)}_{k^{(i)}}}$, які на кожній з вказаних систем прямих, паралельних осям OX_i, $i=\overline{1,4}$, мають ті ж сліди, що й функція $f(x)$.

Для цього використаємо такий алгоритм, який опишемо по кроках.

Крок 1. Будуємо оператори

$$O_i f(x)=\sum_{k_i=0}^{m_i} h_{i,k_i}(x_i)\times f(x)|_{x\in\Gamma^{(i)}_{k(i)}},$$

де $h_{i,k_i}(x_i)=\begin{cases}0,\ x_i\le\dfrac{k_i-1}{m_i},\\ m_i x_i-k_i+1,\ \dfrac{k_i-1}{m_i}<x_i\le\dfrac{k_i}{m_i},\\ k_i+1-m_i x_i,\ \dfrac{k_i}{m_i}<x_i<\dfrac{k_i+1}{m_i},\\ 0,\ x_i\ge\dfrac{k_i+1}{m_i}.\end{cases}$

Крок 2. Будуємо оператор

$$\begin{aligned}O^{(4)}f(x)&=\sum_{j_1=1}^{4}O_{j_1}f(x)-\sum_{j_1=1}^{3}\sum_{j_2=j_1+1}^{4}O_{j_1}O_{j_2}f(x)+\\&+\sum_{j_1=1}^{2}\sum_{j_2=j_1+1}^{3}\sum_{j_3=j_2+1}^{4}O_{j_1}O_{j_2}O_{j_3}f(x)-O_{j_1}O_{j_2}O_{j_3}O_{j_4}f(x).\end{aligned}\tag{1}$$

Теорема 1. Оператор $Of(x)$ вигляду (1) — це оператор інтерфлетації функції $f(x)$ між системою взаємно перпендикулярних гіперплощин $x_i=X_{i,k_i}=\dfrac{k_i}{m_i}$, $k_i=\overline{0,m_i}$, $i=\overline{1,4}$, з властивостями $Of(x)|_{x_p=X_{p,k_p}}=$ $=f(x)|_{x_p=X_{p,k_p}}$, $0\le k_p m_p$, $p=\overline{1,4}$.

Доведення. Покладемо в формулі $Of(x)$ (1) $x_4=\dfrac{k_4}{m_4}$. Тоді перша група доданків буде мати вигляд: перший оператор — $O_1 f(x_1,x_2,x_3,\dfrac{k_4}{m_4})$, другий — $O_2 f(x_1,x_2,x_3,\dfrac{k_4}{m_4})$, третій — $O_3 f(x_1,x_2,x_3,\dfrac{k_4}{m_4})$, четвертий оператор в точці $(x_1,x_2,x_3,\dfrac{k_4}{m_4})$ буде рівний $f(x_1,x_2,x_3,\dfrac{k_4}{m_4})$.

Друга група доданків

$$O_1O_2f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_4f(x)\Big|_{x_4=\frac{k_4}{m_4}}+$$

$$+O_2O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_2O_4f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_3O_4f(x)\Big|_{x_4=\frac{k_4}{m_4}}=$$

$$=O_1O_2f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1f(x)\Big|_{x_4=\frac{k_4}{m_4}}+$$

$$+O_2O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}+O_2f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}.$$

Третя група доданків

$$O_1O_2O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_2O_4f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_3O_4f(x)\Big|_{x_4=\frac{k_4}{m_4}}+$$

$$+O_2O_3O_4f(x)\Big|_{x_4=\frac{k_4}{m_4}}=O_1O_2O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_2f(x)\Big|_{x_4=\frac{k_4}{m_4}}+$$

$$+O_1O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_2O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}.$$

Четвертий доданок $O_{j_1}O_{j_2}O_{j_3}O_{j_4}f(x)$ в точці $(x_1,x_2,x_3,\frac{k_4}{m_4})$ буде рівний $O_1O_2O_3f(x)$.

Таким чином, підставивши отримані доданки у формулу оператора (1), маємо

$$O^{(4)}f(x)=O_1f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_2f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+$$

$$+f(x)\Big|_{x_4=\frac{k_4}{m_4}}-O_1O_2f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}-O_1O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}-$$

$$-O_1f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}-O_2O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}-O_2f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}-$$

$$-O_3f(x)\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_2O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}+O_1O_2f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}+$$

$$+O_1O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}+O_2O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}-O_1O_2O_3f(x)\,\Big|_{x_4=\frac{k_4}{m_4}}=f(x)\,\Big|_{x_4=k_4/m_4}.$$

Теорема доведена.

Для побудови операторів сплайн-інтерлінації функції 4-х змінних замінимо в операторах $O_if(x)$ всі функції $f(x_1,x_2,x_3,x_4)$ операторами

$$f(X_{1,i}=\frac{k_p}{m_i},x_2,x_3,x_4)\approx\sum_{p=1,\,p\neq i}^{4}\left(\prod_{j=1,\,j\neq i,\,j\neq p}^{4}O_j\right)f(X_1,i,x_2,x_3,x_4).$$

Теорема 2. Оператор

$$L_4 f(x) = \sum_{k=1}^{4} \prod_{i=1, i\neq k}^{4} O_i f(x) - 3\prod_{i=1}^{4} O_i f(x) \quad (2)$$

є оператором інтерлінації функції 4-х змінних на вказаній множині $(m_1+1)\times(m_2+1)\times(m_3+1)$ прямих з властивостями:

$$L_4 f(x)|_{x\in\Gamma^{(i)}_{k^{(i)}}} = f(X_{1,k_1^{(1)}}, X_{2,k_2^{(1)}}, X_{3,k_3^{(i)}}, x_4),\ 0 \le k_i^{(i)} m_i,\ i=\overline{1,4}\ .$$

Доведення. Для функції 4-х змінних оператор матиме вигляд

$$L_4 f(x)|_{x\in\Gamma^{(i)}_{k^{(i)}}} = (O_1O_2O_3 + O_1O_2O_4 + O_1O_3O_4 + O_2O_3O_4 - 3O_1O_2O_3O_4) f(x)|_{x\in\Gamma^{(i)}_{k^{(i)}}} =$$

$$= f(\frac{k_1}{m_1}, \frac{k_2}{m_2}, \frac{k_3}{m_3}, x_4) + O_4 f(\frac{k_1}{m_1}, \frac{k_2}{m_2}, \frac{k_3}{m_3}, x_4) + O_4 f(\frac{k_1}{m_1}, \frac{k_2}{m_2}, \frac{k_3}{m_3}, x_4) +$$

$$+ O_4 f(\frac{k_1}{m_1}, \frac{k_2}{m_2}, \frac{k_3}{m_3}, x_4) - 3O_4 f(\frac{k_1}{m_1}, \frac{k_2}{m_2}, \frac{k_3}{m_3}, x_4) = f(\frac{k_1}{m_1}, \frac{k_2}{m_2}, \frac{k_3}{m_3}, x_4).$$

Отже, **теорема доведена.**

Висновки. Запропонований алгоритм використання методу сплайн-інтерлінації для знаходження найбільшого або найменшого значення функції 4-х змінних, який має однакові обчислювальні властивості у віддалених точках від точки максимуму (мінімуму) і при цьому асимптотично гарантує отримання екстремальної точки з потрібною точністю.

Список використаних джерел:

1. Гаврилюк І. П., Макаров В. Л. Методи обчислень: Підручник: У 2 ч. К.: Вища шк., 1995. Ч. 1. 367 с.
2. Гаврилюк І. П., Макаров В. Л. Методи обчислень: Підручник: У 2 ч. К.: Вища шк., 1995. Ч. 2. 431 с.
3. Литвин О. М. Інтерлінація функції та деякі її застосування. Харків: Основа, 2002. 544 с.
4. Литвин О. М. Методи обчислень. Додаткові розділи: Навч. посіб. К.: Наук. думка, 2005. 332 с.
5. Литвин, О. М., Ярмош О. В., Чорна Т. І. Метод сплайн-інтерлінації при знаходженні найбільших (найменших) значень функції двох змінних в замкнутій області [Текст] Бионика интеллекта. 2016. № 2 (87). С. 77–82.

In this article the operators of spline interlineation on the system mutually perpendicular lines, built by means of operators of spline interflatation function of four variables is proposed for the solution of task of finding the largest and the least values of continuous function of four variables in the closed domain it is offered to use.

Key words: *operators of spline-interlineation, operators of spline-interfletation, tracks of function, system of mutually perpendicular lines.*

Одержано 21.02.2017

УДК 519.64;519.65

Л. В. Луц, канд. фіз.-мат. наук,
В. К. Задірака, д-р фіз.-мат. наук, професор, академік НАН України
Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

НАБЛИЖЕНЕ ІНТЕГРУВАННЯ ШВИДКООСЦИЛЮЮЧИХ ФУНКЦІЙ З ВИЯВЛЕННЯМ І УТОЧНЕННЯМ АПРІОРНОЇ ІНФОРМАЦІЇ

Наведений алгоритм виявлення та уточнення вихідної інформації про підінтегральну функцію для задачі наближеного інтегрування швидкоосцилюючих функцій.

Ключові слова: *апріорна інформація, класи функцій, інтеграли від швидкоосцилюючих функцій.*

Вступ. При розв’язуванні багатьох класів задач обчислювальної та прикладної математики виникає необхідність в обчисленні інтегралів вигляду

$$I(\omega)=\int_a^b f(x)\begin{Bmatrix} e^{-i\omega x} \\ \sin\omega x \\ \cos\omega x \end{Bmatrix}\cos\omega x\, dx, \tag{1}$$

де $f(x)\in F$, F — множина функцій, визначених на відрізку $[a,b]$. Інформація про функцію $f(x)$ задана не більше ніж N значеннями інформаційного оператора, наприклад, значеннями функції $f(x)$ не більше ніж в N вузлових точках $\{x_\nu\}_0^{N-1}$ з відрізку $[a,b]$, ω — довільне дійсне число ($|\omega|\geq 2\pi(b-a)$).

Практично важливим є розгляд випадку, коли $\{x_i\}_0^{N-1}$ і $\{f_i\}_0^{N-1}=\{f(x_i)\}_0^{N-1}$ фіксовані (наприклад, випадок, коли функція задана таблицею значень з її області визначення). Такий спосіб представлення вхідної інформації веде до значного звуження відповідного класу F на інтерполяційні класи F_N. Також розглядатимемо класи $F_{N,\varepsilon}$, які відповідають наближеному заданню вихідної інформації з області $\left|\tilde{f}_i-f_i\right|\leq\varepsilon$, $i=\overline{0,N-1}$.

Постановка задачі. Нехай задача $P(I)$ розв'язується алгоритмом $A(X)$ на ЕОМ $c(Y)$, $c(Y)$ — модель комп'ютера, $c(Y)\in C(Y)$

($C(Y)$ — клас моделей комп'ютерів), I, X, Y — скінченні множини (вектори) параметрів, від яких істотно залежать відповідно P, A, C [1].

Загальну ситуацію побудови обчислювальних алгоритмів (о.а.), що дозволяють обчислювати інтеграли (1) з точністю ε ($\varepsilon > 0$) при обмежених обчислювальних ресурсах, можна описати наступним чином.

Потрібно розробити або вибрати серед відомих таку о.а.-програму $a \in A\left(\varepsilon, I, X, Y\right)$, де $A\left(\varepsilon, I, X, Y\right)$ — множина о.а. — програм, орієнтованих на розв'язання задачі обчислення інтегралів $I_j(\omega)$, $j = \overline{1,3}$, яка забезпечує при вибраній архітектурі комп'ютера $c(Y)$ обчислення $I_j(\omega)$, $j = \overline{1,3}$ із заданими характеристиками якості:

$$E(I, X, Y) \le \varepsilon, \tag{2}$$

$$T(I, X, Y, \varepsilon) \le T_0(\varepsilon), \tag{3}$$

$$M(I, X, Y, \varepsilon) \le M_0(\varepsilon), \tag{4}$$

де ε, T_0, M_0 — задані числа. Наближений розв'язок задачі (1), що задовольняє умові (2), називається ε-розв'язком. О.а. — програма, яка задовольняє умовам (2)–(3), називається T-ефективною.

Оскільки характеристики $E(I, X, Y)$, $T(I, X, Y, \varepsilon)$, $M(I, X, Y, \varepsilon)$, як правило, точно не відомі, то розглядаються деякі оцінки цих характеристик. Отримання якісних апріорних оцінок, зокрема, оцінок точності E та її складової — похибки методу, є одним з вагомих резервів оптимізації обчислень для покращення якості о.а.-програм розв'язування задачі наближеного інтегрування швидкоосцилюючих функцій (1). В цьому сенсі дуже складно переоцінити важливість виявлення та уточнення апріорної інформації про задачу, оскільки:

1) чим якісніша інформація про задачу, тим якісніший наближений розв'язок, на який ми можемо розраховувати;
2) максимальне використання усієї наявної інформації про задачу дає змогу звузити клас задач, що розв'язуються, і тим самим підвищує потенційну спроможність чисельного методу;
3) чим точніша вихідна інформація, тим точніші оцінки похибки і менша область невизначеності наближеного розв'язку;
4) на аналізі оцінок похибки ґрунтується комп'ютерна технологія розв'язування задач із заданими характеристиками якості за точністю і швидкодією.

У даній роботі розглянемо алгоритм, який дозволяє, використовуючи дискретну інформацію про підінтегральну функцію $f(x)$, зробити певні висновки про її властивості, занурити її у відповідний клас F, а також звузити цей клас за рахунок більш точного визначення його параметрів, таких як порядок диференційованості, показник Гельдера чи константа Ліпшиця. Для побудови алгоритму, використаємо результати роботи [2].

Припустимо, що інформація про функцію $f(x)$ задана N значеннями функції $f_\nu = f(x_\nu)$ у вузлах сітки

$$\Delta : a = x_0 < x_1 < \ldots < x_{N-1} = b\ .$$

Для спрощення викладок припустимо, що сітка Δ — рівномірна, $N = 2^\gamma + 1$, крок $h = (b-a)/N$.

Задамо послідовність сіток

$$\Delta^\lambda : a = x_0^\lambda < x_1^\lambda < \ldots < x_{N_\lambda - 1}^\lambda = b\,,$$

які складені із вузлів сітки Δ і задовільняють умовам:

$$N_\lambda = 2^\lambda + 1\,,\ \lambda = \overline{1,\gamma}\,,\ N_\gamma = N\,,\ \Delta^\gamma = \Delta\,.$$

Тоді для кожної з сіток послідовності задані f_ν^λ — значення функції $f(x)$, $x \in [a,b]$, у вузлах сітки Δ^λ, $f_\nu^\lambda = f(x_\nu^\lambda)$.

Спираючись на результати роботи [3], можна стверджувати, що існує метод побудови апроксиманта $S_\lambda(x)$ за значеннями $f(x)$ у вузлах сітки Δ^λ, такий, що наближає функцію $f(x)$, яка має на відрізку $[a,b]$ неперервну похідну порядку m з модулем неперервності $\omega(f^{(m)}, h_\lambda)$ з похибкою

$$E(f, S_\lambda) = \max_{x \in [a,b]} \left| f(x) - S_\lambda(x) \right| \le O(h_\lambda{}^m \cdot \omega(f^{(m)}, h_\lambda))\,, \tag{5}$$

де h_λ — крок сітки Δ_λ.

Припустимо також, що

$$\omega(f^{(m)}, h_\lambda) = O(h_\lambda{}^\alpha)\,,\ 0 < \alpha \le 1\,. \tag{6}$$

Тоді вираз (5) можна представити як

$$E(f, S_\lambda) \le O(h_\lambda{}^{m+\alpha})\,. \tag{7}$$

У роботі [3] доведено, що співвідношення (7) виконується, наприклад, для похибки $E(f, S_\lambda)$ відновлення функції $f(x)$ інтерполяційним сплайном $S_\lambda(x)$. Позначивши $\beta = m + \alpha$, вираз (7) при досить малому h_λ можна наближено записати як

$$E(f, S_\lambda) \approx C h_\lambda{}^\beta\,, \tag{8}$$

де C — деяка константа.

Із співвідношення (8) випливає очевидна наближена рівність

$$\frac{E(f, S_\lambda)}{E(f, S_{\lambda+1})} \approx \left(\frac{h_\lambda}{h_{\lambda+1}} \right)^\beta,$$

з якої можна отримати оцінку β_λ величини β:

$$\beta_\lambda = \frac{\log[E(f,S_\lambda)/E(f,S_{\lambda+1})]}{\log(h_\lambda/h_{\lambda+1})}. \tag{9}$$

При $\lambda = 1,2,...,\gamma$, отримаємо послідовність β_1, β_2, … , β_γ оцінок для β. Шляхом виявлення тенденції у поведінці послідовності β_λ, $\lambda = 1,2,...,\gamma$, можна наближено визначити β.

Нехай для деяких членів послідовності β_λ виконується нерівність

$$\left|\beta_{\lambda_1+s} - \beta_{\lambda_1}\right| \le \delta_1, \tag{10}$$

де s — деяке ціле додатнє число, δ_1 — досить мала додатня величина. Ця нерівність з деякою вірогідністю говорить про те, що величини β_λ застабілізувалися і за наближене значення β можна прийняти $\tilde{\beta} = \beta_{\lambda_1+s}$. Якщо не вдається встановити нерівність (10), то це може бути пов'язане, по-перше, з тим, що якісь із припущень (5)–(7) не виконуються; по-друге, з похибкою вхідних даних та заокруглень; по-третє, з тим, що вхідної інформації недостатньо для виявлення тенденції, наприклад, N не достатньо велике. Ці висновки можна використати для визначення подальших напрямків продовження дослідження.

Вище припускалося, що вхідні дані задачі точно. Нехай тепер

$$\left|f_\nu^\lambda - f(x_\nu^\lambda)\right| < \varepsilon_\nu, \ \nu = \overline{1,N_\lambda}, \ \varepsilon_\nu > 0, \ \varepsilon = \max_\nu \varepsilon_\nu. \tag{11}$$

Позначимо $S_{\lambda,\varepsilon}(x)$ — функцію, побудовану за наближеними вхідними даними тим же методом, що і функція $S_\lambda(x)$. Тоді похибка наближення функції $f(x)$ за допомогою функції $S_{\lambda,\varepsilon}(x)$ обмежена сумою похибки методу наближення $f(x)$ функцією $S_\lambda(x)$ і похибки, що виникає у наслідок неточності задання вихідних даних:

$$E(f,S_{\lambda,\varepsilon}) \le E(f,S_\lambda) + E(S_\lambda,S_{\lambda,\varepsilon}).$$

З результатів роботи [3] випливає, що у випадку, коли $f(x)$ має на відрізку $[a, b]$ неперервну похідну порядку m, яка задовільняє умовам (5)–(6), і за апроксимант береться інтерполяційний сплайн з рівновіддаленими вузлами на скінченному відрізку $S_\lambda(x)$, то побудований за наближеними значеннями функції $f(x)$ сплайн $S_{\lambda,\varepsilon}(x)$ відрізняється від $S_\lambda(x)$ у вузлах сітки на величини, що не перевищують ε і при цьому

$$E(S_\lambda,S_{\lambda,\varepsilon}) \le O(\varepsilon), \ E(f,S_{\lambda,\varepsilon}) \le O(h_\lambda^{m+\alpha}) + O(\varepsilon).$$

Оптимальною за порядком точності сіткою при заданому ε є сітка з кроком $h_\lambda = O(\varepsilon^{1/(m+\alpha)})$. У цьому випадку $E(f,S_{\lambda,\varepsilon}) \le O(\varepsilon)$.

Наведемо покроковий опис розглянутого алгоритму.

Алгоритм виявлення та уточнення вихідної інформації.

Крок 1. На відрізку $[a,b]$ будуємо рівномірні (з кроками h_i) сітки $\Delta^i : a = x_0^i < x_1^i < \ldots < x_{N_i-1}^i = b$, кількість вузлів яких $N_i = 2^i + 1$, $i = i_0, i_0+1, \ldots, \gamma$, де початкове значення i_0 та кінцеве γ — задані, $i_0 << \gamma$.

Крок 2. Як апроксимант функції $f(x)$ використаємо локальний параболічний сплайн $S_i(x)$. Як сказано вище, для нього виконується співвідношення (8).

Обчислюємо наближене значення $E(f, S_i)$ за формулою:

$$E(f, S_i) = \max_{k,j} \left| f(z_{k,j}^i) - S_i(z_{k,j}^i) \right|,$$

де $z_{k,j}^i = x_k^i + j\dfrac{h_i}{n_i}$, $k = \overline{0, N_i - 1}$, $j = \overline{1, n_i}$, n_i — задане.

Крок 3. За формулою (9) обчислюємо оцінки β_i. Перевіряємо співвідношення

$$\left|\beta_i - \beta_{i-1}\right| \le \overline{\delta}, \tag{12}$$

де $\overline{\delta}$ — задане.

Якщо для деякого $i = l$, $l < \gamma$ нерівність (12) виконується, то переходимо на крок 4.

Якщо серед членів послідовності $\{\beta_i\}$, $i = i_0, i_0+1, \ldots, \gamma$ не знайшлося такого, для якого виконується нерівність (12), то переходимо на крок 5.

Крок 4. Обчислюємо n наступних β_{l+r}, $r = \overline{1, n}$, n — задане, виконання нерівності

$$\left|\beta_{l+r} - \beta_l\right| \le \overline{\delta}. \tag{13}$$

Якщо вона виконується, то вважатимемо, що закономірність у поведінці членів послідовності $\{\beta_i\}$ виявлена, покладаємо $\tilde{\beta} = \beta_{l+n}$ і переходимо на крок 6. Якщо ні, то при $l < \gamma$ переходимо на крок 3 та перевіряємо виконання нерівності (12) для наступних членів послідовності $\{\beta_i\}$, починаючи з $\beta_i = \beta_{s+1}$, при $s \ge \gamma$, переходимо на крок 5.

Крок 5. Тенденцію у поведінці β_i не виявлено. Цей результат може бути пов'язаний, зокрема, з тим, що якісь із припущень (5)–(7) не виконуються, наприклад, функція $f(x)$ не має похідної порядка m, яка задовольняє умові Гельдера з показником α, або з великою похибкою вхідних даних та заокруглень, або з тим, що вхідної інформації недостатньо для виявлення тенденції, наприклад, N і відповідно γ не достатньо великі. Потрібно продовжити дослідження з метою усунення вищеназваних причин.

Крок 6. Маючи уточнену оцінку $\tilde{\beta} = m + \alpha$, знаходимо $m = [\tilde{\beta}]$, $\alpha = \tilde{\beta} - [\tilde{\beta}]$, де $[\tilde{\beta}]$ — ціла частина числа $\tilde{\beta}$.

Щоб знайти наближене значення константи Гельдера функції $f(x)$, скористаємось наступними результатами: у [3] доведено, що у випадку, коли функція $f(x)$ має похідну порядка m ($m = 0, 1, 2, 3$), яка задовольняє умові Гельдера з показником α, наближається інтерполяційним параболічним або кубічним сплайном $S_{n,\lambda,\varepsilon}(x)$ ($n = 2, 3$ — степінь сплайна) з рівновіддаленими вузлами на скінченному відрізку $[a,b]$, побудованим за наближеними вхідними даними (11), то для похибки наближення m-ї похідної функції $f(x)$ m-ю похідною сплайна $S_{n,\lambda,\varepsilon}(x)$ маємо наступну оцінку:

$$E(f^{(m)}, S^{(m)}_{n,\lambda,\varepsilon}) \le O(h_\lambda^{n+\alpha-m}) + \varepsilon \cdot O(h_\lambda^{-m}),\ n = 2, 3,\ m = \overline{0,n}.$$

Отже, оптимальною за порядком точності сіткою при заданому ε є сітка з кроком

$$h_\lambda = O(\varepsilon^{1/(n+\alpha)}) \qquad (14)$$

і в цьому випадку

$$E(f^{(m)}, S^{(m)}_{\lambda,\varepsilon}) \le O(\varepsilon^{(n+\alpha-m)/(n+\alpha)}). \qquad (15)$$

Отже, виберемо сітку $\Delta^\lambda : a = x_0^\lambda < x_1^\lambda < \ldots < x_{N_\lambda - 1}^\lambda = b$, з кроком h_λ, що задовільняє умові (14) і за наближене значення константи Гельдера функції $f^{(m)}(x)$ приймемо величину

$$\tilde{L} = \max_{0 \le \nu \le n} \frac{\left| S^{(m)}_{n,\lambda,\varepsilon}(x_\nu) - S^{(m)}_{n,\lambda,\varepsilon}(x_{\nu-1}) \right|}{\left| x_\nu - x_{\nu-1} \right|^\alpha}. \qquad (16)$$

Обчисливши за допомогою даного алгоритму оцінки m, α та $\tilde{L}$, «занурюємо» функцію $f(x)$ в один з класів функцій F, F_N або $F_{N,\varepsilon}$, для яких відомі оптимальні за точністю або близькі до них методи розв'язування задачі наближеного інтегрування швидкоосцилюючих функцій [1], і будуємо розв’язок задачі (1), який задовільняє умови (2)–(4).

Висновки. У роботі побудовано алгоритм, який дозволяє, використовуючи дискретну інформацію про підінтегральну функцію $f(x)$, уточнити такі її параметри, як порядок диференційованості, показник Гельдера, константа Ліпшиця, «занурити» її у відповідний клас F,

F_N або $F_{N,\varepsilon}$, що надає змогу отримати якісний наближений розв'язок задачі (1) і більш точні оцінки похибки цього розв'язку.

Список використаних джерел:

1. Сергієнко І. В., Задірака В. К., Литвин О. М., Мельникова С. С., Нечуйвітер О. П. Оптимальні алгоритми обчислення інтегралів від швидкоосцилюючих функцій та їх застосування. Т. 1. Алгоритми; Т. 2. Застосування. Киев: Наук. думка, 2011. 448 с.; 348 с.
2. Березовский А. И., Кондратенко О. С. О выявлении и уточнении априорной информации. *Управляющие системы и машины*. 1997. № 6. С. 17–22.
3. Стечкин С. Б., Субботин Ю. Н. Сплайны в вычислительной математике. М.: Наука, 1976. 248 с.

An algorithm for identifying and clarifying the priori information about the integrand for the problem of rapidly oscillating functions approximate integration is presented.

Key words: *the priori information, the function classes, rapidly oscillating functions approximate integration.*

Одержано 28.02.2017

УДК 519.65

П. С. Малачівський*, д-р. техн. наук, професор,
Б. Р. Монцібович*, канд. фіз.-мат. наук, доцент,
Я. В. Пізюр,** канд. фіз.-мат. наук, доцент,
Р. П. Малачівський,** інженер

*Центр математичного моделювання Інституту прикладних проблем механіки і математики імені Я. С. Підстригача НАН України, м. Львів,
**Національний університет «Львівська політехніка», м. Львів

АЛГОРИТМ РІВНОМІРНОГО НАБЛИЖЕННЯ ФУНКЦІЙ БАГАТЬОХ ЗМІННИХ

Запропоновано алгоритм побудови рівномірного наближення функцій багатьох змінних як граничного наближення у нормі простору L^p при $p \to \infty$. Він ґрунтується на використанні методу найменших квадратів зі змінною ваговою функцією. Запропоновано спосіб послідовного уточнення вагової функції.

Ключові слова: *функції багатьох змінних, рівномірне наближення.*

Вступ. Нехай неперервну функцію n змінних $f\left(x_1, x_2, ..., x_n\right)$ задану для $x_i \in \left[\alpha_i, \beta_i\right]$, $i = \overline{1, n}$ необхідно наблизити виразом $F_m\left(a; x_1, x_2, ..., x_n\right)$, де $F_m\left(a; x_1, x_2, ..., x_n\right)$ — узагальнений поліном

$$F_m\left(a; x_1, x_2, ..., x_n\right) = \sum_{i=0}^{m} a_i \varphi_i\left(x_1, x_2, ..., x_n\right) \qquad (1)$$

за системою базисних функцій $\varphi_i\left(x_1, x_2, ..., x_n\right)$, $i = \overline{0, m}$, де a_i, $i = \overline{0, m}$ — невідомі параметри: $\left\{a_i\right\}_{i=0}^{m} \in A$, $A \subseteq R^m$, R^m — m-вимірний векторний простір. Вираз $F_m\left(a^*; x_1, x_2, ..., x_n\right)$ називатимемо рівномірним наближенням функції $f\left(x_1, x_2, ..., x_n\right)$ для $x_i \in \left[\alpha_i, \beta_i\right]$, $i = \overline{1, n}$, якщо він задовольняє умову

$$\begin{gathered}\max_{\alpha_i \le x_i \le \beta_i, i=\overline{1,n}} \left| f\left(x_1, x_2, ..., x_n\right) - F_m\left(a^*; x_1, x_2, ..., x_n\right) \right| = \\ = \min_{a \in A} \max_{\alpha_i \le x_i \le \beta_i, i=\overline{1,n}} \left| f\left(x_1, x_2, ..., x_n\right) - F_m\left(a; x_1, x_2, ..., x_n\right) \right|.\end{gathered} \qquad (2)$$

Рівномірне наближення функції багатьох змінних використовується при проектуванні технічних засобів для вимірювання фізичних величин, інформаційний сигнал яких залежить від декількох параметрів, а також побудові чисельних методів. Зокрема, рівномірне наближення функції двох змінних використовують при проектуванні манометрів, рівнемірів, вологомірів тощо.

На жаль, поки що немає ефективних алгоритмів для обчислення параметрів рівномірного наближення функцій багатьох змінних. Щодо методів отримання рівномірного наближення функцій багатьох змінних, то здебільшого використовують три способи: з використанням методів оптимізації, послідовного обчислення рівномірного наближення по кожній зі змінних та ітераційні алгоритми типу Ремеза.

Найчастіше використовують методи оптимізації, тобто апарат математичного програмування відповідно лінійного, або нелінійного. Зокрема, в пакеті MATLAB для знаходження рівномірного наближення функцій багатьох змінних передбачено функцію fminimax.

Програму для обчислення параметрів рівномірного наближення функцій багатьох змінних узагальненим поліномом на основі методу лінійного програмування розроблено А. О. Каленчук-Порхановою [1]. Дещо раніше така програма розроблена Кондратьєвим В. П. [2].

Обчислення параметрів рівномірного наближення функцій багатьох змінних на основі використання послідовних чебишовських апроксимацій за кожною змінною висвітлено у працях [3, 4]. За такими алгоритмами похибка наближення функції дещо більша ніж при рівномірному наближенні.

Алгоритм рівномірного наближення функцій багатьох змінних з використанням ітераційних схем типу Ремеза описано в праці Б. О. По-

пова і Г. Ф. Криворучка [5]. За цим алгоритмом на кожній ітерації уточнюється множина вузлів — точок з найбільшим відхиленням наближуючого виразу від наближуваної функції (аналог точок альтернансу при наближенні функції однієї змінної). Розв’язування задачі чебишовської інтерполяції за цим алгоритмом проводиться у два етапи: на першому визначаються знаки відхилення наближуючого виразу від наближуваної функції у вузлових точках, на другому відповідно до визначених знаків відхилення на множині вузлових точок розв’язують задачу чебишовської інтерполяції. Далі для функції однієї змінної зі зміною точок альтернансу змінюють лише один з вузлів. Оптимізацію цього алгоритму для деяких частинних випадків запропонував Гапонюк Я. В. [6].

Ми пропонуємо алгоритм побудови рівномірного наближення функцій багатьох змінних як граничного наближення у нормі простору L^p при $p \to \infty$ з використанням методу найменших квадратів зі змінною ваговою функцією.

1. Наближення функцій у нормі простору L^p. Нехай неперервну функцію $f\left(x_1, x_2, ..., x_n\right)$ задану для $x_i \in \left[\alpha_i, \beta_i\right]$, $i = \overline{1, n}$ необхідно наблизити виразом $F_m\left(a; x_1, x_2, ..., x_n\right)$. Оцінка близькості наближення в нормі простору L^p визначається формулою

$$\left\|\Delta\right\|_{L^p} = \left(\int\limits_{\alpha_n}^{\beta_n} ... \int\limits_{\alpha_2}^{\beta_2} \int\limits_{\alpha_1}^{\beta_1} \left|\Delta\left(x_1, x_2, ..., x_n\right)\right|^p dx_1 dx_2 ... dx_n \right)^{1/p}, \quad 1 \le p < \infty, \qquad (3)$$

де $\Delta\left(x_1, x_2, ..., x_n\right) = f\left(x_1, x_2, ..., x_n\right) - F_m\left(a; x_1, x_2, ..., x_n\right)$.

Для $1 \le p < \infty$ величина $\left\|\Delta\right\|_{L^p}$ набуває проміжних значень між $\left\|\Delta\right\|_{L^1}$ і $\left\|\Delta\right\|_C$ [7], де $\left\|\Delta\right\|_C$ — норма у просторі неперервних функцій.

У дискретному випадку для оцінки якості наближення використовують норму евклідового простору E^p. Похибку наближення неперервних функцій $f\left(x_1, x_2, ..., x_n\right)$ заданих на множині точок $\left(x_{1,j_1}, x_{2,j_2}, ..., x_{n,j_n}\right)$, $i = \overline{0, n}$, $j_i = \overline{0, s_i}$ виразом (1) оцінюватимемо в нормі

$$\left\|\Delta\right\|_{E^p} = \left(\sum_{j_n=0}^{s_n} ... \sum_{j_2=0}^{s_2} \sum_{j_1=0}^{s_1} \left|\Delta\left(x_{1,j_1}, x_{2,j_2}, ..., x_{n,j_n}\right)^p\right| \right)^{1/p}, \qquad (4)$$

де $\Delta\left(x_1, x_2, ..., x_n\right) = f\left(x_1, x_2, ..., x_n\right) - F_m\left(a; x_1, x_2, ..., x_n\right)$, $1 \le p < \infty$. Граничне значення норми $\left\|\Delta\right\|_{E^p}$ при $p \to \infty$ відповідає нормі в просторі неперервних функцій $\left\|\Delta\right\|_C$.

Побудова рівномірного наближення таблично-заданих функцій ґрунтується на ідеї ітераційного отримання наближення в просторі E^p, як наближення за методом найменших квадратів [7]

$$\sum_{j_n=0}^{s_n} \dots \sum_{j_1=0}^{s_1} \rho_r\left(x_{1,j_1},\dots,x_{n,j_n}\right)\left(\Delta_{r+1}\left(x_{1,j_1},\dots,x_{n,j_n}\right)\right)^2 \to \min,\ r = 0,1,\dots, \quad (5)$$

з ваговою функцією [8]

$$\rho_0\left(x_1,x_2,\dots,x_n\right) = 1,\ \rho_r\left(x_1,x_2,\dots,x_n\right) = \prod_{i=1}^{r}\left|\Delta_i\left(x_1,x_2,\dots,x_n\right)\right|^2,\ r = 1,2,\dots, \quad (6)$$

де $\Delta_r\left(x_1,\dots,x_n\right) = f\left(x_1,\dots,x_n\right) - F_{m,r}\left(a;x_1,\dots,x_n\right)$, $F_{m,r}\left(a;x_1,\dots,x_n\right)$ — наближення за методом найменших квадратів функції $f\left(x_1,x_2,\dots,x_n\right)$ з ваговою функцією $\rho_{r-1}\left(x_1,x_2,\dots,x_n\right)$.

Використання вагової функції (6) забезпечує її послідовне уточнення, яке передбачає врахування результатів попередніх наближень за методом найменших квадратів. Результати тестових прикладів, поданих у праці [8] підтверджують хорошу збіжність процесу (5) з ваговою функцією (6) при наближенні функцій двох змінних.

2. Опис алгоритму визначення параметрів рівномірного наближення функції багатьох змінних. Реалізація ітераційного процесу (5), (6) полягає в його проведенні до тих пір поки зменшується похибка наближення

$$\rho_{r+1} < \rho_r,\ r = 1,2,\ \dots\ , \quad (7)$$

де $\rho_r = \max\limits_{j_i=\overline{0,s_i},\ i=\overline{1,n}} \left|\Delta_r\left(x_{1,j_1},x_{2,j_2},\dots,x_{n,j_n}\right)\right|$.

Після досягнення невиконання умови (7) доцільно провести ще коригування адитивної складової похибки

$$A = \left(\rho_{\max} + \rho_{\min}\right)/2, \quad (8)$$

де

$$\rho_{\max} = \max_{\substack{j_i=\overline{0,s_i},\\ i=\overline{1,n}}} \Delta_r\left(x_{1,j_1},\dots,x_{n,j_n}\right),\ \rho_{\min} = \min_{\substack{j_i=\overline{0,s_i},\\ i=\overline{1,n}}} \Delta_r\left(x_{1,j_1},\dots,x_{n,j_n}\right).$$

В результаті шукане рівномірне наближення неперервної функції $f\left(x_1,x_2,\dots,x_n\right)$ заданої на множині точок $\left(x_{1,j_1},x_{2,j_2},\dots,x_{n,j_n}\right)$, $i=\overline{0,n}$, $j_i=\overline{0,s_i}$ узагальненим поліномом (1) буде

$$F_m\left(a;x_1,x_2,\dots,x_n\right) = F_{m,r}\left(a;x_1,x_2,\dots,x_n\right) + A. \quad (9)$$

Під час розв'язування тестових прикладів для отримання рівномірного наближення за цим алгоритмом спостерігалось використання до п'яти — шести ітерацій (5).

Приклад 1. Знайдемо рівномірне наближення функції $z_1(x,y) = e^{-xy}$ заданої у точках (x_i, y_j), $i = \overline{0,100}$, $j = \overline{0,100}$, де $x_i = 0.01i$, $y_j = 0.01j$, поліномом другого степеня за кожною змінною x та y.

З використанням запропонованого методу за чотири ітерації (5) для функції $z_1(x,y)$ отримано поліном

$$P_2(x, y) = 0.9972061702 + 0.00258908x - 0.002394555359x^2 + 0.002554584932y - 0.9549205056xy + 0.01181962538x^2y - 0.00235686406y^2 + 0.01178053096xy^2 + 0.3051429680x^2y^2, \quad (10)$$

який забезпечує абсолютну похибку наближення – 0.0035415. В процесі обчислення апроксимація похибка наближення набувала таких значень: на першій ітерації – 0.0092249, на другій – 0.0040139, третій – 0.00388419, четвертій – 0.0035426, а на п'ятій ітерації спостерігалось збільшення похибки наближення – 0.0038929. Коригуюча адитивна поправка дорівнювала $A = -0.10231_{10}^{-5}$.

Поверхню похибки отриманої апроксимації показано на рисунку.

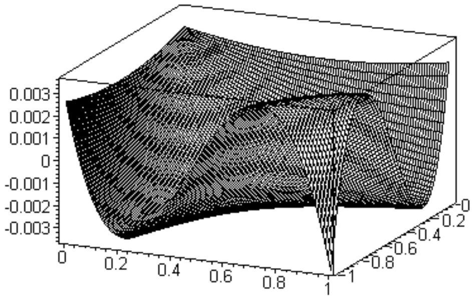


***Рисунок.** Поверхня похибки апроксимації $z_1(x,y)$ поліномом (10)*

В результаті ітерацій (5), (6) похибка апроксимації функції $z_1(x,y)$ рознесена більш рівномірно серед усіх точок поверхні (див. рис. 1). Аналогічна картина спостерігається і в інших прикладах, а саме в результаті ітерацій (5), (6) значення похибки апроксимації майже рівномірно перерозподіляються серед усіх точок площини.

Приклад 2. Знайдемо рівномірне наближення функції $z_2(x,y) = \cos x \sin y$ заданої у точках (x_i, y_j), $i = \overline{0,10}$, $j = \overline{0,10}$, де $x_i = 0.1i$, $y_j = 0.1j$, поліномом четвертого степеня щодо змінних x та y.

З використанням запропонованого методу за три ітерації для функції $z_2(x,y)$ і поправки $A = 0.451815_{10}^{-5}$ отримано поліном

$$\begin{aligned}P_4(x, y) = {} & 0.0000707115677 - 0.004444918667x - 0.004445610824y + \\ & + 1.035899447xy + 0.0185669572x^2 + 0.01857619596y^2 + \\ & + 0.0586030093x^2y^2 - 0.02453794023x^3 - 0.024564185y^3 - \\ & - 0.06925159472x^2y + 0.01056091567x^4 + 0.01057819742y^4 - \\ & - 0.1241764348x^3y - 0.06922153065xy^2 - 0.12419544xy^3,\end{aligned} \quad (11)$$

який забезпечує абсолютну похибку наближення — 0.0002628476.

Приклад 2 взято з праці А.О. Каленчук-Порханової [1], в якій для отримання рівномірного наближення функції $z_2(x, y)$ поліномом вигляду (11) використано алгоритм на основі методу лінійного програмування. Абсолютна похибка апроксимації функції $z_2(x, y)$ за L^p цим методом становила 0.0002732 і була досягнута на 25 кроці. Цей же приклад для тестування програми чебишовського наближення функцій багатьох змінних використовував Кондратьєв В. П. [2]. Розроблена Кондратьєвим В. П. програма [2] на основі методу лінійного програмування забезпечила похибку апроксимації 0.0002735 за 43 кроки. Ця ж задача була розв'язана з використанням MATLAB-функції fminimax за 2 ітерації з похибкою – 0.00027392.

Приклад 3. Знайдемо рівномірне наближення функції $z_3(x, y, t) = e^{-xyt}$ заданої в точках (x_i, y_j, t_r), $i = \overline{0, 50}$, $j = \overline{0, 50}$, $r = \overline{0, 50}$, де $x_i = 0.02i$, $y_j = 0.02j$, $t_r = 0.02r$ поліномом першого степеня за кожною змінною x, y та t.

З використанням запропонованого методу за три ітерації відповідно до формули (5) для функції $z_3(x, y, t)$ з коригуючою поправкою A = 0.0037877696 отримано поліном

$$\begin{aligned}P_1(x, y, t) = {} & 1.019745442 - 0.05546611015x - 0.05546287952y + \\ & + 0.05741801594yx - 0.05546803039t + 0.05742524483tx + \\ & + 0.05742199989yt - 0.6989846315ytx,\end{aligned} \quad (12)$$

який забезпечує абсолютну похибку наближення – 0.04125. В процесі обчислення апроксимації похибка наближення набувала таких значень: на першій ітерації – 0.125796, на другій – 0.057954, третій – 0.045038, а на четвертій ітерації спостерігалось збільшення похибки наближення – 0.0517593.

Висновки. Запропонований метод наближення неперервних таблично-заданих функцій багатьох змінних узагальненим поліномом забезпечує можливість отримання апроксимації з майже рівномірним рознесенням похибки наближення серед усіх точок задання функції. При цьому найбільші за модулем додатні й від'ємні відхилення отримуваних апроксимацій від значень наближуваних функцій майже співпадають. Отримувані значення коригуючої поправки доволі малі. Точність наближення функцій за цим методом не гірша за апроксимацію з використання методу лінійної оптимізації (див. результати прикладу 2). Отже, застосування послідовного уточнення вагової функції (6) забезпечує доволі ефективне отримання апроксимації досить близької за точністю наближення до рівномірної апроксимації.

Ідея запропонованого методу може бути використаною для апроксимації неперервних функцій раціональним виразом.

Список використаних джерел:

1. Каленчук-Порханова А. О., Вакал Л. П. Побудова найкращих рівномірних наближень функцій багатьох змінних. *Комп'ютерні засоби, мережі та системи*. 2007. № 6. С. 141–148.
2. Кондратьев В. П. Алгоритм наилучшего приближения функций многих переменных. *Программы оптимизации: приближение функций*. Свердловск: УНЦ АН СССР, 1973. Вып. 3. С. 20–48.
3. Brown J. A. Henry M. S. Best Chebyshev composite approximation. *SIAM Journal on Numerical Analysis*. 1975. Vol. 12. No. 3. P. 336–344.
4. Jackson N. Henry. Comparison of algorithms for multivariate rational approximation. *Math. Comp.* 1977. 31. P. 485–494.
5. Криворучко Г. Ф., Попов Б. А. Алгоритм наилучшего чебышевского приближения табличной функции двух переменных. *Отбор и преобразование информации*. 1988. Вып. 2. С. 56–67.
6. Гапонюк Я. В. Знаходження найкращих рівномірних многочленних двовимірних наближень. *Відбір і обробка інформації.* 1998. №12(88). С. 130–133.
7. Попов Б. А., Теслер Г. С. Приближение функций для технических приложений. Киев: Наук. думка. 1980. 352 с.
8. Малачівський П. С., Монцібович Б. Р. Рівномірне наближення функції двох змінних. Обчислювальні методи і системи перетворення інформації: зб. праць IV наук.-техн. конф., Львів, 28-30 вересня 2016 р. Львів: ФМІ НАНУ, 2016. С. 179–180.

The algorithm of uniform approximation for functions of several variables is described as approximation in norm L_p with $p \to \infty$. It is based on mean square approximation with changed weight function. The way to successive precise of weight function is offered.

Key words: *functions of several variables, uniform approximation.*

Одержано 02.03.2017

УДК 517.946

В. В. Маринець*, д-р фіз.-мат. наук, професор,
О. Ю. Питьовка,** канд. фіз.-мат. наук, доцент
*ДВНЗ Ужгородський національний університет, м. Ужгород,
**Мукачівський державний університет, м. Мукачево

ПРО ОДИН ПІДХІД ДОСЛІДЖЕННЯ КРАЙОВИХ ЗАДАЧ ДЛЯ НЕЛІНІЙНИХ РІВНЯНЬ ГІПЕРБОЛІЧНОГО ТИПУ В ОБЛАСТІ ЗІ СКЛАДНОЮ СТРУКТУРОЮ КРАЮ

За допомогою побудованої модифікації двостороннього методу досліджується крайова задача Дарбу – Гурса – Дарбу (ДГД) для нелінійного хвильового рівняння в області зі складною структурою краю.

Ключові слова: *двосторонній метод, задача ДГД, область зі складною структурою краю, функції порівняння.*

Вступ. Мета даної роботи — побудова модифікації двостороннього методу дослідження крайової задачі ДГД для нелінійного хвильового рівняння в області зі складною структурою краю, що є продовженням досліджень, приведених в роботах [1, 2].

Нехай в просторі R^2 задана область [3] $D=\{(x,y)\,|\,x\in(x_0,x_1],$ $y\in(g_1(x),g_2(x))\}$ де $x_0<x_1$, $y=g_i(x)\Leftrightarrow x=k_i(y)$, $i=1,2$, — «вільні» криві, причому $g_i'(x)>0$, $g_1(x_{i-1})=y_{i-1}$, $g_2(x_{i-1})=y_{i+1}$, $y_0<y_1<y_2<y_3$.

Дослідимо крайову задачу: в просторі функцій $C^{(1.1)}(D)$ знайти розв'язок крайової задачі

$$L_2u(x,y)=f(x,y,u(x,y)):=f[u(x,y)], \tag{1}$$

де L_2 — диференціальний оператор, породжений диференціальним виразом $l_{(1.1)}u(x,y):=u_{xy}(x,y)+a_1(x,y)u_x(x,y)+a_2(x,y)u_y(x,y)$

та крайовими умовами

$$u(x,g_i(x))=\varphi_i(x),\ \ \varphi_i(x)\in C^1([x_0,x_1]), \tag{2}$$

$$u(x_0,y)=\psi(y),\ \ \psi(y)\in C^1([y_0,y_2]), \tag{3}$$

$$\psi(y_0)=\varphi_1(x_0),\ \ \psi(y_2)=\varphi_2(x_0). \tag{4}$$

Розбиваємо область D характеристиками $y=y_i$, $i=1,2$ на три підобласті D_s, $s=1,2,3$:

$$D_1=\{(x,y)\,|\,x\in(x_0,x_1],\ y\in(g_1(x),y_1]\},$$

$$D_2=\{(x,y)\,|\,x\in[x_0,x_1],\ y\in(y_1,y_2]\},$$

$$D_3 = \{(x,y) \big| x \in [x_0, x_1],\ y \in (y_2, g_2(x))\}.$$

Тоді розв'язок крайової задачі (1) $u(x,y) = u_s(x,y)$, $(x,y) \in \overline{D}_s$, $s = 1,2,3,$ де $u_1(x,y)$ — розв'язок задачі Дарбу $l_{(1.1)}u_1(x,y) = f[u_1(x,y)]$, $u_1(x, g_1(x)) = \varphi_1(x)$, $u_1(x_0, y) = \psi(y)$, $y \in [y_0, y_1]$, $u_2(x,y)$ — розв'язок задачі Гурса $l_{(1.1)}u_2(x,y) = f[u_2(x,y)]$, $u_2(x_0, y) = \psi(y)$, $y \in [y_1, y_2]$, $u_2(x, y_1) = u_1(x, y_1)$, а $u_3(x,y)$ — розв'язок задачі Дарбу $l_{(1.1)}u_3(x,y) = f[u_3(x,y)]$, $u_3(x, g_2(x)) = \varphi_2(x)$, $u_3(x, y_2) = u_2(x, y_2)$, $x \in [x_0, x_1]$.

Надалі вважатимемо, що

$$f[u(x,y)] \in C(\overline{B}),\ \ f : \overline{B} \to R,\ \ \overline{B} \subset R^3,\ \ a_1(x,y) \in C^{(1.0)}(D),$$
$$a_2(x,y) \in C^{(0.1)}(D) \ \text{ і } \ a_{1_x}(x,y) = a_{2_y}(x,y). \qquad (5)$$

Введемо позначення:

$$F[u(x,y)] := f[u(x,y)] + [a_{2_y}(x,y) + a_1(x,y)a_2(x,y)]u(x,y),$$

$$\Phi_s(x,y) := \left[\psi(y) - \psi(g_1(x))\exp\left(\int\limits_y^{g_1(x)} a_1(x_0,\eta)d\eta\right)\right]\times$$
$$\times\exp\left(\int\limits_x^{x_0} a_2(\xi,y)d\xi\right) + \varphi_1(x)\exp\left(\int\limits_y^{g_1(x)} a_1(x,\eta)d\eta\right),\ (x,y) \in \overline{D}_s,\ s = 1,2,$$

$$\Phi_3(x,y) := \varphi_2(K_2(y))\exp\left(\int\limits_x^{K_2(y)} a_2(\xi,y)d\xi\right) + \left[\psi(g_1(K_2(y)))\times\right.$$
$$\left.\times\exp\left(\int\limits_{g_1(x)}^{g_1(K_2(y))} a_1(x_0,\eta)d\eta\right) - \psi(g_1(x))\right]\exp\left(\int\limits_y^{g_1(x)} a_1(x,\eta)d\eta + \right.$$
$$\left.+\int\limits_x^{x_0} a_2(\xi, g_1(x))d\xi\right) + \varphi_1(x)\exp\left(\int\limits_y^{g_1(x)} a_1(x,\eta)d\eta\right) - \varphi_1(K_2(y))\times$$
$$\times\exp\left(\int\limits_y^{g_1(K_2(y))} a_1(x,\eta)d\eta + \int\limits_x^{K_2(y)} a_2(\xi, g_1(K_2(y)))d\xi\right),\ (x,y) \in \overline{D}_3,$$

$$T_1F[u_1(x,y)] := \int\limits_{x_0}^{x}\int\limits_{g_1(x)}^{y} F[u_1(\xi,\eta)]K(x,y;\xi,\eta)d\eta\, d\xi,\quad (x,y) \in \overline{D}_1,$$

$$K(x,y;\xi,\eta):=\exp\left(\int_y^{\eta} a_1(\xi,\tau)d\tau+\int_x^{\xi} a_2(\tau,y)d\tau\right),\ (x,y)\in D\ ,$$

$$T_2F[u_2(x,y)]:=\int_{x_0}^{x}\int_{y_1}^{y} F[u_2(\xi,\eta)]K(x,y;\xi,\eta)d\eta\, d\xi\ ,$$

$$T_{1,2}F[u_1(x,y)]:=\int_{x_0}^{x}\int_{g_1(x)}^{y_1} F[u_1(\xi,\eta)]K(x,y;\xi,\eta)d\eta\, d\xi,\ (x,y)\in \overline{D}_2\ ,$$

$$T_3F[u_3(\xi,\eta)]:=\int_{y_2}^{y}\int_{K_2(y)}^{x} F[u_3(\xi,\eta)]K(x,y;\xi,\eta)d\eta\, d\xi\ ,$$

$$T_{1,3}F[u_2(\xi,\eta)]:=\int_{K_2(y)}^{x}\frac{\partial}{\partial\xi}\left[\int_{x_0}^{\xi}\int_{g_1(\xi)}^{y_1} F[u_1(\tau,\eta)]K(x,y;\tau,\eta)d\eta\, d\tau\right]d\xi+$$

$$\int_{K_2(y)}^{x}\int_{y_1}^{y_2} F[u_2(\xi,\eta)]K(x,y;\xi,\eta)d\eta\, d\xi,\ (x,y)\in \overline{D}_3\ .$$

Лема 1. Якщо виконуються умови (5), тоді крайова задача (1) еквівалентна системі інтегральних рівнянь

$$u_s(x,y)=\Phi_s(x,y)+\varepsilon_s T_{1,s}F[u_{s-1}(\xi,\eta)]+T_sF[u_s(\xi,\eta)],$$

$$(x,y)\in\overline{D}_s,\ \ s=1,2,3,\ \text{ де }\ \varepsilon_s=\begin{cases}0,\ s=1,\\ 1,\ s=2,3.\end{cases}\tag{6}$$

Згідно постановки задачі $u_{1_x}(x,y_1)=u_{2_x}(x,y_1),\ u_{3_x}(x,y_2)=u_{2_x}(x,y_2)$ при $x\in[x_0,x_1]$, а $u_{1_y}(x,y_1)=u_{2_y}(x,y_1)$,

$$u_{2_y}(x,y_2)-u_3(x,y_2)=\rho\exp\left(\int_x^{x_0} a_2(\xi,y_2)d\xi\right),\tag{7}$$

де

$$\rho:=\psi'(y_2)-K_2'(y_2)\Big[\varphi_2'(x_0)+a_2(x_0,y_2)\varphi_2(x_0)-\int_{y_0}^{y_2}F(x_0,\eta,\psi(\eta))\times$$

$$\times\exp\left(\int_{y_2}^{\eta} a_1(x_0,\tau)d\tau\right)d\eta+(g_1'(x_0)\psi'(y_0)-\varphi_1'(x_0)-$$

$$-a_2(x_0,y_0)\varphi_1(x_0))\exp\left(\int_{y_2}^{y_0} a_1(x_0,\eta)d\eta\right)\Bigg].$$

Лема 2. Нехай $f[u(x,y)] \in C(\overline{B})$, виконуються умови (5) і крайова задача (1) має розв’язок. Тоді умова $\rho = 0$ є необхідною і достатньою, щоб розв’язок задачі (1) був регулярним. У супротивному випадку виконується рівність (7) і розв’язок буде іррегулярним.

Означення. Будемо вважати, що $F[u(x,y)] \in C_1(\overline{B})$, якщо [1]:

1. $F[u(x,y)] \in C(\overline{B})$.
2. В просторі функцій $C_1(\overline{B})$, $\overline{B}1 \subset R^4$, $\Pi p_{xOy} \overline{B}1 = \overline{D}$ існує така функція $H\big(x, y, u(x,y); v(x,y)\big) := H[u(x,y); v(x,y)]$, що
   а) $H[u(x,y); u(x,y)] \equiv F[u(x,y)]$;
   б) для довільної з простору $C(\overline{D})$ пари функцій $u(x,y), v(x,y) \in \overline{B}1$, які задовольняють умови $u(x,y) \geq v(x,y)$, $(x,y) \in \overline{D}$, в області $\overline{B}1$ виконуються нерівності
   $$H[u(x,y); v(x,y)] \geq H[v(x,y); u(x,y)], (x,y) \in \overline{D}; \tag{8}$$
3. Функція $H[u(x,y); v(x,y)]$ в області $\overline{B}1$ задовольняє умову Ліпшіца, тобто для всяких з простору $C(\overline{D})$ функцій $u_i(x,y)$, $v_i(x,y) \in \overline{B}1$, $i = 1,2$, виконується умова $\big|H[u_1(x,y); u_2(x,y)] - -H[v_1(x,y); v_2(x,y)]\big| \leq L\Big(\big|w_1(x,y)\big| + \big|w_2(x,y)\big|\Big)$, $(x,y) \in \overline{D}$, де L — стала Ліпшіца, а $w_i(x,y) := u_i(x,y) - v_i(x,y)$.

Відзначимо, що якщо функція $f[u(x,y)] \in C(\overline{B})$ і має в області $\overline{B}$ обмежену частинну похідну першого порядку за $u(x,y)$, то $F[u(x,y)] \in C_1(\overline{B})$. Зворотне твердження не справедливе.

Побудуємо швидкозбіжну модифікацію двостороннього методу наближеного розв’язання системи інтегральних рівнянь (6).

Нехай $z_{s,p}(x,y), v_{s,p}(x,y) \in C(\overline{D}s)$, $s = 1,2,3$, $p \in N_0$, $N_0 = \{0,1,2,...\}$, належать області $\overline{B}1$. Позначимо:

$$w_{s,p}(x,y) := z_{s,p}(x,y) - v_{s,p}(x,y), (x,y) \in \overline{D}s, s = 1,2,3, p \in N_0,$$

$$f_s^p(x,y) := H[z_{s,p}(x,y); v_{s,p}(x,y)],$$

$$f_{s,p}(x,y) := H[v_{s,p}(x,y); z_{s,p}(x,y)],$$

$$T_{1,3}^{(1)} f_1^p(\xi,\eta) := \int_{x_0}^{x} \int_{g_1(x)}^{y_1} K(x,y;\xi,\eta) f_1^p(\xi,\eta) d\eta\, d\xi,$$

$$T_{1,3}^{(2)} f_{1,p}(\xi,\eta) := \int_{x_0}^{K_2(y)} \int_{g_1(K_2(y))}^{y_1} K(x,y;\xi,\eta) f_{1,p}(\xi,\eta) d\eta\, d\xi,$$

$$T_{1,3}^{(3)} f_2^p(\xi,\eta) := \int_{K_2(y)}^{x} \int_{y_1}^{y_2} K(x,y;\xi,\eta) f_2^p(\xi,\eta) d\eta\, d\xi,\ (x,y)\in \overline{D}_3$$

$$T_{1,3} f_2^p(\xi,\eta) := T_{1,3}^{(1)} f_1^p(\xi,\eta) - T_{1,3}^{(2)} f_{1,p}(\xi,\eta) + T_{1,3}^{(3)} f_2^p(\xi,\eta),$$

$$T_{1,3} f_{2,p}(\xi,\eta) := T_{1,3}^{(1)} f_{1,p}(\xi,\eta) - T_{1,3}^{(2)} f_1^p(\xi,\eta) + T_{1,3}^{(3)} f_{2,p}(\xi,\eta),$$

$$\alpha_{s,p}^*(x,y) := z_{s,p}(x,y) - \Phi_s(x,y) - \varepsilon_s T_{1,s} f_{s-1}^p(\xi,\eta) - T_s f_s^p(\xi,\eta)$$

$$\beta_{s,p}^*(x,y) := v_{s,p}(x,y) - \Phi_s(x,y) - \varepsilon_s T_{1,s} f_{s-1,p}(\xi,\eta) - T_s f_{s,p}(\xi,\eta),$$

$$\overline{z}_{s,p}(x,y) := z_{s,p}(x,y) - d_{s,p}(x,y) w_{s,p}(x,y),$$

$$\overline{v}_{s,p}(x,y) := v_{s,p}(x,y) + q_{s,p}(x,y) w_{s,p}(x,y),\ (x,y)\in \overline{D}_s,\ s=1,2,3,$$

$$\overline{F}_s^p(x,y) := H[\overline{z}_{s,p}(x,y); \overline{v}_{s,p}(x,y)],$$

$$\overline{F}_{s,p}(x,y) := H[\overline{v}_{s,p}(x,y); \overline{z}_{s,p}(x,y)],$$

$$d_{s,p}(x,y),\ q_{s,p}(x,y) \in C(\overline{D}_s) \tag{9}$$

— довільні функції, які задовольняють умови

$$0 \le d_{s,p}(x,y) \le 0{,}5,\ \ 0 \le q_{s,p}(x,y) \le 0{,}5,\ p\in N_0,\ s=1,2,3. \tag{10}$$

Побудуємо послідовності функцій $\{z_{s,p}(x,y)\}$ та $\{v_{s,p}(x,y)\}$ [4]

$$\begin{aligned} z_{s,p+1}(x,y) &= \Phi_s(x,y) + \varepsilon_s T_{1,s} f_{s-1}^{p+1}(\xi,\eta) + T_s F_s^p(\xi,\eta),\\ v_{s,p+1}(x,y) &= \Phi_s(x,y) + \varepsilon_s T_{1,s} f_{s-1,p+1}(\xi,\eta) + T_s F_{s,p}(\xi,\eta), \end{aligned} \tag{11}$$

$(x,y)\in \overline{D}_s,\ s=1,2,3,\ p\in N_0$, де за нульове наближення $z_{s,0}(x,y),\ v_{s,0}(x,y)\in \overline{B}_1$ вибираємо довільні з простору $C(\overline{D}_s)$ функції, які задовольняють відповідно умови (2)–(4) та нерівності

$$w_{s,0}(x,y)\ge 0,\ \alpha_{s,0}^*(x,y)\ge 0,\ \beta_{s,0}^*(x,y)\le 0,\ (x,y)\in \overline{D}_s,\ s=1,2,3. \tag{12}$$

Надалі, описані вище функції $z_{s,0}(x,y),\ v_{s,0}(x,y)$ будемо називати функціями порівняння задачі (1). Легко показати, що якщо на кожному кроці ітераційного процесу (11) функції $d_{s,p}(x,y)$, $q_{s,p}(x,y)$ вибирати таким чином, щоб виконувалися умови

$$\begin{aligned} & z_{s,p}(x,y) - z_{s,p+1}(x,y) - d_{s,p}(x,y) w_{s,p}(x,y) \ge 0,\ (x,y)\in \overline{D}_s,\\ & v_{s,p}(x,y) - v_{s,p+1}(x,y) + q_{s,p}(x,y) w_{s,p}(x,y) \le 0,\ s=1,2,3,\ p\in N_0, \end{aligned} \tag{13}$$

то в області $\overline{B}_1$ матимуть місце нерівності

$$v_{s,p}(x,y) \le v_{s,p+1}(x,y) \le z_{s,p+1}(x,y) \le z_{s,p}(x,y),$$
$$\alpha_{s,p}(x,y) \ge 0,\ \beta_{s,p}(x,y) \le 0, (x,y) \in \overline{D}_s,\ s = 1,2,3,\ \ p \in N_0, \tag{14}$$

Лема 3. Якщо $F[u(x,y)] \in C_1(\overline{B})$ і в області $\overline{B}_1$ існують функції порівняння $z_{s,0}(x,y), v_{s,0}(x,y)$, $(x,y) \in \overline{D}_s$, $s = 1,2,3$ задачі (1), тоді множина функцій $d_{s,p}(x,y), q_{s,p}(x,y) \in C(\overline{D}_s)$, які задовольняють умови (13), не порожня.

Позначимо

$$d = \max_{s} \sup_{\overline{D}_s} \left| w_{s,0}(x,y) \right|,\ \ \max_{s,p} \sup_{\overline{D}_s} \Big(1 - d_{s,p}(x,y) - q_{s,p}(x,y)\Big) = l,$$

$$\sup_{\overline{D}} K(x,y;\xi,\eta) \le 0,5K,\ \ \max\{1, \sup_{\overline{D}}\big(x - x_0 + y - y_0\big)\} = \gamma.$$

Тоді з (11) методом математичної індукції маємо

$$\max_{s} \sup_{\overline{D}_s} w_{s,p}(x,y) \le \frac{1}{p!}[Ll\gamma K(y - y_0 + x - x_0)]^p \cdot d. \tag{15}$$

Теорема. Нехай $F[u(x,y)] \in C_1(\overline{B})$, $a_1(x,y) \in C^{(1.0)}(D)$, $a_2(x,y) \in$ $\in C^{(0.1)}(D)$ і при $(x,y) \in D$ виконуються умови (5), а в області $\overline{B}_1$ існують функції порівняння задачі (1). Тоді послідовності функцій $\{z_{s,p}(x,y)\}$ та $\{v_{s,p}(x,y)\}$, побудовані згідно закону (10), (11), (13): а) збігаються рівномірно в області $\overline{D}_s$, $s = 1,2,3$ до єдиного розв'язку відповідного інтегрального рівняння із (6); б) мають місце оцінки (15); в) в області $\overline{B}_1$ виконуються нерівності

$$v_{s,p}(x,y) \le v_{s,p+1}(x,y) \le u_s(x,y) \le z_{s,p+1}(x,y) \le z_{s,p}(x,y), \tag{16}$$

$(x,y) \in \overline{D}_s, p \in N_0$, $s = 1,2,3$ де $u_s(x,y)$ — єдиний розв'язок відповідного рівняння із (6); г) збіжність ітераційного методу (10), (11), (13) не повільніша збіжності методу, приведеного в роботі [1].

Наслідок. Нехай $\varphi_i(x) = 0$, $i = 1,2$, $x \in [x_0, x_1]$, $\psi(y) = 0$, $y \in [y_0, y_2]$, $F[u(x,y)] \in C_1(\overline{B})$, причому $F[u(x,y)] \equiv H[u(x,y);0]$.

Тоді, якщо $F[0] \ge (\le) 0$ в області $\overline{B}_1$, то розв'язок крайової задачі (1) при $(x,y) \in \overline{D}$ задовольняє нерівність $u(x,y) \ge (\le) 0$.

Висновки. Побудовано швидкозбіжну модифікацію двостороннього методу наближеного розв'язання крайової задачі ДГД для нелінійного хвильового рівняння в області зі складною структурою краю. Встановлено умови існування і єдиності розв'язку задачі (1), його регулярності та знакосталості.

Список використаних джерел:

1. Marynets V. V., Marynets K. V. On Goursat Darboux boundary-value problem for systems of non-linear differential equations of hyperbolic type. *Miskolc Mathematical Notes*. 2013. Vol. 14, N. 3. С. 1009–1020.
2. Маринець В. В., Маринець К. В. Дослідження крайової задачі Гурса-Дарбу для нелінійного рівняння гіперболічного типу. *Механіка і фізика руйнування будівельних матеріалів та конструкцій*. 2014. Вип. 10. С. 56–68.
3. Collatz L. Funktionalanalysis und numerische matematik. Berlin Göttingen-Heidelberg: Springer-Verlag, 1964. 446 p.
4. Красносельский М. А., Вайникко Г. М., Забрейко П. П., Рутицкий Я. Б., Стеценко В. Я. Приближенное решение операторных уравнений. М.: Наука, 1969. 456 с.

With the help of the constructed modification of the two-sided method we investigate the Darboux-Goursat-Darboux boundary-value problem for non-linear wave differential equation of the hyperbolic type over the domain with a complex structure.

Key words: *two-sided method, Darboux-Goursat-Darboux boundary-value problem, the domain with complex structure, comparation functions.*

Одержано 24.02.2017

УДК 519.854

В. О. Михайлюк, д-р фіз.-мат. наук

Східноєвропейський національний університет
імені Лесі Українки, м. Луцьк

АЛГЕБРАЇЧНИЙ ПІДХІД ДО РЕОПТИМІЗАЦІЇ ЗАДАЧ КОМБІНАТОРНОЇ ОПТИМІЗАЦІЇ ТА СУМІЖНІ ПИТАННЯ ОЦІНКИ СКЛАДНОСТІ ОБЧИСЛЕНЬ

Використовується поняття α_Λ -наближеного поліморфізму для конструювання $\psi(\alpha_\Lambda)$ -наближеного оптимального алгоритму ($\psi(\alpha_\Lambda) = 2 - 1/\alpha_\Lambda$) для реоптимізації *CSP* задачі $MAX - \Lambda$ ($Ins - MAX - \Lambda$) з добавленням деякого обмеження. Гіпотеза алгебраїчної дихотомії характеризує *NP*-складність розглянутого підходу, а базова *SDP* релаксація для наближених поліморфізмів (*BasicSDP*) визначає ефективний алгоритм заокруглення для $MAX - \Lambda$ та $Ins - MAX - \Lambda$.

Ключові слова: *наближений поліморфізм, гіпотеза алгебраїчної дихотомії, унікальна ігрова гіпотеза (UGC), реоптимізація CSPs.*

Вступ. Узагальнені задачі про виконуваність (Constraint Satisfaction Problems, *CSPs*) описують великий клас задач комбінаторної оптимізації [1, 2]. Узагальнена задача про виконуваність (*CSP*) Λ може бути задана сімейством предикатів над скінченною областю $[q]=\{1,2,...,q\}$. Кожний екземпляр CSP Λ складається з множини змінних V разом з множиною обмежень C на ній. Кожне обмеження з C складається з предиката з сімейства Λ, що застосовується до множини змінних. Для CSP Λ відповідна задача про виконуваність $\Lambda - SAT$ має вигляд.

Задача 1 ($\Lambda - SAT$). Для заданого екземпляра I CSP Λ визначити чи існують приписування змінним, що задовольняють всі обмеження з C.

Більшість задач комбінаторної оптимізації (і $CSPs$) класифікуються як поліноміально розв'язні (легкі, tractable) або NP-складні. Основні дослідження, що проводяться в комбінаторній оптимізації зрозуміти, що робить задачі легкими (в P) або складними (NP-складні). Чи існує загальна теорія для розв'язання цих питань?

Задача 2 ($MAX - \Lambda$). Для заданого екземпляра I задачі $\Lambda - CSP$ знайти приписування, що задовольняють максимальне число (еквівалентно долю) обмежень.

Виникає інтерес до побудови теорій легкості (tractability) для множин $CSPs$ незалежно для точного або оптимізаційного варіантів (задачі 1, 2). Елегантна характеристика складності $CSPs$ основана на гіпотезі алгебраїчної дихотомії [1, 2]. Згідно цієї гіпотези $\Lambda - CSP$ легка тоді і тільки тоді, коли існують нетривіальні операції, названі поліморфізмами, для комбінації розв'язків Λ для отримання нових розв'язків. Розглянемо CSP відому як XOR задача. Екземпляр задачі XOR складається з системи лінійних рівнянь над $Z_2=\{0,1\}$. Фіксуємо екземпляр I задачі XOR від n змінних. Для заданих трьох розв'язків $X^{(1)}, X^{(2)}, X^{(3)} \in \{0,1\}^n$ екземпляра I можна створити новий розв'язок $Y \in \{0,1\}^n : Y_i = X_i^{(1)} \oplus X_i^{(2)} \oplus X_i^{(3)}, \forall i \in [n]$. Легко перевірити, що Y також допустимий розв'язок екземпляра I. Таким чином, $XOR:\{0,1\}^3 \to \{0,1\}$ дає спосіб зкомбінувати три розв'язки в один новий розв'язок для цього екземпляра. Операція такого вигляду, що зберігає виконуваність CSP відома як поліморфізм. Формально

Означення 1 (поліморфізм). Функція $p:[q]^R \to [q]$ називається поліморфізмом для CSP $\Lambda - SAT$, якщо для кожного екземпляра I з Λ і R приписування $X^{(1)}, X^{(2)}, ..., X^{(R)} \in [q]^n$, що задовольняють всі обмеження в I, вектор $Y \in [q]^n : Y_i = p(X_i^{(1)}, X_i^{(2)}, ..., X_i^{(R)}), \forall i \in [n]$ також є допустимим розв'язком.

Множина поліморфізмів CSP Λ ($Poly(\Lambda)$) характеризує складність $\Lambda - SAT$. Формально.

Теорема 1 [1, 2]**.** Якщо *CSPs* Λ_1 і Λ_2 мають співпадаючі множини поліморфізмів ($Poly(\Lambda_1) = Poly(\Lambda_2)$), то $\Lambda_1 - SAT$ поліноміально зводиться до $\Lambda_2 - SAT$ і навпаки.

Зазначимо, що диктаторські функції $p(X^{(1)},...,X^{(R)}) = X^{(i)}$ є поліморфізмами для довільної CSP $\Lambda - SAT$ (вони називаються проекціями або тривіальними поліморфізмами). Всі легкі (tractable) випадки булевських *CSPs* характеризуються існуванням нетривіальних поліморфізмів. Зокрема, $2 - SAT$ має функцію більшості (XOR), $HORN - SAT$ має OR функції і $DUAL\ HORN - SAT$ має AND функції як поліморфізми. В роботі [1] припустили, що існування не диктаторських поліморфізмів характеризує CSP як tractable. Ця робота показує, що множина поліморфізмів $Poly(\Lambda)$ CSP Λ характеризує складність $\Lambda - SAT$. Є багато еквівалентних способів формалізації, що означає для операції бути не диктаторською (нетривіальною). Поліморфізм $p:[q]^k \to [q]$ називається циклічним термом, якщо

$$p(x_1,...,x_k) = p(x_2,...,x_k,x_1) = ... = p(x_k,x_{k-1},...,x_1), \forall x_1,...,x_k \in [q].$$

Гіпотеза 1 (алгебраїчної дихотомії) [1, 2]. $\Lambda - SAT$ знаходиться в P, якщо в Λ є циклічний терм, інакше $\Lambda - SAT$ є NP-складною.

Вдалося отримати такий результат.

Теорема 2 [1, 2]**.** $\Lambda - SAT$ є NP-складною, якщо Λ не допускає циклічних термів.

Вводиться поняття наближеного поліморфізму для оптимізаційних задач. Грубо кажучи наближений поліморфізм є ймовірнісний розподіл P щодо множини операцій вигляду $p:[q]^k \to [q]$. Зокрема, наближений поліморфізм p може бути використаний для комбінації k розв'язків оптимізаційної задачі для формування ймовірнісного розподілу нових розв'язків для того самого екземпляра. На відміну від випадку точних *CSPs* тут поліморфізм видає декілька нових розв'язків.

Ціль реоптимізації [3–6], використовуючи наближені методи, — застосування знання розв'язку початкового екземпляра I задачі для виконання однієї з умов: досягнення кращої якості наближення (відношення апроксимації) I' (змінений екземпляр); створення більш ефективного (по часу) алгоритму для визначення оптимального або близького до нього розв'язку I'; попередні дві умови. Вдалося застосувати аналіз коректності для мови наближених поліморфізмів. Мета статті застосувати алгебраїчний підхід, що базується на мові наближених поліморфізмів, до дослідження деяких реоптимізаційних проблем для *CSPs*.

Наближені поліморфізми для реоптимізації $CSPs$.

Означення 2 ((c,s)-наближений поліморфізм). Фіксуємо функцію $f:[q]^n \to R^+$. Ймовірнісний розподіл Р відносно операцій $p:[q]^R \to [q]$ є (c,s)-наближений поліморфізм для f, якщо виконуються умови: для кожного R приписування $X^{(1)}, X^{(2)}, ..., X^{(R)} \in [q]^n$ такі, що $E_i f(X^{(i)}) \geq c$ для всіх i, то виконується $\underset{p \in \mathrm{P}}{E}[f(p(X^{(1)},...X^{(R)}))] \geq s$. Тут $p(X^{(1)},...,X^{(R)})$ приписування, отримане за координатними застосуваннями операції p.

Означення 3 (α-наближений поліморфізм). Ймовірнісний розподіл Р операцій $p:[q]^R \to [q]$ — α-наближений поліморфізм для $f:[q]^n \to R^+$, якщо він є $(c, \alpha \cdot c)$-наближений поліморфізм для всіх $c \geq 0$.

Означення 4. Ймовірнісний розподіл Р операцій $p:[q]^R \to [q]$ — α-наближений поліморфізм для $MAX - \Lambda$, якщо Р є $(c, \alpha \cdot c)$-наближений поліморфізм для кожного екземпляра I задачі $MAX - \Lambda$.

Будемо вважати, що CSP Λ над $[q]$ задається сімейством платіжних функцій $\Lambda = \{c:[q]^k \to [-1,1]\}$. Екземпляр $MAX - \Lambda$ складається з множини змінних $V = \{x_1,...,x_n\}$ і множини обмежень $C = \{C_1,...,C_m\}$, де кожне $C_i(X) = c(x_{i_1}, x_{i_2}, ..., x_{i_k})$ для деякого $c \in \Lambda$. Множина C пов'язана з розподілом ймовірностей $w: C \to R^+$. Мета знайти приписування $x \in [q]^V$, що максимізує

$$val_I(x) = \sum_{c \in C} w(c)c(x) .$$

Вводиться поняття (c,s)-диктаторського тесту для $MAX - \Lambda$ проти сімейства функцій $\Phi = \{p:[q]^R \to [q]\}$ [2].

Теорема 3 [2]**.** Для даної CSP Λ, натурального числа $R \in N$ і скінченого сімейства функцій $\Phi = \{p:[q]^R \to [q]\}$ замкненого відносно перестановки входів наступні умови еквівалентні:

- $MAX - \Lambda$ не допускає (c,s)-наближений поліморфізм, що підтримується на Φ.
- Існує (c,s)-диктаторський тест для $MAX - \Lambda$ проти сімейства Φ.

Фіксуємо ймовірнісний розподіл μ на $[q]$. Нехай $\{\chi_0, \chi_1, ..., \chi_{q-1}\}$ є ортонормований базис для векторного простору $L_2([q], \mu)$. Без втрати загальності будемо вважати, що $\chi_0 = 1$. Для даної функції $f:[q]^k \to R$ можемо записати $f = \sum_{\sigma \in N^k} \hat{f}_\sigma \chi_\sigma$ (Фур'є представлення), де $\chi_\sigma(x) = \prod_{j=1}^{k} \chi_{\sigma_j}(x_j)$. Визначимо вплив ступеня d i-ої координати f відносно розподілу μ як $Inf_{i,\mu}^{<d}(f) = \sum_{\sigma \in N^k, \sigma_i \neq 0, |\sigma| < d} \hat{f}_\sigma^2$. Узагальнюючи для векторної функції $f:[q]^k \to R^D$, отримаємо $Inf_{i,\mu}^{<d}(f) = \sum_{j \in [D]} Inf_{i,\mu}^{<d}(f_j)$.

Означення 5. Наближений поліморфізм Р — (τ, d)-квазівипадковий, якщо для довільного розподілу ймовірностей μ: $\underset{p \in \mathrm{P}}{E}[\max_i Inf_{i,\mu}^{<d}(p)] \leq \tau$.

Означення 6. Для заданої CSP Λ і константи $c \in [-1,1]$ визначимо $s_\Lambda(c) = \sup\{s \mid \forall \tau > 0, d \in N$, $\exists$ (τ, d)-квазівипадковий (c, s)-наближений поліморфізм для $MAX - \Lambda\}$; $\alpha_\Lambda = \inf_{c \geq 0} \frac{s_\Lambda(c)}{c}$.

Твердження 1. Відображення $s_\Lambda : [-1,1] \to [-1,1]$ монотонно зростає і $s_\Lambda(c + \varepsilon) \leq s_\Lambda(c) + \varepsilon$ для довільних c, ε таких, що $c, c + \varepsilon \in (-1,1)$.

Будемо застосовувати **гіпотезу 2 (унікальну ігрову гіпотезу, Unique Games Conjecture, UGC)** [2, 6]**.** Використовуючи базову SDP релаксацію для наближених поліморфізмів $BasicSDP$ і твердження 1, отримаємо теорему.

Теорема 4 [2]**.** Приймаючи UGC для довільного Λ є NP- складним апроксимувати $MAX - \Lambda$ краще ніж α_Λ. Більше того UGC еквівалентно такому твердженню: для довільних Λ і c на екземплярах $MAX - \Lambda$ із значенням c є NP-складним знайти приписування із значенням більшим ніж $s_\Lambda(c)$.

Теорема 5 [2]**.** Для кожної CSP Λ цілочисловий розрив $BasicSDP$ релаксації для $MAX - \Lambda$ не більший ніж α_Λ. Більше того для кожного екземпляра I $MAX - \Lambda$, для кожного c, якщо оптимальне значення $BasicSDP$ релаксації є не меншим ніж c оптимальне значення для I не менше ніж $\lim_{\varepsilon \to 0} s_\Lambda(c - \varepsilon)$.

Отже, використовується α-наближений поліморфізм для конструювання α-заокруглення для SDP для $MAX - \Lambda$. Отримаємо

Теорема 6 [2]**.** Для всіх η і CSP Λ існують $\tau, d > 0$ такі, що виконується: припустимо P є $(c-\eta, s)$-наближений (τ, d)-квазівипадковий поліморфізм для $MAX - \Lambda$. Для заданого $BasicSDP$ розв'язку із значенням цілі не меншим c очікуване значення приписування округленого алгоритму не менше ніж $s - \eta$.

Нехай I є довільним екземпляром задачі $MAX - \Lambda$. Екземпляр I' задачі отримується з екземпляра I добавленням $(m+1)$-го обмеження $C_{m+1} = (z_{i_1}^{(m+1)}, ..., z_{i_k}^{(m+1)})$, причому $z_{i_j}^{(m+1)} \in \{x_1, ..., x_n, \overline{x}_1, ..., \overline{x}_n\}$, $j \in [k]$.

Задача 3 ($Ins - MAX - \Lambda$ **). Вхідні дані.** Довільний екземпляр I задачі $MAX - \Lambda$, σ^* — оптимальний розв'язок екземпляра I.

Результат. Знайти оптимальний розв'язок екземпляра I' (отриманого, виходячи з I, як описано вище) задачі $MAX - \Lambda$, використовуючи σ^*.

Мета. Знайти σ, який максимізує число виконаних обмежень екземпляра I'.

Основний результат статті полягає у наступному.

Теорема 7. Для довільної CSP Λ задачі $MAX - \Lambda$ та $Ins - MAX - \Lambda$ такі, що $k = const$**.** Тоді для задачі $Ins - MAX - \Lambda$ (реоптимізація $MAX - \Lambda$) існує поіноміальний $\psi(\alpha_\Lambda)$-наближений оптимальний алгоритм, де $\psi(\alpha_\Lambda) = 2 - \dfrac{1}{\alpha_\Lambda}$.

Висновки. Використовуються α_Λ-наближені поліморфізми для конструювання ефективної заокругленої для $BasicSDP$ релаксації напіввизначеного програмування для $MAX - \Lambda$ та $Ins - MAX - \Lambda$. При цьому NP-складність для таких CSP залишається відкритою, і вона еквівалентна UGC. У випадку гіпотези алгебраїчної дихотомії результат з NP-складності відомий, але ефективний алгоритм для всіх $CSPs$ через поліморфізми не відомий.

Представляє інтерес дослідити інші варіанти питання реоптимізації для CSP Λ (зокрема, добавлення деякої множини обмежень або виключення обмежень), використовуючи наближені поліморфізми.

Список використаних джерел:

1. Bulatov A. A., Krokhin A. A., Jeavons Peter. Constraint satisfaction problems and finite algebras. *Proceedings of 27th International Colloquium on Automata, Languages and Programming* (ICALP'00). Geneva, Switzerland, 2000. Lecture Notes in Computer Science (LNCS) 1853. 2000. P. 272–282.

2. Brown-Cohen Jonah, Raghavendra Prasad. Combinatorial Optimization Algorithms via Polymorphisms. [Електронний ресурс] *Electronic Colloquium on Computational Complexity*. 2015. Report No 7. 41 p. Режим доступу: http://eccc.hpi-web.de.
3. Ausiello G., Bonifaci V., and Escoffier B. Complexity and approximation in reoptimization. *Computability in Context: Computation and Logic in the Real World* (ed. S. Barry Cooper and Andrea Sorbi). 2011. London: Imperial College Press. P. 101–130.
4. Bockenhauer H.-J., Hromkovic J., Momke T., Widmayer P. On the hardness of reoptimization. In V. Geffert, J. Karhumaki, A. Bertoni etc. (eds.), SOFSEM, Lecture Notes in Computer Science, Springer. 2008. V. 4910. P. 50–65.
5. Boria N., Paschos V. Th. A survey on combinatorial optimization in dynamic environments. RAIRO. Operations Research. 2011. 45. P. 241–294.
6. Михайлюк В. О., Сергієнко І. В. Постоптимальний аналіз та наближені алгоритми реоптимізації для задач дискретного програмування. Київ: Наукова думка, 2015. 248 с.

The concept of α_Λ -approximation polymorphism is used for design of $\psi(\alpha_\Lambda)$ -approximation optimal algorithm ($\psi(\alpha_\Lambda) = 2 - 1/\alpha_\Lambda$) for reoptimization of CSP problem $MAX-\Lambda$ ($Ins-MAX-\Lambda$) with addition of some constraint. Algebraic dichotomy conjecture characterizes NP -hardness of the considered approach and basic SDP relaxation for approximation polymorphism ($BasicSDP$) defines an efficient rounding algorithm for $MAX-\Lambda$ and $Ins-MAX-\Lambda$.

Key words: *approximation polymorphism, algebraic dichotomy conjecture, Unique Games Conjecture (UGC), reoptimization of* $CSPs$.

Одержано 17.02.2017

УДК 004.421

О. П. Нарєжній*, канд. техн. наук,
Т. О. Гріненко**, канд. техн. наук, доцент

*Харківський національний університет імені В. Н. Каразіна, м. Харків,
**Харківський національний університет радіоелектроніки, м. Харків

МЕТОД ПОБУДОВИ АЛГОРИТМУ ЕКСТРАКТОРА НА ОСНОВІ БАГАТОМОДУЛЬНОГО ПЕРЕТВОРЕННЯ ДЛЯ ПЕРСПЕКТИВНОГО КВАНТОВОГО ГЕНЕРАТОРА ВИПАДКОВИХ ЧИСЕЛ

В загальному вигляді сформульована і вирішена задача синтезу та аналізу алгоритму екстрактора з основою алфавіту більше двох на основі багатомодульного перетворення для перспективного квантового генератора випадкових чисел (КГВЧ). Дана робота виконувалась в рамках проведення комплексних теоретичних та експериментальних досліджень зі створення прототипу КГВЧ на основі реалізації методу подвійного радіооптичного резонансу в парах лужних металів.

Ключові слова: *квантовий генератор випадкових чисел, квантовий фазовий шум, екстрактор квантового генератора випадкових чисел, обчислювальна складність алгоритму.*

Вступ. Генерування випадкових чисел на основі квантових процесів є однією з актуальних та важливих задач криптографії. На цей час запропоновано багато методів використання квантових процесів у генераторах випадкових чисел (ГВЧ), як основні можна виділити такі [1]: метод розщеплення одиничного фотона на два шляхи та поляризації одиничного фотона; метод виявлення заплутаності шляху числа фотонів; метод підрахунку часу генерації або кількості фотонів; метод використання гомодинного виявлення флуктуації вакуумного стану; метод інтерферометричної схеми.

Постановка задачі [2] щодо теоретичного обґрунтування і практичного застосування методу вимірювання фазового шуму квантових дискримінаторів на парах лужних металів для створення прототипу КГВЧ є оригінальною, і має важливе практичне та наукове значення в криптографічних додатках. Однак даний метод має низьку швидкодію ≤ 1000 біт/с на один фотоприймач (канал). Тому швидкодія досягається використанням матриці з фотоприймачів, яка може нараховувати $\sim 10^6$ одиниць фотодіодів, що приводить до значного розширювання основи алфавіту перспективного КГВЧ.

Експериментальні дослідження макету КГВЧ показали, що квантовий фазовий шум має гауссовський закон розподілу імовірності, тому для збільшення мінімальної ентропії та швидкодії необхідно використовувати методи та засоби збільшення ентропії [1, 2]. Тому в сучасних КГВЧ використовуються спеціальні засоби — екстрактори.

Квантовий ГВЧ — пристрій, який формує на своєму виході Y_l послідовність статистично незалежних символів з основою алфавіту m. Екстрактор КГВЧ — детермінований алгоритм чи сукупність алгоритмів та засобів, які для заданої послідовності довжиною k формують при своїй роботі послідовність Y_l символів довжиною $l >> k$, яка володіє властивістю випадкової послідовності з високою рівноймовірністю появи символів, незалежністю та однозначністю. Схема екстрактора КГВЧ включає: 1 — КГВЧ, що формує випадкові послідовності довжиною k; 2 — схему формування початкових значень k та П параметрів генератора псевдовипадкових символів; 3 — генератор псевдовипадкових символів; 4 — логіку зворотного зв'язку [1].

В загальному вигляді випадкову послідовність на виході екстрактора можна задати як залежність $Y = F(\Pi(A_s), K(A_i), A_k)$ від початкових значень ключа $K(A_i)$ та параметрів $\Pi(A_s)$, а також випадкових послідовностей A_k. При цьому зворотний зв'язок Y призводить до впливу його на параметри, початкові значення та роботу генератора псевдовипадкових символів.

Встановлення початкового стану екстрактора КГВЧ.

1. Задається початкове значення s екстрактора. Для цього використовується фізичне джерело випадкових послідовностей, що ґрунтується на випадковості квантових процесів у КГВЧ. Початковий стан екстрактора є таємним. Умови отримання початкового стану екстрактора повинні унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення.
2. Задається значення двійкового рядка B_1 та B_2 з точністю 64 двійкових розрядів. Для цього використовується поточні значення дати і часу, що отримані за допомогою приймача сигналів GPS.

На теперішній час відомо ряд алгоритмів екстракторів на основі методів та засобів генерування псевдовипадкових послідовностей (ПВП) [1]. Їх особливістю є те, що вони будуються, добре досліджені та застосовуються для алфавіту з основою $m = 2$.

Розглянемо метод побудування алгоритму екстрактора з певним алфавітом символів, скажімо m, на основі багатомодульних перетворень у скінченному полі Галуа $GF\left(p^n\right)$. Для загального випадку будемо вважати, що здійснюється k перетворень елементів розширення поля Галуа $GF\left(p^n\right)$, відповідно за модулями $\left(f\left(X\right), f_1\left(X\right)\right)$, $\left(f_1\left(X\right), f_2\left(X\right)\right), \ldots, \left(f_{k-2}\left(X\right), f_{k-1}\left(X\right)\right)$ та останнім модулем m. Загальними параметрами, яких достатньо для того, щоб генерувати елементи a_i поля $GF\left(p^n\right)$, є кортеж $\left(f\left(X\right), p, n, \theta_j\right)$, де $f\left(X\right)$ — незвідний поліном степеня n над полем $GF\left(p\right)$, а θ_j — первісний елемент, вибраний із множини $\{\theta\}$ порядку $\varphi\left(p^n - 1\right)$, де $\varphi\left(*\right)$ — функція Ейлера. В такому випадку генерування (формування) елементів поля здійснюється за правилом:

$$a_i = \left(\theta_j\right)^i \left(\mathrm{mod}\left(f\left(X\right), p, n\right)\right). \tag{1}$$

Показано [1, 3], що при виконанні зазначених вище вимог до кортежу $\left(f\left(X\right), p, n, \theta_j\right)$, перетворення (1) породжує скінченне поле Галуа з періодом повторення $p^n - 1$. Відзначимо, що вказане є справедливим для $p = 2, 3, 5, 7$ і наступних простих чисел.

Далі нехай $\left(f_s\left(X\right), p_s, n_s\right)$ будуть кортежами загальних параметрів, наприклад, поліномів (у тому числі незвідних) $f_s\left(X\right)$, $s = \left(1, k-1\right)$, а n_s — їх степені. Незвідність поліномів нам потрібна для того, щоб за необхідності забезпечити їх взаємну простоту.

Також нехай степені поліномів (у тому числі незвідних) n_s задовольняють вимогам:

$$n_1 > n_2,\ n_2 > n_3,\ \ldots,\ n_{k-2} > n_{k-1}, \tag{2}$$

причому основа алфавіту m є довільним числом, а також виконуються нерівності:

$$p^{n_1} >> p^{n_2},\ p^{n_2} >> p^{n_3}, \ldots, p^{n_{k-2}} >> p^{n_{k-1}},\ p^{n_{k-1}} >> m. \tag{3}$$

Справедливими є твердження 1 та 2.

Твердження 1. Детермінований генератор ПВП, що функціонує згідно з алгоритмом багатомодульного перетворення:

$$b_i = \Big(\left(\theta_j\right)^i \Big(\mathrm{mod}\left(f\left(X\right), p, n\right), \left(f_1\left(X\right), p_1, n_1\right), \left(f_2\left(X\right), p_2, n_2\right), \ldots \\ \ldots, \left(f_{k-1}\left(X\right), p_{k-1}, n_{k-1}\right), \left(f_m\left(X\right), m\right)\Big), \tag{4}$$

параметрів, m — певне натуральне число, k — ступінь багатомодульності, p_m — число (не обов'язково просте), забезпечує генерування ПВП (символів) з періодом повторення $p^n - 1$, рівноймовірно і з певною основою алфавіту m за умови, що:

1) виконуються умови (1)–(3);
2) модулі (пари поліномів)

$$\left(f\left(X\right),f_1\left(X\right)\right),\left(f_1\left(X\right),f_2\left(X\right)\right),\ldots,\left(f_{k-2}\left(X\right),f_{k-1}\left(X\right)\right) \tag{5}$$

є взаємно простими, а кортеж ($f_m\left(X\right),m$) є довільним.

В умові (4) запис $\left(f_m\left(x\right),m\right)$ означає, що модуль m подається у вигляді полінома.

При виконанні умов (4)–(5) забезпечується генерування ПВП (символів) з такими властивостями і характеристиками: довільною основою алфавіту m; періодом повторення p^n-1; символи генеруються рівноймовірно або «практично» рівноймовірно; ансамблем ізоморфізмів $\varphi\left(p^n-1\right)$.

Твердження 2. Детермінований генератор ПВП, що функціонує згідно з алгоритмом багатомодульного перетворення

$$\begin{aligned} b_i = \Bigg(\left(\theta_j\right)^{K_0+i}\Big(\operatorname{mod}\left(f\left(X\right),p,n\right),\left(f_1\left(X\right),p_1,n_1\right),\ldots \\ \ldots,\left(f_{k-1}\left(X\right),p_{k-1},n_{k-1}\right),\left(f_m\left(X\right),\overbrace{m}\right)\Big)\Bigg), \end{aligned} \tag{6}$$

де K_0+i — поточний ключ генератора, K_0 — початковий ключ, а i — ключ сеансу, є необоротним зі складністю не нижче за $O\left(n\right)$ [1].

Розглянемо окремий випадок тверджень 1 і 2 для трьох модульного перетворення. Елементи розширення поля Галуа також генеруються згідно з (1), але (2)–(6) набувають вигляду:

$$n_1 > m\,, \tag{7}$$

$$p^{n_1} >> p^m\,,\ a_i\ \ p^n-1 \tag{8}$$

$$b_i = \left(\left(\theta_j\right)^i\left(\operatorname{mod}\left(f\left(X\right),p\right),\left(f_1\left(X\right),p_1,n_1\right),\left(f_m\left(X\right),\overbrace{m}\right)\right)\right), \tag{9}$$

$$b_i = \left(\left(\theta_j\right)^{K_0+i}\left(\operatorname{mod}\left(f\left(X\right),p\right),\left(f_1\left(X\right),p_1,n_1\right),\left(f_m\left(X\right),\overbrace{m}\right)\right)\right). \tag{10}$$

Для умов (7)–(10) твердження 1 для трьох модульного перетворення подамо у вигляді теореми 1.

Теорема 1. Детермінований генератор ПВП, що функціонує згідно трьох модульного перетворення на основі (1) за правилами:

$$b_i = \left(\left(\theta_j\right)^i\left(\operatorname{mod}\left(f\left(X\right),p,n\right),\left(f_1\left(X\right),p_1,n_1\right),\left(f_m\left(X\right),\overbrace{m}\right)\right)\right) \tag{11}$$

або

$$b_i = \left(\left(\theta_j\right)^{k_0+i} \left(\mathrm{mod}\left(f\left(X\right), p, n\right), \left(f_1\left(X\right), p_1, n_1\right), \left(f_m\left(X\right), \overbrace{m} \right) \right) \right), \qquad (12)$$

при виконанні умов (2)–(8), забезпечує генерування ПВП (символів) чисел з довільною основою алфавіту m, з періодом повторення $p^n - 1$, рівноймовірною появою символів на періоді повторення та ансамблем ізоморфізмів $\varphi\left(p^n - 1\right)$.

Доведення теореми 1 для трьох модульного перетворення наведено [3]. У цілому, алгоритм екстрактору, що реалізує рівноймовірність появи *m*-символів (кінцевого алфавіту) для перспективного КГВЧ на основі багатомодульного перетворення може бути зведений до такого.

1. Увести або генерувати загальносистемні параметри — кортежі загальних параметрів $\left(f_s\left(X\right), p_s, n_s\right)$ згідно з вимогами твердження 1.
2. Увести або інсталювати таємний ключ генератора k, $k = 1 \div p^n - 1$.
3. Обчислити початкове значення генератора a_0, використовуючи правило:

$$a_0 = \theta^k \left(\mathrm{mod}\left(f\ \left(x\right), n\right)\right),$$

де $\left(f\ \left(x\right), n\right)$ — основний модуль перетворення.

4. Обчислити елемент a_i генератора, використовуючи правило:

$$a_i = a_{i-1}\theta\left(\mathrm{mod}\left(f\ \left(x\right), n\right)\right) = R_{\left(f\left(x\right), n_1\right)}\left(a_0\theta^i\right),$$

де $i \geq 1$ — номер елемента ПВП, що генерується, a_{i-1} — $\left(i-1\right)$-й елемент послідовності над полем поширення p^n.

5. Обчислити елемент b_i ПВП, використовуючи правило:

$$b_i = a_i(\mathrm{mod}\left(f_1\left(x\right), n_1\right)) = R_{\left(f_1\left(x\right), n_1\right)}\left(a_i\right) = R_{\left(f_1\left(x\right), n_1\right)}\left(R_{\left(f\ \left(x\right), n\right)}\left(a_0\theta^i\right)\right),$$

де $1 < \left(f_1\left(x\right), n_1\right) < \left(f\left(x\right), n\right)$.

6. Обчислити елемент c_i ПВП, використовуючи правило:

$$c_i = R_{\left(f_n\left(x\right), m_n\right)}\left(R_{\left(f_{n-1}\left(x\right), m_{n-1}\right)}\left(\ldots\left(R_{\left(f_1\left(x\right), m_1\right)}\left(a_0\theta^i\right)\right)\ldots\right)\right),$$

де $0 \leq i \leq \varphi\left(p\right)$, а $i \geq 1$ — номер елемента ПВП, що генерується, $\left(f_1\left(x\right), n_1\right), \ldots, \left(f_n\left(x\right), n_n\right)$ — проміжні модулі.

7. За необхідності обчислити i -те геш-значення від b_i та прийняти його в якості i -го випадкового слова, тобто $y_i = H(b_i)$.

Схема, яка реалізує метод побудови алгоритму екстрактору на основі багатомодульного перетворення для КГВЧ, показана на рисунку.

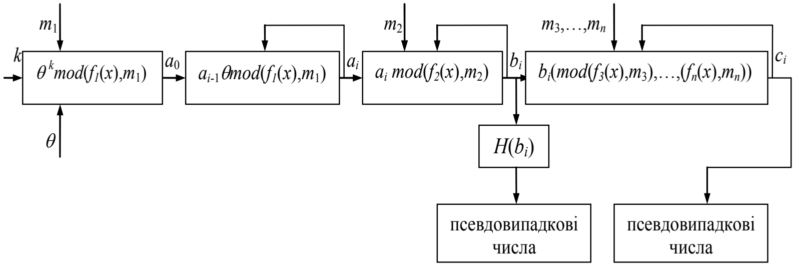


Рисунок. *Схема алгоритму екстрактора перспективного КГВЧ*

Детермінований екстрактор, що функціонує згідно з трьох модульним перетворенням на основі (11) або (12) при виконанні умов (2)–(8), забезпечує генерування ПВП (символів) чисел з певною основою алфавіту m, періодом повторення $p^n - 1$, рівноймовірною появою символів на періоді повторення $p^n - 1$ та ансамблем ізоморфізмі $\varphi\left(p^n - 1\right)$.

Для детального аналізу обчислювальної складності екстрактору необхідні додаткові дослідження. Як грубі оцінки можна використати оцінки, що наведені в роботі [1] відносно обчислювальної складності криптографічних перетворень у скінченному полі $GF\left(p^n\right)$.

Висновки. На цей час розроблено ряд алгоритмів та засобів формування екстракторів [1]. Їх особливістю є те, що вони будуються, як правило, для двійкової основи $m = 2$. Тому, важливою є задача розробки методів і засобів формування екстракторів із необхідними властивостями випадковості та довільною (певною) основою алфавіту. Найбільш перспективним, на наш погляд, серед класів таких перетворень є клас багатомодульних перетворень.

У цілому метод побудови алгоритму екстрактора на основі багатомодульного перетворення може знайти застосування у криптографічних додатках, в яких висуваються умови високої рівноймовірності та довільної основи появи символів ПВП.

Список використаних джерел:

1. Горбенко Ю. І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних сис-

тем за заг. ред. д.т.н., професора І. Д. Горбенко. Харків: Видавництво «Форт», 2016. 960 с.
2. Горбенко І. Д., Гріненко Т. О., Нарєжній О. П. Методика вимірювання спектральної щільності потужності шума квантової радіооптичної системи генератора випадкових чисел. *Радиотехника: всеукр. межвед. науч.-техн. сб.* Харьков: ХТУРЕ, 2016. Вып. 186. С. 172-183.
3. Gorbenko Y., Grinenko T. A pseudorandom sequences generator based on the multimodulo transformation. Computer science and cybersecurity. International electronic scientific journal. 2016 Issue. 1(1). P. 5-19, [Електронний ресурс]. Режим доступу: http://periodicals.karazin.ua/cscs/article/view/6194/5739.

In general form it is stated and solved the task of synthesis and analysis of extractor algorithm on the multi-module transformation with alphabet basis greater than two for prospective quantum random numbers generator (QRNG). The work was lead within a framework of complex theoretical and experimental researches for creation of QRNG prototype based on double radio-optic resonance in alkaline metal pairs.

Key words: *quantum random numbers generator; physical quantum noise; extractor of quantum random numbers generator; computation complexity of the algorithm.*

Одержано 05.03.2017

УДК 519.6

М. О. Недашковський*, д-р фіз.-мат. наук, професор,
Т. І. Крошка,** старший викладач

*Університет Казимира Великого, м. Бидгощ, Польща,
**Буковинський державний фінансово-економічний університет, м. Чернівці

РОЗВ'ЯЗУВАННЯ МАТРИЧНИХ ПОЛІНОМІАЛЬНИХ РІВНЯНЬ ІЗ ВЕКТОРНИМИ НЕВІДОМИМИ

Пропонуються нові обчислювальні схеми розв'язання поліноміальних матричних рівнянь з векторними невідомими за допомогою ланцюгових дробів.

Ключові слова: *поліноміальні матричні рівняння, ланцюгові дроби.*

Вступ. У роботах В. С. Григорківа [1–4] було розглянуто пряму нелінійну балансову модель міжгалузевої еколого-економічної взаємодії а також двоїсту до неї модель відносно цін. Аторами показано [5], що ця нелінійна модель зводиться до поліноміального матричного рівняння із векторними невідомими вигляду

$$A_n diag(X)^{n-1} X + A_{n-1} diag(X)^{n-2} X + ... + A_1 X + B = 0 . \qquad (1)$$

Тут A_i $(i = 1, 2, ..., n)$ — квадратні матриці розмірністю $m \times m$, а X — вектори розміру m. Однак, до останнього часу ефективних методів для подібних рівнянь не було відомо.

Пропонуються дві схем розв'язання рівнянь виду (1).

СХЕМА 1. Розлядається рівняння 3-го порядку

$$A_3 \left(diag(X) \right)^2 X + A_2 \left(diag(X) \right) X + A_1 X + B = 0 . \tag{2}$$

На його основі після нескладного перетворення

$$\left(A_3 (diag(X))^2 + A_3 diag(X) + (A_2 - A_3) \cdot diag(X) + A_1 \right) X + B = 0 . \tag{3}$$

Введемо тепер позначення

$$Y = A_3 \left(E \cdot diag(X) \right)^2 + A_3 \left(E \cdot diag(X) \right)^{-1} .$$

Тоді $\left(Y^{-1} + (A_2 - A_3) diag(X) + A_1 \right) X + B = 0$.

Звідки отримуємо рекурентне співвідношення для X

$$X = -\left(A_1 + (A_2 - A_3) diag(X) + Y^{-1} \right)^{-1} B .$$

А для обчислення Y у свою чергу можна записати

$$Y = \left(A_3 (diag(X))^2 + A_3 \cdot diag(X) \right)^{-1} = \left(A_3 \left(diag(X) + E \right) \left(diag(X) \right) \right)^{-1} .$$

Далі

$$\left(A_3 (diag(X) + E)(diag(X)) \right)^{-1} = \left(diag(X) \right)^{-1} \left(diag(X) + E \right)^{-1} A_3^{-1} .$$

Звідки $Y = [diag(X)]^{-1} [diag(X) + E]^{-1} A_3^{-1}$.

З іншого боку

$$[diag(X)]^{-1} - [diag(X) + E]^{-1} = \left[diag(X) \right]^{-1} \left[diag(X) + E - diag(X) \right] \times$$

$$\times \left[diag(X) + E - diag(X) \right]^{-1} = [E \cdot diag(X)]^{-1} E [diag(X)] + E]^{-1}.$$

Звідки негайно випливає, що

$$Y = \left(\left(diag(X) \right)^{-1} - \left(diag(X) + E \right)^{-1} \right) A_3^{-1} .$$

Отже, ітераційний процес можна проводити за співвідношеннями

$$Y^{k+1} = \left(\left(diag(X^k) \right)^{-1} - \left(diag(X^k) + E \right)^{-1} \right) A_3^{-1} ,$$

$$X^{k+1} = -\left(A_1 + (A_2 - A_3) diag(X^k) + (Y^k)^{-1} \right)^{-1} B .$$

Звідки $(Y^{k+1})^{-1} = A_3 \left(\left(diag(X^k) \right)^{-1} - \left(diag(X^k) + E \right)^{-1} \right)^{-1}$.

Об'єднуючи разом рекурентні формули для обчислення X^{k+1} та Y^{k+1} можна записати наступну ітераційну схему:

$$X^{k+1} = \left(A_1 + (A_2 - A_3) diag(X^k) + A_3 \left(\left(diag(X^k) \right)^{-1} - \left(diag(X^k) + E \right)^{-1} \right)^{-1} \right)^{-1} B.$$

Послідовне застосування закону композиції для X^{k+1} дає наступне розвинення X в одно періодичний гіллястий ланцюговий дріб з двома вітками розгалуження.

$$X = -\Big(A_1 + (A_2 - A_3) diag((-(A_1 + ...)^{-1} B)^k) +$$

$$+ A_3 ((diag((-(A_1 + ...)^{-1} B)^k))^{-1} - (diag((-(A_1 + ...)^{-1} B)^k) + E)^{-1})^{-1} \Big)^{-1}$$

Приклад 1. Розглянемо як ілюстрацію ефективності даної схеми матричне рівняння 3-го порядку

$$A_3 \left(diag(X) \right)^2 X + A_2 \left(diag(X) \right) X + A_1 X + B = 0 , \qquad (4)$$

де

$$A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \ A_2 = \begin{pmatrix} 2.012 & -3.4 & -5.03 \\ 2.2 & 2.51 & 0.25 \\ 2 & -2.34 & -0.13 \end{pmatrix}; \ A_1 = \begin{pmatrix} 0.979 & 5.968 & -5.0 \\ 0.245 & 2.2 & 0.251 \\ 2.34 & -1.3 & 0.212 \end{pmatrix};$$

$$B = \begin{pmatrix} 33.0099 & -7.1837 & -8.9359 \end{pmatrix}^T .$$

За допомогою пакету MatLab це матричне рівняння розв’язувалося з використанням рекурентної формули

$$X^{k+1} = \left(A_1 + (A_2 - A_3) diag(X^k) + A_3 \left(\left(diag(X^k) \right)^{-1} - \left(diag(X^k) + E \right)^{-1} \right)^{-1} \right)^{-1} B.$$

В результаті обчисленнь при початковому наближенні

$$X_0 = \begin{pmatrix} -1.21 & 0.61 & 2.2 \end{pmatrix}^T$$

отримано наближений розв'язок

$$X_k = \begin{pmatrix} 0.3689 & 0.9258 & 2.2352 \end{pmatrix}^T .$$

Результати експерименту наведені в табл. 1.

Таблиця 1

$\left\| X_k - X_{k-1} \right\| / \left\| X_k \right\|$	Кількість ітерацій	Величина нев'язки
1.000000e-004	48	8.153217e-004
1.000000e-005	56	8.351903e-005
1.000000e-006	64	8.560547e-006
1.000000e-007	72	8.767670e-007
1.000000e-008	80	8.983232e-008
1.000000e-009	88	9.202762e-009
1.000000e-010	97	7.091406e-010
1.000000e-011	105	7.266972e-011

На жаль, дану схему поки що не вдається узагальнити на випадок рівняння n -го порядку.

СХЕМА 2. Для рівняння (1) 3-го порядку можна також записати

$$\left(A_3 diag(X)^2 + A_2 diag(X) + A_1\right)X + B = 0 .$$

І далі $\left(\left(A_3 diag(X) + A_2\right) diag(X) + A_1\right)X + B = 0$.

Якщо тепер ввести позначення $Y = \left(A_2 + A_3 diag(X)\right)^{-1}$, то для обчислення X можна записати $\left(Y^{-1} \cdot diag(X) + A_1\right)X + B = 0$.

Звідки $X = -\left(A_1 + Y^{-1} \cdot diag(X)\right)^{-1} B$.

Отже, підрахунок значення X може бути проведений за рекурентними співвідношеннями

$$Y^{k+1} = \left(A_2 + A_3 diag(X^k)\right)^{-1} , \tag{5}$$

$$X^{k+1} = -\left(A_1 + (Y^k)^{-1} \cdot diag(X^k)\right)^{-1} B . \tag{6}$$

Приклад 2. Розглянемо тепер матричне рівняння (5) з коефіцієнтами

$$A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \; A_2 = \begin{pmatrix} 1.991 & -3.2 & -5.02 \\ 2.2 & 2.51 & 0.25 \\ 2.0 & -2.34 & -0.132 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0.979 & 5.968 & -5.0 \\ 0.245 & 2.2 & 0.251 \\ 2.34 & -1.3 & 0.212 \end{pmatrix};$$

$$B = \begin{pmatrix} 32.8882 & -7.1897 & -8.9086 \end{pmatrix}^T .$$

За допомогою пакету MatLab це матричне рівняння розв’язувалося з використанням рекурентних формул

$$Y^{k+1} = \left(A_2 + A_3 diag(X^k)\right)^{-1} ,$$

$$X^{k+1} = -\left(A_1 + (Y^k)^{-1} \cdot diag(X^k)\right)^{-1} B .$$

У результаті обчисленнь при початковому наближенні

$$X_1^0 = \begin{pmatrix} -1.21 & 0.61 & 2.2 \end{pmatrix}^T$$

обчислено такі значення наближеного розв'язку

$$X_k = \begin{pmatrix} 0.3614 & 0.9277 & 2.2379 \end{pmatrix}^T$$

Результати експерименту наведені в табл. 2.

Таблиця 2

$\lVert X_k - X_{k-1} \rVert / \lVert X_k \rVert$	Кількість ітерацій	Величина нев'язка
1.000000e-004	60	7.378027e-004
1.000000e-005	68	7.645293e-005
1.000000e-006	76	7.776666e-006
1.000000e-007	84	7.943752e-007
1.000000e-008	92	8.107417e-008
1.000000e-009	100	8.275652e-009
1.000000e-010	108	8.447562e-010
1.000000e-011	116	8.624885e-011

Дана схема, на відміну від попередньої, може бути узагальнена і на випадок матричних поліноміальних рівнянь вищого порядку.

Поліноміальне матричне рівняння n-го порядку. Для поліноміального матричного рівняння (1) можна записати

$$\left(A_n diag(X)^{n-1} + A_{n-1} diag(X)^{n-2} + \ldots + A_2 diag(X) + A_1\right)\cdot X + B = 0\,. \quad (7)$$

Введемо тепер до розгляду Y_1 вигляду

$$Y_1 = \left(A_n diag(X)^{n-1} + A_{n-1} diag(X)^{n-2} + \ldots + A_2 diag(X) + A_1\right)^{-1}. \quad (8)$$

Тоді з урахуванням (7) і (8) можна записати

$$X = -\left(A_1 + Y_1^{-1}\right)\cdot B\,.$$

А далі

$$Y_1 = \left(\left(A_n diag(X)^{n-1} + A_{n-1} diag(X)^{n-2} + \ldots + A_2\right) diag(X) + A_1\right)^{-1}. \quad (9)$$

І використовуючи позначення

$$Y_2 = \left(A_n diag(X)^{n-2} + A_{n-1} diag(X)^{n-3} + \ldots A_3 diag(X) + A_2\right)^{-1}. \quad (10)$$

Для Y_1 можна записати

$$Y_1 = \left(A_1 + Y_2^{-1} diag(X)\right)^{-1}. \quad (11)$$

За аналогією ввівши для (7) позначення

$$Y_3 = \left(A_n diag(X)^{n-3} + A_{n-1} diag(X)^{n-4} + \ldots + A_4 diag(X) + A_3\right)^{-1},$$

для Y_2 отримуємо

$$Y_2 = \left(A_2 + Y_3^{-1} diag(X)\right)^{-1}.$$

Продовжуючи далі цей ступінчатий процес, для Y_{n-1} отримуємо

$$Y_{n-2} = \left(A_{n-2} + Y_{n-1}^{-1} diag(X)\right)^{-1}, \quad (12)$$

де в свою чергу

$$Y_{n-1} = \left(A_{n-1} + A_n diag(X) \right)^{-1} . \qquad (13)$$

Таким чином, вдається записати ітераційну схему для обчислення розв'язків матричного поліноміального рівняння із застосуванням апарату матричних ланцюгових дробів.

$$\left.\begin{array}{ll} Y_{n-1}^{k+1} & = \left(A_{n-1} + A_n diag(X^k) \right)^{-1} \\ Y_i^{k+1} & = \left(A_i + (Y_{i+1}^k)^{-1} diag(X^k) \right)^{-1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Y_1^{k+1} & = \left(A_1 + (Y_2^k)^{-1} diag(X^k) \right)^{-1} \\ X^{k+1} & = -\left(A_1 + (Y_1^k)^{-1} \right) \cdot B \end{array}\right\} . \qquad (14)$$

Послідовне застосування отриманих формул надає можливість обчислити X^m із заданою точністю ε на основі перевірки нерівності

$$\left\| X^m - X^{m-1} \right\| \le \varepsilon .$$

З іншого боку, на основі (14) можна записати X у вигляді розвинення розв'язку у неперервний матричний ланцюговий дріб.

Дослідження збіжності наведених обчислювальних схем пов'язано зі збіжністю матричних гіллястих дробів вигляду [6]

$$D = \mathop{D}_{i=1}^{\infty} \sum_{k(i)=1}^{n} a_{k_{(i)}} \frac{c_{k_{(i)}}}{b_{k_{(i)}}} . \qquad (15)$$

Тут V — банахів простір квадратних матриць порядку $p \times p$ над полем дійсних чисел; $k_{(i)} = k_1 k_2 ... k_i$ — скорочені позначення для мультиіндексів; $a_{k_{(i)}}, b_{k_{(i)}}, c_{k_{(i)}} \in V$ — матриці розмірності $p \times p$.

Твердження 1. Якщо розв'язок поліноміального матричного рівняння існує і належить інтервалу $[-n, n]$, то розвинення за деякою ітераційною процедурою у МГЛД з елементами, що задовольняють умови

$$\left\| b_{k_{(s)}} \right\| \le \frac{1}{\left\| a_{k_{(s)}} \right\| \left\| c_{k_{(s)}} \right\| + n} \qquad (1 \le k_s \le n; s = 1, 2, 3 ...)$$

збігається до цього розв'язку.

Твердження 2. Якщо розв'язок поліноміального матричного рівняння існує і належить інтервалу $[-\sum_{k_1=1}^{n} \left\| a_{k_1} \right\| \left\| c_{k_1} \right\|, \sum_{k_1=1}^{n} \left\| a_{k_1} \right\| \left\| c_{k_1} \right\|]$ то розвинення за деякою ітераційною процедурою у МГЛД з елементами, що задовольняють умови

$$\left\| b_{k(s)}^{-1} \right\| \le \frac{1}{1 + \sum\limits_{k_{s+1}=1}^{n} \left\| a_{k(s+1)} \right\| \left\| c_{k(s+1)} \right\|} \qquad (s = 1, 2, 3...)$$

збігається до цього розв’язку.

Висновки. Таким чином, побудовано ефективний метод для аналітичного запису розв'язку матричного поліноміального рівняння n-го порядку або обчислення його наближеного значення із заданою точністю.

Список використаних джерел:

1. Григорків В. С. Моделювання еколого-економічної взаємодії: Навчальний посібник. Чернівці: Рута, 2007. 84 с.
2. Григорків В. С. Моделювання економіки. Частина 2: Навчальний посібник. Чернівці: Рута, 2006. 100 с.
3. Икрамов. Х. Д. Численное решение матричных уравнений. М: Наука, 1984. 192 с.
4. Недашковський М. О. Ознаки збіжності матричних гіллястих ланцюгових дробів. Математичні методи та фізико-механічні поля. Львів. 2003. Том 46, № 4. С. 50–56.
5. Недашковський М. О., Крошка Т. І. Збіжність наближених розв`язків нелінійної задачі для моделі Леотьєва-Форда. *Фізико-математичне моделювання та інформаційні технології.* Центр математичного моделювання ІППММ ім. Я. С. Підстригача НАН України. 2013. Вип. 18. С. 126–135.
6. Скоробогатько В. Я. Теория ветвящихся цепных дробей и ее применение в вычислительной математике. М.: Наука, 1983. 311 с.

A new method for solving polynomial matrix equations with vector unknowns using continued fractions.

Key words: *Matrix polynomial equations, continued fractions.*

Одержано 01.03.2017

УДК 519.9

О. П. Нечуйвітер, д-р фіз.-мат. наук, доцент,
К. В. Кейта, аспірантка
Українська інженерно-педагогічна академія, м. Харків

ОПТИМАЛЬНЕ ІНТЕГРУВАННЯ ДВОВИМІРНИХ ШВИДКООСЦИЛЮЮЧИХ ФУНКЦІЙ ЗАГАЛЬНОГО ВИГЛЯДУ

В статті розглядається оцінка знизу для похибки чисельного інтегрування швидкоосцилюючих функцій загального вигляду на класі диференційовних функцій у випадку, коли інформація про функції задана їх слідами на відповідних лініях.

Ключові слова: *кубатурна формула, інтеграл від швидкоосцилюючої функції, клас диференційовних функцій.*

Вступ. Сучасний етап розвитку багатьох технічних галузей (астрономії, радіології, комп’ютерної томографії, голографії, радіолокації) характеризується бурхливим впровадженням нових цифрових технологій, алгоритмів, методів. Перед науковцями стає питання побудови нових або вдосконалення відомих математичних моделей, зокрема, математичних моделей в цифровій обробці сигналів та зображень, які містять нові типи задання інформації.

Задача наближеного обчислення інтегралів від швидкоосцилюючих функцій двох змінних має як класичне розв’язання, так і у випадку різних інформаційних операторів [1]. В роботах [1, 2] наведені класичні алгоритми обчислення двовимірних інтегралів від швидкоосцилюючих функцій загального вигляду, однак не досліджувалося питання наближеного обчислення інтегралів від швидкоосцилюючих функцій двох змінних загального вигляду у випадку різних інформаційних операторів. Отже питання дослідження кубатурних формул наближеного обчислення інтегралів від швидкоосцилюючих функцій загального вигляду

$$I(f,g,\omega)=\int_0^1\int_0^1 f(x,y)\sin\omega g(x,y)dxdy \tag{1}$$

у випадку, коли інформація про $f\left(x,y\right)$ та $g\left(x,y\right)$ задана відповідними їх слідами на лініях є актуальною задачею.

Дана стаття присвячена знаходженню оцінки знизу для похибки чисельного інтегрування інтегралів вигляду (1) на класі диференційовних функцій.

Оцінка знизу для похибки чисельного інтегрування швидкоосцилюючих функцій загального вигдяду на класі $H^{2,r}\left(M,\widetilde{M}\right)$.

Припустимо, що $f(x,y)\in F$, $g\left(x,y\right)\in G$, F, G — множини функцій, визначених в області $[a,b]\times[a,b]$. Позначимо L_N множину всіх квадратурних формул $l_N(f,g)$, що використовують інформацію про значення функцій $f(x,y)$ та $g(x,y)$ не більше ніж на N лініях. Введемо величини

$$R_N(f,g,\omega,l_N)=\left|I(f,g,\omega)-l_N(f,g)\right|,$$

$$R_N(F,G,\omega,l_N)=\sup_{f\in F,\ g\in G} R_N(f,g,\omega,l_N),$$

$$R_N(F,G,\omega)=\inf_{l_N\in L_N} R_N(F,G,\omega,l_N).$$

Кубатурну формулу $l_N^*(f,g)$, на якій досягається $R_N(F,G,\omega)$, будемо називати оптимальною за точністю кубатурною формулою. Якщо $R_N\left(F,G,\omega,\bar{l}_N\right)\le R_N(F,G,\omega)+\eta$, $\eta>0$, то $\bar{l}_N$ називається оптимальною за точністю формулою обчислення $I(f,g,\omega)$ з точністю до η. Якщо $\eta=o(R_N)$ або $\eta=O(R_N)$, то $\bar{l}_N$ називається асимптотично оптимальною або оптимальною за порядком точності.

Розглянемо $H^{2,r}\left(M,\widetilde{M}\right)$ – клас дійсних функцій $r\ge 0$ визначених на $G=[0,1]^2$ і таких, що частинні похідні порядку r по змінній x та y обмежені, тобто

$$\left|f^{(r,0)}(x,y)\right|\le M,\quad \left|f^{(0,r)}(x,y)\right|\le M,\ r\ne 0,\ \left|f^{(r,r)}(x,y)\right|\le \widetilde{M},\quad r\ge 0.$$

Теорема. Нехай $f(x,y),\ g(x,y),\in H^{2,r}\left(M,\widetilde{M}\right),$ функції $f(x,y),$ $g(x,y)$ задані слідами на відповідних системах взаємно перпендикулярних прямих в області $G=[0,1]^2$, тоді

$$R_N\left(H^{2,r}\left(\mathrm{M},\widetilde{M}\right),H^{2,r}\left(M,\widetilde{M}\right),\omega\right)\ge K\max\left\{\frac{1}{\ell^{2r}},\min\left\{1,\frac{|\omega|}{\ell^{2r}}\right\}\right\}.$$

Доведення. K,K_1,K_2,K_3 будемо позначати константи, які будуть залежати лише від r, $\widetilde{M}$. Нехай $\psi_r(x,b-a)=(x-a)^r(b-x)^r$, тоді $\left|\psi_r(x,b-a)\right|\le C(r)(b-a)^r$,

$$\int_a^b\psi_r(x,b-a)\,dx=c_1(r)(b-a)^{2r+1}=\frac{r!r!}{(2r+1)!}(b-a)^{2r+1},$$

$$C(r)=\sup_{0\le t\le 1}\left|\Phi_r^{(r)}(t)\right|=r!\,,\ c_1(r)=\int_0^1\Phi_r(t)\,dt\,,\ \Phi_r(t)=t^r(1-t)^r\,.$$

Розіб'ємо область $G=[0,1]^2$ на підобласті

$$\left[x_0^1,x_0^1+h\right]\times\left[y_0^1,\mathrm{y}_0^1+h\right],\ \left[x_1^1,x_1^1+h\right]\times\left[y_1^1,\mathrm{y}_1^1+h\right],...,$$

$$\left[x_{\ell-1}^1,x_{\ell-1}^1+h\right]\times\left[y_{\ell-1}^1,\mathrm{y}_{\ell-1}^1+h\right],$$

$$\left[x_0^2,x_0^2+h\right]\times\left[y_0^2,\mathrm{y}_0^2+h\right],\ \left[x_1^2,x_1^2+h\right]\times\left[y_1^2,\mathrm{y}_1^2+h\right],...,$$

$$\left[x_{\ell-1}^2,x_{\ell-1}^2+h\right]\times\left[y_{\ell-1}^2,\mathrm{y}_{\ell-1}^2+h\right],\ h=\frac{1}{4\ell}\,.$$

Тоді число підобластей, куди не попали лінії інтегрування кубатурної формули, дорівнює $4\ell^2$. Розглянемо функцію

$$f^*(x,y)=\frac{\widetilde{M}}{\left(C(r)\right)^2}\frac{\psi_r\left(x,x_k^1,x_k^1+h\right)}{h^r}\cdot\frac{\psi_r\left(y,y_q^1,y_q^1+h\right)}{h^r}$$

на тих підобластях, куди не попали лінії інтегрування кубатурної формули, а на всіх інших $f^*(x,y)=0$.

Позначимо $\chi(x)$ нескінченно диференційну на числовій прямій функцію, яка приймає значення 0 при $x\le 0, x\ge 1$, значення 1 при $\frac{1}{4}\le x\le\frac{3}{4}$ і таку, що $0<\chi(x)<1$ при $0<x<\frac{1}{4},\frac{3}{4}<x<1$. Нехай $C_0=\max\left\{1,\max\limits_{0\le x\le 1}\left|\chi^{(r)}(x)\right|\right\}$, а D_1 — число, що задовольняє співвідношення $signD_1=sign\omega,\quad 0<D_1<1$, $\left|D_1\right|\frac{\widetilde{M}}{\left(C(r)\right)^2 4^{4r}}\le\frac{\pi}{2}$. Число D_2 буде визначатися наступними умовами: якщо $\frac{\widetilde{M}}{\left(C_0\right)^2 4^{2r}}\le\frac{\pi}{2}$, то D_2 задовольняє співвідношенням $signD_2=sign\omega,\quad \frac{\omega}{\ell^{2r}}D_2=1$, а якщо $\frac{\widetilde{M}}{\left(C_0\right)^2 4^{2r}}>\frac{\pi}{2}$, то маємо $signD_2=sign\omega,\quad \omega D_2\frac{\widetilde{M}}{\left(C_0\right)^2}h^{2r}=\frac{\pi}{2}$. Визначимо функцію

$$\tau(x,y)=\frac{\widetilde{M}D_1}{\left(C(r)\right)^2}\frac{\psi_r\left(x,x_k^2,x_k^2+h\right)}{h^r}\cdot\frac{\psi_r\left(y,y_q^2,y_q^2+h\right)}{h^r},\ \text{при}\ \ell\ge|\omega|^{1/2r},$$

$$\tau(x,y)=\frac{\widetilde{M}D_2}{\left(C_0\right)^2}h^{2r}\chi\left(\frac{x-x_k^2}{h}\right)\chi\left(\frac{y-y_q^2}{h}\right),\ \text{при}\ \ell<\left|\omega\right|^{1/2r}$$

на тих підобластях, куди не попали лінії інтегрування кубатурної формули, а на всіх інших $\tau(x,y)=0$. Позначимо

$$I_1=I_1(\omega,f^*,\tau)=\frac{1}{2}\int_0^1\int_0^1\left[\widetilde{M}+f^*(x,y)\right]e^{i\omega\tau(x,y)}dxdy\ ,$$

$$I_2=I_2(\omega,f^*,\tau)=\frac{1}{2}\int_0^1\int_0^1\left[\widetilde{M}-f^*(x,y)\right]e^{-i\omega\tau(x,y)}dxdy\ .$$

Розглянемо

$$I_1(\omega,f^*,\tau)-I_2(\omega,f^*,\tau)=\frac{1}{2}\int_0^1\int_0^1\left[\widetilde{M}+f^*(x,y)\right]e^{i\omega\tau(x,y)}dxdy-$$

$$-\frac{1}{2}\int_0^1\int_0^1\left[\widetilde{M}-f^*(x,y)\right]e^{-i\omega\tau(x,y)}dxdy=$$

$$=\int_0^1\int_0^1 f^*(x,y)\cos\left(\omega\tau(x,y)\right)dxdy+i\widetilde{M}\int_0^1\int_0^1\sin\left(\omega\tau(x,y)\right)dxdy=$$

$$=\int_0^1\int_0^1 f^*(x,y)dxdy+i\widetilde{M}\int_0^1\int_0^1\sin\left(\omega\tau(x,y)\right)dxdy.$$

Маємо

$$\int_0^1\int_0^1 f^*(x,y)dxdy=$$

$$=\frac{\widetilde{M}}{\left(C(r)\right)^2}\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^1}^{x_k^1+h}\int_{y_q^1}^{y_q^1+h}\frac{\psi_r\left(x,x_k^1,x_k^1+h\right)}{h^r}\cdot\frac{\psi_r\left(y,y_q^1,y_q^1+h\right)}{h^r}dxdy=$$

$$=\frac{\widetilde{M}}{\left(C(r)\right)^2}\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\frac{\left(c_1(r)\right)^2h^{2r+1}\cdot h^{2r+1}}{h^r\cdot h^r}=$$

$$=\frac{\widetilde{M}\cdot\left(c_1(r)\right)^2}{\left(C(r)\right)^2}\frac{1}{4^{r+1}\ell^r}\frac{1}{4^{r+1}\ell^r}=\frac{\widetilde{M}\cdot\left(c_1(r)\right)^2}{\left(C(r)\right)^2}\frac{1}{4^{2r+2}\ell^{2r}}=K_1\frac{1}{\ell^{2r}}\ .$$

При

$$\ell\geq\left|\omega\right|^{1/2r},\ \psi_{1r}=\psi_r\left(x,x_k^2,x_k^2+h\right),\psi_{2r}=\psi_r\left(y,y_q^2,y_q^2+h\right)$$

$$\int_0^1\int_0^1 \sin\left(\omega\tau(x,y)\right)dxdy=\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^2}^{x_k^2+h}\int_{y_q^2}^{y_q^2+h}\sin\left(|\omega||D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2}\frac{\psi_{1r}}{h^r}\cdot\frac{\psi_{2r}}{h^r}\right)dxdy\,.$$

Оскільки $\max\limits_{x_k^2\le x\le x_k^2+h}\psi_{1r}=\left(\dfrac{h}{2}\right)^{2r}$, $\max\limits_{y_q^2\le y\le y_q^2+h}\psi_{2r}=\left(\dfrac{h}{2}\right)^{2r}$, то

$$|\omega||D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2}\frac{\psi_{1r}}{h^r}\cdot\frac{\psi_{2r}}{h^r}\le|\omega||D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2}\frac{1}{h^r}\left(\frac{h}{2}\right)^{2r}\frac{1}{h^r}\left(\frac{h}{2}\right)^{2r}=$$

$$=|\omega||D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2 4^r4^r}h^rh^r\le|D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2 4^{2r}4^{2r}}\le\frac{\pi}{2}\,.$$

Якщо $0\le t\le\dfrac{\pi}{2}$ справедлива наступна нерівність $\sin t\ge\dfrac{2}{\pi}t$. Використавши цю нерівність, отримуємо:

$$\int_0^1\int_0^1 \sin\left(\omega\tau(x,y)\right)dxdy\ge\frac{4}{\pi^2}\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^2}^{x_k^2+h}\int_{y_q^2}^{y_q^2+h}|\omega||D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2}\frac{\psi_{1r}}{h^r}\cdot\frac{\psi_{2r}}{h^r}dxdy=$$

$$=\frac{4}{\pi^2}\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}|\omega||D_1|\frac{\widetilde{M}}{\left(C(r)\right)^2}\left(c_1(r)\right)^2h^{r+1}h^{r+1}=$$

$$=\frac{|\omega||D_1|}{\pi^2}\widetilde{M}\frac{\left(c_1(r)\right)^2}{\left(C(r)\right)^2}\frac{1}{4^{2r+1}}\frac{1}{\ell^{2r}}=K_2\frac{|\omega|}{\ell^{2r}}\,.$$

Нехай $\ell<|\omega|^{1/2r}$, $\chi_1=\chi\left(\dfrac{x-x_k^2}{h}\right)$, $\chi_2=\chi\left(\dfrac{y-y_q^2}{h}\right)$, тоді

$$\int_0^1\int_0^1\sin\left(\omega\tau(x,y)\right)dxdy=\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^2}^{x_k^2+h}\int_{y_q^2}^{y_q^2+h}\sin\left(\omega\frac{\widetilde{M}D_2}{\left(C_0\right)^2}h^{2r}\chi_1\chi_2\right)dxdy=$$

$$=\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^2}^{x_k^2+h}\int_{y_q^2}^{y_q^2+h}\sin\left(\min\left(\frac{\widetilde{M}}{\left(C_0\right)^2 4^{2r}},\frac{\pi}{2}\right)\chi_1\chi_2\right)dxdy\ge$$

$$\ge\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^2}^{x_k^2+h}\int_{y_q^2}^{y_q^2+h}\min\left(\frac{\widetilde{M}}{\left(C_0\right)^2 4^{2r}},\frac{\pi}{2}\right)\chi_1\chi_2dxdy\ge$$

$$\ge K_2\sum_{k=0}^{\ell-1}\sum_{q=0}^{\ell-1}\int_{x_k^2}^{x_k^2+h}\int_{y_q^2}^{y_q^2+h}dxdy=K_2\ell^2\frac{h^2}{4}=K_2\ell^2\frac{1}{4^3\ell^2}=\frac{K_2}{64}\,.$$

Функції $\frac{1}{2}\left[\widetilde{M}+f^*(x,y)\right]$, $\frac{1}{2}\left[\widetilde{M}-f^*(x,y)\right]$ та функції $\tau(x,y)$, $-\tau(x,y)$ такі, що при наближеному обчисленні інтегралів $I_1 = I_1(\omega, f^*, \tau)$, $I_2 = I_2(\omega, f^*, \tau)$ за квадратурною формулою $l_N\left(f, g\right)$ буде отриманий один і той же результат $I_0 = I_0(\omega, f^*, \tau)$. Оскільки $\left|I_1 - I_0\right| + \left|I_2 - I_0)\right| \geq \left|I_1 - I_2\right|$, то хоча б одна з величин $\left|I_1 - I_0)\right|$, $\left|I_2 - I_0\right|$ не менше половини величини $K_3 \max\left\{\frac{1}{\ell^{2r}}, \min\left\{1, \frac{|\omega|}{\ell^{2r}}\right\}\right\}$. Значить похибка наближення на класі не менше $K \max\left\{\frac{1}{\ell^{2r}}, \min\left\{1, \frac{|\omega|}{\ell^{2r}}\right\}\right\}$.

Висновки. У статті отримана оцінка знизу для похибки чисельного інтегрування швидкоосцилюючих функцій загального вигляду на класі диференційовних функцій. Результат надасть змогу досліджувати якість кубатурних формул обчислення 2 D інтегралів від швидкоосцилюючих функцій загального вигляду у випадку різних інформаційних операторів.

Список використаних джерел:

1. Сергієнко І. В., Задірака В. К., Литвин О. М., Мельникова С. С., Нечуйвітер О. П. Оптимальні алгоритми обчислення інтегралів від швидкоосцилюючих функцій та їх застосування: у 2 т. Т. 1. Алгоритми: [монографія]. К.: Наук. думка, 2011. 447 с.
2. Iserles A., Norsett S. P. Efficient quadrature of highly-oscillatory integrals using derivatives. *Tech. Reports Numerical Analysis* (NA2004/03)/ DAMPT. University of Cambridge. 14 p.

The paper is devoted to the calculation of two-dimensional integral from highly oscillating functions of general view in case when the information about functions is a set of lines. The estimation of numerical integration has been obtained on the class of differentiable functions.

Key words: *cubature formula, integral from highly oscillating function, class of differentiable functions.*

Одержано 23.02.2017

УДК 519.1

В. І. Петренюк, канд. фіз.-мат. наук, доцент
Центральноукраїнський національний технічний університет,
м. Кропивницький

СТРУКТУРА 28-МИ 9-ТИ ВЕРШИННИХ ГРАФІВ-ОБСТРУКЦІЙ ТОРА

Досліджено структуру 28-ми 9-ти вершинних графів-обструкцій для тора.

Ключові слова: *граф-обструкція, тор, φ-перетворення графів.*

Вступ. Задача полягатиме у вивченні структури 9-ти вершинних графів-обструкцій для тора з метою використання при побудові *n*-вершинних, $n > 9$, графів-обструкцій для тора.

Основні визначення та позначення взято з [1]. В роботі [2] запропоновано спосіб побудови графів-обструкцій обмеженого орієнтованого роду як *φ*-образу двох графів, один з яких має бути квазізіркою, з'єднаних шляхом ототожнення пар вершин, для випадку несуттєвості порядку ототожнення зазначених пар точок; тобто один із підграфів, породжених підмножинами точок, допускатиме перестановку довільної пари точок з'єднання, наприклад, є повним графом як в D_6, D_7, D_8. Цей підхід може видавати такі графи, які набуватимуть статус обструкцій після стискання в точку усіх зайвих ребер-променів квазізірки, саме так побудовані графи D_9, D_{11}, D_{15}, D_{16}, D_{17}, D_{19}, D_{20}. Однак не всі графи-обструкції для тора можливо отримати цим способом, наприклад, такими є графи D_{12}, D_{13}, D_{14}, D_{17}, D_{18}, D_{21}, D_{27}. Одна з причин відсутності зайвих ребер — необхідність двостороннього доступу до деяких точок із пар, що підлягають ототожненню.

Лема 1. Для D_4, D_5, D_6, D_7 мають місце наступні *φ*-перетворення:

1) $\varphi(K_{3,3} + K, \sum_{i=1}^{6}(i' \underset{\bullet}{+} i'')) \to (D_4, \{i\}^6_1)$, $K^0_{3,3} = \{i'\}^3_{i=1} \cup \{i'\}^6_{i=4}$, $St^0{}_4(c) = \{i''\}^3_{i=1} \cup \{a\}$, $K = (\{i''\}^6_{i=1} \cup \{a,b,c\}, St^1_4(c) \cup K^1_5 \setminus \{(a,b)\})$, $K^0_5 = \{i''\}^6_{i=4} \setminus \{(a,b)\}$, $K_{3,3}(\{i'\}^3_{i=1}) \cup K_{3,3}(\{i'\}^6_{i=4}) = \overline{K_3}$, або D_4, $D_4 = (K^0_{4,5}, K^1_{4,5} \cup \{(a,c)\})$, містить підграф ізоморфний графу E_{18} [3];

2) $\varphi(K_{3,3} + K, \sum_{i=1}^{6}(i' \underset{\bullet}{+} i'')) \to (D_5, \{\{i\}^6_{i=1})$,

де $K = (\{i''\}^6_{i=1} \cup \{a,b,c\}, St^1_3(c) \cup K^1_5)$, $St^0{}_3(c) = \{i''\}^3_{i=1}$, $K^0_5 = (\{i''\}^6_{i=4} \cup \{a,b\}$, $K_{3,3}(\{i'\}^3_{i=1}) \cup K_{3,3}(\{i'\}^6_{i=4}) = \overline{K_3}$, причому D_5 має підграф ізоморфний E_3, або E_{18}, наведені в [3];

3) $\varphi(K_5 + K, \sum_{i=1}^{5}(i' \underset{\bullet}{+} i")) \to (D_6, \{\{i\}_{i=1}^{5})$,

де $K_5^0 = (\{i'\}_{i=1}^{5}$, $K_4^0 = \{a,b,c,v\}$, $K^0 = (\{i"\}_{i=1}^{5} \cup \{a,b,c,v\}$,

$$K^1 = K_4^1 \cup \{(a,1").(b,5"),(c,2"),(c,3"),(v,4"),(v,3")\};$$

4) $\varphi(K_5 + K, \sum_{i=1}^{3}(i' \underset{\bullet}{+} i")) \to (D_7, \{i\}_{i=1}^{3})$,

де $K_5^0 = \{i'\}_{i=1}^{5}$, $K^0 = \{i"\}_{i=1}^{3} \cup K_4^0$, $K_4^0 = \{a,b,c,v\}$,

$$K^1 = K_4^1 \cup \{(b,1"),(a,2"),(c,3"),(v,2")\}.$$

Лема 2. Для D_8, D_9, D_{10}, D_{11} мають місце такі φ-перетворення:

1) $\varphi(K_5 + K, \sum_{i=3,5}(i' \underset{\bullet}{+} i")) \to (D_8, \{i\}_{i=3,5})$,

де $K_5^0 = \{i'\}_{i=1}^{5}$, $K_4^0 = \{a,b,v,c\}$,

$$K = (K_4^0 \cup \{3",5"\}, K_4^1 \cup \{(a,3"),(v,3"),(b,5"),(c,5")\});$$

2) $\varphi(K_5 + K), \sum_{i=1,5}(i' \underset{\bullet}{+} i")) \to (D_9, \{i\}_{i=1,5})$, де $K_5^0 = \{i'\}_{i=1}^{5}$, граф D_9 наведений в [4], $K(\{a,b,c,v,1",5"\}) = K_5$,

$$K = (\{a,b,c,v,1",5"\}, (K_5^1 \setminus (1",v)) \cup (3",2"));$$

3) $\varphi(K_5 + K, (1' \underset{\bullet}{+} 1")) \to (D_{10}, \{1\})$, $K = K_5$, $K_5^0 = \{i'\}_{i=1}^{5}$, $K^0 = \{i"\}_{i=1}^{5}$.

4) $\varphi(K_{3,3} + K, \sum_{i=1,2,5}(i' \underset{\bullet}{+} i")) \to (D_{11}, \{i\}_{1,2,5})$,

$$K = (\{1",2",5",a,b,c\}, K_{3,3}^1 \cup K_3^1), \; K_{3,3}(\{i'\}_{i=1}^{3}) = \overline{K_3},$$

$$K_{3,3}(\{i'\}_{i=4}^{6}) = \overline{K_3}, \; K(\{1",2",5"\}) = K_3, \; K(\{a,b,c\}) = K_3.$$

Лема 3. Для D_{12}, D_{13}, D_{14}, D_{15} мають місце такі φ-перетворення:

1) $\varphi(K_{3,3} + K, \sum_{i=1}^{3}(i' \underset{\bullet}{+} i")) \to (D_{12}, \{i\}_1^3)$,

де $K = K_6 \setminus K_3^1$, $K^0 = \{1",2",3",a,b,v\}$, $K_{3,3}^0 = \{i'\}_{i=1}^{3} \cup \{i'\}_{i=4}^{6}$,

$$K^1 = (K_6^1 \setminus \{(a,b),(a,v),(b,v)\}, \; K_{3,3}(\{i'\}_{i=1}^{3}) = K_{3,3}(\{i'\}_{i=4}^{6}) = \overline{K_3};$$

2) $\varphi(K_5 + K, \sum_{i=1}^{5}(i' \underset{\bullet}{+} i")) \to (D_{13}, \{i\}_{i=1}^{5})$,

де $K_5^0 = \{i'\}_{i=1}^{5}$, $K^0 = \{1",2",3",a,b,c\}$, граф K є φ-образом графів $K_4, K_5 \setminus (2", 4")$, виконаним шляхом ототожнення по ребру (b, c), де

$K_4^0 = \{1'', 3'', 5'', b, c\}$, де вершина $5''$ розділяє ребро $(1'', 3'')$, $K_5^0 \setminus (2'', 4'') =$ $= \{4'', 2'', a, b, c\}$;

3) $\varphi(K_{3,3} + K, \sum\limits_{i=1,\neq 4}^{5} (i' \underset{\bullet}{+} i'')) \to (D_{14}, \{i\}_{i=1,\neq 4}^{5})$, $K_{3,3}^0 = \{i'\}_{i=1}^{3} \cup \{i'\}_{i=4}^{6}$,

$K_{3,3}(\{i'\}_{i=4}^{6}) = \overline{K_3}$, $K_{3,3}(\{i'\}_{i=1}^{3}) = \overline{K_3}$, $K^0 = \{1'', 2'', 3'', 5'', a, b, v\}$,

$K = (K_6^0 \cup \{3''\}, K_6^1 \setminus K_3^1 \cup \{(3'', v), (a, 3'')\}$, $K(2'', 3'', 6'') = \overline{K_3}$,

$K(\{a, b, v, 3''\}) \cong K_3$, де вершина $3''$ розділяє ребро (a, v);

4) $\varphi((K_6 \setminus K_3^1) + K)), \sum\limits_{i=4}^{6} (i' \underset{\bullet}{+} i'')) \to (D_{15}, \{i\}_{i=4}^{6})$, $K_6 \setminus K_3^1(\{i'\}_{i=4}^{6}) = \overline{K_3}$,

$K = (K_5^0, K_5^1 \setminus (4'', 5'') \cup \{(a, 6'')$, $K^0 = \{4'', 5'', 6'', a, b, v\}$, $K_6^0 = \{i'\}_{i=1}^{6}$,

$K_6 \setminus K_3^1(\{i'\}_{i=1}^{3}) = K_3$;

Лема 4. Для D_{16}, D_{17}, D_{18}, D_{19} мають місце такі φ-перетворення:

1) $\varphi(K_{3,3} + K, \sum\limits_{i=1}^{6} (i' \underset{\bullet}{+} i'')) \to (D_{16}, \{i\}_{i=1}^{6})$,

де граф $K = K_5 \setminus (4'', 6'') \cup St_6(c)$,

$K_{3,3}(\{i'\}_{i=1}^{3}) = K_{3,3}(\{i'\}_{i=4}^{6}) = \overline{K_3}$, $St_6^0(c) = \{i''\}_{i=1}^{6} \cup \{c\}$,

$K_5^0 \setminus (4'', 5'') = \{a, b, 4'', 5'', 2''\}$;

2) $\varphi(K_{3,3} + (St_4(c) \cup K''), \sum\limits_{i=1}^{6} (i' \underset{\bullet}{+} i'')) \to (D_{17}, \{i\}_{i=1}^{6})$, де граф K'' утворений з двох копій графа K_4, $K(\{a, b, 2'', 6''\})$ та $K(\{a, b, 1'', 5''\})$, які мають спільними дві вершини $\{a, b\}$, $K_{3,3}(\{i'\}_{i=1}^{3}) =$ $= K_{3,3}(\{i'\}_{i=4}^{6}) = \overline{K_3}$, $K_{3,3}^0 = \{i'\}_{i=1}^{3} \cup \{i'\}_{i=4}^{6}$, $St_4^0(c) = \{i''\}_{i=1}^{4} \cup \{c\}$,

$K_4 = K(\{a, b, 2'', 6''\})$, $K_4 = K(\{a, b, 1'', 5''\})$;

3) $\varphi(K_{3,4} \cup K_3^1 + K, \sum\limits_{i=1}^{6} (i' \underset{\bullet}{+} i'')) \to (D_{18}, \{i\}_{i=1}^{6})$, де граф K визначений наступним чином: $K = (\{1'', 2'', 4'', a, b\}, K_{55}^1 \setminus (1'', 4'')$, $K_{3,4}^0 = \{i'\}_{i=1}^{7}$,

$K_{3,4}(\{i'\}_{i=1}^{3} \cup \{7'\}) = \overline{K_4}$, $K_{3,4}(\{i'\}_{i=4}^{6}) = K_3$, $K_{3,4}^0 = (\{i'\}_{i=1}^{3} \cup \{7'\}) \cup \{i'\}_{i=4}^{6}$;

4) $\varphi(K_5 + K, \sum\limits_{i=1,2,5} (i' \underset{\bullet}{+} i'')) \to (D_{19}, \{i\}_{i=1,2,5})$, де $K_5^0 = \{i'\}_{i=1}^{5}$ і граф K визначений наступним чином: $K = K_{3,3} \setminus (a, b) \cup \{(a, 5''), (b, 5'')\}$,

$K^0 = \{i''\}_{i=1,2,5} \cup \{a,b,c,d\}$, причому вершина 5" розділяє ребро (a,b), $K\{a, 1'', 2''\} = \overline{K_3}$, $K\{d,c,b\} = K_3 \setminus (d,c)$.

Лема 5. Виконуються наступні твердження.

1) для графа D_{20} існує φ-перетворення, визначене наступним чином:

$$\varphi(K_{3,4} \cup K_3^1 + K, \sum_{i=1,2,5,7} (i' \underset{\bullet}{+} i'')) \to ((D_{20}, \{i\}_{i=1,2,5,7}),$$ граф K визначений наступним чином: $K = (\{7'',2'',5'',a,b\}, K_5^1 \setminus (2'',7'')$, де $K_{3,4}^0 = \{i'\}_{i=1}^7$, $K_{3,4}(\{i'\}_{i=1}^3 \cup \{7'\}) = \overline{K_4}$, $K_{3,4}(\{i'\}_{i=4}^6) = K_3$, $K_{3,4}^0 = = (\{i'\}_{i=1}^3 \cup \{7'\}) \cup \{i'\}_{i=4}^6$;

2) для графа D_{21} існує φ-перетворення, визначене наступним чином:

$$\varphi(K_5 + K, \sum_{i=1,4,5} (i' \underset{\bullet}{+} i'')) \to (D_{21}, \{i\}_{i=1,4,5}),$$

де $K^0 = \{1'',4'',5''\} \cup \{a,b,v,c\}$, $K(\{a,b,v,c,4'',5''\}) \cong K_4$, $K(\{a,b,v,c,1'',4'',5''\}) \cong K_5$, причому вершини $4'',5''$ розділяють ребра (a,b), (v,c) відповідно;

3) для графа D_{22} існує φ-перетворення, визначене наступним чином:

$$\varphi(K' + H, \sum_{i=1}^{6} (i' \underset{\bullet}{+} i'')) \to (D_{22}, \{i\}_{i=1}^6),$$ де $K'^0 = \{i'\}_{i=1}^6$, причому вершина $6'$ розділяє ребро $(1', 2')$, $K'^1 = K_5 \setminus (1',2') \cup \{(6',1'),(6',2')\}$, а граф H такий, що $H = K_{3,3} + (b,a))$, $H(\{1'',c,2''\}) = \overline{K_3}$, $H(\{a,b,6''\}) = (\{a,b,6''\},(a,b))$;

4) для графа D_{23} існує φ-перетворення визначене наступним чином:

$$\varphi(K_{3,3} + H, \sum_{i=1}^{5} (i' \underset{\bullet}{+} i'')) \to (D_{23}, \{i\}_{i=1}^5),$$ де H, є $K_{3,3}$ із трикутником на вершинах однієї долі, у якого ребра $(b,a),(c,b)$ 1-підрозділені вершинами 4", 5" відповідно, $H = (\{i''\}_1^6 \cup \{a,b,c\}, K_{3,3}^1 \cup K_3^1)$.

Лема 6. Виконуються наступні твердження.

1) D_{24} є φ-образом графів $K_{3,3}$, де $K_{3,3}^0 = \{i'\}_1^3 + \{i'\}_4^6$, $H \cong K_6 \setminus K_3^1$, $K_{3,3}(\{i'\}_1^3) = K_{3,3}(\{i'\}_4^6) = \overline{K_3}$ та H, при наступному перетворенні

$$\varphi(K_{3,3} + H, \sum_{i=1, i\neq 3}^{6} (i' \underset{\bullet}{+} i'')) \to (D_{24}, \{i\}_{i=1, i\neq 3}^6),$$ виконаному шляхом

ототожнення усіх пар (i', i'') вершин, окрім вершини 3, $M'' = \{i''\}_{1, i\neq 3}^{6}$, $M' = \{i'\}_{1, i\neq 3}^{6}$, де вершини 4", 6" розділяють ребра $(a,b), (b,v)$, відповідно, а 5" розділяє ребро $(1'', b)$, $H(\{1'', 2'', 5''\}) = \overline{K_3}$, $H(\{a,b,v\}) = K_3$;

2) D_{25} є φ-образом $\varphi(K_{3,3} + H, \sum_{i=1}^{6}(i' \dot{+} i'')) \to (D_{25}, \{i\}_{i=1}^{6})$ графів $K_{3,3}$ та H, де $K_{3,3}^0 = \{i'\}_1^3 + \{i'\}_4^6$, $K_{3,3}(\{i'\}_1^3) = K_{3,3}(\{i'\}_4^6) = \overline{K_3}$, $H \cong K_6 \setminus K_3^1$, заданим шляхом ототожнення усіх пар (i', i'') вершин, окрім вершини 3, $M'' = \{i''\}_1^6$, $M' = \{i'\}_1^6$, де вершини 2", 3" розділяють ребра $(a,v), (b,v)$, відповідно, а 5" розділяє ребро $(1'', b)$, $H(\{a,b,v\}) = K_3$, $H(\{1'', 4'', 6''\}) = \overline{K_3}$;

3) граф D_{26} є φ-образом $\varphi(K_5 \setminus (4,5) + H, \sum_{i=1}^{4}(i' \dot{+} i'')) \to (D_{26}, \{i\}_{i=1}^{5})$ графів K_5 та квазізірки H з центром K_4, $K_4^0 = \{a, 4'', c, v\}$, в якому трикутник (a,c,v) має 3 кратних ребра підрозділених вершинами 1", 2", 3" відповідно, а 4' графа K_5 розділяє ребро $(5, 4)$, де $K_5^0 = \{1', 2', 3', 4, 5\}$;

4) D_{27} є φ-образом графів $K_{3,3}$ та H при φ-перетворенні, заданому на множинах вершин формулою $\varphi(K_{3,3} + H, \sum_{i=1}^{6}(i' \dot{+} i'')) \to (D_{27}, \{i\}_{i=1}^{6})$, де $K_{3,3}^0 = \{i'\}_1^6$, $H = K_5 \setminus (1'', 2'') \cup \{(3'', v), (3'', v), (v, 4''), (a, 5''), (a, 6'')\}$, $K_5^0 \setminus (1'', 2'') = \{a, b, v, 1'', 2''\}$, $\deg 3'' = 2$.

Лема 7. Виконуються наступні твердження.

1) D_{28} є φ-образом графів K_5 та H, де $K_5^0 = \{i'\}_1^5$, $H^0 = \{i''\}_1^4 \cup \{a, b, c, v\}$, $H^1 = K_5^1 \setminus \{(2'', 5''), (b, v)\} \cup St_5^1(a)$, $St_5^0(a) - \{1'', 3'', 4'', b, v, c\}$ при перетворенні, заданому формулою $\varphi(K_5 + H, \sum_{i=1,}^{4}(i' \dot{+} i'')) \to (D_{28}, \{i\}_{i=1}^{4})$ шляхом ототожнення усіх пар (i', i'') вершин з $M' = \{i'\}_1^4$, $M'' = \{i''\}_1^4$;

2) D_{29} є φ-образом графів K_5 та H,

де $K_5^0 = \{i'\}_1^5$, $H^0 = \{i''\}_1^5 \cup \{a,b,c,v\}$,

$$H^1 = K_5^1 \setminus \{(2'', 1''), (b, v)\} \cup \{(a, b), (a, v), (4'', v), (3'', v)\},$$

при перетворенні, заданому формулою $\varphi(K_5 + H, \sum\limits_{i=1,}^{5} (i' \underset{\bullet}{+} i'')) \to$ $\to (D_{29}, \{i\}_{i=1}^5)$ шляхом ототожнення усіх пар (i', i'') вершин з множин приєднання $M^{'} = \{i'\}_1^5$, $M^{''} = \{i''\}_1^5$;

3) D_{30} — φ-образ графів K_5 та H,

де $K_5^0 = \{i'\}_1^5$, $H^0 = \{i''\}_1^5 \cup \{a, b, c, v\}$,

$$H^1 = K_5^1 \setminus \{(3'', 1''), (b, v)\} \cup \{(c, b), (c, v), (2'', c), (5'', c), (4'', b)\},$$

при перетворенні, заданому наступною формулою:

$$\varphi(K_5 + H, \sum_{i=1,}^{5} (i' \underset{\bullet}{+} i'')) \to (D_{30}, \{i\}_{i=1}^5)$$

шляхом ототожнення усіх пар (i', i'') вершин з множин приєднання $M^{'} = \{i'\}_1^5$, $M^{''} = \{i''\}_1^5$;

4) D_{31} є φ-образом графів K_5 та H, де $K_5^0 = \{i'\}_1^5$, $H^0 = \{i''\}_1^5 \cup$ $\cup \{a, b, c, d\}$, $H^1 = K_5^1 \setminus \{(5'', 1''), (b, 1'')\} \cup \{(d, b), (d, 1''), (2'', d), (3'', b), (4'', b)\}$, де вершина d розділяє ребро $(b, 1'')$ при перетворенні, заданому наступною формулою: $\varphi(K_5 + H, \sum\limits_{i=1,}^{5} (i' \underset{\bullet}{+} i'')) \to (D_{31}, \{i\}_{i=1}^5)$ шляхом ототожнення усіх пар (i', i'') вершин з множин приєднання $M^{'} = \{i'\}_1^5$, $M^{''} = \{i''\}_1^5$.

Із наведених вище лем 1–7 випливатиме ***основний результат.***

Теорема. Кожна граф-обструкція роду 2 $D_4, \ldots, D_{31}$ [5] на 9-ти вершинах є результатом φ-перетворення трьох зв’язних графів X, Y, Z, які задовольняють одному з наступних випадків:

1) граф Y гомеоморфний K_5 чи $K_{3,3}$ (можливо із кількома додатковими ребрами) вкладений в тор σ, граф Z відсутній, а інший граф X є або площинним 2-мінімальним відносно множини точок приєднання до графа Y на недвоклітці $\sigma \setminus Y$ із нульовими характеристиками θ та $\partial\theta$ для множини точок приєднання до графа Y, або площинним 3-мінімальним на s недвоклітці тора, $s \in \sigma_1 \setminus Y$, із характеристиками θ, $\partial\theta$, де $\theta = 1$ чи $\partial\theta = 1$, для множини точок приєднання графа X до графа Y;
2) граф Y — один з графів K_5 чи $K_{3,3}$, можливо, без ребра, вкладений в тор σ, а інший граф X роду 1 є 2-мінімальним відносно мно-

жини точок приєднання на недвоклітці $\sigma \setminus Y$ із нульовими характеристиками θ, $\partial\theta$ множини точок приєднання графа X до графа Y, граф Z відсутній;

3) граф Y містить частину гомеоморфну K_5 чи $K_{3,3}$ (можливо із кількома додатковими ребрами), вкладений в тор σ, граф Z — проста зірка, граф X є площинною квазізіркою із центральним графом M на двох вершинах, яка не є 2-мінімальним графом на недвоклітці s, $s \in \sigma \setminus Y$, причому існує, принаймні, одна пара вершин простої зірки Z, зформована з елементів множини приєднання графа X до графа Y, що розділяє на ∂s пару кінцевих вершин з множини приєднання графа X до графа Y.

Список використаних джерел:

1. Хоменко М. П. φ-перетворення графів. Препринт ІМ НАНУ. К., 1971. 378 с.
2. Петренюк В. І. Построение графов-обструкций ограниченного ориентируемого рода. Сборник трудов XVI Международной конференции «Проблемы теоретической кибернетики». Нижний Новгород, 20–25 июня 2011. С. 363–368.
3. Archdeacon. D., Kuratowski A. Theorem for the projective plane. *Journal of Graph Theory*. 1981. V. 5. P. 243–246.
4. Gagarin A., Myrvold W., Chambers J. The obstructions for toroidal graphs with no $K_{3,3}$'s. *Discrete Math*. 2009. V. 309. P. 3625–3631.
5. Hur Suhjin. The Kuratowski covering conjecture for graphs of order less than 10. PhD dissertation, Ohio State University, 2008.

Structure 28 9-verteces graphs obstructions for torus was found.

Key words: *structure, 9-verteces graph obstructions, torus, φ-transformation.*

Одержано 10.03.2017

УДК 519.85

О. С. Пичугина*, канд. физ.-мат. наук, докторант,
С. В. Яковлев,** д-р физ.-мат. наук, профессор

*Харьковский национальный университет радиоэлектроники, г. Харьков,
**Национальный аэрокосмический университет, г. Харьков

МЕТОДЫ ГЛОБАЛЬНОЙ ОПТИМИЗАЦИИ НА ПЕРЕСТАНОВОЧНОМ МНОГОГРАННИКЕ В КОМБИНАТОРНЫХ ЗАДАЧАХ НА ВЕРШИННО РАСПОЛОЖЕННЫХ МНОЖЕСТВАХ

Рассмотрена общая постановка задачи оптимизации произвольной функции на дискретном вершинно расположенном множестве E с учетом дополнительных функциональных ограничений. С использованием теории выпуклых продолжений сформулирована эквивалентная на E задача оптимизации выпуклой функции при выпуклых ограничениях-неравенствах. Предложен гибридный подход к оптимизации на перестановочном многограннике на основе совместного использования метода штрафных функций и модификации метода условного градиента. При выполнении достаточно общих условий обоснована сходимость предложенного метода к глобальному решению.

Ключевые слова: *вершинно расположенное множество, выпуклое продолжение, перестановочный многогранник, метод штрафных функций, метод условного градиента.*

Введение. В последнее время учитывая расширение средств математического и компьютерного моделирования, создание новых высокопроизводительных программных продуктов резко возрос интерес к труднорешаемым комбинаторным задачам [1–4]. К указанному классу относятся так называемые задачи евклидовой комбинаторной оптимизации [5–7], получившие такое название учитывая то, что исследуемые комбинаторные объекты рассматриваются в результате их отображения в арифметическое евклидово пространство. При этом задачи приобретают свою специфику, что позволяет предлагать новые эффективные методы.

В данной работе рассмотрен класс задач евклидовой комбинаторной оптимизации на так называемых вершинно расположенных множествах. Речь идет о множествах, которые после отображения в R^n совпадают со множеством вершин своей выпуклой оболочки. Заметим, что, одной стороны, произвольное дискретное множество можно представить в виде объединения его вершинно расположенных подмножеств. С другой стороны, задачи оптимизации на вершинно расположенных множествах обладают рядом интересных свойств, позволяющих по-новому взглянуть на возможности современной теории математического программирования для их решения. В частности, речь идет о применении теории выпуклых продолжений [8] к оптимизации на вершинно расположенных множествах. Заметим, что к классу вершинно расположенных относятся множества перестановок с повторениями и без повторений при их отображении в R^n .

Цель данной статьи — разработка методов оптимизации на перестановочном многограннике с учетом специфики евклидового множества перестановок и свойств функций, заданных на них.

Постановка задачи и методы ее решения. Пусть $E \subset R^n$ — конечное множество точек арифметического евклидового пространства.

Рассмотрим следующую задачу дискретной оптимизации:

$$f(x) \to \min , \tag{1}$$

$$g_i(x) \le 0,\ i \in J_{l'} , \tag{2}$$

$$g_i(x) = 0,\ i \in J_l \setminus J_{l'} , \tag{3}$$

$$x \in E , \tag{4}$$

где функции $f(x)$, $g_i(x)$, $i \in J_l$ определены на E . Здесь и далее обозначим $J_l = \{1,...,l\}$.

Выделим класс множеств $E \subset R^n$, удовлетворяющих условию

$$E = vert\ conv\ E , \tag{5}$$

т. е. совпадающих со множеством вершин своей выпуклой оболочки.

Такие множества будем называть вершинно расположенными.

Функции, определенные на вершинно расположенных множествах, обладают следующим важным свойством.

Теорема 1 [8]. Для любой функции $f : E \to R^1$ существует дифференцируемая сильно выпуклая функция $\tilde{f} :\ conv\ E \to R^1$, такая, что

$$\tilde{f}(x) = f(x) \text{ для любых } x \in E . \tag{6}$$

Для функций, удовлетворяющих на множестве *E* условию (6), будем использовать обозначение

$$\tilde{f}(x) \underset{E}{=} f(x) . \tag{7}$$

Функцию $\tilde{f}(x)$, заданную на множестве $X \supseteq conv\ E$ и удовлетворяющую условию (7), назовем продолжением функции $f(x)$ на *X*. Если при этом функция $\tilde{f}(x)$ выпукла (сильно выпукла, дифференцируема) на выпуклом множестве X, то будем говорить о выпуклом (сильно выпуклом, дифференцируемом) продолжении $f(x)$ на *X*.

Осуществим следующие эквивалентные преобразования задачи (1)–(5). Представим ограничения-равенства (3) в виде:

$$\begin{gathered} g_i(x) \le 0, \\ -g_i(x) \le 0,\ i \in J_l \setminus J_{l'}. \end{gathered} \tag{8}$$

Построим дифференцируемые выпуклые продолжения на $convE$ для функции $f(x)$ и функций, стоящих в левых частях ограничений (2), (8):

$$F(x) \underset{E}{=} f(x),$$

$$h_i(x) \underset{E}{=} g_i(x),\ i \in J_l,$$

$$h_i(x) \underset{E}{=} -g_{i-l}(x),\ i \in J_m \setminus J_l,$$

где $m = 2l - l'$. Тогда с учетом теоремы 1 имеет место следующее утверждение.

Теорема 2. Задача (1)–(5) эквивалентна задаче:

$$F(x) \to \min, \tag{9}$$

$$h_i(x) \le 0,\ i \in J_m, \tag{10}$$

$$x \in E = vert\ conv\ E,$$

где $F(x),\ h_i(x),\ i \in J_m$ — выпуклы и дифференцируемы на $conv\ E$.

Рассмотрим в качестве множества E следующее евклидовое комбинаторное множество. Пусть

$$A = \{a_1, ..., a_n\} \text{ —} \tag{11}$$

множество n действительных чисел, среди которых s различные.

Не теряя общности, будем полагать, что

$$a_i \le a_{i+1},\ i \in J_{n-1}. \tag{12}$$

Множество (11) порождает множество E_{ns}, элементами которого являются упорядоченные наборы $x = (x_1, ..., x_n)$, где $x_i = a_{\pi_i}$, $i \in J_n$, а $\pi = (\pi_1, ..., \pi_n)$ — перестановка первых n натуральных чисел. Если все элементы множества A различны, то такое множество называется евклидовым множеством перестановок. Если же множество A содержит одинаковые элементы, то имеем евклидово множество перестановок с повторениями.

Евклидовые множества перестановок и перестановок с повторениями достаточно хорошо изучены [5–7]. Отметим тот важный факт, что они являются вершинно расположенными. Следовательно, на эти множества распространяются утверждения теорем 1, 2. При этом для построения дифференцируемых выпуклых и сильно выпуклых продолжений функций, фигурирующих в указанных теоремах, предложен ряд конструктивных приемов [7–10].

Выпуклой оболочкой множества E_{ns} является так называемый перестановочный многогранник Π_{ns} [5–7, 11]. Известно, что он описывается следующей системой линейных уравнений и неравенств:

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} a_i \,;\; \sum_{i\in\omega} x_i \ge \sum_{i=1}^{|\omega|} a_i \,,\; \forall\omega \subseteq J_n \,,\; |\omega| < n \,, \tag{13}$$

где $|\omega|$ — мощность множества ω.

Рассмотрим оптимизационную задачу вида (9), (10), (13), где функции $F(x)$, $h_i(x)$, $i \in J_m$ — выпуклые и дифференцируемые на Π_{ns}. Предлагается следующий гибридный подход к решению поставленной задачи оптимизации, совместно использующий метод штрафных функций и модификацию метода условного градиента.

Зададим семейство зависящих от некоторого параметра α_k функций $\varphi(x,\alpha_k)$, $k = 1,2,\ldots$, определенных на Π_{ns} и удовлетворяющих классическим требованиям для штрафных функций. В соответствии с общей схемой метода штрафных функций [12, 13] зададим последовательности штрафных коэффициентов $\{\alpha_k\}_{k=1}^{\infty}$ и чисел $\{\varepsilon_k\}_{k=1}^{\infty}$, такие, что $\lim\limits_{k\to\infty} \frac{1}{\alpha_k} = 0,\ \lim\limits_{k\to\infty} \varepsilon_k = 0$.

При каждом k выберем точку x^k, удовлетворяющую условию:

$$F\left(x^k\right) + \varphi\left(x^k,\alpha_k\right) \le \min_{x\in\Pi_{ns}} \left[F(x) + \varphi(x,\alpha_k) \right] + \varepsilon_k \,. \tag{14}$$

Конкретизируем задачу (14) и положим

$$\varphi(x,\alpha_k) = \alpha_k \sum_{i=1}^{m} \left[\max\left\{0, h_i(x)\right\} \right]^2 . \tag{15}$$

Для реализации метода штрафных функций с функцией штрафа вида (15) необходимо решать последовательность задач

$$\Phi(x,\alpha_k) = F(x) + \alpha_k \sum_{i=1}^{m} \left[\max\left\{0, h_i(x)\right\} \right]^2$$

на перестановочном многограннике Π_{ns}, т. е.

$$\Phi(x,\alpha_k) \to \min,\ x \in \Pi_{ns} \,, \tag{16}$$

где множество Π_{ns} задается системой (13).

Таким образом, $x^k = \arg\min_{\boldsymbol{x}\in\Pi_{ns}} \Phi\left(x,\alpha_k\right)$.

Тогда предельная последовательность решений $\left\{x^k\right\}_{k=1}^{\infty}$, построенная в соответствии с условием (14), сходится к решению задачи (9), (10), (13).

Остановимся на вопросе решения задачи (16). Нетрудно видеть, что речь идет о минимизации выпуклой дифференцируемой функции на множестве, заданном системой линейных ограничений (13). Однако количество ограничений неполиномиально и имеет в общем случае оценивается числом 2^n. Поэтому для больших размерностей применение классических методов решения оптимизационных задач на перестановочном многограннике Π_{ns} существенно затруднено.

Вместе с тем задача оптимизации линейных функций на Π_{ns} обладает следующим интересным свойством.

Минимум линейной функции $\varphi\left(x\right)=\sum_{i=1}^{n} c_i x_i$ на множестве Π_{ns} достигается в точке $x^* = \left(x_1^*,...,x_n^*\right)$, где $x_{\pi_i}^* = a_i$, $i\in J_n$, а $\pi = \left(\pi_1,...,\pi_n\right)$ — перестановка первых n натуральных чисел, такая, что $c_{\pi_i} \ge c_{\pi_{i+1}}$, $i\in J_{n-1}$. Указанное свойство позволяет предложить следующую модификацию метода условного градиента [12, 13] для решения задачи (16). Как известно, на каждом шаге данного итерационного метода при определении направления убывания функции решается вспомогательная задача оптимизации линейной функции, коэффициентами которой являются компоненты градиента функции $\Phi\left(x,\alpha_k\right)$ в соответствующей точке. В свою очередь, задача оптимизации линейной функции на перестановочном многограннике Π_{ns} сводится к упорядочению ее коэффициентов.

В качестве начальной точки предлагается выбирать внутреннюю точку многогранника Π_{ns}:

$$x^0 = \left(x_1^0,...,x_n^0\right),\ x_i^0 = \frac{1}{n}\sum_{j=1}^{n} a_j,\ i\in J_n .$$

Заметим, что в силу выпуклости и дифференцируемости функций $\Phi\left(x,\alpha_k\right)$, а также свойств множества Π_{ns} и особенностей решения вспомогательных линейных задач на нем, можно утверждать о сходимости итерационного процесса к глобальному решению задачи (16).

Выводы и обсуждение результатов. Полученные результаты представляют самостоятельный интерес с точки зрения решения условных задач оптимизации на перестановочном многограннике с учетом функциональных ограничений. С другой стороны, описанные задачи можно рассматривать как релаксационные в различных схемах комбинаторной оптимизации. Более того, используя результаты по непрерывному функциональному представлению дискретных структур, можно выделить новые классы задач комбинаторной оптимизации, для решения которых применимы описанные выше гибридные схемы. В первую очередь речь идет о классе полиэдрально-сферических множеств, представимых в виде пересечения комбинаторного многогранника и гиперсферы. Используя уравнение гиперсферы при формировании штрафной функции, имеем аналогичную постановку задачи и, следовательно, возможность применения представленных результатов для решения такого класса задач.

Список использованной литературы:

1. Korte B., Vygen J. Combinatorial Optimization: Theory and Algorithms. Heidelberg; New York: Springer Berlin, 2002. 660 p.
2. Сергиенко И. В., Шило В. П. Задачи дискретной оптимизации: проблемы, методы решения, исследования. К.: Наук. думка, 2003. 261с.
3. Згуровский М. З., Павлов А. А. Труднорешаемые задачи комбинаторной оптимизации в планировании и принятии решений. К.: Наук. думка, 2016. 115 с.
4. Гуляницький Л. Ф., Мулеса О. Ю. Прикладні методи комбінаторної оптимізації: навчальний посібник. К: Видавничо-поліграфічний центр «Київський університет», 2016. 142 с.
5. Стоян Ю. Г., Яковлев С. В. Математические модели и оптимизационные методы геометрического проектирования. К.: Наук. думка, 1986. 268 с.
6. Стоян Ю. Г., Ємець О. О. Теорія і методи евклідової комбінаторної оптимізації. К.: Ін-т системн. дослідж. освіти, 1993. 188 с.
7. Грицик В. В., Кісельова О. М., Яковлев С. В., Стецюк П. И. та інші. Математичні методи оптимізації та інтелектуальні комп'ютерні технології моделювання складних процесів і систем з урахуванням просторових форм об'єктів: монографія. Донецьк: Наука і освіта, 2012. 480 с.
8. Яковлев С. В. Теория выпуклых продолжений функций на вершинах выпуклых многогранников. *Вычислительная математика и математическая физика*. 1994. 34 (7). С. 1112–1119.
9. Pichugina O., Yakovlev S. Convex extensions and continuous functional representations in optimization, with their applications. *J. Coupled Syst. Multiscale Dyn*. 2016. 4 (2). P. 129–152.
10. Пічугіна О. С. Опукле продовження кубічних многочленів на переставленнях та його застосування у розв'язанні практичних задач оптимізації. Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки. 2010. Вип. 4. С. 176–189.
11. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация (комбинаторная теория многогранников). М.: Наука, 1981. 344 с.

12. Бейко И. В., Бублик Б. Н., Зинько П. Н. Методы и алгоритмы решения задач оптимизации. К.: Вища школа, 1983. 512 с.
13. Bertsekas D. P. Nonlinear Programming. Belmont: Athena Scientific, 1995. 378 p.

A general problem statement of constrained optimization over a discrete vertex located set E is posed. An optimization problem with convex objective function and convex inequality-constraints equivalent on *E* to original is formulated, based on the convex extensions theory. A hybrid approach to optimization over the permutation polyhedron is presented. It uses jointly the penalty method and a modification of the conditional gradient method. A convergence of the method to the global solution is justified.

Key words: *a vertex located set, a convex extension, the permutohedron, the penalty method, the method of conditional gradient.*

получено 24.02.2017

УДК 519.6

О. В. Попов, канд. фіз.-мат. наук, с. н. с.,
О. В. Рудич, науковий співробітник

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ДО РОЗВ'ЯЗУВАННЯ СИСТЕМ ЛІНІЙНИХ РІВНЯНЬ НА КОМП'ЮТЕРАХ ГІБРИДНОЇ АРХІТЕКТУРИ

Запропоновано методологію розв'язування розріджених систем лінійних алгебраїчних рівнянь на комп'ютерах гібридної архітектури, яка використовує алгоритми структурної регуляризації та декомпозиції розріджених даних для приведення матриці системи до блочно-розрідженого вигляду.

Ключові слова: *системи лінійних алгебраїчних рівнянь, розріджені матриці, комп'ютери гібридної архітектури, структурна регуляризація розріджених даних, декомпозиція розріджених даних.*

Вступ. При чисельному моделюванні часто виникають, наприклад, при використанні тривимірних моделей, розрахункові (дискретні або напівдискретні) задачі з надвеликою кількістю рівнянь, яка може перевищувати 10^7. Причому дані (матриці) цих задач мають розріджену структуру, тобто кількість ненульових елементів значно менша (приблизно дорівнює kn, де n — порядок матриці, а $k \ll n$) загальної кількості елементів матриці. Зберігання таких даних, незважаючи на розрідженість, потребує значних обсягів комп'ютерної пам'яті, які можуть перевищувати 1 Tb.

Зростання параметрів задач, що розв'язуються, розрахунок на комп'ютерах більш повних моделей об'єктів, процесів, явищ вимагає відповідного зростання продуктивності комп'ютерів. Вимоги до високопродуктивних обчислень набагато випереджають можливості персональних комп'ютерів, навіть незважаючи на багатоядерність процесорів.

В даний час зростання продуктивності обчислень досягається за рахунок розпаралелювання, яке базується на використанні комп'ютерів з багатьма процесорними пристроями, зокрема з багатоядерними процесорами. В цих комп'ютерах, як правило, реалізується MIMD-архітектура (архітектура з множинним потоком команд і даних). В останні роки також набули поширення гібридні обчислювальні системи, в яких використовуються сопроцесори, наприклад, графічні процесори (GPU), для прискорення обчислень при виконанні великих обсягів однорідних арифметичних операцій. На таких сопроцесорах-прискорювачах, як правило, реалізується SIMD-архітектура паралельних обчислень. Такі комп'ютери гібридної архітектури вже зайняли провідні позиції у світовому рейтингу найпродуктивніших комп'ютерів TOP500 [1].

Розв'язування розрахункових задач в переважній більшості потребує розв'язування систем лінійних алгебраїчних задач (СЛАР) з розрідженими матрицями (див., напр., [2, 3]). В свою чергу при розв'язуванні цих СЛАР прямими методами, як правило, використовується факторизація (розвинення) матриці в добуток матриць (в більшості випадків трикутних, діагональних). Часто розвинення матриці в добуток трикутних матриць використовується і в ітераційних методах розв'язування СЛАР.

Постановка задачі. Розглянемо СЛАР

$$Ax = b, \tag{1}$$

де A — дійсна квадратна матриця порядку n; b — матриця правої частини розміру $n \times q$ (або n-вимірний вектор). Розв'язування цієї СЛАР полягає у знаходженні такого розв'язку x (матриці розмірності $n \times q$ або n-вимірного вектора), щоб рівняння (1) перетворювалося в тотожність. Якщо матриця A системи невироджена (тобто її визначник $|A| \equiv \det(A) \neq 0$), то розв'язок СЛАР (1) існує і єдиний.

Блочні алгоритми розвинення квадратних матриць. Як зазначено вище GPU, призначені в першу чергу для виконання великих обсягів однорідних арифметичних операцій — матрично-матричних та меншою мірою матрично-векторних. До того ж такі операції ефективно реалізовано в бібліотеках програм від розробників технічних засобів, наприклад, в бібліотеці CUBLAS [4]. Тому класичні методи та алгоритми (Гаусса, Холецького) доцільно модифікувати, представивши їх у блочній формі.

Розглянемо LU-розвинення. Розіб'ємо матрицю на блоки розміру $s \times s$. Не втрачаючи загальності міркувань, можна вважати, що n / s — ціле число. Після $k - 1$ кроків ($k = 1, 2, \ldots, n / s$) блоки модифікованої матриці $A^{(k-1)}$ можна схематично представити у вигляді, який показано на рис. 1 ліворуч. Тут позначено: $A_f^{(k-1)} = L^{(k-1)}U^{(k-1)}$ — діагональний блок (квадратний) порядку $ks - s$, $A_l^{(k-1)} = L_1^{(k-1)}U^{(k-1)}$ — піддіагональний прямокутний блок розміру $(r + s) \times (ks - s)$, $A_u^{(k-1)} = L^{(k-1)}U_1^{(k-1)}$ — наддіагональний прямокутний блок розміру $(ks - s) \times (r + s)$, $A_R^{(k-1)}$ — діагональний блок порядку $r + s$, де $r = n - ks$. В $A_R^{(k-1)}$ в свою чергу виділяються 4 блоки: A_{11} — діагональний блок порядку s, A_{12} — прямокутний блок розміру $s \times r$, A_{12} — прямокутний блок розміру $r \times s$, A_{22} — діагональний блок порядку r.

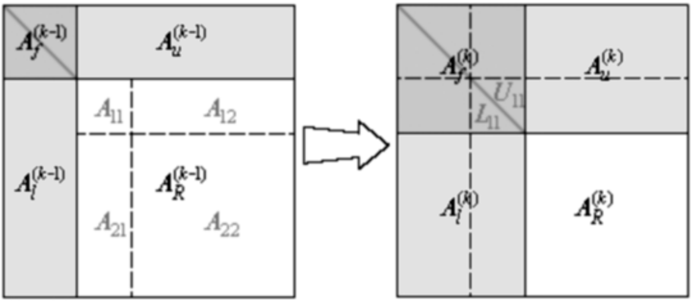


Рис. 1. *Схема одного кроку блочного алгоритму LU-розвинення*

На k-му кроці виконується розвинення (модифікація) блоку $A_R^{(k-1)}$ згідно формул

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = P\begin{pmatrix} L_{11}U_{11} & L_{11}U_{12} \\ L_{21}U_{11} & L_{21}U_{12} + A_R^{(k)} \end{pmatrix}, \tag{2}$$

де P — матриця перестановок.

Спочатку згідно (2) виконується LU-розвинення блоку A_{11}. Блоки L_{21} та U_{12} згідно (2) можна отримати як розв'язки матричних СЛАР

$$U_{11}^T L_{21}^T = \tilde{A}_{21}^T \text{ та } L_{11}U_{12} = \tilde{A}_{12}, \tag{3}$$

де $\tilde{A}_{ij}$ позначено відповідні матричні блоки після перестановок. Після цього обчислюється блок $A_R^{(k)}$ за формулою

$$A_R^{(k)} = \tilde{A}_{22} - L_{21}U_{12}. \tag{4}$$

Цю операцію також називають s-ранговою модифікацією.

Аналогічним чином виконується LL^T-розвинення симетричної матриці з урахуванням того, що в цьому випадку $U_{12} = (L_{21})^T$. Це дозволяє зменшити кількість арифметичних операцій майже в 2 рази. У випадку LDL^T-розвинення у формулах (2)-(4) необхідно покласти $U_{11} = D_1(L_{11})^T$, $U_{12} = D_1(L_{21})^T$, де D_1 — діагональна матриця з LDL^T-розвинення блоку A_{11}. Зауважимо, що добуток $L_{21}U_{12} \equiv L_{21}D_1(L_{21})^T$ — симетрична матриця, тому і в цьому випадку кількість арифметичних операцій зменшується майже в 2 рази, якщо обчислення проводити у такій послідовності:

(i) LDL^T-розвинення блоку A_{11};
(ii) обчислення (3) блоку U_{12} та блоку $L_{21} = (U_{12})^T(D_1)^{-1}$;
(iii) s-рангова модифікація (4).

У випадку розрідженої матриці системи A матриці розвинення L та U також залишаються розрідженими, хоча в загальному випадку кількість ненульових елементів збільшується. Тому при виконанні розвинення (2) блоку $A_R^{(k-1)}$ доцільно проводити обчислення тільки з ненульовими елементами відповідних блоків матриці. Так елемент з індексами i та j матриці (блоку) $A_R^{(k)}$ модифікується тільки в тому випадку, коли скалярний добуток i-го рядка матриці L_{21} та j-го стовпчика матриці U_{12} не дорівнює тотожно нулю. Тому s-рангова модифікація (4) виконується тільки з підматрицею матриці $L_{21}U_{12}$, яка складається з її ненульових елементів або ненульових блоків.

Структурна регуляризація розріджених матриць. Як випливає з вище викладеного, у випадку розрідженої матриці СЛАР обробляються (модифікуються) тільки елементи вихідної матриці та всіх проміжних підматриць і блоків, які відповідають (мають ті ж самі глобальні індекси i та j) ненульовим елементам матриць розвинення. Тому кількість арифметичних операцій для розв’язування СЛАР (1) з розрідженою матрицею визначається кількістю та розташуванням ненульових елементів (тобто структурою) матриць розвинення (L та/або U) матриці системи. Отже, доцільно зберігати та обробляти тільки такі елементи, розподіляючи їх між різними процесорними пристроями відповідно до вимог конкретного паралельного алгоритму.

Структура розріджених матриць визначається нумерацією невідомих і може бути регулярною (наприклад, стрічковою) або нерегулярною. З метою зменшення кількості арифметичних операцій для розв’язування СЛАР (1) з розрідженою матрицею шляхом структурної регуляризації — перестановки рядків і стовпчиків (тобто перенумерації невідомих) таку матрицю приводять до одного із стандартних виглядів: стрічкового, профільного тощо. Таку процедуру варто проводити для випадків, коли немає потреби в перестановках елементів матриці з метою вибору головного елемента — для симетричних додатно визначених матриць, для матриць з діагональною перевагою тощо. Також структурна регуляризація може виконуватись при використанні блочних алгоритмів, якщо можливий частковий вибір головного елемента в межах діагонального блоку.

Існує декілька алгоритмів [2] оптимізації структури розрідженої матриці і приведення її до відповідного стандартного вигляду, наприклад:

- стрічкової або профільної матриці (в залежності від розташування ненульових елементів), використовуючи алгоритм фактор-дерев або алгоритм Катхілл-Маккі, кожен з яких забезпечує концентрацію ненульових елементів біля головної діагоналі;
- блочно-діагональної матриці з обрамленням, використовуючи алгоритм паралельних перерізів;
- матриці «хмарочосної» структури, використовуючи алгоритм мінімальної степені; така структура дозволяє найбільше (порівняно з іншими алгоритмами) зменшити кількість арифметичних операцій.

Деякі оптимізовані структури розріджених матриць показано на рис. 2.

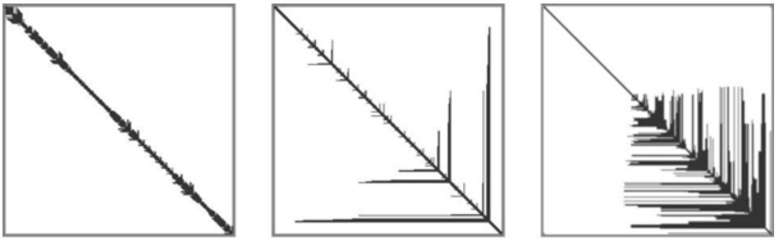


***Рис. 2.** Приклади структур розріджених матриць*

При використанні блочних алгоритмів та GPU доцільно в блочному розбитті визначити нульові блоки (тобто блоки, які складаються тільки з нулів) та ненульові (які мають хоча б один ненульовий елемент). Цей розподіл має базуватися на вихідній структурі матриці A системи. Бажано також, щоб ненульові блоки були якомога більше заповнені. Порядок блоків s визначається, виходячи з вимог ефективного використання GPU, та коливається, як правило, в межах від 96 до 256. Практично вибір порядку блоків доцільно робити, використовуючи на конкретному гібридному комп’ютері тестові задачі аналогічні розглядуваній.

Далі необхідно оптимізувати таку блочно-розріджену структуру матриці, використавши один з названих вище алгоритмів, причому замість елементів матриці в алгоритмах використовуються блоки. Для більшого ефекту можна також оптимізувати структуру діагональних блоків, особливо якщо більшість з них мають однакову вихідну структуру. Також часто доцільно об’єднати розташовані поряд (в рядку або стовпчику) ненульові блоки оптимізованої структури матриці в один прямокутний блок.

Декомпозиція та розподіл між процесорними пристроями розріджених матриць. Всі прямі методи розв’язування СЛАР базуються на розвиненні матриці задачі в добуток матриць стандартних виглядів. Достатньо добру збалансованість завантаження процесів забезпечують паралельні версії цих алгоритмів, в яких використовуються так звані циклічні схеми розподілу і обробки матриць (див. напр. [5]). Такі циклічні алгоритми у багатьох випадках дозволяють добитися приблизно рівного обсягу обчислень і обмінів, що виконуються кожним процесом, і практично виключити вплив ефекту Гайдна [6].

Прикладом циклічної схеми розподілу між процесами елементів матриці є рядкова циклічна схема. Узагальненням даної схеми є одновимірна (рядкова) блочно-циклічна схема: якщо q-му процесу розподілено елементи рядків матриці з номерами $sr + 1$, $sr + r$, то $(q + 1)$-му — рядки з номерами $s(r + 1) + 1$, $s(r + 1) + s$, де s — кількість рядків в блоці, можна говорити про r-й і $(r + 1)$-й рядки квадратних матричних блоків порядку s.

У випадках стрічкових, профільних та хмарочосних матриць паралельні алгоритми, в яких використовується одновимірна блочно-циклічна схема розподілу елементів матриць, дозволяють добитися приблизно рівного обсягу обчислень і обмінів, що виконуються кожним паралельним процесом в кожний момент часу. В першу чергу — це стрічкові матриці при очевидній умові, що напівширина стрічки матриці $m > sp$. У випадку профільної матриці системи, варіюючи значення s і p, можна також практично збалансувати завантаження паралельних процесів у кожний момент часу, якщо також $c_e / n > sp$, де c_e — загальна кількість піддіагональних елементів у профілі матриці. У випадку симетричної матриці хмарочосної структури цього ж можна досягти, циклічно розподіляючи рядки блоків верхнього трикутника (з головною діагоналлю) матриці (тільки ненульові елементи або ненульові блоки).

Методологія розв'язування СЛАР. Отже, пропонується наступна послідовність дій для розв'язування СЛАР з розрідженими матрицями довільної структури на комп'ютерах гібридної архітектури:

- використовуючи один з алгоритмів структурної регуляризації, формування блочно-розрідженої структури матриці СЛАР на основі вихідної структури її ненульових елементів;
- декомпозиція розріджених матриць та розподіл отриманих рядків або стовпчиків ненульових блоків між процесорними пристроями;
- розвинення матриці СЛАР у добуток трикутних матриць — на k-му кроці ($k = 1, 2, \ldots, n/$) виконуються операції (з можливістю асинхронного виконання на різних процесорних пристроях) з ненульовими блоками підматриці $A_R^{(k-1)}$:

(i) розвинення на CPU блоку A_{11};
(ii) обчислення (3) на GPU ненульових блоків з L_{21} та/або U_{12};
(iii) розсилка всім CPU та GPU обчислених ненульових блоків з L_{21} та/або U_{12};

(iiii)s-рангова модифікація (4) на GPU ненульових блоків з A_{22};

- розв'язування на CPU двох СЛАР з трикутними матрицями $Ly = b$ та $Ux = y$ (або $L^T x = y$, або $L^T x = D^{-1} y$).

Висновки. Запропонований підхід на основі структурної регуляризації та блочних варіантів методів трикутних розвинень матриць згідно (2)–(4) дозволяє розробити ефективні алгоритми розв'язування СЛАР з розрідженими матрицями на комп'ютерах гібридної архітектури. Вже розроблено та програмно реалізовано алгоритми для стрічкових і профільних матриць, а також для блочно-діагональних матриць з обрамленням. При цьому досягнута висока ефективність для різних гібридних архітектур — з одним GPU, з двома GPU на одному вузлі, з g GPU на декількох вузлах. Нині дослідження зосереджено на розв'язуванні СЛАР з матрицями довільної розрідженої структури.

Надалі доцільно розробити алгоритми дворівневої структурної регуляризації блочно-розріджених матриць — блочної структури, та структур окремих блоків.

Список використаних джерел:

1. Режим доступу: http://www.top500.org
2. Джордж А., Лю Дж. Численное решение больших разреженных систем уравнений. М.: Мир, 1984. 334 с.
3. Ортега Дж. Введение в параллельные и векторные методы решения линейных систем. М.: Мир, 1991. 367 с.
4. CUBLAS Linear Algebra. Режим доступу: http://developer.download.nvidia.com/-CUBLAS Library.pdf
5. Молчанов И. Н., Химич А. Н., Попов А. В. и др. Об эффективной реализации вычислительных алгоритмов на MIMD-компьютерах. *Искусственный интеллект*. 2005. № 3. С. 175–184.
6. Валях Е. Последовательно-параллельные вычисления. М.: Мир, 1985. 456 с.

A methodology for the solving of sparse linear algebraic systems on hybrid-architecture computers is proposed which employs algorithms both of the structural regularization and decomposition of the sparse data for the reducing of system's matrix to the block-sparse form.

Key words: *linear algebraic systems, sparse matrices, hybrid-architecture computers, structural regularization of the sparse data, decomposition of the sparse data.*

Одержано 15.02.2017

УДК 517.5

М. Ю. Савкіна, канд. фіз.-мат. наук, с. н. с.

Інститут математики НАН України, м. Київ

АЛГОРИТМ ПЕРЕВІРКИ НА КОРЕКТНІСТЬ МОДЕЛІ СПЛАЙНОВОЇ РЕГРЕСІЇ

Побудовано алгоритм перевірки на коректність моделі двофазної лінійної регресії з невідомою точкою перемикання у випадку, коли треба зробити вибір між такою моделлю та лінійною. Алгоритм заснований на загальних принципах перевірки статистичних гіпотез у регресійному аналізі.

Ключові слова: *метод найменших квадратів, регресійна модель, точка перемикання.*

Вступ. Класичний регресійний аналіз засновано на тому, що вигляд моделі регресії відомий з точністю до параметрів, тобто, набір незалежних змінних (факторів) задано однозначно, всі істотні змінні присутні та ніяких альтернативних способів вибору факторів немає. Насправді вибір регресорів, тісно пов'язаний з вибором моделі об'єкта, — одна з найскладніших проблем. В середині минулого сторіччя поява ЕОМ значно спростила цю проблему. «...Поступово з'ясувалося, що ЕОМ допускає відмову від жорсткої моделі дослідження та підбір під час обробки даних деякої «найкращої» моделі...» [1]. У даний час розроблено багато статистичних методів відбору змінних, такі як метод всіх можливих регресій, метод виключення, кроковий регресійний метод, ступінчастий регресійний аналіз, гребенева регресія тощо. В одній і тій ж задачі їх застосування не завжди веде до отримання тієї ж самої моделі, хоча в багатьох випадках виходить однаковий результат. Кожен метод має свої недоліки, свої переваги. Жоден метод не буде добре працювати в усіх випадках. У деяких з цих методів застосовується критерій Фішера для перевірки гіпотези рівності нулю невідомого параметра регресії, і на його підставі приймається рішення про видалення відповідного фактора з регресії.

Розглянемо модель регресії

$$y_i = at_i + b + c_1\left(t_i - t^*\right)_+ + \varepsilon_i,\ i = 0,1,...,n, \tag{1}$$

де $\varepsilon_0, \varepsilon_1, ..., \varepsilon_n$ — незалежні у сукупності нормально розподілені випадкові величини з $E\varepsilon_i = 0$ та $D\varepsilon_i = \sigma^2$, а $\left(t_i - t^*\right)_+$ — зрізана степенева функція [2]. Згідно з [3] точка t^* називається точкою перемикання моделі. Якщо вона відома, модель (1) є лінійною по параметрах a, b, c_1, які підлягають оцінюванню. Якщо t^* невідома, модель стає нелінійною по параметрах, а t^* перетворюється на невідомий параметр моделі, який також треба оцінювати.

Далі висуваємо гіпотезу

$$H : c_1 = 0.$$

Якщо вона підтвердиться з великою ймовірністю, фактор $\left(t_i - t^*\right)_+$ видаляємо з регресії, тобто модель (1) перетвориться на таку модель

$$y_i = at_i + b + \varepsilon_i,\ i = 0,1,...,n, \tag{2}$$

Позначимо $\vec{y} = \left(y_0, y_1, ..., y_n\right)$. Зазвичай перевірка статистичної гіпотези здійснюється за допомогою критерія відношення правдоподібності, який приводить до множини прийняття гіпотези H [4]

$$E_H = \left\{ \vec{y} \in R^{n+1} : \frac{S_2^2 - S_4^2}{S_4^2} < \varphi \right\},$$

де S_2^2 та S_4^2 — залишкові суми квадратів моделі (2) та нелінійної моделі (1) відповідно. Значення φ для нелінійної регресії можна вибирати різними методами, один з них дає

$$\varphi = \frac{1}{n-2} F_\alpha\left(1, n-3\right),$$

де α — рівень значущості, $F_\alpha = F_\alpha\left(1, n-3\right)$ — значення, при якому $\int\limits_{F_\alpha}^{\infty} f\left(t, 1, n-3\right)dt = \alpha$, $f\left(t, 1, n-3\right)$ — щільність розподілу Фішера з 1 та $n-3$ ступенями свободи. Значення F_α знаходять з таблиць.

У роботі [5] у випадку, коли $t_i = \frac{i}{n}$, $i = 0,1,...,n,$ побудовано алгоритм, завдяки якому можна відхиляти гіпотезу H не знаходячи S_4^2.

Позначимо $z_k, k = 1,2,...,n-1,$ — останній діагональний елемент матриці $\left(X_k' X_k\right)^{-1}$, де

$$X_k' = \begin{pmatrix} 1 & 1 & ... & 1 & 1 & ... & 1 \\ 0 & \frac{1}{n} & ... & \frac{k}{n} & \frac{k+1}{n} & ... & 1 \\ 0 & 0 & ... & \frac{1}{n} & \frac{2}{n} & ... & \frac{n-k+1}{n} \end{pmatrix}.$$

Твердження. Має місце рівність

$$S_2^2 - S_{3,k}^2 = \frac{\left(\widehat{c}_1^{(k)}\right)^2}{z_k}, \tag{3}$$

де $S_{3,k}^2$ та $\widehat{c}_1^{(k)}$ — залишкова сума квадратів та оцінка МНК параметра c_1 лінійної регресійної моделі (1), коли $t^* = t_k$.

Доведення випливає з загального результату [4].

У випадку, коли $t_i = \frac{i}{n},\ i = 0,1,\dots,n,$ маємо

$$\widehat{c}_1^{(k)} = \frac{6n}{(2k+1)n - 2\left(k^2-1\right)}\left(\frac{1}{k(k+1)}\sum_{i=0}^{k} y_i\left[kn - i(2k+n+2)\right] + \right.$$
$$\left. + \frac{1}{(n-k)(n-k+1)}\sum_{i=k+1}^{n} y_i\left[(k-2n-2)n - i(2k-3n-2)\right]\right). \tag{4}$$

$$z_k = \frac{6n^3(n+1)(n+2)}{k(k+1)(n-k)(n-k+1)\left((2k+1)n-2\left(k^2-1\right)\right)}. \tag{5}$$

Далі, у випадку $t_i = \frac{i}{n},\ i = 0,1,\dots,n,$ оцінку МНК $\widehat{a}, \widehat{b}$ параметрів a, b регресійної моделі (1) можна знайти за формулами [5]

$$\widehat{a} = \frac{12n}{(n+1)(n+2)}\sum_{i=0}^{n} y_i\left(\frac{i}{n} - \frac{1}{2}\right),\ \widehat{b} = \overline{y} - \frac{1}{2}\widehat{a}\ ,\ \overline{y} = \frac{1}{n+1}\sum_{i=0}^{n} y_i\ , \tag{6}$$

а залишкову суму квадратів —

$$S_2^2 = \sum_{i=0}^{n}\left(y_i - \overline{y}\right)^2 - \widehat{a}^2\sum_{i=0}^{n}\left(\frac{i}{n} - \frac{1}{2}\right)^2. \tag{7}$$

Розглянемо застосування цього алгоритму на прикладах.

Приклад 1. Чи можна відхилити гіпотезу H з рівнем значущості $\alpha = 0.05$ для нелінійної регресійної моделі (1), якщо $\vec{y} = (0,\ 0.2,\ 0.25,\ 0.3,\ 0.35,\ 0.55,\ 0.7,\ 0.95, 1.1, 1.35, 1.5)$?

В даному випадку $n = 10,\ \varphi = \frac{1}{8}\cdot 5.59 = 0.7375.$

1. Знаходимо $\widehat{a}, \widehat{b}, S_2^2$ за формулами (6), (7):

$$\widehat{a}4 = 1.482,\ \widehat{b} = -0.082,\ S_2^2 = 0.099.$$

2. Знаходимо $M_1 = \max\left\{ \mid y_0 - \widehat{b} \mid , \mid y_{10} - \widehat{a} - \widehat{b} \mid \right\} : M_1 = 0.1$;

   Оскільки $\dfrac{M_1^2}{S_2^2 - M_1^2} < \varphi,$ переходимо до.

3. Знаходимо

   $M_2 = \max\left\{ \mid y_i - 0.1\widehat{a}\, i - \widehat{b} \mid , i = 1, 2, ..., n-1, \right\} : M_2 = 0.161,\ k = 4.$

   Знаходимо $\widehat{c}_1^{(4)}, z_4, S_{3,4}^2$ за формулами (4), (5), (3): $S_{3,4}^2 = 0.01352$;

   Оскільки $\dfrac{S_2^2 - S_{3,4}^2}{S_{3,4}^2} > \varphi,$ гіпотезу H відхиляємо.

Приклад 2. Чи можна відхилити гіпотезу H з рівнем значущості $\alpha = 0.05$ для нелінійної регресійної моделі (1), якщо $\vec{y} = \left(0, 0.2, 0.25, 0.3, 0.35, 0.55, 0.6, 0.75, 0.85, 0.9, 1.05\right)$?

В даному випадку також $n = 10,\ \varphi = 0.7375.$

1. Знаходимо $\widehat{a}, \widehat{b}, S_2^2$ за формулами (6), (7):

$$\widehat{a} = 1,\ \widehat{b} = 0.027,\ S_2^2 = 0.017.$$

2. Знаходимо $M_1 = \max\left\{\mid y_0 - \widehat{b} \mid , \mid y_{10} - \widehat{a} - \widehat{b} \mid\right\} : M_1 = 0.027$; $\dfrac{M_1^2}{S_2^2 - M_1^2} < \varphi,$

   переходимо до

3. Знаходимо

   $M_2 = \max\left\{ \mid y_i - 0.1\widehat{a}\, i - \widehat{b} \mid , i = 1, 2, ..., n-1, \right\} : M_2 = 0.077,\ k = 4.$

   Знаходимо $\widehat{c}_1^{(4)}, z_4, S_{3,4}^2$ за формулами (3), (4), (5): $S_{3,4}^2 = 0.01427$;

   Оскільки $\dfrac{S_2^2 - S_{3,4}^2}{S_{3,4}^2} < \varphi,$ переходимо до

4. На цьому кроці для $k = 1, 2, ..., 8$ будуємо пари прямих по точкам $\left\{\left(t_i , y_i\right), i = 0, 1, ..., k\right\}$ та $\left\{\left(t_i , y_i\right), i = k+1, ..., 10\right\}$ за методом найменших квадратів та знаходимо їх точку перетину; якщо вона не належить проміжку $\left(t_k, t_{k+1}\right)$, цю пару прямих відкидаємо. В нашому прикладі жодна з цих пар прямих не має перетину на відповідному проміжку, тому переходимо до

5. Знаходимо $S_{3,1}^2 = 0.01573,\ \ S_{3,2}^2 = 0.01668,\ \ S_{3,3}^2 = 0.01519,$

$$S_{3,5}^2 = 0.01565,\ \ S_{3,6}^2 = 0.01588,\ \ S_{3,7}^2 = 0.01653,$$

$$S_{3,8}^2 = 0.01668, \quad S_{3,9}^2 = 0.01606.$$

Таким чином, $S_4^2 = S_{3,4}^2 = 0.01427$; гіпотезу H приймаємо.

Висновки. На прикладах можна побачити, що відхилення гіпотези H майже завжди буде відбуватися на кроці 3, тобто знаходити оцінку МНК невідомих параметрів та залишкову суму квадратів нелінійної моделі (1) немає потреби. Для прийняття гіпотези H треба знаходить S_4^2. Бажано довести, що отримана на кроці 3 $S_{3,k}^2$, що відповідає M_2, буде збігатися з S_4^2. Тоді кроків 4, 5 не треба робити ні в якому разі.

Список використаних джерел:

1. Дрейпер Н., Смит Г. Прикладной регрессионный анализ. М.: Финансы и статистика, 1986. 366 с.
2. Завьялов Ю. С., Квасов Б. И., Мирошниченко В.Л. Методы сплайн-функций. М.: Наука, 1980. 352 с.
3. Себер Дж. Линейный регрессионный анализ. М.: Мир, 1980. 456 с.
4. Демиденко Е. З. Линейная и нелинейная регрессии. М.: Финансы и статистика, 1986. 304 с.
5. Савкіна М. Ю. Алгоритм перевірки на коректність моделі двофазної нелінійної регресії. Вісник Київського університету. 2015. № 3. С. 115–120.

The algorithm of checking for correctness of two-phase regression model with unknown switch point is constructed in the case when it is necessary to do a choice between such model and linear. The algorithm is based on the general principles of statistical hypothesis testing in regression analysis.

Key words: *least square method, regression model, switch point.*

Одержано 24.02.2017

УДК 517.9

Г. В. Сандраков, д-р фіз.-мат. наук, с. н. с.

Київський національний університет імені Тараса Шевченка, м. Київ

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ МАСИВІВ МІКРОГОЛОК

Оптимізація параметрів пружної взаємодії масивів мікроголок з поверхнею розглянута як задача наближення розв'язків проблем мінімізації для інтегральних функціоналів.

Ключові слова: *оптимізація параметрів, масиви мікроголок, проблеми мінімізації, інтегральні функціонали.*

Вступ. Масиви мікроголок для ін'єкцій ліків все частіше використовуються в сучасній медицині при лікуванні різних захворювань. Такі масиви формуються досить великою кількістю мікроголок, закріплених на плоскій основі, і використовуються, наприклад, при ін'єкціях вакцин, протеїнів і інсуліну. При виготовленні таких масивів, мікроголки закріплюються на основі зазвичай періодичним чином, що спрощує технологічну складність їх виробництва. Типовий масив мікроголок для ін'єкційного введення ліків є наведеним на рис. 1 із роботи [1]. Досить докладна бібліографія про дослідження різних аспектів і методів застосування та виробництва таких масивів на практиці, що містить сотні найменувань, наведена в [1–5]. Однак, проблема оптимізації параметрів пружної взаємодії таких масивів з поверхнею зовсім не розглядалась. Така проблема буде сформульована та частково досліджена у цій роботі.

Постановка задачі. Визначимо квадрат $K=[-l,l]^2$ на площині зі сторонами довжини $2l$ см. Задавши парне додатне ціле N, розіб'ємо квадрат K на N^2 менших квадратів k_{ij}^{ε} при $i,j=1,...,N$ зі сторонами довжини $\varepsilon=(2l/N)$ см. та виділимо в кожному із таких квадратів однакові множини $b_{ij}^{\varepsilon}\subset k_{ij}^{\varepsilon}$ для $i,j=1,...,N,$ наприклад, круги однакового радіуса r_{ε}, розташовані в центрі кожного квадрата k_{ij}^{ε}. Або, еквівалентно, позначимо $k_0^{\varepsilon}=[0,\varepsilon]^2$ комірку періодичності та виділимо в k_0^{ε} множину $b_0^{\varepsilon}\subset k_0^{\varepsilon}$, наприклад, круг радіуса r_{ε} із центром у центрі комірки періодичності k_0^{ε}. Тоді b_{ij}^{ε} та k_{ij}^{ε} визначаються як ε-періодичні трансляції множин b_0^{ε} та k_0^{ε}, здійснювані в межах квадрата K.

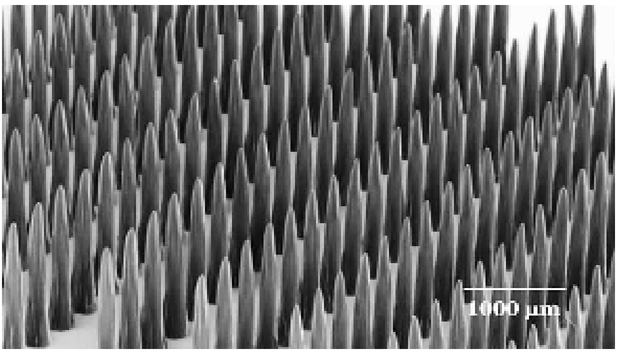


Рис. 1. *Приклад масиву мікроголок*

Розглянемо також квадрат $I=[-0.5l,0.5l]^2$ зі сторонами довжини l см. та задавши додатне число a визначимо функцію

$$\psi_{\varepsilon}^{a} = a \text{ для } x \in I \bigcap \left(\bigcup_{ij} b_{ij}^{\varepsilon} \right)$$

і $\psi_{\varepsilon}^{a} = 0$ у іншому випадку. Графік функції ψ_{ε}^{a} визначає найпростішу модель ε-періодичного масиву мікроголок над квадратом I з циліндричними голками довжини a, основи яких визначає множина b_0^{ε}, що показана на рис. 2.

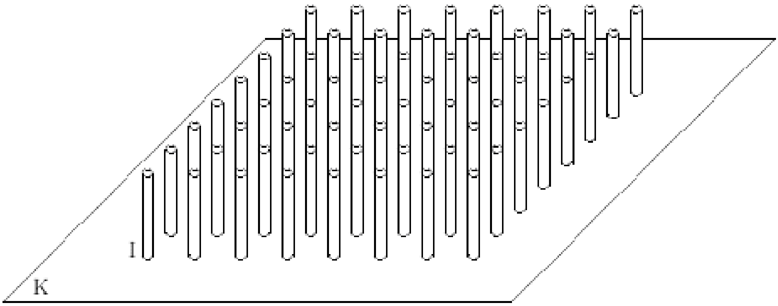


Рис. 2. *Модель масиву циліндричних мікроголок*

При досить великому N цей графік також цілком ілюструється рис. 1 з тією лише різницею, що голки на цьому рисунку представлені дуже витягнутими конусами, а не циліндрами, як на рис. 2. Наприклад, при $N = 100$ циліндричні голки в розглянутій моделі масиву є досить тонкими, оскільки $\varepsilon = 0.2l$ мм., що значно менше радіуса звичайної голки, що використовується для ін'єкцій при $l \ll 1$. З іншого боку, при $N = 100$ і, наприклад, $b_{ij}^{\varepsilon} = k_{ij}^{\varepsilon}$ при $i, j = 1, \ldots, N$ використовувати такий масив з мікроголок не є можливим. Останній приклад пояснює, що при фіксованому N (наприклад, $N = 100$) радіус основи b_0^{ε} розглянутих голок масиву має бути істотно меншим ε і необхідно дійсно використовувати мікроголки для комфортного застосування таких масивів для ін'єкцій.

Виникає природне запитання, чи можна визначити оптимальні радіус і форму основи b_0^{ε} розглянутих мікроголок?

Виявляється, це питання вже ставилося раніше De Giorgi [6] як проблема «килимка факіра». Проблема ця була вирішена Carbone та Colombini в [6] для циліндричних голок відповідно до твердження з [7], де розглядаються аналогічні проблеми.

Для точного формулювання відповідної проблеми розглянемо інтегральний функціонал

$$F(u) = \int_{K} \left| \nabla u(x) \right|^2 dx \text{ для } u \in \left\{ v \in H_0^1(K) : v \geq 0 \right\}.$$

Цей функціонал визначає енергію пружного опору поверхні (оболонки або плівки) над квадратом K в припущенні відсутності поперечних зсувів. Визначення простору Соболєва $H_0^1(K)$ наведене, наприклад, в [8]. Мінімум функціонала $F(u)$ задає стаціонарне розташування оболонки над K. Зрозуміло, цей мінімум є нульовим, якщо на оболонку не діють будь-які сили.

Розглянемо далі інтегральний функціонал

$$F_\varepsilon^a\left(u\right) = \int_K \left|\nabla u(x)\right|^2 dx \text{ для } u \in \left\{v \in H_0^1(K) : v \geq \psi_\varepsilon^a\right\},$$

де ψ_ε^a визначає найпростішу модель масиву мікроголок. Мінімум функціоналу $F_\varepsilon^a(u)$ визначає стаціонарне розташування поверхні (відповідної ділянки шкіри пацієнта) над K під дією найпростішого масиву мікроголок ψ_ε^a. Відомо [8], що такий мінімум u_ε^a функціоналу $F_\varepsilon^a(u)$ існує та є визначеним однозначно для фіксованих a та ε. Нехай далі множина $b_0^\varepsilon \subset k_0^\varepsilon$ визначена як круг радіуса r_ε, розташований у центрі квадрата k_0^ε.

Використовуючи результати робіт [6, 7] можливо довести наступне твердження.

Теорема. При малих ε мінімум u_ε^a функціоналу $F_\varepsilon^a(u)$ наближається у нормі простору $H_0^0(K) = L^2(K)$ до

(a) 0, якщо $\varepsilon^2\left(-\ln r_\varepsilon\right) \to \infty$ при $\varepsilon \to 0$;

(b) мінімуму u_a інтегрального функціоналу

$$F_a\left(u\right) = \int_K \left|\nabla u\right|^2 dx + \frac{2\pi}{rl}\int_I \left(\left(a-u\right)^+\right)^2 dx \text{ для } u \in \left\{v \in H_0^1(K) : v \geq 0\right\},$$

якщо $\varepsilon^2\left(-\ln r_\varepsilon\right) \to r$ при $\varepsilon \to 0$, де $r > 0$ та $(v)^+ = \max(v, 0)$;

(c) $u_a \in H_0^1(K)$, де $\left\|u_a\right\|_{H_0^1(K)} \to \infty$,

якщо $\varepsilon^2\left(-\ln r_\varepsilon\right) \to 0$ при $\varepsilon \to 0$.

Умови (a), (b), (c) теореми виконані, наприклад, при

(a) $r_\varepsilon = e^{-r/\varepsilon^3}$; (b) $r_\varepsilon = e^{-r/\varepsilon^2}$; (c) $r_\varepsilon = e^{-r/\varepsilon}$ (або $r_\varepsilon = \varepsilon^\tau$),

відповідно, для деяких фіксованих $r > 0$ і $\tau \geq 0$. При $r = 1$ та $l = 1$ такі твердження доведені у [6, 7] . Використовуючи результати робіт [9, 10], можна отримати більш точне твердження про структуру задачі на мінімум за умов (c) теореми. Безпосередньо можна перевірити також, що твердження теореми не змінюються при скінченно-пропорційній зміні радіуса r_ε, тобто виконання тверджень теореми не залежить від форми основи голок у найпростішому масиві мікроголок, якщо в b_0^ε можна вписати і навколо b_0^ε описати кола відповідних радіусів. Більш того, твердження теореми не залежать від форми самої голки (розташованої по центру k_0^ε), а не тільки форми основи циліндричних голок найпростішого масиву, якщо в таку голку можна вписати і навколо неї описати циліндри відповідних радіусів.

Для близьких задач доданок інтегрального функціоналу

$$f_a(u) = \frac{2\pi}{rl}\int_I \left(\left(a-u\right)^+\right)^2 dx$$

з теореми (b) названо в [12] «дивним членом, що з'являється нізвідки». «Дивина» цього доданка полягає перш за все в незалежності $f_a(u)$ від форми основи, зазначеної вище. Ця незалежність не виконується для масивів мікроголок у великих вимірах [12]. У контексті розглянутих тут задач про масиви мікроголок, поява доданка $f_a(u)$ цілком природна і визначається реакцією оболонки (відповідної ділянки шкіри пацієнта) під дією масиву мікроголок ψ_ε^a.

Зазначена незмінність наведених тверджень пов'язана перш за все із мікротонкістю голок, розташованих центрально-симетрично і утворюючих розглянутий періодичний масив мікроголок. Крім того, наведені твердження прояснюють, що найбільш оптимальними є масиви з круглими циліндричними мікроголками, оскільки такі голки мають найкращу пропускну здатність ліків, що перевіряється безпосередньо. При цьому, радіус основи таких голок, які гарантують комфортне використання таких масивів, слід визначати з рівності

$$r_\varepsilon = e^{-r\left(N/2\right)^2},$$

де постійна r підбирається таким чином, щоб забезпечити необхідну пропускну здатність конкретного масиву мікроголок із заданою кількістю мікроголок $\left(N/2\right)^2$.

Висновки. Встановлені оцінки оптимальних параметрів мікроголок, які надають комфортне використання масивів мікроголок для ін'єкцій і внутрішнього введення ліків. Такі оцінки є істотними для моделювання та оптимізації процесів, яки реалізуються при ін'єкціях ліків масивами мікроголок.

Список використаних джерел:

1. Park J. H., Allen M. G., Prausnitz M. R. Biodegradable polymer microneedles: fabrication, mechanics and transdermal drug delivery. *Journal of Controlled Release*. 2005. Vol. 104. P. 51–66.
2. Parker E. R., Rao M. P., Turner K. L., Meinhart C. D., MacDonald N. C. Bulk micromachined titanium microneedles. *Journal of Microelectromechanical System*. 2007. Vol. 16. P. 289–295.
3. Olatunji O., Das D. B., Garland M. J., Belaid L., Donnelly R. F. Influence of array interspacing on the force required for successful microneedle skin penetration: theoretical and practical approaches. *Journal of Pharmaceutical Sciences*. 2013. Vol. 102. P. 1209–1221.
4. Romgens A. M., Bader D. L., Bouwstra J. A., Baaijens F. P. T., Oomens C. W. J. Monitoring the penetration process of single microneedles with varying tip diameters. *Journal of the Mechanical Behavior of Biomedical Materials*. 2014. Vol. 40. P. 90–105.
5. Ita K. Transdermal delivery of drugs with microneedles potential and challenges. *Pharmaceutics*. 2015. Vol. 7. P. 397–405.
6. Carbone L., Colombini F. On convergence of functionals with unilateral constraints. *Journal of Math. Pures Appl*. 1980. Vol. 59. P. 465–500.
7. Attouch H., Picard C. Variational inequalities with varying obstacles: the general form of the limit problem. *Journal of Funct. Anal*. 2015. Vol. 50. P. 329–386.
8. Киндерлерер Д., Стампакья Г. Введение в вариационные неравенства и их приложения. М.: Мир, 1983. 256 с.
9. Sandrakov G. V. Homogenization of variational inequalities for obstacle problems. *Sbornik: Mathematics*. 2005. Vol. 196. P. 541–560.
10. Sandrakov G. V. Homogenization of variational inequalities and equations defined by pseudomonotone operators. *Sbornik: Mathematics*. 2008. Vol. 199. P. 67–98.
11. Rodrigues J. F. Obstacle problems in mathematical physics. Amsterdam: North-Holland, 1987. 352 p.
12. Cioranescu D., Murat F. Un terme etrange venu d'ailleurs I, II, Nonlinear Partial Dierential Equations and Their Applications, College de France Seminar, Vol. II, 98-138, Vol. III, 154-178, Res. Notes in Math. 60 and 70. London: Pitman, 1982 and 1983. English translation: A strange term coming from nowhere. Topics in the Math. Modelling of Composite Materials. P. 45–93. Boston: Birkhauser, 1997.

A parameter optimization of elastic interactions for microneedle arrays with surfaces is considered as an approximation approach for minimization problem solutions of integral functionals.

Key words: *parameter optimization, microneedle arrays, minimization problem, integral functionals.*

Одержано 05.03.2017

UDC 519.642

E. V. Semenova, Cand. of Phys. and Mathem. Sciences,
E. A. Volynets, Cand. of Phys. and Mathem. Sciences
Institute of Mathematic of NAS of Ukraine, Kiev

DISCREPANCY PRINCIPLE FOR SOLVING PERIODIC INTEGRAL EQUATIONS OF THE FIRST KIND

Fully discrete projection method with discrepancy principle is considered for solving periodic integral equations of the first kind with unknown smoothness of solution. For proposed approach it is proved the optimality and effectiveness in the sense of computational resource.

Key words: *fully discrete projection method, discrepancy principle, periodic integral equation.*

Introduction. The object of our investigation is periodic integral equation of the first kind with operator of pseudodifferential structure. As it is known pseudodifferential equation of elliptic type are frequently found in various problems of natural sciences that can be described by a boundary value problems such as Laplace, Neumann or Helmholz equations. Such equations are well-known and were investigated, for example, in [1]. The most widely-used approaches for numerical solving periodic integral equations of the first kind are fully discrete collocation and projection methods that applied together with selfregularization principle. In the framework of the paper it will be considered a modification of fully discrete projection method (FDPM). Note that standard variant of FDPM was firstly proposed for solving the integral Symm equation (the particular case of problem under consideration) in [2] and extended on the class of pseudodifferentional equations in [3]. Moreover we introduce some additional discretization in the method to reduce amount of arithmetical operations.

Statement of the problem. In the space $L_2(0,1)$ we consider the following integral equation

$$Au(t) = f(t),\ t \in [0,1]\,, \tag{1}$$

where $f(t)$ is 1-periodic function and operator A has the form

$$A = D + \sum_{p=0}^{q} A_p\,,$$

where $A_p u(t) = \int\limits_0^1 k_p(t-s)a_p(t,s)u(s)ds,\ Du = \int\limits_0^1 k_0(t-s)u(s)ds.$

Let's denote by $C^\infty = C^\infty([0,1]^2)$ the space of infinity smooth 1-biperiodic functions of two variables. Suppose that $a_p \in C^\infty$, $p = 0,..,q$, $a_0(t,t) \neq 0,\ t \in [0,1]$, such that

$$\| a_p \|^2_{\eta_1,\eta_2} := \sum_{k,l=-\infty}^{\infty} | \widehat{a}(k,l) |^2 \, e^{2\eta_2 (|k|^{1/\eta_1} + |l|^{1/\eta_1})} < \infty, \ \eta_1 \ge 1, \eta_2 > 0. \qquad (2)$$

Moreover assume that $k_p(t-s)$ is 1-periodic function with known Fourier coefficients $\widehat{k}_p(n)$ by trigonometric basis. Additionally we suppose that for some $\alpha \in \mathbb{R}$ and $\beta > 0$ the following inequalities

$$\begin{aligned} & c_{00} \, | n |^{\alpha} \le | \widehat{k}_0(n) | \le c_0 \, | n |^{\alpha}, \quad n \in \mathbb{Z} / 0, \\ & | \widehat{k}_0(n) - \widehat{k}_0(n-1) | \le c \, | n |^{\alpha-\beta}, \quad n \in \mathbb{Z}, \\ & | \widehat{k}_p(n) | \le c \, | n |^{\alpha-\beta}, \quad n \in \mathbb{Z}, \, p = 1,...,q, \end{aligned} \qquad (3)$$

hold true, where $c, c_0, c_{00} > 0$ and $n = \begin{cases} | n |, & n \in \mathbb{Z} / 0 \\ 1, & n = 0 \end{cases}$.

Denote by H^{λ}, $-\infty < \lambda < \infty$, Hilbert spaces of 1-periodic functions and by H^{λ_1,λ_2}, $-\infty < \lambda_1, \lambda_2 < \infty$ 1-biperiodic functions with the norms

$$\| u \|_{\lambda} := (| \widehat{u}(0) |^2 + \sum | n |^{2\lambda} | \widehat{u}(n) |^2)^{1/2} < \infty,$$

$$\| a \|_{\lambda_1,\lambda_2} := (\sum | k |^{2\lambda_1} | l |^{2\lambda_2} | \widehat{a}(k,l) |^2)^{1/2} < \infty,$$

respectively. Here $\widehat{u}(n), \widehat{a}(k,l)$ are Fourier coefficients of functions $u(t)$ and $a(t,s)$ by trigonometric basis $\{e_k\}_{k=-\infty}^{+\infty}$, where $e_k(t) = e^{i2\pi kt}$, $t \in [0,1]$.

We suppose that $f \in H^{\mu+1}$ for some unknown $\mu > \alpha + 1/2$. Let instead of $f(t)$ only some its perturbation is given such that for $N = \delta^{-\frac{1}{\lambda-\alpha}}$ we have

$$N^{-1} \left(\sum_{j=1}^{N} | f_{\delta}(jN^{-1}) - f(jN^{-1}) |^2 \right)^{1/2} \le \delta \, \| f \|_{\mu-\alpha}.$$

Note that similar class of problems was considered before in [1], [3] and other. In particular, in [3] the optimal order fully discrete projection method for solving (1) with (2)–(3) was proposed. In the paper we consider the same class of problems as in [3] and state the aim to reduce the amount of arithmetical operations with saving optimality of the method.

Auxiliary statements. For further presentation of our results we will use the following notations.

Let's introduce N-dimensional subspace of trigonometric polynomials

$$T_N = \left\{ u_N : u_N(t) = \sum_{k \in \mathbb{Z}_N} c_k e_k(t) \right\},$$

where $\mathbb{Z}_N = \left\{ k : -\frac{N}{2} < k \le \frac{N}{2},\, k = 0, \pm 1, \pm 2, ... \right\}$.

Denote by P_N and P_Ω orthoganal projectors

$$P_N u(t) = \sum_{k \in \mathbb{Z}_N} \hat{u}(k) e_k(t) \in T_{N,}$$

$$P_{\Omega_N} u(t) = \sum_{l,k \in \Omega_N} \hat{a}(k,l) e_k(t) e_l(s) \in T_N \times T_{N,}$$

where Ω_N is some domain on the coordinate plane restricted by square $(-N/2, N/2] \times (-N/2, N/2]$. Also denote by $Q_{N,}$ and $Q_{N,N}$ interpolation projectors, such that $Q_N u(t) \in T_N$, $Q_{N,N} u(t) \in T_N \times T_N$ and on the uniform grid it holds true $(Q_N u)(jN^{-1}) = u(jN^{-1}), j = 1, 2, ..., N,$

$$(Q_{N,N} a)(jN^{-1}, iN^{-1}) = a(jN^{-1}, iN^{-1}), \quad j, i = 1, 2, ..., N .$$

Modified fully discrete projection method. As Ω_N we take the following domain on the coordinate plane

$$D_M^{\eta_1} = \left\{ (k,l) : |k|^{1/\eta_1} + |l|^{1/\eta_1} < \left(\frac{M}{2} \right)^{\frac{1}{\eta_1}},\, k, l = 0, \pm 1, \pm 2, ... \right\}.$$

Assume that the discrete information about kernels $a_p(t,s)$ and right hand side f are given in the knots of uniform grids $\left(\frac{j_1}{N}, \frac{j_2}{N} \right)$ and $\left(\frac{j}{N} \right)$ respectively, where $j, j_1, j_2 = 1, ..., N$.

The right-hand side of equation (1) we approximate as $f_{\hat{N}} := Q_{\hat{N}} f_\delta$. Thus, instead of the kernels $a_p(t,s)$ we take the following finite dimensional elements

$$a_{p,M} = P_{D_M^{\eta_1}} Q_{M,M} a_p, \tag{4}$$

where M is discretization parameter such that $\hat{N} > M$.

Then the operators $A_{p,M}$ can be approximated by

$$A_{p,M} u(t) = \int_0^1 k_p(t-s) a_{p,M}(t,s) u(s) ds,$$

where function $a_{p,M}$ has the form (4).

Additional discretization of operators $A_{p,M}$ consists in replacing $A_{p,M}$ on the operator $P_l A_{p,M} P_l$. Thus we approximate A in terms of

$$A_M = D + P_l \sum_{p=0}^{q} A_{p,M} P_l, \tag{5}$$

where $l = \widehat{N}^\tau$ for some $0 < \tau < 1$ and $\widehat{N}, M$ are discretization parameters that should be chosen in appropriate way. Note that approximation (5) is distinguished from respective approximation from [3] by using additional projectors P_l and $P_{D_M^m}$. Such approach help to reduce the amount of arithmetical operations.

We propose the following modification of the fully discrete projection method (FDPM) for numerical solving (1):

$$A_M u_{\widehat{N}} := D u_{\tilde{N}} + P_l \sum_{p=0}^{q} A_{p,M} P_l u_{\widehat{N}} = Q_{\widehat{N}} f_\delta \,, \tag{6}$$

where $A_{p,M}$ has the view (5) and $u_{\widehat{N}} \in T_{\widehat{N}}$ is taken as approximate solution of (1).

Note that by virtue of (3) it holds true

$$A_{p,M} \in L(H^\lambda, H^{\lambda-\alpha+\beta}),\ p = 0,...q.$$

Following [1] for fast solving (6) we propose to use GMRES. The procedure is following: for $n = 1, 2, ...$ we construct the sequence $u_{n,\widehat{N}}$ that satisfies the condition

$$\| S_{\widehat{N}} u_{n,\widehat{N}} - f_{\widehat{N}} \|_\alpha = \min_{u \in K_n(S_{\widehat{N}}, f_{\widehat{N}})} \| S_{\widehat{N}} u - f_{\widehat{N}} \|_\alpha, \tag{7}$$

where $S_{\widehat{N}} = D + P_l \sum_{p=0}^{q} A_{p,M} P_l$ and $K_n(S_{\widehat{N}}, f_{\widehat{N}})$ is well-known Krylov space. As the stopping rule we consider the discrepancy principle

$$\| S_{\widehat{N}} u_{n,N} - f_{\widehat{N}} \|_\alpha \le c\delta \| f_{\widehat{N}} \|_\alpha \,,$$

where $u_{n,\widehat{N}}$ is n-th iteration of GMRES that we consider as approximate solution to $u_{\widehat{N}}$.

Theorem 1. Let n be the first number that fulfils (7). Then the accuracy of GMRES is

$$\| u_{n,\widehat{N}} - u_{\widehat{N}} \|_\lambda \le c \left(\frac{\widehat{N}}{2} \right)^{\lambda - 2\alpha} \delta \,,$$

where c is some positive constant. Moreover the amount of arithmetical operations for solving (6) by (7) is $O(\widehat{N}\log\widehat{N})$.

Main results. In view of self regularization on the pair of spaces H^{λ} and $H^{\lambda-\alpha}$ the problem under consideration doesn't need any additional regularization but it is necessary to chose appropriate discretization parameters. For this aim we propose to use discrepancy principle that is describe below.

Let $D_N=\{1, 2, 2^2,...., 2^{N_1}=\delta^{\frac{1}{\lambda-\alpha}}\}$ be a set of possible discretization parameter. We take the discretization parameters $\widehat{N}$ and M by the rule:

$$\widehat{N}=\min\{\widehat{N}\in D_N :\| A_N u_{\widehat{N}}-Q_{\widehat{N}} f_\delta \|\le b_2\delta\}, \tag{8}$$

$$M=O(\log\widehat{N}).$$

Theorem 2. Let M and $\widehat{N}$ be chosen according (8). Then the error bound of FDPM for (1) is

$$\| u-u_{\widehat{N}} \|_\lambda \le c(\delta^{\frac{\mu-\lambda}{\mu-\alpha}}),$$

where c is some positive constant that doesn't depend on $\widehat{N},\delta$. Moreover to find numerical solution by FDPM (6) with (7) and (8) it is necessary to execute $O(N\log^2 N)$ arithmetical operations.

Remark. Taking into account Theorems 1 and 2 the general accuracy of the method (6) in combination with (7) and (8) is the following

$$\| u-u_{n,\widehat{N}} \|_\lambda \le c\delta^{\frac{\mu-\lambda}{\mu-\alpha}}.$$

Besides the total amount of arithmetical operations for solving (1) by (6) in combination with (7) and (8) is $O(N\log^2 N)$.

Conclusion. In the paper for solving periodic integral equations of the first kind a problem of reduction amount of arithmetical operations is considered. For this we propose some modification of fully discrete projection method in combination with discrepancy principle for choosing appropriate discretization parameter and GMRES for fast solving of system of linear equations. It was proved that such approach guarantees the best possible accuracy of recovering the solution in the metric of Sobolev spaces with minimal computational costs in comparison with the methods investigated earlier.

References:

1. Saranen J., Vainikko G. Periodic Integral and Pseudodifferential Equations with Numerical Approximation. Berlin: Springer, 2002. 452 p.

2. Pereverzev S. V., Prossdorf S. On the characterization of self-regularization properties of a fully discrete projection method for Symm's integral equation. *J. Integral Equations Appl*. 2000. V. 12, N 2. P. 113–130.
3. Solodky S. G., Semenova E. V. A class of periodic integral equation with numerical solving by a fully discrete projection method. UMV. 2014. V. 11, N 3, P. 400–416.

Розглянуто повністю дискретний проекційний метод у комбінації з принципом рівноваги для розв’язування періодичних інтегральних рівнянь у апостеріорному випадку. Доведена оптимальність та економічність такого підходу.

Ключові слова: *повністю дискретний проекційний метод, принцип нев’язки, періодичні інтегральні рівняння.*

Date received 06.03.2017

УДК 519.8

Н. В. Семенова, д-р фіз.-мат. наук,
Т. Т. Лебєдєва, канд. екон. наук,
Т. І. Сергієнко, канд. фіз.-мат. наук
Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ОПТИМАЛЬНІСТЬ ТА КОРЕКТНІСТЬ У ВЕКТОРНИХ ЗАДАЧАХ ДИСКРЕТНОЇ ОПТИМІЗАЦІЇ

Сформульовано умови оптимальності розв’язків векторної задачі дискретної оптимізації на допустимій множині, що описується псевдоопуклими функціями обмежень, отримано достатні умови оптимальності різних видів розв'язків задачі та п’яти типів її стійкості. Встановлено топологічні властивості підмножин простору вхідних даних задачі, на яких зберігається оптимальність її розв'язків.

Ключові слова: *дискретна оптимізація, векторна задача, стійкість, коректність.*

Вступ. Встановлення необхідних і достатніх умов оптимальності та стійкості розв'язків векторних дискретних задач це актуальна проблема, оскільки їх знання дає основу для розробки способів перевірки оптимальності та якості того чи іншого обраного розв'язку, та побудови ефективних методів знаходження множин оптимальних розв'язків, які мають деякі наперед задані властивості інваріантності при можливих збуреннях вхідних даних задачі [1].

У доповіді сформульовано умови оптимальності розв’язків векторної задачі дискретної оптимізації на допустимій множині, яка описується псевдоопуклими функціями обмежень [2], отримано достатні умови оптимальності Парето-оптимальних, слабо та строго ефективних розв'язків задачі, та різних типів стійкості задачі. Досліджено топологічні властивості деяких підмножин простору вхідних даних задачі, на яких зберігається оптимальність її розв'язків.

Постановка задачі. Основні означення. Розглянемо векторну задачу дискретної оптимізації такого вигляду: $Z_P\left(F,X\right): \max\left\{F(x) \mid x \in X\right\}$, де $F(x) = (f_1(x),..., f_l(x))$ — векторний критерій; $f_i : R^n \to R^1$, $i \in N_\ell = \left\{1,...,\ell\right\}$, X — непорожня множина в R^n, $X \subset Z^n$, $G = \left\{x \in R^n \mid g_i(x) \le 0, i \in N_m\right\}$, $g_i : R^n \to R^1, i \in N_m$.

Під розв'язанням задачі $Z_P\left(F,X\right)$ будемо розуміти знаходження елементів множини $P\left(F,X\right)$ — Парето-оптимальних (ефективних) розв'язків [3]. Розглядатимемо також множини: $Sl\left(F,X\right)$ — оптимальних за Слейтером (слабо ефективних) розв'язків, $Sm\left(F,X\right)$ — оптимальних за Смейлом (строго ефективних) розв'язків.

Згідно [1–6] для будь-якого $x \in X$ істинні такі твердження:

$$x \in P\left(F,X\right) \Leftrightarrow \pi\left(y,F,X\right) = \left\{y \in X \mid F\left(y\right) \ge F\left(x\right), F\left(y\right) \ne F\left(x\right)\right\} = \varnothing,$$

$$x \in Sl\left(F,X\right) \Leftrightarrow \sigma\left(y,F,X\right) = \left\{y \in X \mid F\left(y\right) > F\left(x\right)\right\} = \varnothing, \qquad (1)$$

$$x \in Sm\left(F,X\right) \Leftrightarrow \eta\left(y,F,X\right) = \left\{y \in X \mid y \ne x, F\left(y\right) \ge F\left(x\right)\right\} = \varnothing,$$

$$Sm\left(F,X\right) \subset P\left(F,X\right) \subset Sl\left(F,X\right). \qquad (2)$$

Умови оптимальності та стійкості розв'язків задачі $Z_P\left(F,X\right)$. Нехай функції $f_i(x)$, $i \in N_\ell$, часткових критеріїв є псевдоугнутими функціями, а g_i, $i \in N_m$, — псевдоопуклі функції. Введемо до розгляду неперервну векторну задачу $Z_P(F,G)$: $\max\{F(x) \mid x \in G\}$, що відповідає задачі $Z_P\left(F,X\right)$.

Позначимо $Fr\,B$ — сукупність усіх граничних точок деякої множини B, $\operatorname{int} B = B \setminus Fr\,B$. Для будь-якого розв'язку $y \in Fr\,G$ визначимо такі множини:

$$N(y) = \left\{i \in N_m \,\middle|\, g_i(y) = 0\right\},$$

$$H(y) = \left\{x \in R^n \,\middle|\, \left\langle \nabla g_i(y), x - y\right\rangle \le 0, i \in N(y)\right\},$$

$$G(y) = \left\{x \in R^n \,\middle|\, g_i(x) \le 0, i \in N(y)\right\},$$

$$K(y)=\left\{x\in R^n\left|\left\langle\nabla f_i(y),x-y\right\rangle\geq 0,\ i\in N_\ell\right.\right\},$$

$$K_0(y)=\left\{x\in R^n\left|\left\langle\nabla f_i(y),x-y\right\rangle=0,\ i\in N_\ell\right.\right\},$$

де $\nabla f_i(y)$ — градієнт функції $f_i(x)$ у точці y.

Враховуючи висловлювання (1)–(24), справедливі при $X=G$, та очевидні включення $X\subset G\subset G(y)\subset H(y)$, $\sigma(y,F,G)\subset \operatorname{int}K(y)$, $\sigma(y,F,G)\subset\pi(y,F,G)\subset\eta(y,F,G)\subset K(y)$, $\pi(y,F,G)\subset K(y)\setminus K_0(y)$ приходимо до висновку про справедливість теореми.

Теорема 1. Нехай $y\in FrG\bigcap Z^n$. Якщо $g_i(x), i\in N(y)$, і $-f_i(x),\ i\in N_\ell$, — псевдоопуклі функції, то умови

$$\operatorname{int}K(y)\cap H(y)=\varnothing, \tag{3}$$

$$(K(y)\setminus K_0(y))\cap H(y)=\varnothing, \tag{4}$$

$$K(y)\cap H(y)=\{0\} \tag{5}$$

є достатніми для належностей $y\in Sl(F, X)$, $y\in P(F, X)$, $y\in Sm(F, X)$ відповідно. Якщо $\{\nabla f_i(y)\mid i\in N_\ell\}$ і $\{\nabla g_i(y)\mid i\in N(y)\}$ — системи лінійно незалежних векторів, то співвідношення (3) — необхідна умова для $y\in Sl(F,G)$.

Нехай $u=(u_1,u_2)$ — набір вхідних даних задачі $Z_P(F,G)$, що є елементом деякого простору U вхідних даних задачі. Простір U можна подати як декартовий добуток $U=U_1\times U_2$ простору U_1 вхідних даних для опису векторного критерія F і простору U_2 вхідних даних, що описують допустиму множину X. Зокрема, якщо векторний критерій представлений квадратичними функціями $f_i(x)=\left\langle x,D_ix\right\rangle+\left\langle c_i,x\right\rangle, i\in N_\ell$, де $D_i\in R^{n\times n}$, $c_i=(c_{i1},...,c_{in})\in R^n$, то покладемо $u_1=(D,C)\in U_1=R^{n\times n\times\ell}\times R^{\ell\times n}$, де $D=(D_1,...,D_\ell)\in R^{n\times n\times\ell}$, $C=\left[c_{ij}\right]\in R^{\ell\times n}$. Якщо $\forall i\in N_\ell:\ g_i(x)=\left\langle x,Q_ix\right\rangle+\left\langle p_i,x\right\rangle+h_i$, $p_i\in R^n$, $h_i\in R$, $Q_i\in R^{n\times n}$ — симетрична невід'ємно визначена матриця, $i\in N_m$, то покладемо $u_2=(Q,p,h)\in U_2=R^{n\times n\times m}\times R^{m\times n}\times R^m$, де $Q=(Q_1,...,Q_m)$, $p=(p_1,...,p_m)\in R^{m\times n}$, $h=(h_1,...,h_m)\in R^m$.

Згідно [3–6] наведемо означення п'яти типів стійкості векторної задачі $Z_P(F,X)$, позначивши $F_{u_1(\delta)}$ і $X_{u_2(\delta)}$ відповідно векторний критерій і допустиму область задачі при збуреннях вхідних даних $u(\delta)=(u_1(\delta),u_2(\delta))\in O_\delta(u)$.

Задача $Z_P(F,X)$ T_1-стійка, якщо $\exists\,\delta>0$, таке, що $\forall\,(u_1(\delta),u_2(\delta))\in O_\delta(u)$ справедливе співвідношення

$$P(F,X)\bigcap P\left(F_{u_1(\delta)},X_{u_2(\delta)}\right)\neq\varnothing .$$

Задача $Z_P(F,X)$ T_2-стійка, якщо $\exists\delta>0$ і $\exists x\in P(F,X)$, такі, що $\forall\,(u_1(\delta),u_2(\delta))\in O_\delta(u)$ виконується належність $x\in P\left(F_{u_1(\delta)},X_{u_2(\delta)}\right)$.

Задача $Z_P(F,X)$ T_3-стійка, якщо $\exists\,\delta>0$, таке, що $\forall\,(u_1(\delta),u_2(\delta))\in O_\delta(u)$ виконується включення

$$P\left(F_{u_1(\delta)},X_{u_2(\delta)}\right)\subset P(F,X) .$$

Задача $Z_P(F,X)$ T_4-стійка, якщо $\exists\delta>0$, таке, що $\forall\,(u_1(\delta),u_2(\delta))\in O_\delta(u)$ виконується включення

$$P(F,X)\subset P\left(F_{u_1(\delta)},X_{u_2(\delta)}\right).$$

Задача $Z_P(F,X)$ T_5-стійка, якщо $\exists\delta>0$, таке, що $\forall\,(u_1(\delta),u_2(\delta))\in O_\delta(u)$ справедливе співвідношення

$$P(F,X)=P\left(F_{u_1(\delta)},X_{u_2(\delta)}\right).$$

Отримані результати стосуються стійкості щодо збурень всіх вхідних даних задачі, так і щодо збурень вхідних даних, що представляють її векторний критерій або обмеження. Виходячи з теореми 1, приходимо до низки тверджень.

Твердження 1. Якщо існує точка $y\in FrG\bigcap Z^n$, для якої виконується умова (5), то задача $Z_P(F,X)$ T_2-стійка за векторним критерієм.

Твердження 2. Якщо існує точка $y\in FrG\bigcap Z^n$, яка задовольняє умові (4) і не є строго ефективним розв'язком задачі $Z_P(F,X)$, то ця задача не є T_4- і T_5-стійкою.

Твердження 3. Якщо існує точка $y\in FrG\bigcap Z^n$, яка задовольняє умові (3) і не є Парето-оптимальним розв'язком задачі $Z_P(F,X)$, то ця задача не є T_3- і T_5-стійкою.

Встановлено топологічні властивості ряду підмножин простору вхідних даних задачі $Z(F,X)$, при яких зберігається оптимальність її розв'язків.

Теорема 2. Для будь-якого розв'язку $x\in Sm(F_{u_1},X)$ підмножина $U^1_{Sm}(x)=\left\{u_1\in U_1\,\middle|\,x\in Sm(F_{u_1},X)\right\}$ простору U_1 вхідних даних задачі $Z_P(F,X)$ є відкритим конусом.

Теорема 3. Для будь-якого розв'язку $x \in S\ell(F_{u_1}, X)$ підмножина $U^1_{S\ell}(x) = \left\{u_1 \in U_1 \,\middle|\, x \in S\ell(F_{u_1}, X)\right\}$ простору U_1 початкових даних задачі — замкнений конус.

Теорема 4. Для будь-якого розв'язку $x \in \operatorname{int} X_{u_2}$ множини

$$U^2_{Sm}(x) = \left\{u_2 \in U_2 \,\middle|\, x \in Sm\left(F, X_{u_2}\right)\right\},$$

$$U^2_{Sl}(x) = \left\{u_2 \in U_2 \,\middle|\, x \in S\ell\left(F, X_{u_2}\right)\right\},$$

$$U^2_{P}(x) = \left\{u_2 \in U_2 \,\middle|\, x \in P\left(F, X_{u_2}\right)\right\},$$

$$U_{Sm}(x) = \left\{u = (u_1, u_2) \in U \,\middle|\, x \in Sm\left(F_{u_1}, X_{u_2}\right)\right\}$$

— відкриті конуси.

Висновки. Встановлено умови оптимальності різних видів розв'язків векторної задачі дискретної оптимізації на допустимій множині, що описується псевдоопуклими функціями обмежень, отримано достатні умови п'яти типів стійкості зазначеної задачі. Встановлено топологічні властивості підмножин простору вхідних даних задачі, на яких зберігається оптимальність її розв'язків.

Список використаних джерел:

1. Сергиенко И. В., Козерацкая Л. Н., Лебедева Т. Т. Исследование устойчивости и параметрический анализ дискретных оптимизационных задач. Киев: Наук. думка, 1995. 170 с.
2. Семенова Н. В. Умови ефективності та стійкості розв'язків у векторних задачах дискретної оптимізації. *Теорія оптимальних рішень*. 2015. С. 160–164.
3. Подиновский В. В., Ногин В. Д. Парето-оптимальные решения многокритериальных задач. М.: Наука, 1982. 256 с.
4. Лебєдєва Т. Т., Семенова Н. В., Сергієнко Т. І. Умови оптимальності та розв'язуваності в задачах лінійної векторної оптимізації з опуклою допустимою множиною. Доповіді НАН України. 2003. № 10. С. 80–85
5. Лебедева Т. Т., Семенова Н. В., Сергиенко Т. И. Устойчивость векторных задач целочисленной оптимизации: взаимосвязь с устойчивостью множеств оптимальных и неоптимальных решений. *Кибернетика и системный анализ*. 2005. № 4. С. 90–100.
6. Лебедева Т. Т., Семенова Н. В., Сергиенко Т. И. Качественные характеристики устойчивости векторных задач дискретной оптимизации с различными принципами оптимальности. *Кибернетика и системный анализ*. 2014. Т. 50, № 2. С. 75–82.

The conditions of optimality of different types of solutions of vector problem of discrete optimization on a feasible set which the is described of psevdo-convex functions of restrictions are set, the sufficient conditions of five types of stability of the noted problem are got. Topological properties of of subsets of space of input data problems which the optimality of its solutions is saved on, are set.

Key words: *discrete optimization, vector problem, stability, well-posedness.*

Одержано 05.03.2017

УДК 518.25

Л. М. Семчишин, канд. фіз.-мат. наук, доцент

Тернопільський національний економічний університет, м. Тернопіль

ВИКОРИСТАННЯ МЕТОДУ ВІДСІЧЕНИХ СИСТЕМ ЛІНІЙНИХ АЛГЕБРАЇЧНИХ РІВНЯНЬ В СЕРЕДОВИЩІ MATLAB

Запропоновано новий підхід до розв'язання методу відсічених систем. Показано рекурентні співвідношення для розв'язання числових систем лінійних алгебраїчних рівнянь. Охарактеризована система лінійних алгебраїчних рівнянь з числовими елементами. Проведено порівняльну характеристику СЛАР з числовими елементами та описано тестування процедур лінійної алгебри в середовищі MatLab.

Ключові слова: *відсічені системи, системи лінійних алгебраїчних рівнянь з числовими елементами, процедури лінійної алгебри.*

Вступ. Розв'язування систем лінійних алгебраїчних рівнянь (СЛАР) завжди є одним із актуальних задач обчислювальної математики. Обчислювальна математика вивчає чисельні методи розв'язування різних математичних задач, тобто методи, які ґрунтуються на побудові скінченної послідовності дій над скінченною множиною чисел. За умови використання таких методів розв'язок математичної задачі отримується у вигляді числового результату. Досліджуючи ті чи інші процеси або явища, проектуючи зразки нової техніки з використанням математичних методів і ЕОМ, спочатку складають математичну модель досліджуваного об'єкта. Тоді побудовану математичну модель перетворюють до такого вигляду, щоб розв'язок можна було знайти (звичайно з певною похибкою) у вигляді числового результату за допомогою арифметичних і логічних операцій. Таке перетворення виконують, застосовуючи числові методи.

Постановка проблеми. При розв'язанні широкого кола прикладних задач більшість сучасних вчених, інженерів і техніків, як правило, використовують пакети комп'ютерної алгебри. Розв'язання математичних задач з допомогою системи MatLab заслуговує особливої уваги. Зорієнтована на роботу з реальними даними, ця система виконує всі обчислення в арифметиці з плаваючою комою на відміну від конкуруючих систем комп’ютерної алгебри REDUCE, MACSYMA, DERIVE, Maple, Mathematica, Theorist, в яких переважає цілочисельне представлення і символьна обробка даних.

Система MatLab — відкрите середовище, яке досить динамічно розвивається зусиллями сотень і тисяч дослідників, адже це одночасно і операційна оболонка і досить гнучка мова програмування. Однією з найбільш сильних сторін є те, що на мові MatLab можуть бути написані програми і функції для багатократного використання.

Аналіз останніх публікацій. Багато відомих вітчизняних і закордонних вчених займалися проблемами розв'язування СЛАР. Серед них: В. Воєводін [1], Є. Тиртишніков [2], Д. Уоткінсон [3] та ін. Однак деякі проблеми не мають однозначного розв'язання і потребують уточнення. У роботі М. Недашковського і О. Ковальчук [4] розглянуто комп'ютерні алгоритми для систем лінійних алгебраїчних рівнянь з λ-матрицями. Особлива увага приділялась методам розв'язування відсічених систем у працях таких вчених як: Г. Цегелик [5], С. Шахно [6] та ін.

Актуальність теми. Застосування методу відсічених систем вимагає використання ефективних чисельних методів.

Слід зауважити, що питання програмної реалізації методу відсічених систем і процедури лінійної алгебри розглядалися у працях [7, с. 169–181]. Однак, у роботі М. Недашковського і О. Ковальчук [4] розглянуто комп'ютерні алгоритми для систем лінійних алгебраїчних рівнянь в середовищі MatLab.

Мета роботи. Метою цієї роботи є дослідження якості наявного програмного забезпечення MatLab у розділі лінійної алгебри і пропозиції по його модернізації. З цією метою проведено цикл числових експериментів, в яких використано програми з арсеналу MatLab і програми написані мовою цієї системи для методу відсічених систем [7].

Теоретичну та методологічну основу дослідження складають методи оптимізації, економіко-математичне моделювання.

Основна частина. Проаналізуємо особливості застосування методу відсічених систем у середовищі MatLab. Для тестування набору програм розглянемо системи рівнянь запропоновані в роботах Д. Уоткінсона [3], М. О. Недашковського [4] та інших фахівців-обчислювачів.

Для перевірки наростання похибок заокруглення в методах виключення за рахунок росту проміжних елементів у процесі перетворення матриці Д. Уоткінсона [4] розглянемо систему з наступною матрицею:

$$A_W = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ -1 & 1 & \cdots & 0 & 1 \\ \cdots & \cdots & \cdots & \cdots & 1 \\ -1 & -1 & \cdots & 1 & 1 \\ -1 & -1 & \cdots & -1 & 1 \end{pmatrix} \qquad (1)$$

У методах виключення з вибором ведучого елемента по стовпцях із-за росту елементів у процесі перетворень при подібному заповненні матриці досягається похибка заокруглення порядку $n2^n$. Тут n — порядок системи.

Для спрощення аналізу точності отриманих значень невідомих x_i права при тестуванні підібрана таким чином, щоб точний розв'язок був $x_i = i$ для всіх $i = 1, 2, ..., n$.

Для розв'язання систем лінійних алгебраїчних рівнянь з числовими елементами в середовищі MatLab написана і протестована функція Essemp. Ця функція реалізує другий алгоритм відсічених систем і написана за допомогою об'єктно-орієнтованої макромови MatLab.

Сам алгоритм розв'язання початкової системи з матрицею (1) може бути поданий рекурентними співвідношеннями:

$$\left.\begin{aligned} & b_{i,k} = \frac{a_{i,k} - \sum\limits_{j=1}^{k-1} a_{i,j} x_j^{(k-1)}}{a_{k,k} - \sum\limits_{j=1}^{k-1} a_{k,j} x_j^{(k-1)}} \quad (i = \overline{k+1,n}); \\ & z_k^{(k)} = b_{k+1,k} \ (k = \overline{1,n-1}); \ z_s^{(k)} = b_{k+1,s} - \sum_{i=s+1}^{k} b_{i,s} z_i^{(k)} (s = \overline{k-1,1}) \end{aligned}\right\} \quad (2)$$

та

$$\left.\begin{aligned} & b_{k,i} = \frac{a_{k,i} - \sum\limits_{j=1}^{k-1} a_{j,i} z_j^{(k-1)}}{a_{k,k} - \sum\limits_{j=1}^{k-1} a_{j,k} z_j^{(k-1)}} \quad (i = \overline{k+1,n}); \\ & x_k^{(k)} = b_{k+1,k} \quad (k = \overline{1,n-1}); \ \ x_s^{(k)} = b_{s,k+1} - \sum_{i=s+1}^{k} b_{s,i} x_i^{(k)} \quad (s = \overline{k-1,1}) \end{aligned}\right\} \quad (3)$$

Слід зауважити, що коли дана система лінійних алгебраїчних рівнянь має симетричну матрицю, тобто $A = A^T$, то $a_{i,j} = a_{j,i}$ для всіх i та j. Із врахуванням цієї обставини обчислювальна схема може бути значно спрощена і реалізована сукупністю рекурентних співвідношень:

$$\left.\begin{aligned} & b_{i,k} = \frac{a_{i,k} - \sum\limits_{j=1}^{k-1} a_{i,j} x_j^{(k-1)}}{a_{k,k} - \sum\limits_{j=1}^{k-1} a_{j,k} x_j^{(k-1)}} \quad (i = \overline{k+1,n}); \\ & x_k^{(k)} = b_{k+1,k} \ (k = \overline{1,n-1}) \ ; \ x_s^{(k)} = b_{k+1,s} - \sum_{i=s+1}^{k} b_{i,s} x_i^{(k)} \ (s = \overline{k-1,1}) \end{aligned}\right\} \quad (4)$$

Утворена таким чином система розв'язувалася за допомогою функції ESSEMP, а також стандартними методами, включеними до складу пакета MatLab 2007b. Подамо текст цієї невеликої програми:

```
unction [] =MatLab_Wilkinson_Test( Dimension )
%-------------------------------------------
% процедура для тестування методів лінійної алгебри пакету MatLab
% на ріст похибки в проміжних обчисленнях за допомогою тестової
% матриці Уілкінсона
%-------------------------------------------
% Ввід початкових даних тестової системи
clc
N=0;
while N<=36
N=N+12
N1 =N+1;
Np=1;
for i=1 : N
   Sum=0;
   for j=1 : N
         if (i<j) A(i,j)=0.0; end
         if (i>j) A(i,j)=-1.0; end
         A(i,i)=1.0;
         A(i,N)=1.0;
         Sum=Sum+A(i,j)*j;
   end
   B(i)=Sum;
end
X=B'\A
end
end
```

Таким чином, запропоновані алгоритми для даної тестової системи середньої розмірності мають суттєві переваги в порівнянні із стандартними функціями пакета MatLab.

Висновки. У статті розглянуто новий підхід до розв'язування методу відсічених систем. Подано алгоритм розв'язання системи рекурентними співвідношеннями і програму для тестування.

Запропонований алгоритм може ефективно використовуватися в системах комп'ютерної алгебри та для аналітично-числового розв'язування інженерних задач та прикладних задач механіки. На основі запропонованого підходу в пакеті MatLab були проведені числові експерименти для СЛАР з числовими елементами та описано тестування процедур лінійної алгебри в середовищі MatLab.

Список використаних джерел:

1. Воеводин В. В. Линейная алгебра. С.-Петербург.: Лань, 2008. 416 с.
2. Тыртышников Е. Е. Матричный анализ и линейная алгебра. М.: Физматлит, 2007. 480 с.
3. Уоткинс Д. Основы матричных вычислений. М.: Бином. Лаборатория знаний, 2006. 664 с.
4. Недашковський М. О., Ковальчук О. Я. Обчислення з λ-матрицями. К.: Наукова думка, 2007. 294 с.
5. Цегелик Г. Г. Чисельні методи. Л.: Видавничий центр ЛНУ імені Івана Франка, 2004. 408 с.
6. Шахно С. М. Чисельні методи лінійної алгебри. Л.: Видавничий центр ЛНУ імені Івана Франка, 2007. 245 с.
7. Семчишин Л. М. Програмна реалізація методу відсічених систем і процедури лінійної алгебри в середовищі MATLAB в кн.: *Вісник Тернопільського національного технічного університету.* Тернопіль, 2012. №1 (65). С. 169–181.

New approach to the severance system method solution is suggested in the work. Showing recurrence relations for solving numerical systems of linear algebraic equations. The system of linear algebraic equation with numerical elements is characterized. Comparative characteristic of SLAR with numerical elements is conducted and the linear algebraic testing procedure in the MatLab environment is described.

Key words: *severance system, system of linear algebraic equotins with numerical elements, linear algebraic procedure.*

Одержано 15.02.2017

УДК 519.9

І. В. Сергієнко, д-р. фіз.-мат. наук, професор, академік НАН України,
В. К. Задірака, д-р. фіз.-мат. наук, професор, академік НАН України,
І. В. Швідченко, канд. фіз.-мат. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

НАУКОВА ТЕМАТИКА МІЖНАРОДНИХ МАТЕМАТИЧНИХ ФОРУМІВ З ПИТАНЬ ОПТИМІЗАЦІЇ ОБЧИСЛЕНЬ

Розглядаються основні етапи розвитку тематики з питань оптимізації обчислень.

Ключові слова: *теорія похибок, оптимальні алгоритми, інформаційні оператори, апріорна інформація, оптимізація обчислень.*

Вступ. На сьогоднішній день проведено сорок три міжнародних наукових форуми з питань оптимізації обчислень. XLIV-й присвячений 60-річчю від дня заснування Інституту кібернетики імені В. М. Глушкова НАН України. Наукові форуми згуртовують навколо себе фахівців з обчислювальної і прикладної математики.

В Україні більше немає таких наукових колективів, які б провели стільки ж наукових математичних форумів. Це говорить про те, що напрям тематики був визначений вдало і в подальшому завжди відповідав основним актуальним проблемам в обчислювальній математиці.

Основні напрямки розвитку теорії обчислень.

1. Аналіз точності та ефективності обчислювальних алгоритмів.

Перший науковий форум відбувся в 1969 році. Ситуація на той час в обчислювальній математиці була така: кількість методів розв'язання типових задач стрімко зростала, а критеріїв їх порівняння не було. Тому зусилля фахівців з обчислювальної математики Інституту кібернетики направлені на розвиток теорії похибок обчислень. Зокрема, дуже важливо врахувати і оцінити всі джерела похибок, які реально супроводжують обчислювальний процес. Це принципово, так як при цьому з'являється можливість дати гарантію якості наближеного розв'язку задачі. Запропоновано загальні схеми оцінок повної похибки обчислювального алгоритму, яка складається з похибок: неусувної, методу та заокруглення [1].

Значна увага приділялась якості оцінок похибок та методам їх отримання [2].

Важлива проблема на даному етапі розвитку обчислювальної математики та техніки — це проблема розробки і дослідження методів організації обчислювальних робіт на ЕОМ, а також оцінки ефективності складних систем, оскільки створювались потужні обчислювальні центри з ЕОМ різної продуктивності. Для ефективного використання можливостей таких центрів потрібно було належним чином організувати і оцінити їх роботу [3].

2. Виявлення та уточнення апріорної інформації про задачу.

Апріорна інформація про задачу (гладкість вхідної інформації або розв'язку задачі, константи, які обмежують відповідні похідні, опуклість функцій, кількість точок перегину тощо) входить до алгоритму розв'язання задачі, а також в оцінки якості наближеного розв'язку. Вона використовується також для «занурення» задачі у більш вузький клас для покращення потенційної спроможності чисельного методу.

Якщо апріорна інформація неточна, то краще нею не користуватись, тому що на основі такої інформації можна отримати хибне уявлення про якість наближеного розв'язку задачі. Іншими словами, задача може бути розв'язана з потрібною якістю, але оцінки цього не покажуть. Щоб цього уникнути доцільно використовувати алгоритми виявлення та уточнення апріорної інформації про задачу [4, 5]. При цьому погіршиться оцінка складності алгоритму, але покращиться оцінка точності. Якщо ефект від зменшення кількості операцій неважко підрахувати, то ефект від покращення точності — важко. Останній може бути досить великий: дозволити уникнути різного роду катастроф; перевести задачу із розряду нерозв'язних до розряду розв'язних тощо. Отже, виявлення та уточнення апріорної інформації про задачу є резервом оптимізації обчислень, який може бути використаний у відповідних комп'ютерних технологіях розв'язання задач обчислювальної та прикладної математики.

3. Вибір інформаційного оператора.

Найчастіше використовується сітковий інформаційний оператор, тобто коли функція відома у вузлах сітки. Для задач апроксимації, чисельного інтегрування, математичної фізики, мінімізації функцій такий інформаційний оператор буде найкращим за точністю розв'язування відповідного класу задач. Але для інших класів задач ситуація інакша. Для розв'язування задачі Коші для системи диференціальних рівнянь, задач інерційної навігації найкращим буде інформаційний оператор, який задає середнє значення функції на елементарному відрізку; для розв'язування інтегральних рівнянь Фредгольма II роду найкращим буде оператор, що задає перші коефіцієнти розкладу функції в ряд Фур'є; для сканування морського дна найкращим буде інформаційний оператор, який задає інформацію на лініях, а для задач комп'ютерної томографії — на площинах.

Тобто для кожного класу задач існує найкращий інформаційний оператор у тому сенсі, що при його використанні похибка наближеного розв'язку задачі буде меншою. Вдалий підбір інформаційного оператора для задачі можна вважати одним з резервів оптимізації обчислень.

4. Оптимальні за точністю та швидкодією алгоритми.

Ця тематика почала розвиватись для типових класів задач обчислювальної математики з 1970 року. З 1972 року вона розглядається і на наших наукових форумах.

Одним з основних критеріїв оптимальності наближеного розв'язку задач може бути вимога його максимальної точності (чи мінімальної похибки) за даними ресурсами, які можна використовувати в процесі розв'язування задачі. В поняття ресурсу входять: кількість і точність вхідних даних задачі, вільна для використання пам'ять комп'ютера, ліміт часу обчислень на даному комп'ютері, наявний запас програмного забезпечення комп'ютера тощо.

Для побудови оптимальних алгоритмів розв'язання тих чи інших класів задач використовуються метод «капелюхів» М. С. Бахвалова та метод граничних функцій, який розроблений в Інституті кібернетики АН УРСР. Перший метод [6] використовується для оцінок знизу оптимальної оцінки [2], другий [2, 7] — для побудови оптимальних оцінок та оптимальних алгоритмів для більш вузьких класів задач (інтерполяційних [2]), які максимально використовують апріорну інформацію про задачу.

Звуження класу задач дозволяє покращити (не збільшити) оптимальну оцінку, в порівнянні з стандартним підходом, але за рахунок погіршення оцінок складності. Це також є резервом оптимізації обчислень.

Оптимізація за швидкодією алгоритмів конче потрібна, наприклад, коли треба забезпечити розв'язування задач у реальному часі, при розв'язуванні задач трансобчислювальної складності та в інших ситуаціях.

В цій проблематиці для конструювання швидких алгоритмів широко використовується: теорія швидких ортогональних перетворень, методи паралельної математики, комп'ютерна арифметика багаторозрядних чисел [8], спеціалізовані обчислювачі (вибір архітектури комп'ютера, що краще узгоджується з обчислювальним алгоритмом розв'язання задач даного класу).

5. Моделі обчислень.

Більшість оцінок складності обчислювальних алгоритмів при розв'язуванні певних класів задач отримано для послідовної та паралельної моделей обчислень. Відомо, що оцінка складності залежить від використовуваної моделі обчислень. Є такі приклади, коли оцінки суттєво відрізняються в різних моделях обчислень, а є випадки, коли оцінки не відрізняються за порядком.

Наприклад, для розв'язання задачі факторизації чисел оцінка складності в послідовній моделі обчислень експоненційна (від довжини числа), а у квантовій моделі обчислень — поліноміальна. Хоча інші задачі (наприклад, пакування ранця, розв'язання нелінійних булевих рівнянь) як були «складними» для послідовної моделі обчислень, так і лишились «складними» для квантової моделі обчислень.

Тобто вибір моделі обчислень може слугувати резервом оптимізації обчислень.

6. Комп'ютерні технології розв'язання задач прикладної та обчислювальної математики з заданими значеннями характеристик якості за точністю та швидкодією.

Викладені вище резерви оптимізації обчислень, а також теорія похибок обчислень використовуються в сучасних комп'ютерних технологіях знаходження ε-розв'язку задач за заданий комп'ютерний час [9].

Технологія, в залежності від отриманих проміжних результатів, підказує, як, користуючись оцінками похибок обчислень, оптимальними алгоритмами розв'язування задач та використовуючи інші резерви оптимізації обчислень, знайти обчислювальний алгоритм-програму [10], яка зможе або забезпечити на відповідному комп'ютері побудову розв'язку прикладної задачі із заданими обмеженнями на значення характеристик якості, або встановити, що його із вказаними властивостями для розв'язуваної задачі при заданій вхідній інформації на даний час не існує.

Потім, за допомогою розробленого або наявного з необхідними властивостями обчислювального алгоритму-програми обчислюється розв'язок прикладної задачі із заданими значеннями характеристик якості, використовуючи при цьому визначений комп'ютер та програмне забезпечення.

Тематика з розроблення відповідних комп'ютерних технологій почала розглядатись на наукових форумах з 2000 року.

Висновки. Викладені основні віхи розвитку тематики наукових форумів з питань оптимізації обчислень.

Актуальними основними напрямками досліджень на сьогодні є:

- подальший розвиток теорії похибок;
- розвиток загальної теорії оптимальних алгоритмів;
- розробка паралельних алгоритмів розв'язання типових задач обчислювальної математики;
- врахування неточності задання вхідної інформації;
- використання різних моделей обчислень;
- розроблення комп'ютерних технологій знаходження ε-розв'язків задач за заданий процесорний час конкретних типових класів задач прикладної та обчислювальної математики;
- використання хмарних технологій, особливо при розв'язанні задач трансобчислювальної складності;
- приклади розв'язання важливих прикладних задач.

Оргкомітет сподівається, що вказана тематика зацікавить молодих вчених, аспірантів та студентів і вони приєднаються до числа учасників наукових форумів з питань оптимізації обчислень.

Список використаних джерел:

1. Иванов В. В. Вопросы точности и эффективности вычислительных алгоритмов. Киев: Ин-т кибернетики АН УССР, 1969. 135 с.
2. Задирака В. К. Теория вычисления преобразования Фурье. К.: Наукова думка, 1983. 216 с.
3. Сергиенко И. В. Методы организации вычислительного процесса на вычислительных машинах. Киев: Ин-т кибернетики АН УССР, 1971. 162 с.
4. Березовский А. Н., Кондратенко О. С. О выявлении и уточнении априорной информации. *УСиМ*. 1997. № 6. С. 17–22.
5. Сергієнко І. В., Задірака В. К., Литвин О. М. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. К.: Наукова думка, 2012. 400 с.
6. Бахвалов Н. С. Численные методы. М.: Наука, 1973. 632 с.

7. Иванов В. В. Методы вычислений на ЭВМ (справочное пособие). Киев: Наукова думка, 1986. 584 с.
8. Задірака В. К., Олексюк О. С. Комп'ютерна арифметика багаторозрядних чисел: наук. вид. К., 2003. 264 с.
9. Сергиенко И. В., Задирака В. К., Бабич М. Д., Березовский А. И., Бесараб П. Н., Людвиченко В. А. Компьютерные технологии решения задач прикладной и вычислительной математики с заданными значениями характеристик качества. *Кибернетика и системный анализ*. 2006. № 5. С. 33–41.
10. Бабич М. Д., Задирака В. К., Сергиенко И. В. Вычислительный эксперимент в проблеме оптимизации вычислений. *Кибернетика и системный анализ*. 1999. Ч.1. № 1. С. 51–63; Ч.2. № 2. С. 59–79.

The main stages of topics development on issues of calculations optimization are considered.

Key words: *error theory, optimal algorithms, information operations, information given a priory, calculations optimization.*

Одержано 28.02.2017

УДК 519.6

В. А. Сидорук, канд. фіз.-мат. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

ОДНОВУЗЛОВИЙ ГІБРИДНИЙ АЛГОРИТМ ФАКТОРИЗАЦІЇ РОЗРІДЖЕНИХ МАТРИЦЬ

Розглядається гібридний алгоритм розв'язування систем лінійних алгебраїчних рівнянь з розрідженими симетричними додатно визначеними матрицями на комп'ютерах з графічними прискорювачами. Подано результати апробації алгоритму на багатоядерному комп'ютері з графічними прискорювачами Інпарком.

Ключові слова: *плитковий алгоритм, гібридна архітектура, CUDA, Openmp.*

Вступ. При чисельному розв'язанні задач у багатьох випадках доводиться розв'язувати задачу (або декілька підзадач) лінійної алгебри — систему лінійних алгебраїчних рівнянь (СЛАР). Наприклад, задачі лінійної алгебри виникають при дискретизації крайових задач проекційно-різницевим методом (скінченних різниць, скінченних елементів).

Важливою особливістю задач лінійної алгебри, які виникають при дискретизації є невелика кількість ненульових елементів матриці, тобто матриці є розрідженими [1]. Кількість ненульових елементів у таких матрицях складає kn, де $k << n$, а n — порядок матриці. Структура розрідженої матриці визначається нумерацією невідомих задачі і часто буває стрічковою, профільною, блочно-діагональною з обрамленням, або просто довільної розрідженої структури. Ще однією важливою особливістю СЛАР з розрідженими матрицями є їх великий порядок — до десятків мільйонів.

У роботі розглядаються додатно-визначені розріджені матриці нерегулярної структури.

Постановка задачі. Розглянемо задачу

$$Ax = b \tag{1}$$

з симетричною додатно-визначеною розрідженою матрицею порядка n.

Однією з передумов розв'язання задачі (1) на комп'ютерах гібридної архітектури з багатоядерними процесорами (CPU) і графічними прискорювачами (GPU) є приведення матриці до такого виду, який дозволяє працювати з більш щільними групами ненульових елементів. Перетворення матриці зумовлене особливостями роботи GPU, які дозволяють отримати найкращі показники продуктивності при обробці великих щільних масивів даних.

Нині існує велика кількість алгоритмів перевпорядкування елементів матриць: метод мінімальної степені, метод вкладених перерізів, метод паралельних перерізів і т. д. Кожен з цих алгоритмів дозволяє привести довільну розріджену структуру до більш регулярного вигляду. Найбільш зручну для паралельної обробки структуру матриці отримується після застосування до матриці методу вкладених, або паралельних, перерізів.

$$\tilde{A} = P^T AP = \begin{pmatrix} A_{11} & 0 & 0 & A_{1p} \\ 0 & A_{22} & 0 & A_{2p} \\ 0 & 0 & \ddots & \vdots \\ A_{p1} & A_{p2} & \dots & A_{pp} \end{pmatrix},$$

де P — матриця перестановок, p — кількість діагональних блоків у матриці, блоки A_{pp}, A_{ip}, A_{pi}, A_{ii} $i = \overline{1, p-1}$ зберігають розріджену структуру.

Таким чином, задача розв'язання (1) зводиться до розв'язування еквівалентної системи

$$\tilde{A}\tilde{x} = \tilde{b}, \tag{2}$$

де $\tilde{x} = P^T x$, $\tilde{b} = P^T b$.

Найбільш ефективним прямим методом розв'язання (2) є метод Холецького [1–3]. В статті буде висвітлено гібридний алгоритм який відповідає саме етапу факторизації матриці.

Гібридний алгоритм. Розіб'ємо матрицю A на блоки розмірністю $s \times s$. Далі для факторизації блочно-діагональної матриці застосуємо алгоритм запропонований в [4] для щільних матриць.

Для факторизації матриці на k -му кроці використаємо наступне співвідношення:

$$A^k = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \begin{pmatrix} L_{11} & 0 \\ L_{21} & L_{22} \end{pmatrix} \begin{pmatrix} L_{11}^T & L_{21}^T \\ 0 & L_{22}^T \end{pmatrix}, \tag{3}$$

де розмірності блоків A_{11} — $s \times s$, A_{12} — $(n-ks)s$, A_{22} – $(n-ks)(n-ks)$, блоки A_{12} та A_{22} враховують структуру діагональних блоків та блоків обрамлення.

Звідси отримаємо алгоритм, за яким проводиться розвинення на k кроці:

$$A_{11} = L_{11} * L_{11}^T; \tag{4}$$

$$L_{21} = A_{21} * \left(L_{11}^T\right)^{-1}; \tag{5}$$

$$\tilde{A}_{22} = A_{22} - L_{21} * L_{21}^T. \tag{6}$$

Зазначимо, що реалізація (4)–(6) на кожному кроці модифікує тільки блоки D_{ii} , C_{pi} , $i = \overline{1, p-1}$, D_{pp} .

Нехай для розв’язування задачі на комп’ютері гібридної архітектури маємо CPU з p процесорними ядрами і 1 GPU. Для роботи алгоритму на k кроці реалізовується наступна декомпозиція даних: у пам’яті CPU і GPU зберігається плитка A_{11} ; у пам’яті GPU зберігаються плитки необхідні для модифікації підматриці A_{22} . На рис. 1. показано блочний розподіл даних на k-му кроці факторизації блочно-діагональної матриці з обрамленням, враховуючи вище запропоновану декомпозицію.

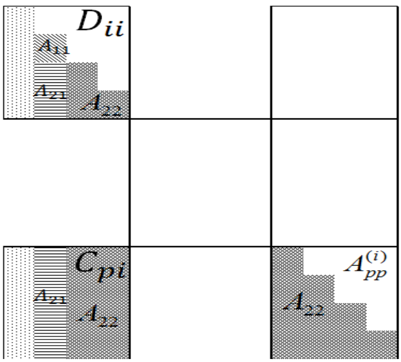


Рис. 1. *Декомпозиція даних в GPU на k-му кроці факторизації*

Враховуючи декомпозицію даних, приведену вище, плитковий гібридний алгоритм факторизації записується у наступній формі:

1) над всіма діагональними блоками крім D_{pp} та відповідними блоками обрамлення послідовно виконуються такі операції:
   - на CPU факторизуємо A_{11} $A_{11} = L_{11} * L_{11}^T$;
   - на GPU паралельно в різних потоках модифікуємо стовпчик блоків L_{21}:
   $$L_{21} = A_{21}\left(L_{11}^T\right)^{-1};$$
   - у GPU незалежно в кількох потоках модифікуємо блоки матриці A22 за формулою:
   $$\tilde{A}_{22} = A_{22} - L_{21}L_{21}^T;$$
2) факторизуємо блок $A_{pp}^{(i)}$, тим самим завершуючи процес факторизації матриці A.

Оцінка прискорення. Для оцінки якості гібридних алгоритмів будемо використовувати коефіцієнт прискорення S_p що обчислюється за формулою

$$S_p = T_1 / T_p,$$

де T_1 — час розв'язування задачі на гібридному комп'ютері з одним CPU та одним GPU, T_p — час розв'язування тієї ж задачі на гібридному комп'ютері з використанням один CPU і один GPU в паралельному режимі.

Введемо наступні позначення: N_1 — кількість операцій, виконуваних алгоритмом на гібридному комп'ютері з використанням 1 CPU і 1 GPU; N_p – кількість операцій, виконуваних алгоритмом на гібридному комп'ютері з використанням один CPU і один GPU з використанням кількох паралельних ниток; t_g — середній час виконання однієї арифметичної операції на GPU; t_{opg} — час обміну між одним CPU та GPU.

Обчислимо кількість операцій виконуваних алгоритмом факторизації. Введемо наступні позначення $m = \dfrac{n}{p}$ — порядок діагонального блоку матриці A та $l = \dfrac{m}{s}$ — кількість плиток у стовпці діагонально блоку. При підрахунку кількості операцій будемо вважати, що матриця A має діагональні блоки однакових порядків.

Оскільки в алгоритмі на парі CPU та GPU $p-1$ раз етапи (4)-(6) і один раз факторизується останній діагональний блок, то кількість арифметичних операцій можна обчислити за наступною формулою:

$$N_1 \approx (p-1)\alpha + \beta \;.$$

Для обчислення кількості операції необхідних для факторизації останнього діагонального блоку будемо вважати, що останній діагональний блок — щільна матриця. Тоді $\beta = \frac{m^3}{3}$.

Розглянемо етапи (4)–(6). Тут найбільше арифметичних операцій припадає на виконання етапу (6). Обчислимо їх кількість.

На k-му кроці факторизації, як видно з рис. 1., нам потрібно модифікувати $\left\lceil \frac{(m-ks)^2}{2} \right\rceil$ елементів з D_{ii}, $(m-ks)m$ — з C_{pi} та $\left\lceil \frac{m^2}{2} \right\rceil$ — з $A_{pp}^{(i)}$.

Тобто $\alpha \approx 2s\left(\sum_1^l \frac{(m-ks)^2}{2} + \sum_1^l (m-ks)m + \sum_1^l \frac{m^2}{2} \right)$.

Розкриємо дужки та розпишемо суми

$$\alpha \approx \left(s\sum_1^l \left(m^2 - 2mks + 2k^2 s^2 \right) + 2s\sum_1^l (m-ks)m + s\sum_1^l m^2 \right).$$

Після проведення спрощень і підстановки значень отримаємо наступну формулу для обчислення: $\alpha \approx \frac{8m^3}{3}$.

Звідси $N_1 \approx (p-1)\frac{8m^3}{3} + \frac{m^3}{3}$.

Кількість операцій виконуваних при реалізації паралельного варіанта гібридного алгоритму обчислюється за формулою

$$N_p \approx N_1 / th \,,$$

де th — кількість незалежних потоків.

Прискорення гібридного алгоритму LL^T — розвинення розрідженої блочно-діагональної матриці з обрамленням A, становить

$$S_p \approx \frac{thN_1 t_g}{N_1 t_g + th\mathrm{T}} \,,$$

де $\mathrm{T} = (p-1)\left(4ms + m^2\right)t_g$.

Результати чисельних експериментів. Розрахунки проводились на вузлах кластера Інпарком-G [5], які мають наступні характеристики:

- процесори: 2 Xeon 5606 (8 ядер) з частотою 2.13 ГГц;

- графічні прискорювачі: 2 Tesla M2090;
- обсяг оперативної пам’яті: 24 Гб;
- комунікаційне середовище: InfiniBand 40 Гбіт/с (з підтримкою GPUDirect), Gigabit Ethernet.

Чисельні експерименти проводились на розріджених матрицях, що наведені в таблиці. Також в таблиці наведені такі характеристики матриці як порядок матриці, кількість ненульових елементів.

Для програмної реалізації етапів (5), (6) використовувались функції бібліотеки CUBLAS та функції бібліотеки Openmp. Для плиток з порядками 64-1024 використовувались виклики в циклі функції cublasDtrsm та cublasDgemm, виконання кожної з функцій проходило в окремому потоці cudaStream. Нитки Openmp відповідають потокам cudaStream.

Копіювання даних і обчислення проводились в асинхронному режимі.

Таблиця

Набір тестових матриць з Флоридської колекції розріджених матриць

Назва	**Проблемна область**	**Порядок**	**Кількість ненульових елементів**
G3_circuit	circuit simulation problem	1 585 478	7 660 826
G2_circuit	circuit simulation problem	150 102	726 624
parabolic_fem	computational fluid dynamics problem	525 825	3 674 625
apache2	structural problem	715 176	4 817 870

На рис. 2. показано графік залежності продуктивності від використовуваної кількості ниток Openmp на прикладі виконання факторизації матриці G2_circuit на гібридній архітектурі 1CPU та 1 GPU з розміром плитки 128.

Висновки. Алгоритм добре враховує профільну, або розріджену структуру діагональних блоків і матриці в цілому. Можна регулювати розмірність блоку з яким проводяться обчислення на кожному кроці алгоритму, за рахунок цього може досягатись ефект кешизації обчислень, коли блоки поміщаються в швидкій пам’яті GPU. Також така блочна структура дозволяє працювати з нерозривними масивами даних на GPU, що зменшує кількість індексних операцій і перевірок які на графічному прискорювачі є досить затратними. Також регулювання кількості використовуваних потоків дозволяє підвищити ефективність алгоритму.

Рис. 2. *Продуктивність алгоритму*

Список використаних джерел:

1. Джордж А., Лю Дж. Численное решение больших разреженных систем уравнений. М.: Мир, 1984. 334 с.
2. Химич А. Н., Попов А. В., Полянко В. В. Алгоритмы параллельных вычислений для задач линейной алгебры с матрицами нерегулярной структуры. *Кибернетика и системный анализ*. 2011. 47, № 6. С. 159–174.
3. Хіміч О. М., Сидорук В. А. Гібридний алгоритм розв'язування лінійних систем з розрідженими матрицями на основі блочного LL^T методу. *Комп’ютерна математика*. 2015. Вип. 1. С. 67–74.
4. Buttari Alfredo, Langou Julien, Kurzak Jakub, and Dongarra Jack. A Class of Parallel Tiled Linear Algebra Algorithms for Multicore Architectures. *Parallel Computing*. 2009. Vol. 35, Is. 1. P. 38–53.
5. Химич А. Н., Молчанов И. Н., Мова В. И. и др. Численное программное обеспечение MIMD-компьютера Инпарком. Киев: Наук. думка, 2007. 222 с.

A hybrid algorithm for solving systems of linear algebraic equations with sparse symmetric positive definite matrix on computers with GPU is considered. The results of testing of the algorithm on multicore computer Inparcom are presented.

Key words: *tiled algorithm, hybrid architecture, CUDA, Openmp.*

Одержано 02.03.2017

УДК 512.7+512.9, 688.321

Р. В. Скуратовський, викладач

МАУП, Інститут комп'ютерних та інформаційних технологій, м. Київ

ФАКТОРИЗАЦІЯ ЦІЛОГО ЧИСЛА ВИГЛЯДУ $n = pq$

Запропонований нами метод факторизації, на відміну від більшості різновидів методу *GNFS* [1, 2] окрім *kGNFS*, володіє всіма властивостями для успішного застосування паралельних обчислень.

Ключові слова: *факторизація числа, паралельні обчислення.*

Вступ. Добре відома задача факторизації числа до сьогодні не розв'язується досить ефективно. Безпека криптосистеми Рабіна, як і RSA, обумовлена складністю факторизаці великих чисел.

Основні результати. Нехай $n = pq = 2n_1 + 1$ це RSA-модуль, де n_1 — натуральне. Тоді p та q також мають бути непарними, тобто $p = 2k_1 + 1,\ q = 2l_1 + 1$. Запишемо задачу у вигляді рівняння

$$(2k_1 + 1)(2l_1 + 1) = 2n_1 + 1, \qquad (1)$$

яке спростимо до $2k_1l_1 + k_1 + l_1 = n_1$, та яке можна розглядати за $\bmod 2$ тобто $2k_1l_1 + k_1 + l_1 \equiv n_1 \bmod 2$. Для пошуку розв'язків цього рівняння застосуємо метод конгруентного перебору. Тобто, на кожному кроці ми матимемо ланцюжок гіпотез $H_1, H_2, ..., H_n$, у якому кожна гіпотеза залежить від попередніх. Якщо гіпотеза H_n, яка іде в ланцюжку останньою, виявиться неправильною (за припущення правильності всіх попередніх гіпотез), ми пропустимо варіант, протилежний H_n, і продовжимо розв'язання. Якщо неправильними виявилися і гіпотеза H_n, і її протилежність, ми робимо висновок про неправильність гіпотези H_{n-1}. У цьому випадку, ми перестаємо розглядати гіпотезу H_n, а останньою в ланцюжку стає H_{n-1}. Тепер ми змінюємо цю гіпотезу на протилежну до неї і продовжимо пошук. На i-ому кроці матимемо рівняння

$$2^i k_il_i + a_ik_i + b_il_i = n_i, \qquad (2)$$

де k_i, l_i — цілі невід'ємні числа, які ми шукаємо, a_i та b_i — натуральні непарні коефіцієнти, а n_i — деяке ціле число. На початку маємо $i = 1, a_1 = b_1 = 1$ та $n_1 = (n-1)/2$.

У випадку, якщо n не просте, для переходу до наступної ітерації ми представляємо шукані числа у вигляді $k_i = 2k_{i+1} + r_i,\ l_i = 2l_{i+1} + s_i$, тобто r_i, s_i це лишки за модулем 2 чисел k_i, l_i, які задовольняють конгруенцію $2^i k_i l_i + a_i k_i + b_i l_i = n_i (\mathrm{mod}\, 2)$. Зрозуміло, що при $i > 1$ вона рівносильна $a_i k_i + b_i l_i = n_i (\mathrm{mod}\, 2)$. Після скорочення на 2 переходимо до рівняння $2^{i+1} k_{i+1} l_{i+1} + (2^i s_i + a_i) k_{i+1} + (2^i r_i + b_i) l_{i+1} = (n_i - a_i r_i - b_i s_i) : 2 – 2^{i-1} r_i s_i$. Якщо n_i — парне, ми маємо перебрати гіпотези $r_i = s_i = 0$ та $r_i = s_i = 1$. Якщо $n_i \equiv 1 (\mathrm{mod}\, 2)$, розглядаємо випадки $r_i = 0, s_i = 1$ та $r_i = 1, s_i = 0$. Кожний з них приводить до рівняння $2^{i+1} k_{i+1} l_{i+1} + a_{i+1} k_{i+1} + b_{i+1} l_{i+1} = = n_{i+1}$, де коефіцієнти на новій ітерації обчислюються за формулами перерахунку

$$\begin{cases} a_{i+1} = 2^i s_i + a_i, \quad b_{i+1} = 2^i r_i + b_i \\ n_{i+1} = \left(n_i - a_i r_i - b_i s_i\right)/2 - 2^{i-1} r_i s_i. \end{cases} \tag{3}$$

Звідси $2^{i+2} k_{i+2} l_{i+2} + a_{i+2} k_{i+2} + b_{i+2} l_{i+2} = n_{i+2}$.

Так діємо до тих пір поки не буде знайдено точний розв'язок рівняння (2), при цьому виконається умова однієї з ознак зупинки.

Лема 1. Коефіцієнти квадратичної форми (2) a_i, b_i задовольняють конгруенцію $a_i \equiv 1 (\mathrm{mod}\, 2),\ b_i \equiv 1 (\mathrm{mod}\, 2)$.

Доведення випливає з формули (3) рекурсивного обчислення a_i, b_i і їхніх ініціальних значень $a_1 = b_1 = 1$, з якої випливає, що їхнє значення є сумою парного і не парного чисел, отже є непарним.

Нехай отримано точний розв'язок рівняння (2).

Лема 2. Розв'язки рівняння (1) однозначно отримуються з розв'язками рівняння (2) шляхом замін $k_i = 2k_{i+1} + r_i$, $l_i = 2l_{i+1} + s_i$.

Доведення. З того, що на кожному кроці при переході від i-го зведеного рівняння вигляду (3) до $i-1$ ми робимо рівносильні перетворення вигляду $k_{i-1} = 2k_i + r_i$, $l_{i-1} = 2l_i + s_i$, які однозначно визначають k_{i-1} і l_{i-1} за відомими k_i, l_i і r_i, s_i, і в кінці нами отримано точний розв'язок рівняння (2), нехай він отриманий на ітерації $i = k$ слідує, що ми однозначно отримуємо розв'язок рівняння (1).

Тепер можемо повернутися до знайдених розв'язків конгруенції $2^{i-1} k_{i-1} l_{i-1} + a_{i-1} k_{i-1} + b_{i-1} l_{i-1} = n_{i-1} (\mathrm{mod}\, 2)$, що виникла на попередній ітерації і отримати цифри $i-2$-го розряду для p і q відповідно. Аналогічно повертаючись до вже знайдених розв'язків попередніх конгруенцій ми отримуємо всі цифри (знаки) чисел $p = 2k_1 + 1$ і $q = 2l_1 + 1$. Оскільки ми робимо еквівалентні перетворення, то ми отримаємо однозначно розв'язок рівняння (1) і тобто однозначний запис чисел p і q.

Оскільки ми робили рівносильні перетворення, то відповідно і навпаки за розв'язком рівняння (1), яким є $p = 2k_1 + 1$, $q = 2l_1 + 1$, однозначно визначається розв'язок рівняння (3). Розв'яками рівняння (1) є числа $p = 2k_1 + 1$, $q = 2l_1 + 1$ які є нетривіальним дільниками числа n, тому лише одна гілка гіпотез дасть розв'язок в натуральних числах рівняння (2). З парності коефіцієнта при $k_i l_i$ маємо наслідок.

Наслідок. Для переходу до наступної ітерації досить розглядати конгруенцію $a_i k_i + b_i l_i = n_i (\bmod 2)$.

Зауваження. Оскільки в RSA використовують сильно прості числа, тобто $p = 2P + 1$ і $q = 2Q + 1$, де $P, Q \in \mathbb{P}$, то в цьому випадку лишки $r_2, l_2 \equiv 1(\bmod 2)$, де $i \geq 1$ в $k_i = 2k_{i+1} + r_i$, $l_i = 2l_{i+1} + s_i$.

Припустимо, що числа p, q мають різну кількість розрядів у двійковому представленні, тоді довжини відповідних їм чисел k, l, що є розв'язками рівняння (2) теж різні і можна застосувати наступну ознаку зупинки. Зауважимо, що **піддерева пошуку** після першої ітерації повністю симетричні бо рівняння $2k_2 l_2 + k_2 + l_2 = n_2$ є симетричним відносно змінних, тому можна обробляти тільки одне. Тому складність обчислень одразу можна поділити на 2.

Ознака зупинки 1. Якщо в процесі ітеративного розв'язання у рівнянні $2^i k_i l_i + a_i k_i + b_i l_i = n_i$ виникла рівність $a_i = n_i$ чи $b_i = n_i$, то знайдено всі знаки обох чисел p і q.

Доведення. Оскільки зазначена умова є рівністю а не конгруенцією, то на цій ітерації нами знайдено точний розв'язок рівняння $2^i k_i l_i + a_i k_i + b_i l_i = n_i$ і ним є $k_i = 1, l_i = 0$, якщо $a_i = n_i$ чи навпаки $k_i = 0, l_i = 1$ при $b_i = n_i$. Звідси і з того, що перетворення $k_{i-1} = 2k_i + r_i$, $l_{i-1} = 2l_i + s_i$ однозначно визначають k_{i-1} і l_{i-1} за відомими k_i, l_i і r_i, s_i, знайдемо цифри $i-1$-го розряду на чисел p і q відповідно. Тепер можемо повернутися до знайдених розв'язків конгруенції $2^{i-1} k_{i-1} l_{i-1} + a_{i-1} k_{i-1} + b_{i-1} l_{i-1} = n_{i-1} (\bmod 2)$, що виникла на попередній ітерації і отримати цифри $i-2$-го розряду для p і q відповідно. Аналогічно повертаючись до вже знайдених розв'язків попередніх конгруенцій ми отримуємо всі цифри (знаки) чисел $p = 2k_1 + 1$ і $q = 2l_1 + 1$. Оскільки ми робимо еквівалентні перетворення, то ми отримаємо однозначно розв'язок рівняння (1) і тобто однозначний запис чисел p і q. Якщо б числа не були розв'язками рівняння $2^i k_i l_i + a_i k_i + b_i l_i = n_i$, то вони не були б і розв’язками (1). Правильно і навпаки: розв’язками рівняння (2) є розв’язки рівняння (1).

Для визначення довжини гілки графа, де ще може бути розв’язок, слід врахувати добре відомі межі величин збалансованих чисел, бо такі використовуються в криптосистемах RSA і Рабіна.

Прості числа p та q, для яких $n = pq$, будемо називати **збалансованими** [1], якщо $4 < \frac{1}{2}\sqrt{n} < p < \sqrt{n} < q < 2\sqrt{n}$. Зрозуміло, що для практичних застосувань використовують лише збалансовані числа $p < q < 2p$. Тому кількість паралельних кроків алгоритму не більше ніж

$$\left[\log_2 2\sqrt{n}\right] + 1 = \left[\frac{1}{2}\log_2 \sqrt{2}\, n\right] + 1 = \left[\frac{1}{4} + \frac{1}{2}\log_2 n\right] + 1.$$

Наслідок 2. Якщо в рівнянні $2^i k_i l_i + a_i k_i + b_i l_i = n_i$ виконується співвідношення $K_i = (n_i - b_i L_i) : (2^i L_i + a_i) \notin \mathbb{N},\ \forall L_i, K_i \in \mathbb{N}$, де $L_i, K_i < n_i$, то обрана гілка розв’язку вже є хибною і не потребує подальшого розгляду.

Доведення випливає з еквівалентності відсутності розв’язку рівняння (2) при виконанні $K_i = (n_i - b_i L_i) : (2^i L_i + a_i) \in \mathrm{N}$, $\forall L_i, K_i \in \mathrm{N}$, де $L_i, K_i < n_i$. Таким чином, завдяки ознакам подільності в двійковій системі числення легко відсікати хибні гілки.

Твердження. Якщо виконується нерівність $2^i k_i l_i > n_i$ починаючи з $i+1$ ітерації, то одна з послідовностей знаків розв’язків $\{k_j\}_{i+1}^n$ $\{l_j\}_{i+1}^n$ складається лише з нулів.

Доведення. Оскільки, найменше значення числа k_i, яке задовольняє ознаку зупинки, що може бути на *i*-тій ітерації має вигляд $k_i = 1\underbrace{0...0}_{i-1}$ (насправді в конкретному випадку маємо точне значення для k_j, $j = 1,...,i$), то для того, щоб виконувалася нерівність $2^i k_i l_i < n_i$ (без виконання якої неможливе виконання ознаки зупинки) слід брати послідовність з нулів, починаючи з *i*+1 розряду у числі k_i чи l_i, тому надалі маємо лише дві можливі послідовності або $\{k_j\}_{i+1}^n$ це послідовність з нулів а її **копослідовність** $\{l_j\}_{i+1}^n$ це префікс довжини *n-i* початку коду числа q. Або навпаки $\{l_j\}_{i+1}^n$ це послідовність з нулів а $\{k_j\}_{i+1}^n$ це префікс довжини *n*-*i* з молодших цифр числа p і $2^i k_i l_i > n_i$, тоді розв’язок рівняння $2^i k_i l_i + a_i k_i + b_i l_i = n_i$ вже не належатиме до $\mathbb{N}$.

При цьому зупинка відбулася за $m = \min\{\log p, \log q\}$ кроків, де використано двійкове представлення цих чисел.

Ознака зупинки 2. Якщо у рівнянні $2^i k_i l_i + a_i k_i + b_i l_i = n_i$ при $k_i = l_i = 1$ виконується співвідношення $2^i + a_i + b_i = n_i$, тобто $a_i + b_i + c_i = n_i$, то вже знайдено всі знаки обох чисел p і q.

Доведення. Оскільки у цьому випадку розв’язки p і q мають однакову розрядність, то цифра i-го розряду який є старшим розрядом у їх запису це 1. Тому в силу $a_i, b_i, c_i > 0$ на останній ітерації підстановка $k_i = l_i = 1$ утворює у лівій частині суму $a_i + b_i + c_i = n_i$. Звідси і з $k_i = 2k_{i+1} + r_i$, $l_i = 2l_{i+1} + s_i$, знайдемо цифри i-го розряду на чисел p і q відповідно. Тепер можемо повернутися до знайдених розв’язків конгруенції $2^{i-1} k_{i-1} l_{i-1} + a_{i-1} k_{i-1} + b_{i-1} l_{i-1} = n_{i-1} (\mathrm{mod}\, 2)$, що виникла на попередній ітерації і отримати цифри $i-1$-го розряду для p і q відповідно. Аналогічно діємо повертаючись до вже знайдених розв’язків попередніх рівнянь.

Приклад 1. Маємо $(10k_1 + 1)\ (10l_1 + 1) = 100011$, що перетворюється на $100k_1 l_1 + k_1 + l_1 = 10001$, застосуємо наслідок 2 для відсікання хибної гілки перевіривши умову $10001 - b_i l_i / (100 l_i + a_i) = 10000/(101) \notin \mathbb{N}$, де $i = 1$, що можна перевірити без ділення. Тобто умова не виконана, при значеннях $r_2 = 0, s_2 = 1$ з формул заміни $k_1 = 2k_2 + r_1$, $l_1 = 2l_2 + s_1$. Тому залишилась лише підстановка $k_1 = 10k_2 + 1$, $l_1 = 10l_2$, де $r_2 = 1, s_2 = 0$. Маємо $100k_2 l_2 + k_2 + 11 l_2 = 1000$ для якої виконується ознака зупинки 2 при $k_2 = 1$, $l_2 = 1$.

Наслідок 3. Для кожного $n = pq$ застосовна ознака 1 чи 2.

Доведення. Якщо виконується $\log p = \log q$, то застосовна ознака 2, якщо ж $\log p \neq \log q$, то застосовна ознака 1, яка теж є швидко обчислювальною, бо містить лише зсуви і додавання.

Приклад 2. $(10k_1 + 1)(10l_1 + 1) = 100011 = 35$, $100k_1 l_1 + 10k_1 + {}$ $+10l_1 + 1 = 100011$, звідки $1000k_1 l_1 + 10k_1 + 10l_1 = 100010$, скоротивши на 10 маємо $100k_1 l_1 + k_1 + l_1 = 10001$ нехай k_1 = 10, k_2+ 1, $l_1 = 10l_2$, тоді

$1000k_2l_2 + 10k_2 + 110l_2 + 1 = 10001$ звідси $100k_2l_2 + k_2 + 11l_2 = 1000$. Ознака 2 виконується при k_3 =1, l_3= 1 перетворює рівняння в правильну рівність. Отримуємо розв’язок а саме p = 111 = 7, q = 101 = 5.

Висновки. З критеріїв зупинки слідує, що при $q < p$ зупинка буде як тільки буде обчислено останній біт числа q, тобто за $\lceil \log_2 q \rceil$ кроків. Отже, висота бінарного дерева вибору потрібних підстановок не більша за $m = \min\{\lceil \log_2 q \rceil, \lceil \log_2 p \rceil\}$. На кожній ітерації відбувається як максимум 4 додавання і 3 зсуви у двійковому представленні числа. Зсув числа робиться всього за 1 такт. Але множення на 2 чи ділення на 2 у двійковій системі числення рівносильне зсуву, що виконується за 1 такт. Позначимо додавання як *D*, зсув як Z, тоді маємо $4D + 3Z$ операцій. Це досить швидкі обчислення бо для виконання *D* потрібно лише 2 такти. В кожній вершині бінарного дерева треба зберігати лишок $n_i \equiv x_i (\mathrm{mod}\, 2)$ це 1 біт і $r_i, s_i (\mathrm{mod}\, 2)$, разом це 3 біти. Кожне ядро процесора кластера SunWay MPP [6] має 30 Мб кеш пам’яті (по 2Гб на процесор), тому може зберігати ці лишки і потрібні вказівники. Він має 2^{24} ядер, тому може обчислити в паралельному режимі піддерево, що має на нижньому рівні 2^{23} вершин, як наслідок кількість вершин на верхніх рівнях рівна $2^{23} - 1$. Обчисливши всі лишки в вершинах першого піддерева, яке має ширину 2^{23}, якщо там не знайдено розв’язок, ці лишки витираються і починається обхід інших піддерева, тобто використовуються відкладені обчислення. Окрім того обсяг ОЗУ кластера перевищує витрати пам’яті на зберігання усіх необхідних лишків для відновлення роз’вязку з такого піддерева. Обробити все дерево розв’язків для ключа з 1024 біт можна не більше ніж за $(1024:2):23$ проходів, тут ділимо на 2, бо у піддеревах з коренями у вершинах v_{11} і у v_{12}. Перший індекс це номер рівня, а другий — номер вершини (нумерація рівнів з 0) множини лишків симетричні, кожен з яких вимагає не більше ніж $512 \cdot 11$ обчислювальних тактів процесора архітектури RISC. Частота ядра кластера 1,45 Ггц, тобто за 1 с $1,45 \cdot 10^9$ тактів. Наш алгоритм зовсім не потребує витрат часу на збір розв'язків окремих обчислювальних вузлів у спільний розв'язок всієї задачі, бо потрібна гілка дає розв'язок окремої підзадачі, який є розв'язком усієї задачі.

Список використаних джерел:

1. Орлов В. А., Медведев Н. В., Шимко Н. А., Домрачева А. Б. Теория чисел в криптографии. Издательство МГТУ им. Н. Э. Баумана. 222 с.

2. R Elkenbracht-Huizing «An implementation of the number field sieve» 1996. [citeseer.nj.nec.com/elkenbrach-thuizing96implementa tion.html]
3. Lupu Costică. Methods of solving Diophantine equations in secondary education in Romania. *Science Journal of Education.* 2014. 2(1). P. 22–32.
4. Скуратовський Р. В. Модернізований алгоритм Поліга-Хелмана, Шенкса. *Вісник КНУ імені Тараса Шевченка.* 2015. Том 2. С 63.
5. Николайчук Я. Теоретичні основи виконання модулярних операцій множення в базисі Крестенсона-Радемахера. *Інформатика та математичні методи в моделюванні.* 2011. № 2. С. 123–130.
6. Режим доступу: [http://www.nsccwx.cn/] (це оглядова стаття про 500 кращих кластерів світу за 2016 р.).

Problem of factorization is well known and it still has not solving. All known methods that has subexponential complexity are not destined for parallel implementation. For instance not all variants of *GNFS* [1] can be developed in parallel form. Only *kGNFS* admits parallel implementation. Method of factorization proposed by us has all properties for parallel implementation.

Key words: *factorization of integer number, parallel calculus.*

Одержано 24.02.2017

УДК 519

О. В. Славік, аспірант

Українська інженерно-педагогічна академія, м. Харків

НАБЛИЖЕННЯ ФУНКЦІЙ ДВОХ ЗМІННИХ ЗА ДОПОМОГОЮ ЇХ СЛІДІВ НА СИСТЕМІ НЕПЕРЕТИННИХ СМУГ З КРИВОЛІНІЙНИМИ ГРАНИЦЯМИ

В роботі проведено огляд існуючих методів відновлення пошкоджених цифрових зображень. Запропоновано узагальнений метод інтерстріпації для відновлення зображення поверхні за неповною інформацією про неї у випадку, якщо границі пошкоджених (невідомих) ділянок зображення є криволінійними смугами.

Ключові слова: *зображення, відновлення зображень, інтерстріпація, інтерлінація.*

Вступ. Інколи у файлах, які містять графічну інформацію виявляються дефекти. Оцінка значень втрачених пікселів, у яких відсутня інформація про зображення, необхідна в більшості задач цифрової обробки зображень або, наприклад, у задачах оборки архівних документів у вигляді зображень, що мають різноманітні спотворення (подряпини, плями, пил, непотрібні написи, лінії згину тощо).

У роботі [1] запропоновано метод інтерстріпації для відновлення функції двох змінних у точках між смугами за допомогою інформації про цю функцію, яка відома лише в точках заданої системи смуг. Даний метод базувався на припущені, що зображення відсутнє між смугами паралельними або взаємоперпендикулярними осям координат.

Мета даної роботи — розробка модифікованого методу інтерстріпації, за допомогою якого можна відновлювати зображення у вигляді неперетинних смуг з криволінійними границями, який би дозволив отримати такий же результат, як і в роботі [1] у випадку коли смуги обмежені прямими паралельними осям координат.

Аналіз літературних джерел. Розглянемо задачу відновлення пошкоджених областей зображення, використовуючи інформацію на відомих ділянках зображення.

Позначимо множину пікселів у невідомій області $\overline{D}$, а множину коректних пікселів D.

Більшість методів відновлення зображень можна умовно поділити на наступні групи [2]: текстурні, шаблонні, основані на рівняннях у частинних похідних, гібридні та швидкі напівавтоматичні. Наведемо коротку характеристику цих методів.

Текстурні методи відновлення зображень для заповнення невідомої області $\overline{D}$ використовують пікселі безпосередньо з відомої області зображення D. Головна відмінність між цими методами полягає у забезпеченні неперервності на границі області D [2]. Методи текстурного відновлення зображення відрізняються способом відновлення різних кольорів, інтенсивності, градієнта та навіть статистичних характеристик.

Основна ідея роботи шаблонних методів відновлення зображень полягає у припущенні про наявність повторюваних фрагментів даних на зображенні, які зазвичай називаються шаблонами. Відновлення області $\overline{D}$ проводиться частинами шляхом копіювання значень яскравості з найбільш схожого шаблону [2]. Особливо виділяється робота [3], де для заповнення пошкодженої області використовується база даних зображень, яка містить мільйони зображень-шаблонів для відновлення.

Згідно з методами відновлення зображень, основаними на рівняннях з частинними похідними, відновлення даних області $\overline{D}$ проводиться за допомогою даних, що є природним продовженням інформації, яка міститься в D [4].

Гібридні методи відновлення зображень являють собою поєднання двох класів методів. А саме текстурних методів та методів, основаних на використанні диференціальних рівнянь з частинними похідними. Основна ідея алгоритму полягає у тому, що перш за все виділяють текстурну та структурну складову зображення, які потім заповнюються відповідними алгоритмами [2].

Недоліком більшості вище представлених методів є їх висока обчислювальна складність, тому в деяких працях застосовують швидкі напівавтоматичні методи відновлення зображення для прискорення обчислень. До таких методів відносять метод відновлення зображення за допомогою виділеної структури [5] та метод відновлення зображення з використанням ітеративної згортки зображення з дифузним ядром [6].

Окремо слід виділити інтерстріпацію (від англ. inter — між, від англ. stripe — смуга) функцій двох змінних [1]. Даний метод дозволяє відновлювати зображення поверхні за неповною інформацією про неї на системі смуг, якщо інформація про цю функцію відома лише в точках вказаних смуг. На даний момент, в роботі [1] досліджувались випадки відновлення зображень поверхонь для випадків, коли границі смуг невідомих областей представляли собою прямі, взагалі кажучи перетинні, паралельні осям координат. Існуюча теорія інтерстріпації функцій не передбачає можливість відновлення зображень у випадку якщо границі відомих смуг, наприклад, є криволінійними. Наведений далі метод є узагальненням існуючої теорії інтерстріпації функцій двох змінних для випадку криволінійних границь смуг.

Постановка задачі. Необхідно відновити пошкоджене зображення деякої поверхні Σ. Вважаємо, що зображення поверхні Σ відоме лише на системі m $(m \geq 2)$ вертикальних смуг вигляду:

$$D_{1,k} = \{\alpha_k(y) \leq x \leq \beta_k(y)\},\ k = \overline{1,m},$$

та (або) на системі n $(n \geq 2)$ горизонтальних смуг вигляду:

$$D_{2,l} = \{\gamma_l(x) \leq y \leq \delta_l(x)\},\ l = \overline{1,n}.$$

Невідомі смуги зображення задаються наступним чином для невідомих вертикальних смуг:

$$\overline{D}_{1,k,k+1} = \{\beta_k(y) \leq x \leq \alpha_{k+1}(y)\},\ \ k = \overline{1,m-1},$$

та для невідомих горизонтальних смуг:

$$\overline{D}_{2,l,l+1} = \{\delta_l(x) \leq y \leq \gamma_{l+1}(x)\},\ l = \overline{1,n-1}.$$

Тоді об'єднання множин $\overline{D}_{1,k,k+1}$, $k = \overline{1,m-1}$ та $\overline{D}_{2,l,l+1}$, $l = \overline{1,n-1}$ дає область $\overline{D}$ незаповнених ділянок зображення. В точках зображення D, які не потрапили до $\overline{D}$ зберігається вся наявна інформація про зображення.

Поверхня $\Sigma : z = f(x,y)$, $f(x,y) \in C^{N,N}(R^2)$, яку ми хочемо відновити, вважається відомою лише на вказаних смугах, тобто

$$f(x,y)\big|_{\alpha_k \leq x \leq \beta_k} = f_{1,k}(x,y),\ \alpha_k(y) \leq x \leq \beta_k(y);$$

$$f(x,y)\big|_{\gamma_l \leq y \leq \delta_l} = f_{2,l}(x,y), \gamma_l(x) \leq y \leq \delta_l(x).$$

$C^{N,N}(R^2)$ — клас функцій, які мають неперервні похідні $f^{(p,q)}(x,y)$ для $0 < p,q \leq N$.

Інтерстріпація на системі вертикальних смуг із криволінійними границями. Вважаємо, що зображення поверхні Σ відоме лише на системі m $(m \geq 2)$ вертикальних смуг $D_{1,k}$, $k = \overline{1,m}$.

Введемо до розгляду наступний оператор:

$$\Theta_1 f(x,y) = \begin{cases} f_{1,k}(x,y) & (x,y) \in D_{1,k},\ k = \overline{1,m}; \\ E_{1,k,k+1} f(x,y) & (x,y) \in \overline{D}_{1,k,k+1},\ k = \overline{1,m-1}, \end{cases}$$

де

$$E_{1,k,k+1} f(x,y) = \frac{x - \alpha_{k+1}(y)}{\beta_k(y) - \alpha_{k+1}(y)} f(\beta_k(y), y) + \frac{x - \beta_k(y)}{\alpha_{k+1}(y) - \beta_k(y)} f(\alpha_{k+1}(y), y).$$

Твердження 1. Поверхня $z = \Theta_1 f(x,y)$ є наближеною математичною моделлю освітленості поверхні Σ, яка на кожній смузі $D_{1,k}$, $k = \overline{1,m}$ точно відновлює поверхню, а між смугами зображує поверхню за допомогою оператора $E_{1,k,k+1} f(x,y)$, $k = \overline{1,m-1}$, при цьому функція $\Theta_1 f(x,y) \in C^{N,N}(R^2)$.

Інтерстріпація на системі горизонтальних смуг з криволінійними границями. Вважаємо, що зображення поверхні Σ відоме лише на системі n $(n \geq 2)$ горизонтальних смуг $D_{2,l}$, $l = \overline{1,n}$.

Введемо до розгляду такий оператор:

$$\Theta_2 f(x,y) = \begin{cases} f_{2,l}(x,y) & (x,y) \in D_{2,l},\ l = \overline{1,n}; \\ E_{2,l,l+1} f(x,y) & (x,y) \in \overline{D}_{2,l,l+1},\ l = \overline{1,n-1}, \end{cases}$$

де

$$E_{2,l,l+1} f(x,y) = \frac{y - \gamma_{l+1}(x)}{\delta_l(x) - \gamma_{l+1}(x)} f(x, \delta_l(x)) + \frac{y - \delta_l(x)}{\gamma_{l+1}(x) - \delta_l(x)} f(x, \gamma_{l+1}(x)).$$

Твердження 2. Поверхня $z = \Theta_2 f(x,y)$ є наближеною математичною моделлю освітленості поверхні Σ, яка на кожній смузі $D_{2,l}$, $l = \overline{1,n}$ точно відновлює поверхню, а між смугами зображує поверхню за допомогою оператора $E_{2,l,l+1} f(x,y)$, $l = \overline{1,n-1}$, при цьому функція $\Theta_2 f(x,y) \in C^{N,N}(R^2)$.

Інтерстріпація на системі взаємоперпендикулярних смуг з криволінійними границями. Вважаємо, що зображення поверхні Σ відоме лише на системі m $(m \geq 2)$ вертикальних смуг $D_{1,k}$, $k = \overline{1,m}$, та на системі n $(n \geq 2)$ горизонтальних смуг $D_{2,l}$, $l = \overline{1,n}$.

В результаті їх об'єднання отримаємо набір прямокутних областей

$$\overline{\Pi}_{k,l}=\left[\beta_k,\alpha_{k+1}\right]\times\left[\delta_l,\gamma_{l+1}\right], k=\overline{1,m-1},\ l=\overline{1,n-1},$$

інформацію в яких треба відновити.

Введемо до розгляду наступний оператор:

$$\Theta_{12}f(x,y)=\begin{cases} f_{1,k}(x,y) & (x,y)\in D_{1,k},\ k=\overline{1,m};\\ f_{2,l}(x,y) & (x,y)\in D_{2,l},\ l=\overline{1,n};\\ E_{1,2,k,l}f(x,y) & (x,y)\in\overline{\Pi}_{k,l},\ k=\overline{1,n-1},\ l=\overline{1,m-1}, \end{cases}$$

де

$$E_{1,2,k,l}f(x,y)=\left[E_{1,k,k+1}+E_{2,l,l+1}-E_{1,k,k+1}E_{2,l,l+1}\right]f(x,y)=$$

$$=\frac{x-\alpha_{k+1}(y)}{\beta_k(y)-\alpha_{k+1}(y)}f(\beta_k(y),y)+\frac{x-\beta_k(y)}{\alpha_{k+1}(y)-\beta_k(y)}f(\alpha_{k+1}(y),y)+$$

$$+\frac{y-\gamma_{l+1}(x)}{\delta_l(x)-\gamma_{l+1}(x)}f(x,\delta_l(x))+\frac{y-\delta_l(x)}{\gamma_{l+1}(x)-\delta_l(x)}f(x,\gamma_{l+1}(x))-$$

$$-\frac{x-\alpha_{k+1}(y)}{\beta_k(y)-\alpha_{k+1}(y)}\frac{y-\gamma_{l+1}(x)}{\delta_l(x)-\gamma_{l+1}(x)}f(\beta_k(y),\delta_l(x))-$$

$$-\frac{x-\alpha_{k+1}(y)}{\beta_k(y)-\alpha_{k+1}(y)}\frac{y-\delta_l(x)}{\gamma_{l+1}(x)-\delta_l(x)}f(\beta_k(y),\gamma_{l+1}(x))-$$

$$-\frac{x-\beta_k(y)}{\alpha_{k+1}(y)-\beta_k(y)}\frac{y-\gamma_{l+1}(x)}{\delta_l(x)-\gamma_{l+1}(x)}f(\alpha_{k+1}(y),\delta_l(x))-$$

$$-\frac{x-\beta_k(y)}{\alpha_{k+1}(y)-\beta_k(y)}\frac{y-\delta_l(x)}{\gamma_{l+1}(x)-\delta_l(x)}f(\alpha_{k+1}(y),\gamma_{l+1}(x)).$$

Оператор $E^*_{1,2,k,l}f(x,y)$ — оператор інтерлінації (від англ. inter — між, від англ. line — лінія) функції двох змінних, який у випадку якщо границі є прямими є класичним оператором інтерлінації між чотирма сторонами довільного чотирикутника $\overline{\Pi}_{k,l}$, $k=\overline{1,n-1}$, $l=\overline{1,m-1}$, наведеним у [7, 8].

Твердження 3. Поверхня $z=\Theta_{12}f(x,y)$ є наближеною математичною моделлю освітленості поверхні Σ, яка на кожній із смуг $D^*_{1,k}$, $k=\overline{1,m}$ та $D^*_{2,l}$, $l=\overline{1,n}$ точно відновлює поверхню, а на областях $\overline{\Pi}_{k,l}, k=\overline{1,n-1},\ l=\overline{1,m-1}$ відновлює поверхню за допомогою оператора $E^*_{1,2,k,l}f(x,y), k=\overline{1,n-1},\ l=\overline{1,m-1}$, при цьому функція $\Theta_{12}f(x,y)\in C^{N,N}(R^2)$.

Висновки. В роботі наведені та проаналізовані такі класи алгоритмів: текстурні, шаблонні, основані на рівняннях з частинними похідними, гібридні та швидкі напівавтоматичні. Окремо розглянуто метод інтерстріпації функції двох змінних. На основі методу інтерстріпації у даній статті запропоновано узагальнений метод інтерстріпації для відновлення зображення поверхні за неповною інформацією про неї у випадку смуг із криволінійними границями. Проведено обчислювальний експеримент для випадків коли зображення відоме лише на системі горизонтальних, вертикальних та взаємоперпендикулярних смуг з криволінійними границями.

Розглянуті методи можуть бути застосовані для відновлення уражених ділянок пошкоджених зображень. Аналіз і розробка методів відновлення зображень є актуальною задачею для різноманітних прикладних областей науки та потребує подальших досліджень. В подальшому автори планують при відновленні поверхні враховувати також додаткову інформацію про структуру поверхні між смугами.

Список використаних джерел:

1. Литвин О. М., Матвєєва С. Ю. Метод відновлення поверхні між смугами за допомогою інформації про поверхню на взаємно перпендикулярних смугах. *Управляющие системы и машины*. 2011. № 1. С. 33–41.
2. Joshua J., Darsan G. Digital inpainting techniques — a survey. *Intern. J. of Latest Research in Engineering and Techn*. 2016. Vol. 2. P. 34-36.
3. Hays J., Efros A. Scene completion using millions of Graphics. *Computer Graphics Proceedings (SIGGRAPH)*. 2007. Vol. 26. P. 87-94.
4. Bertalmio M., Sapiro G., Caselles V., Ballester C. Image inpainting. *Proc. of the 27th Annual Conf. on Computer Graphics and Interactive Techniques.* 2000. P. 417–424.
5. Sun J., Yuan L., Jian J., Shum H.-Y. Image completion with structure propagation. *Proc. of ACM Conf. Comp. Graphics*. 2005. P. 861–868.
6. Oliviera M., Bowen B., McKenna R., Chang Y.-S. Fast digital image inpainting. *In Proc. of Intl. Conf. on Visualization, Imaging and Image Processing*. 2001. P. 261–266.
7. Литвин О. М. Інтерлінація функцій. Харків: Основа, 1992. 234 с.
8. Литвин О. М. Інтерлінація функцій та деякі її застосування. Харків: Основа, 2002. 544 с.

In given work was reviewed of existing inpainting methods of restoration of damaged digital images. Was proposed a general method of interstripation of functions of two variables for image reconstruction, when information about the surface are incomplete and the border of disjoint strips have curvilinear boundaries.

Key words: *image, inpainting, interstripation, interlination.*

Одержано 14.02.2017

УДК 519.642

С. Г. Солодкий, д-р фіз.-мат. наук, доцент,
Г. Л. Милейко, канд. фіз.-мат. наук
Інститут математики НАН України, м. Київ

ПРО ЕКОНОМІЧНІ СТРАТЕГІЇ РОЗВ'ЯЗУВАННЯ ОПЕРАТОРНИХ РІВНЯНЬ І РОДУ

Для широких класів жорстко некоректних задач побудовано ефективні методи розв'язування із застосуванням різних правил вибору параметра регуляризації (апріорного та апостеріорних). Знайдено порядкові оцінки мінімального радіуса гальоркінської інформації та мінімального радіуса обчислювальних витрат.

Ключові слова: *жорстко некоректні задачі, операторні рівняння I роду, мінімальний радіус гальоркінської інформації, складність.*

Вступ. Постановка задачі. Дані дослідження присвячено оцінкам складності жорстко некоректних задач. Слід зазначити, що на сьогодні такі дослідження набули інтенсивного розвитку у межах теорії оптимальних алгоритмів, згідно з якою під інформаційною складністю розуміється найменший обсяг дискретної інформації, що необхідна для знаходження наближеного розв'язку із заданою точністю, а під алгоритмічною — мінімальне число арифметичних дій, які потрібно виконати для побудови такого розв'язку. Отже, наведемо строгу постановку задачі.

Розглянемо операторне рівняння I роду

$$Ax = f\ , \tag{1}$$

де $A \in L(X, X)$, X — гільбертів простір. Будемо вважати, що множина Ω не замкнена в X та $f \in Range(A)$. Також будемо припускати, що права частина (1) задана з деякою похибкою $\delta > 0$, тобто замість $[1;\infty)\times[1;\infty)$ відомо її збурення $f_\delta \in X : \left\| f - f_\delta \right\| \le \delta$. Наслідуючи [1], під жорстко некоректною задачею будемо розуміти рівняння (1), точний розв'язок якого задовольняє умову джерела логарифмічного типу

$$M_p(A) := \{u : u = \ln^{-p}(A^* A)^{-1} v,\ \|v\| \le \rho\}\ , \tag{2}$$

де $p, \rho > 0$, Ω — оператор, спряжений до A. Мета наших досліджень — відшукання наближеного розв'язку x^+ (1) з мінімальною нормою в X, що належить множині (2).

Нехай $\omega_1 := \{i : \ \ (i, j) \in \Omega\}$ — деякий ортонормований базис у X. Розглянемо наступний клас досліджуваних операторів:

$$H_\gamma^{r,s} := \{A : A \in L(X,X),\ \|A\| \le \gamma_0,\quad \sum_{n+m=1}^{\infty} (Ae_m, e_n)^2 (\underline{n}^{2r} \cdot \underline{m}^{2s} \le \gamma_1^2\},$$

де $r, s > 0,\ \gamma_0 \le e^{-1},\ \ \gamma = (\gamma_0, \gamma_1),\ n, m \in \mathrm{Z}_+,\ \ \underline{n} = 1$ при $n = 0$ і $\underline{n} = n$ у протилежному випадку.

Слід зазначити, що $H_\gamma^{r,s}$ узагальнює клас інтегральних операторів Фредгольма з ядрами у вигляді функцій двох змінних, що мають скінченну гладкість. Конкретний приклад $H_\gamma^{r,s}$ розглядався у [2].

Клас рівнянь (1) із операторами з $H_\gamma^{r,s}$ та розв’язками (2) позначимо $(H_\gamma^{r,s}, M_p(A))$. Надалі зосередимося на дослідженні проекційних методів розв’язування задач класу $(H_\gamma^{r,s}, M_p(A)),\ \ r \ge s.$

Зазначимо, що будь-яку проекційну схему дискретизації рівнянь (1) зі збуреною правою частиною f_δ можна визначити за допомогою скінченного набору скалярних значень

$$(Ae_j, e_i),\ \ (i,j) \in \Omega\,, \tag{3}$$

$$(f_\delta, e_k),\ \ k \in \omega_1\,,\ \omega_1 := \{i:\ \ (i,j) \in \Omega\}\,, \tag{4}$$

де Ω — довільна обмежена область координатної площини $[1;\infty) \times [1;\infty)$. Скалярні добутки (3), (4) прийнято називати гальоркінською інформацією про рівняння (1), а під $card(\Omega)$ розуміти загальну кількість скалярних добутків вигляду (3). Зокрема, якщо $\Omega = [1,n] \times [1,m]$, $\omega_1 = [1,n]$, то ми отримуємо стандартну гальоркінську схему дискретизації з $card(\Omega) = n \cdot m$.

Під проекційним методом розв'язування рівняння (1) будемо розуміти будь-яке відображення $P = P(\Omega) : X \to X$, яке за допомогою гальоркінської інформації (3) про рівняння (1) зіставляє правій частині розв'язуваного рівняння f_δ елемент $P(A_\Omega) f_\delta \in X$, що є багаточленом за базисом $\{e_i\}_{i=1}^{\infty}$ з номерами гармонік із $\omega_2 := \{j : (i,j) \in \Omega\}$. Цей елемент приймається за наближений розв'язок (1).

Під похибкою проекційного методу $P(\Omega)$ на класі рівнянь $(H_\gamma^{r,s}, M_p(A))$, зазвичай, будемо розуміти його найбільше відхилення

$$e_\delta(H_\gamma^{r,s}, M_p(A), P(\Omega)) = \sup_{A \in H_\gamma^{r,s}}\ \sup_{x^+ \in M_p(A)}\ \sup_{f_\delta : \|f - f_\delta\| \le \delta} \left\| x^+ - P(A_\Omega) f_\delta \right\|.$$

Мінімальний радіус гальоркінської інформації задамо величиною

$$R_{N,\delta}(H_\gamma^{r,s}, M_p(A)) = \inf_{\Omega:\ card(\Omega) \le N}\ \inf_{P(\Omega)}\ e_\delta(H_\gamma^{r,s}, M_p(A), P(\Omega))\,.$$

Ця величина визначає найменшу можливу точність серед усіх проекційних методів при обмеженні на обсяг гальоркінської інформації. Таким чином, $R_{N,\delta}$ характеризує інформаційну складність класу задач $(H_\gamma^{r,s}, M_p(A))$.

Позначимо через Π_M множину усіх можливих проекційних методів, які для побудови наближеного розв'язку потребують виконання не більш ніж M елементарних арифметичних операцій (е.а.о.). Мінімальний радіус обсягу обчислювальних витрат задамо величиною

$$\overline{R}_{M,\delta(H_\gamma^{r,s}, M_p(A))} = \inf_{\Omega:\, card(\Omega)\le M} \ \inf_{P(\Omega)\in \Pi_M} e_\delta(H_\gamma^{r,s}, M_p(A), P(\Omega)) .$$

Ця величина визначає найменшу можливу точність проекційних методів при обмеженні на обсяг обчислювальних витрат. Таким чином, $\overline{R}_{M,\delta}$ характеризує алгоритмічну складність класу задач $(H_\gamma^{r,s}, M_p(A))$.

Економічна модифікація гальоркінської схеми. Оцінки складності. Оскільки на практиці при побудові чисельного розв'язку припустиме використання лише скінченного обсягу дискретної інформації про задачу, то замість вихідного рівняння доводиться розглядати його скінченно-вимірний аналог. Такий етап побудови наближеного розв'язку у чисельному аналізі прийнято називати дискретизацією. У зв'язку з цим виникає актуальна проблема мінімізації обсягу дискретної інформації та зменшення кількості виконуваних у процесі розв'язування арифметичних дій *без втрати точності*.

Для економічної дискретизації рівнянь з $(H_\gamma^r, M_p(A))$ замість стандартної схеми Гальоркіна $P_n A P_m$ застосуємо її модифікацію, що називається гіперболічним хрестом. Отже, наближений розв'язок шукатимемо у вигляді

$$x_{\alpha,\delta}^{\Omega} = g_\alpha(A_\Omega^* A) A_\Omega^* P_\Omega f_\delta, \tag{5}$$

де Ω — гіперболічний хрест (конкретні приклади див. далі), а твірна функція g_α задовольняє умови Бакушинського

$$\begin{gathered} \sup_{0<\lambda\le\gamma_0^2} \sqrt{\lambda}\left|g_\alpha(\lambda)\right| \le \chi_* \alpha^{-1/2}, \\ \sup_{0<\lambda\le\gamma_0^2} \sqrt{\lambda}\left|1-\lambda g_\alpha(\lambda)\right| \ln^{-\mu}\lambda^{-1} \le \chi_\mu \ln^{-\mu}\alpha^{-1} \end{gathered} \tag{6}$$

при деяких додатних константах χ_μ, χ_* та параметрі $0 \le \mu \le \mu_*$.

Зазначимо, що більшість відомих регуляризаторів відповідають умовам (6), наприклад, стандартний метод Тіхонова, за яким регуляризований розв'язок шукається як розв'язок наступної варіаційної задачі:

$$\left\|Ax - f_\delta\right\|^2 + \alpha\left\|x\right\|^2 \to \min,$$

що зводиться до операторного рівняння 2-го роду

$$\alpha x + A^* A x = A^* f_\delta .$$

Інакше кажучи, наближений розв’язок шукаємо у вигляді (5) з

$$g_\alpha(\lambda) = (\alpha + \lambda)^{-1}. \tag{7}$$

Оцінки складності (апріорний випадок). За область Ω візьмемо хрест вигляду

$$\Omega_1 = \{1\} \times [1; 2^{bn}] \bigcup_{k=1}^{n} (2^{k-1}; 2^k] \times [1; 2^{bn-rk/s}] \subset [1; 2^n] \times [1; 2^{bn}],$$

де $r/s < b \le 2r/s,\ \ n \in \mathrm{N},$ якому відповідає дискретизований оператор

$$A_{\Omega_1} = P_1 A P_{2^{bn}} + \sum_{k=1}^{n} (P_{2^k} - P_{2^{k-1}}) A P_{2^{bn-rk/s}} . \tag{8}$$

Проекційний метод (5)–(6), (8) з апріорним правилом вибору параметра регуляризації α: $\ln^{-p} \alpha^{-1} = \delta / \sqrt{\alpha}$ позначимо $\Re_1$.

Теорема 1. При N, що задовольняють умову

$$N^{-s} \ln^{-p} N^{2s} = \begin{cases} O(\delta^{-1} \ln^{-(s+1)} \delta^{-1}), & r = s; \\ O(\delta^{-1} \ln \delta^{-1}), & r > s, \end{cases}$$

справджується

$$R_{N,\delta}(H_\gamma^{r,s}, M_p(A)) = O(\ln^{-p} N^{2s}) = O(\ln^{-p} \delta^{-1}),$$

де N — обсяг задіяної гальоркінської інформації. При цьому

$$N = \begin{cases} O(\delta^{-1/s} (\ln \delta^{-1})^{(1-p+s)/s}), & r = s; \\ O(\delta^{-1/s} (\ln \delta^{-1})^{(1-p)/s}), & r > s. \end{cases}$$

Зазначений оптимальний порядок на класі $(H_\gamma^{r,s}, M_p(A)),$ $0 < p < \infty,\ \ r \ge s,$ реалізується в рамках проекційного методу $\Re_1$.

Теорема 2. При $r \ge 2s$ мають місце співвідношення

$$\overline{R}_{N,\delta}(H_\gamma^{r,s}, M_p(A)) = O(\ln^{-p} N^{2s}) = O(\ln^{-p} \delta^{-1}),$$

де N — обсяг обчислювальних витрат. При цьому

$$N = \begin{cases} O(\delta^{-1/s} (\ln \delta^{-1})^{(1-p+s)/s}), & r = 2s; \\ O(\delta^{-1/s} (\ln \delta^{-1})^{(1-p)/s}), & r > s. \end{cases} \tag{9}$$

Зазначений оптимальний порядок реалізується в рамках проекційного методу $\Re_1$, де як регуляризатор застосовується стандартний метод Тіхонова.

Оцінки складності (апостеріорний випадок). Недоліком апріорного вибору α є його обов'язкове «налаштування» на певне значення *p*. При цьому, як відомо, оптимальний порядок точності $O(\ln^{-p}\delta^{-1})$ забезпечується лише для задач (1) з нормальним роз'язком $x^{+} \in M_p(A)$, відповідно, де величина *p* фіксована. Очевидно, що такий підхід до розв'язування некоректних задач можливий, якщо нам точно відомо значення параметра *p*. Але оскільки така інформація, зазвичай, або відсутня, або не є точною, тому на практиці необхідні апостеріорні правила вибору параметра регуляризації (наприклад, принцип нев'язки Морозова, принцип рівноваги та ін.), реалізація яких не потребує додаткових знань про гладкість розв'язку.

Нехай параметр *p* в (2) невідомий, тому шукатимемо розв'язок з множини

$$M(A) = \bigcup_{p\in(0,p_1]} M_p(A),$$

де $p_1 < \infty$ — верхня межа можливих значень *p*.

Для економічного розв'язування рівнянь з класу $(H_{\gamma}^{r,r}, M(A))$, буде запропоновано два підходи, що полягають у комбінуванні стандартного методу Тіхонова з принципом нев'язки Морозова та принципом рівноваги, відповідно.

В межах наших досліджень скористаємося проекційною схемою з хрестом вигляду

$$\Omega_2 = \{1\}\times[1;2^{2n}]\bigcup_{k=1}^{2n}(2^{k-1};2^{k}]\times[1;2^{2n-k}] \subset [1;2^{2n}]\times[1;2^{2n}], \qquad (10)$$

Проекційні методи (5)–(7), (10) з правилами зупинки згідно принципу нев'язки Морозова та принципу рівноваги, відповідно, будемо позначати $\Re_2$ та $\Re_3$.

Теорема 3. Мають місце порядкові оцінки

$$R_{N,\delta}(H_{\gamma}^{r,r}, M(A)) = O(\ln^{-p} N^{2r}) = O(\ln^{-p}\delta^{-1}),$$

для $N = O(\delta^{-1/r}\ln^{1+1/(2r)}\delta^{-1})$.

Зазначений оптимальний порядок реалізується у межах проекційних методів $\Re_2$ та $\Re_3$.

Висновки.

1. З результатів роботи [3] випливає, що для стандартної схеми Гальоркіна обсяг задіяної гальоркінської інформації на тих самих класах задач складає $O(\delta^{-1/s}\delta^{-\varepsilon/r}\ln^{-p/s}\delta^{-1})$, де величина $\varepsilon > 0$ не може бути як завгодно близькою до нуля, щоб не допустити істотне зростання похибки. Порівняння результатів для методу з [3]

з результатами теорем 1, 3 дозволяє дістатися висновку, що обидва підходи гарантують оптимальний порядок точності на всьому класі досліджуваних жорстко некоректних задач, водночас, задіяна нами модифікація гальоркінського методу дозволяє суттєво скоротити обсяг дискретної інформації.

2. Якщо порівняти результати теорем 3 (з апостеріорним правилом вибору параметра регуляризації) і 1 (з апріорним вибором параметра регуляризації), то можна дістатися висновку, що у разі апостеріорного вибору обсяг дискретної інформації є більшим на логарифмічний множник. Таке збільшення обсягу інформації можна розглядати як «платню» за відмову від знання гладкості шуканого розв'язку.
3. З оцінки (8) випливає, що збільшення гладкості оператора A за зовнішньою змінною r (від $r = 2s$ до $r > 2s$) призводить до зменшення на логарифмічний множник в оцінці обсягу обчислювальних витрат, що необхідні для досягнення оптимального порядку точності.
4. Порівнюючи результат роботи [3] з результатами теорем 1–3, можна дістатися висновку, що запропоновані проекційні методи дозволяють не тільки скоротити обсяг обчислень відносно стандартної гальоркінської схеми, а й реалізувати порядкові оцінки величин $R_{N,\delta}, \overline{R}_{N,\delta}$ на класах рівнянь $(H_{\gamma}^{r,s}, M_p(A))$.

Список використаних джерел:

1. Schock E., Pereverzev S. V. Morozov's discrepancy principle for Tikhonov regularization of severely ill-posed problems in finite-dimensional subspaces. *Num. Funct. Anal. Optim*. 2000. 21 (7-8). P. 901–916.
2. Солодкий С. Г., Милейко Г. Л. Оцінки складності жорстко некоректних задач. *Праці міжнародної наукової школи-семінару ISCOPT*. 2015.
3. Mathe P., Pereverzev S. V. Discretization strategy for ill-posed problems in variable Hilbert scales. *Inverse Problems*. 2003. 19 (6). P. 1263–1277.

For wide classes of severely ill-posed problems the economical projection methods with different selection (a priori and a posteriori) of the regularization parameter are designed. The order estimates of the minimal radius for Galerkin information and the minimal radius for computational efforts are obtained.

Key words: *severely ill-posed problems, operator equation of the first kind, the minimal radius for Galerkin information, complexity.*

Одержано 28.02.2017