6. Nemirovski A. Prox-method with rate of convergence O(1/t) for variational inequalities with Lipschitz continuous monotone operators and smooth convex-concave saddle point problems. *SIAM Journal on Optimization*. 2004. Vol. 15. P. 229–251.
7. Semenov V.V. A Version of the Mirror descent Method to Solve Variational Inequalities. *Cybernetics and Systems Analysis*. 2017. Vol. 53. P. 234–243.

A MODIFIED EXTRA-GRADIENT METHOD WITH BREGMAN DIVERGENCE FOR VARITIONAL INEQUALITIES

A new method of extra-gradient type for the approximate solution of variational inequalities with pseudo-monotone and Lipschitz-continuous operators acting in a finite-dimensional linear normed space is proposed. A theorem on the convergence of the method is proved and, in the case of a monotone operator, non-asymptotic estimates of the effectiveness of the method are obtained.

Key words: *variational inequality problem, monotonicity, pseudo-monotonicity, Lipschitz condition, extra-gradient method, Bregman divergence.*

Получено 12.02.2019

УДК 519.615.7
DOI: 10.32626/2308-5878.2019-19.137-141

В. Ю. Семенов*, канд. фіз.-мат. наук,
Є. В. Семенова**, канд. фіз.-мат. наук

***Інститут кібернетики імені В. М. Глушкова НАН України;
ТОВ «Дельта СПЕ», м. Київ,
****Інститут математики НАН України, м. Київ

МЕТОД РОЗВ'ЯЗАННЯ СИСТЕМ БІТОВИХ РІВНЯНЬ НА ОСНОВІ ПРИНЦИПУ ГІЛОК ТА ГРАНИЦЬ

Розв'язання систем рівнянь над бітовими полями є актуальною задачею для галузей криптографії, теорії завадостійкого кодування інформації, роботехніки, астрофізики та інших областей. У даній статті запропоновано метод розв'язування бітових рівнянь, що базується на методології гілок та границь (branch-and-bound). Запропонована методологія вже буда використана авторами для розв'язання систем нелінійних алгебраїчних рівнянь. Метод може бути використаний не тільки для систем бітових рівнянь, а також і для розв'язання систем бітових рівнянь над довільними скінченними полями Галуа $GF(n)$. Важливою особливістю запропонованого методу є те, що він дозволяє знайти усі розв'язки системи бітових рівнянь при будь-якому співвідношенні кількості змінних та кількості рівнянь. У статті наведено алгоритм, що реалізує послідовність дій, необхідну для реалізації запропонованого методу розв'язування систем бітових рівнянь. Алгоритм виконує послідовне зниження порядку системи (кількості змінних). Запропонована методика є спорідненою до методики

Constrained Propagation, що використовується у задачах розв'язання систем нелінійних алгебраїчних рівнянь та задач глобальної мінімізації функцій. Також у статті наведено чисельні приклади, що демонструють роботу метода при розв'язанні систем бітових рівнянь у випадку квадратичних нелінійностей. При цьому також досліджені різні комбінації кількості рівнянь та кількості невідомих, а також окремо розглянуто випадок розрідженої системи рівнянь. Показано, що метод має перевагу в кількості операцій перед методом прямого перебору можливих розв'язків системи рівнянь.

Ключові слова: *бітові рівняння, метод гілок та границь.*

Вступ. Розв'язання рівнянь над бітовими полями — актуальна задача, зокрема для криптографії, теорії завадостійкого кодування, роботехніки та інших областей [1]. Для розв'язання цієї задачі використовуються багато різних підходів, включаючи лінеаризацію систем рівнянь, алгоритми, що базуються на базисі Гребнера [2], методи прямого перебору та інші.

У статті запропоновано метод розвязування бітових рівнянь виду

$$f_i(x_1,...,x_n) = 0, i = 1,...,m \qquad (1)$$

над полем $GF(2)$, тобто $x_i \in \{0,1\}, 1 \le i \le n$.

Запропонований метод розвязання систем (1) базується на методології гілок та границь (branch-and-bound) [3], яка вже була застосована авторами в роботі [4] для розв'язання систем нелінійних алгебраїчних рівнянь. Особливістю методу є те, що він дозволяє знайти усі розв'язки системи бітових рівнянь при будь-якому співвідношенні кількості змінних та кількості рівнянь.

Опис алгоритму. Отже, ми розглядаємо систему рівнянь (1). На початку, пов'яжемо із змінними $x_1,...,x_n$ вектор стану $(x_1,...,x_n)$, кожна з координат якого може приймати значення «0», «1» и «2». Значення «0» та «1» є фіксованими, а значення «2» означає, що відповідна змінна може приймати одно з можливих значень: «0» чи «1».

На початку роботи алгоритму вектор розв'язків цілком складається із значень «2»: $(x_1,...,x_n) = (2,...,2)$. В процесі роботи алгоритму вектор стану, в якому є змінна, що приймає значення «2», замінюється на два вектори, в кожному з яких ця змінна приймає значення «0» та «1» відповідно. У результаті, розмірність (кількість невідомих) системи (1) знижується, щонайменше, на одиницю. Після підстановки значень «0» чи «1» в кожне з рівнянь можливі наступні варіанти.

1. Якщо ми отримали рівняння 1 = 0, то даний вектор змінних має бути відкинутим. Робота алгоритму по даній гілці зупиняється.
2. Якщо ми отримали рівняння 0 = 0, то усі значення змінних, сумісні із даним вектором, є розв'язком для даного рівняння. Виконується перехід до аналізу наступного рівняння.

3. Якщо поточне рівняння можна представити у вигляді $x_j g(x_1,...,x_n)=1$, то робиться висновок, що $x_j=1$.
4. Якщо поточне рівняння можна представити у вигляді $(1-x_j)g(x_1,...,x_n)=1$, то робиться висновок, що $x_j=0$.
5. Якщо перераховані умови не виконуються для жодного з рівнянь та у векторі стану присутнє, щонайменше, одне значення «2» (тобто $x_k=2$ для деякого індексу k), то вектор стану $(x_1,...,x_n)$ замінюється на два вектори, в яких значення k-ї координати дорівнює «0» та «1» відповідно.

Експериментальні результати. У даному дослідженні ми розглядаємо випадок, у якому функції f_i є квадратичними:

$$f_i(x_1,...,x_n)=a_i+\sum_{k=1}^{n}b_{ik}x_k+\sum_{k,l=1}^{n}c_{ikl}x_kx_l;i=1,...,m \qquad (2)$$

де $a_i,b_{ik},c_{ikl}\in\{0,1\}$. Не втрачаючи загальності розглядання, можна припустити, що $c_{ij}=0,i\geq j$.

На початку роздивимось простий приклад, що являє собою систему із одного рівняння з трьома змінними:

$$x_1+x_2+x_1x_2+x_1x_3+x_2x_3+1=0. \qquad (3)$$

Діаграма розв'язання рівняння (3) за допомогою запропонованого алгоритму зображена на рисунку. Як видно, отриманими розв'язками рівняння (3) є $\{x_1=0,x_2=1,x_3=0\}$, $\{x_1=1,x_2=0,\ x_3=0\}$, $\{x_1=1,x_2=1\}$ (для останнього розв'язку третя координата може приймати довільне значення). Також зазначимо, що кількість гілок (тобто підстановок) в дереві складає 4, що є меншим, ніж для прямого перебору розв'язків ($2^3=8$).

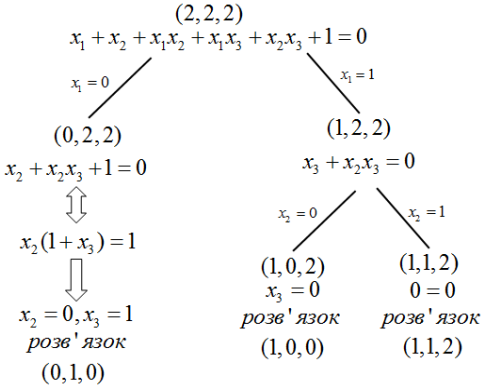

Рисунок. *Діаграма роботи методу при розв'язанні рівняння* (3)

Зазначимо, що якщо додати до системи (3) ще одне рівняння

$$\begin{cases} x_1 + x_2 + x_1x_2 + x_1x_3 + x_2x_3 + 1 = 0; \\ x_1 + x_2 + x_3 + x_1x_2 = 0, \end{cases}$$

то ми отримуємо лише один розв'язок $\{x_1 = 1, x_2 = 1, x_3 = 1\}$ за рахунок усього двох підстановок.

Як інший приклад розглянемо систему (2) з коефіцієнтами, що з рівною ймовірністю приймають значення «0» та «1». Залежність кількості розв'язків (N_s) та кількості підстановок алгоритму (N_b) від параметрів $m = 16,\ n = 16$ наведено у табл. 1.

Таблиця 1

(m, n)	N_b	N_s
(16,16)	12193	1
(12,16)	13133	15
(8,16)	12985	271
(8,16)	12985	271

Зазначимо, що кількість гілок (підстановок) у будь-якому випадку є меншою, ніж для прямого перебору розв'язків ($2^{16} = 65536$).

Тепер розглянемо випадок розрідженої матриці $C = \{c_{ikl}\}$ із формули (2). Коефіцієнт заповнення розрідженої матриці становив 2.6 %. Залежність кількості розв'язків та кількості підстановок алгоритму від параметрів (m, n) наведено у табл. 2.

Таблиця 2

(m, n)	N_b	N_s
(16,16)	2735	1
(12,16)	2185	11
(8,16)	6575	242

У цьому випадку ми також спостерігаємо, що кількість гілок (підстановок) у будь-якому випадку є меншою, ніж для прямого перебору розв'язків ($2^{16} = 65536$). Залежність кількості розв'язків (N_s) та кількості підстановок алгоритму (N_b) від параметрів $m = 16, n = 16$ наведено у табл. 2.

Висновки. У статті запропоновано метод розв'язування бітових рівнянь, що базується на методології гілок та границь (branch-and-bound), а також алгоритм, що реалізує послідовність дій, необхідну для реалізації запропонованого методу. Наведено чисельні приклади, що демонструють роботу методу при розв'язанні систем бітових рівнянь у випадку квадратичних нелінійностей. Показано, що метод

має перевагу у кількості операцій перед метод прямого перебору можливих розв'язків системи рівнянь.

Метод може бути узагальнений для розв'язання рівнянь над полями $GF(n), n > 2$.

Подяка. Семенов В. Ю. висловлює подяку професору Віденського університету А. Ноймайеру за важливі поради при виконанні цього дослідження.

Список використаних джерел:

1. Лидл Р., Нидеррайтер Г. Конечные поля: Т. 1. Пер. с англ. М.: Мир, 1988. 430 с.
2. Faugère J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). *Proc. Int. Symp. Symbolic and Algebraic Computation*. N.-Y., 2002. P. 75–83.
3. Neumaier A. Complete Search in Continuous Global Optimization and Constraint Satisfaction. *Acta Numerica*. 2004. P. 383–408.
4. Семенов В. Метод нахождения всех корней системы нелинейных алгебраических уравнений, основанный на операторе Кравчика. *Кибернетика и системный анализ.* 2015. Вып. 51, № 5. С. 169–175.

METHOD FOR THE SOLUTION OF SYSTEMS OF BIT EQUATIONS BASED ON BRANCH-AND-BOUND PRINCIPLE

Solution of systems of bit equations is an important task for the cryptography, theory of error-correction coding, information coding, robotechnics, astrophysics and other fields. In this paper we propose a method for the solution of bit equations based on the branch-and-bound methodology. The proposed methodology was already used by the authors for the solution of systems of nonlinear algebraic equations. The method can be applied not just for the systems of bit equations, but also for the equations over arbitrary finite Galois field *GF*(*n*). The important feature of proposed method is that it allows to find all solutions of system of bit equations for any combination of number of equations and number of variables. The algorithm for the implementation of the proposed method is given. The algorithm performs subsequent decreasing of the order of the system (i. e. number of variables). The proposed methodology is close to the method of Constrained Propagation which is used for the solution of the systems of nonlinear equations and global minimization tasks. Numerical examples demonstrating the application of the method to the solution of systems of quadratic bit equations is also shown. Different combinations of the number of variables and the number of equations are considered. It is shown that the method has advantage over the direct search approach for the solution of the system of bit equations.

Key words: *bit equations, branch-and-bound.*

Одержано 14.01.2019