УДК 51.681.3

С.Л. КРЫВЫЙ

КОМБИНАТОРНЫЙ МЕТОД РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ ОГРАНИЧЕНИЙ

Аннотация. Рассмотрены комбинаторный метод построения базиса множества решений систем линейных ограничений в области действительных чисел и улучшенный метод построения минимального порождающего множества решений в области натуральных чисел. Дан краткий обзор этих методов в других дискретных областях.

Ключевые слова: линейные ограничения, линейные диофантовые ограничения, базис множества решений.

ВВЕДЕНИЕ

В настоящей работе приводится краткий обзор фактов, связанных с решением проблемы выполнимости множества ограничений, а также алгоритмов построения базиса множества решений систем линейных ограничений и минимального порождающего множества решений в области действительных и натуральных чисел соответственно. Статья является продолжением работ [1–8]. В основе рассматриваемых алгоритмов лежит *TSS*-метод построения минимального порождающего множества решений систем линейных однородных диофантовых уравнений в множестве натуральных чисел N [1]. К такого рода системам и методам их решений сводятся задачи проектирования компьютерных сетей, математических игр [9, 10], криптографии [11], ассоциативно-коммутативной унификации [12], распараллеливания циклов [13] и многие другие задачи.

Известно, что процесс решения систем линейных неоднородных уравнений или системы линейных однородных и неоднородных неравенств может быть сведен к решению систем линейных однородных уравнений (СЛОУ), основное место которым уделено в настоящей статье. Следует заметить, что в общем случае такое сведение увеличивает размерность пространства, что сказывается на эффективности вычислений.

ПРОБЛЕМА ВЫПОЛНИМОСТИ СИСТЕМЫ ОГРАНИЧЕНИЙ

Основным понятием, необходимым для формулировки проблемы выполнимости, является понятие n-арного отношения, заданного на некотором множестве D. Множество всех отношений на D обозначим R_D.

Языком ограничений L на D называется некоторое непустое множество $L \subseteq R_D$.

Определение 1. Для произвольного множества D и произвольного языка ограничений L на D проблемой выполнимости ограничений (Constraint Satisfaction Problem) $CSP(L)$ называется решение следующей комбинаторной проблемы [14].

Дана тройка $P = (V, D, C)$, в которой V — множество переменных, C — конечное множество ограничений $\{C_1, \ldots, C_p\}$, каждое ограничение $C_i \in C$ — это пара (s_i, R_i), где s_i — n-ка переменных длины n, а $R_i \in L$ — n_i-арное отношение на D, называемое отношением ограничения.

Определить, существует ли решение ограничения, т.е. функция $\varphi : V \to D$ такая, что $\forall (s, R) \in C$, где $s = (v_1, \ldots, v_n)$, n-ка $(\varphi(v_1), \ldots, \varphi(v_n)) \in R$, и если существует, то какая сложность нахождения такого решения?

Множество D в этом случае называется областью проблемы. Множество всех решений CSP вида $P = (V, D, C)$ обозначается $\mathrm{Sol}(P)$.

Если множество D является множеством действительных чисел $\mathcal{R}$ или множеством рациональных чисел $\mathcal{Q}$, то такая область называется непрерывной областью. А если множество D называется дискретной областью, то оно является одним из следующих множеств: Z — множеством целых чисел, N — множеством натуральных чисел, Z_m — кольцом вычетов по модулю составного числа m, F_p — полем вычетов по модулю простого числа p или областью $\{0,1\}$.

Для того чтобы выявить вычислительную сложность CSP, необходимо определить, каким образом кодируется проблема в виде конечной последовательности символов. Предполагается, что во всех случаях представление выбрано так, что сложность определения допуска данного ограничения такой n-ки значений переменных из своей области ограничений является полиномиальной функцией от длины представления. Все сложностные оценки, приводимые ниже, относятся к арифметической модели сложности вычислений.

Определение 2. Язык ограничений L называется полиномиальным, если $CSP(L')$ может быть решена в полиномиальном времени для каждого конечного подмножества $L' \subseteq L$.

Язык ограничений L называется NP-полным, если $CSP(L')$ является NP-полной проблемой для некоторого конечного подмножества $L' \subseteq L$.

Отметим, что отношения языка ограничений L могут представляться различными способами, например системой уравнений, элементами которых являются решения этой системы.

Пусть D — произвольная область и $L = L_{\mathrm{lin}}$ — язык ограничений, состоящий из таких отношений на D, элементами которых являются все решения некоторой системы линейных уравнений над D.

Произвольное отношение из L_{lin}, а также произвольная проблема $CSP(L_{\mathrm{lin}})$ могут быть представлены некоторой системой линейных уравнений (СЛУ) над D:

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_p(x) = a_{p1}x_1 + \ldots + a_{pq}x_q = b_p. \end{cases} \tag{1}$$

Здесь $a_{ij}, b_i \in D$; $x_i \in D$, где $D \in \{\mathcal{R}, \mathcal{Q}, Z, N, \{0,1\}, F_p, Z_m\}$ — одна из областей.

Решением СЛУ называется такой вектор $c = (c_1, c_2, \ldots, c_q)$, который при подстановке вместо x_j значений c_j в $L_i(x)$ дает тождества $L_i(c) \equiv b_i$ для всех $i = 1, 2, \ldots, p$. СЛУ называется однородной (СЛОУ), если все b_i равны нулю; в противном случае СЛУ называется неоднородной (СЛНУ).

Пусть S есть СЛОУ и $e_1 = (1, 0, \ldots, 0, 0)$, $e_2 = (0, 1, \ldots, 0, 0)$, $\ldots$, $e_q = (0, 0, \ldots, 0, 1)$ — единичные векторы из множества D^q, которые называются векторами канонического базиса множества D^q. Введем на множестве D^q отношение порядка $\ll$, которое определяется следующим образом: если $x = (x_1, \ldots, x_q)$, $y = (y_1, \ldots, y_q) \in D^q$, то $x \ll y$ тогда и только тогда, когда $x_i \le y_i$ для всех $i = 1, \ldots, q$. Это отношение является частичным порядком.

Пусть M — множество решений системы S. Поскольку эта система однородная, то нулевой вектор всегда является ее решением. Это решение будем называть тривиальным, а любое решение системы S, отличное от тривиального, назовем нетривиальным решением.

СЛОУ S назовем несовместной, если множество M состоит только из тривиального решения, в противном случае систему назовем совместной.

Рассмотрим краткий обзор языков линейных ограничений над непрерывными и дискретными областями.

СИСТЕМЫ ЛИНЕЙНЫХ ОГРАНИЧЕНИЙ НАД ПОЛЕМ $\mathcal{R}$

Однородные уравнения. Пусть дано линейное однородное уравнение (ЛОУ)

$$a_1x_1 + a_2x_2 + \ldots + a_qx_q = 0, \tag{2}$$

где $a_i \in R,\ i = 1, 2, \ldots, q$.

Не ограничивая общности, предположим, что $a_1 \neq 0$, тогда, комбинируя этот коэффициент с остальными, построим множество векторов

$$s_1 = (a_2, -a_1, 0, 0, \ldots, 0, 0),\ s_2 = (a_3, 0, -a_1, 0, \ldots, 0, 0), \ldots,$$

$$s_{q-2} = (a_{q-1}, 0, 0, 0, \ldots, -a_1, 0),\ s_{q-1} = (a_q, 0, 0, 0, \ldots, 0, -a_1).$$

Очевидно, что построенные векторы являются решениями уравнения (2). Если некоторые коэффициенты в ЛОУ равны нулю, то это множество векторов, которое будем называть *TSS*-множеством, пополняется соответствующими векторами канонического базиса.

Лемма 1. *TSS*-множество является базисом множества решений уравнения (2). Сложность построения *TSS*-множества пропорциональна величине q^2.

Доказательство. Пусть $s = (b_1, b_2, \ldots, b_q)$ — произвольное решение (2), тогда

$$s + \frac{b_2}{a_1}s_1 + \frac{b_3}{a_1}s_2 + \ldots + \frac{b_q}{a_1}s_{q-1} = \left(b_1 + \frac{a_2b_2 + a_3b_3 + \ldots + a_qb_q}{a_1}, 0, 0, \ldots, 0\right) =$$

$$= \left(\frac{a_1b_1 + a_2b_2 + a_3b_3 + \ldots + a_qb_q}{a_1}, 0, 0, \ldots, 0\right) = (0, 0, \ldots, 0).$$

Отсюда получаем

$$s = -\frac{b_2}{a_1}s_1 - \frac{b_3}{a_1}s_2 - \ldots - \frac{b_q}{a_1}s_{q-1}.$$

Таким образом, в силу произвольности s *TSS*-множество является базисом множества решений (2).

Сложность построения одной комбинации требует q шагов, а всех таких векторов $q-1$. Следовательно, сложность построение всего *TSS*-множества составляет $O(q^{2)}$.

Лемма доказана.

Пример 1. Найти базис множества решений ЛОУ

$$1{,}2x_1 + 1{,}5x_2 + 0{,}7x_3 + 0{,}4x_4 = 0.$$

Согласно доказанному выше этот базис составляют векторы

$$s_1 = (1{,}5; -1{,}2; 0; 0),\ s_2 = (0{,}7; 0; -1{,}2; 0),\ s_3 = (0{,}4; 0; 0; -1{,}2).$$

Так, решение $s = (4; -1; 1; -10)$ в этом базисе имеет представление

$$s = \frac{1}{1{,}2}s_1 - \frac{1}{1{,}2}s_2 + \frac{10}{1{,}2}s_3.$$

Системы однородных уравнений. Пусть дана СЛОУ S вида (1). Рассмотрим множество векторов канонического базиса $M_0' = \{e_1, \ldots, e_n\}$ и первое урав-

нение $L_1(x) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q = 0$ системы S. Построим базис $B_1 = \{e_1, \ldots, e_m\}$ множества всех решений этого ЛОУ описанным выше способом. Возьмем функцию $L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q$ и рассмотрим ЛОУ вида

$$L_2(e_1)y_1 + L_2(e_2)y_2 + \ldots + L_2(e_m)y_m = 0. \tag{3}$$

Заметим, что если все $L_2(e_i) = 0$, то уравнение $L_2(x) = 0$ из (1) линейно выражается через $L_1(x)$ и его можно удалить из СЛОУ S. Поэтому будем предполагать, что все уравнения в S линейно независимы.

Найдем базис $B' = \{r_1, r_2, \ldots, r_{m-1}\}$ множества решений ЛОУ (3) вышеописанным способом и построим по векторам из B' соответствующие комбинации векторов из B_1. Обозначим это множество $M = \{s_1, s_2, \ldots, s_{m-1}\}$.

Лемма 2. Множество M является базисом множества решений СЛОУ

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = 0. \end{cases} \tag{4}$$

Доказательство. Очевидно, что все элементы из M являются решениями СЛОУ S. Пусть $x = (x_1, \ldots, x_q)$ — произвольное решение СЛОУ (4), тогда в силу леммы 1

$$x = d_1e_1 + \ldots + d_me_m,$$

где $e_i \in B_1$, $i = 1, \ldots, m$. Подставляя x в $L_2(x)$ из (4), получаем ЛОУ

$$d_1L_2(e_1) + \ldots + d_mL_2(e_m) = c_1d_1 + \ldots + c_md_m = 0, \tag{5}$$

т.е. вектор $(d_1, d_2, \ldots, d_m)$ является решением ЛОУ (5) и, следовательно, он представляется в виде неотрицательной линейной комбинации векторов из B':

$$(d_1, \ldots, d_m) = f_1r_1 + \ldots + f_{m-1}r_{m-1}.$$

Но тогда

$$x = d_1e_1 + \ldots + d_me_m = f_1's_1 + \ldots + f'_{m-1}s_{m-1},$$

а это значит, что x представляется в виде неотрицательной линейной комбинации векторов из M. В силу произвольности вектора x получаем справедливость леммы.

Теорема 1. Пусть M — *TSS*-множество, построенное описанным выше способом для СЛОУ S. Тогда M является базисом множества всех решений этой СЛОУ.

Сложность построения базиса пропорциональна величине pq^2, где p — число уравнений, а q — количество неизвестных в СЛОУ.

Доказательство проводится индукцией по числу k уравнений в СЛОУ S.

Базис индукции ($k = 2$) имеет место в силу леммы 2. Предположим, что теорема справедлива для всех $k < p$. Тогда *TSS*-множество решений СЛОУ S', состоящей из первых $p-1$ уравнения, в силу предположения индукции является базисом множества решений S'.

Повторяя рассуждения, аналогичные используемым при доказательстве леммы 2, имеем справедливость утверждения теоремы. Оценка временной сложности, приведенная в формулировке теоремы, очевидным образом вытекает из построений *TSS*-множества и леммы 1.

Теорема доказана.

Пример 2. Найти базис множества решений СЛОУ

$$S = \begin{cases} 2{,}1x_1 + 1{,}1x_2 + 0x_3 + x_4 + 2{,}3x_5 = 0, \\ 0{,}5x_1 + 0{,}2x_2 + 1x_3 + 0x_4 - 1{,}3x_5 = 0, \\ 0{,}1x_1 + 0x_2 + 2{,}5x_3 + 2x_4 + 0x_5 = 0. \end{cases}$$

Решение. Базисом множества решений первого ЛОУ этой системы является

$$s_1 = (1{,}1; -2{,}1; 0; 0; 0),\ s_2 = (0; 0; 1; 0; 0),$$

$$s_3 = (1; 0; 0; -2{,}1; 0),\ s_4 = (2{,}3; 0; 0; 0; -2{,}1).$$

Находим $L_2(s_1) = 0{,}13$, $L_2(s_2) = 1$, $L_2(s_3) = 0{,}5$, $L_2(s_4) = 3{,}88$ и строим ЛОУ $0{,}13\,y_1 + 1\,y_2 + 0{,}5\,y_3 + 3{,}88\,y_4 = 0$. Базис множества решений этого ЛОУ состоит из векторов $r_1 = (1; -0{,}13; 0; 0)$, $r_2 = (0{,}5; 0; -0{,}13; 0)$, $r_3 = (3{,}88; 0; 0; -0{,}13)$. Получаем векторы множества решений для первых двух уравнений из S, соответствующие векторам r_1, r_2, r_3:

$$s'_1 = s_1 - 0{,}13 s_2 = (1{,}1; -2{,}1; -0{,}13; 0; 0),$$

$$s'_2 = 0{,}5 s_1 - 0{,}13 s_3 = (0{,}42; -1{,}05; 0; 0{,}273; 0),$$

$$s'_3 = 3{,}88 s_1 - 0{,}13 s_4 = (3{,}969; -8{,}148; 0; 0; 0{,}273).$$

Находим значения $L_3(s'_1) = -0{,}215$, $L_3(s'_2) = 0{,}588$, $L_3(s'_3) = 0{,}3969$, строим ЛОУ $0{,}215\,y_1 + 0{,}588\,y_2 + 0{,}3969\,y_3 = 0$ и получаем его решения: $r'_1 = (0{,}588; 0{,}215; 0)$, $r'_2 = (0{,}3969; 0; 0{,}215)$. Строим соответствующие им векторы базиса множества решений СЛОУ S

$$m_1 = 0{,}588 s'_1 + 0{,}215 s'_2 = (0{,}7371; -1{,}46055; -0{,}7644; 0{,}058695; 0),$$

$$m_2 = 0{,}3969 s'_1 + 0{,}215 s'_3 = (1{,}289925; -2{,}58531; -0{,}051597; 0;\ 0{,}058695).$$

Системы неоднородных уравнений. Пусть дано СЛНУ вида (1). С использованием метода решения СЛОУ приведем СЛНУ (1) к виду

$$S' = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - b_1 x_0 = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - b_2 x_0 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_p(x) = a_{p1}x_1 + \ldots + a_{pq}x_q - b_p x_0 = 0. \end{cases} \tag{6}$$

Пусть $B = \{s_1, s_2, \ldots, s_m\}$ — базис множества решений СЛОУ (6). Разобъем множество B на два подмножества:

$$B_0 = \{s_i \in B : s_i = (d_{i1}, d_{i2}, \ldots, d_{iq}, 0)\},$$

$$B_1 = \{s_j \in B : s_j = (d_{j1}, d_{j2}, \ldots, d_{jq}, d)\},$$

где $d \neq 0$. Если множество B_1 не имеет вектора, в котором $d = 1$, то разделим все координаты вектора $s_j \in B_1$ на число d. Получим вектор $s'_j = \left(\frac{d_{j1}}{d}, \frac{d_{j2}}{d}, \ldots, \frac{d_{jq}}{d}, 1\right)$. Тогда общее решение СЛНУ (1) примет вид

$$x = s''_j + c_1 s'_{i1} + \ldots + c_r s'_{ir},$$

где $s''_j = \left(\frac{d_{j1}}{d}, \frac{d_{j2}}{d}, \ldots, \frac{d_{jq}}{d}\right)$ — частное решение СЛНУ из (1), а $s'_i = (d_{i1}, d_{i2}, \ldots, d_{iq})$ образуются из векторов множества B_0 путем отбрасывания последней координаты.

Действительно, множество B_0 составляют векторы, являющиеся базисом множества всех решений СЛОУ, которая соответствует СЛНУ (1) в силу теоремы 1. Векторы из множества B_1 — это частные решения такой СЛНУ. По любому вектору этого множества в случае необходимости строим вектор s''_j. Однако стоит обратить внимание на порядок построения векторов из множества B. Проиллюстрируем это на примере.

Пример 3. Построим множество решений СЛНУ

$$S' = \begin{cases} L'_1(x) = -3x - 4y + 5z - 6u = 2, \\ L'_2(x) = 2x + 3y - 2z + u = -1, \\ L'_3(x) = x - y - z + 2u = 1. \end{cases}$$

СЛОУ S для системы S' принимает вид

$$S = \begin{cases} L_1(x) = -3x - 4y + 5z - 6u - 2x_0 = 0, \\ L_2(x) = 2x + 3y - 2z + u + x_0 = 0, \\ L_3(x) = x - y - z + 2u - x_0 = 0. \end{cases}$$

Строим базис множества решений СЛОУ S приведенным выше методом. Для первого уравнения системы TSS-множество состоит из таких векторов:

$$s_1 = (-4, 3, 0, 0, 0),\ s_2 = (5, 0, 3, 0, 0),\ s_3 = (-2, 0, 0, 1, 0),\ s_4 = (-2, 0, 0, 0, 3).$$

Заметим, что первые три вектора составляют базис множества решений ЛОУ, соответствующего первому уравнению системы S', а последний вектор, преобразованный к виду $(-2/3, 0, 0, 0, 1)$, — частное решение этого уравнения. Если упорядочивать векторы-решения СЛОУ S на каждом шаге вычислений так, чтобы вначале стояли векторы-решения соответствующей СЛОУ для S', то это непосредственно приводит к базису множества решений без дополнительных преобразований построенных векторов.

Следуя этому порядку, находим значения $L_2(x)$ на векторах s_1, s_2, s_3, s_4: 1, 4, -3, -1, откуда получаем уравнение $w_1 + 4w_2 - 3w_3 - w_4 = 0$. Решения этого уравнения имеют вид $(4, -1, 0, 0)$, $(-3, 0, -1, 0)$, $(-1, 0, 0, -1)$. Этим решениям соответствуют решения системы первых двух уравнений (после сокращения на НОД их координат)

$$s'_1 = 4s_1 - s_2 = (-7, 4, -1, 0, 0),$$

$$s'_2 = -3s_1 - s_3 = (14, -9, 0, -1, 0),$$

$$s'_3 = -s_1 - s_4 = (2, -1, 0, 0, -1).$$

Значения $L_3(x)$ на этих векторах равны -10, 21, 4, откуда получаем уравнение $-10w_1 + 21w_2 + 4w_3 = 0$. Решения этого уравнения имеют вид $(21, 10, 0)$, $(4, 0, 10)$. Этим решениям соответствуют решения всей системы (после сокращения на -1, т.е. НОД их координат): $(7, 6, 21, 10, 0)$, $(4, -3, 2, 0, 5)$.

Таким образом, базис множества решений СЛНУ состоит из векторов $B_0 = \{s_1 = (7, 6, 21, 10, 0)\}$ и $B_1 = \{s_2 = (4, -3, 2, 0, 5)\}$. Тогда $s''_2 = \left(\frac{4}{5}, -\frac{3}{5}, \frac{2}{5}, 0\right)$ — частное решение СЛНУ. Следовательно, общее решение имеет вид $x = s''_2 + cs'_1$, где $c \in \mathcal{R}$ — произвольное число, а $s'_1 = (7, 6, 21, 10)$.

СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Системы линейных однородных неравенств (СЛОН). Рассмотрим СЛОН

$$S' = \begin{cases} L'_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q \geq 0, \\ L'_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q \geq 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L'_p(x) = a_{p1}x_1 + \ldots + a_{pq}x_q \geq 0. \end{cases} \tag{7}$$

Преобразуем эту систему к СЛОУ, вводя p дополнительных неизвестных:

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - y_1 = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - y_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_p(x) = a_{p1}x_1 + \ldots + a_{pq}x_q - y_p = 0. \end{cases}$$

Построим базис B множества решений этой СЛОУ, следуя порядку генерации, определенному выше, и разобьем это множество на два подмножества: $B_0 = \{s_1, \ldots, s_k\}$ и $B_1 = \{r_1, \ldots, r_m\}$. Включаются в первое подмножество векторы, последние p координат которых равны нулю, а во второе подмножество — векторы, последние p координат которых неотрицательны. Отбрасывая в векторах подмножеств B_0 и B_1 последние p координат, получаем базис множества решений исходной СЛОН.

Пример 4. Построим множество решений СЛОН

$$S' = \begin{cases} L'_1(x) = -3x - 4y + 5z - 6u \geq 0, \\ L'_2(x) = 2x + 3y - 2z + u \geq 0, \\ L'_3(x) = x - y - z + 2u \geq 0. \end{cases}$$

СЛОУ S для системы S' принимает вид

$$S = \begin{cases} L_1(x) = -3x - 4y + 5z - 6u - y_1 + 0 + 0 = 0, \\ L_2(x) = 2x + 3y - 2z + u + 0 - y_2 + 0 = 0, \\ L_3(x) = x - y - z + 2u + 0 + 0 - y_3 = 0. \end{cases}$$

Строим базис множества решений СЛОУ S' приведенным выше методом. Для первого уравнения системы *TSS*-множество состоит из таких векторов:

$$(-4, 3, 0, 0, 0, 0, 0),\ (5, 0, 3, 0, 0, 0, 0),\ (-6, 0, 0, 3, 0, 0, 0),$$

$$(-1, 0, 0, 0, 3, 0, 0),\ (0, 0, 0, 0, 0, 1, 0),\ (0, 0, 0, 0, 0, 0, 1).$$

Первые три вектора составляют базис множества решений ЛОУ, соответствующего первому неравенству системы S, а последние три вектора представляют частные решения первого неравенства этой системы.

Следуя установленному выше порядку решений, находим значения $L_2(x)$ на этих векторах: $1, 4, -9, -2, -1, 0$, откуда получаем уравнение $w_1 + 4w_2 - 9w_3 - 2w_4 - w_5 + 0w_6 = 0$. Решения этого уравнения имеют вид $(4, -1, 0, 0, 0, 0)$, $(9, 0, 1, 0, 0, 0)$, $(2, 0, 0, 1, 0, 0)$, $(1, 0, 0, 0, 1, 0)$, $(0, 0, 0, 0, 0, 1)$. Им соответствуют такие решения системы первых двух уравнений (после сокращения на их НОД):

$$(-7, 4, -1, 0, 0, 0, 0),\ (14, -9, 0, -1, 0, 0, 0),\ (-3, 2, 0, 0, 1, 0, 0),$$

$$(-4, 3, 0, 0, 0, 1, 0),\ (0, 0, 0, 0, 0, 0, 1).$$

Значения $L_3(x)$ на этих векторах равны $-10, 21, -5, -7, -1$. Отсюда получаем уравнение $-10w_1 + 21w_2 - 5w_3 - 7w_4 - w_5 = 0$. Решения этого уравнения имеют вид $(21, 10, 0, 0, 0)$, $(-1, 0, 2, 0, 0)$, $(-7, 0, 0, 10, 0)$, $(-1, 0, 0, 0, 10)$. Им соответствуют следующие решения:

$$(7, 6, 21, 10, 0, 0, 0),\ (1, 0, 1, 0, 2, 0, 0),$$

$$(9, 2, 7, 0, 0, 10, 0),\ (7, -4, 1, 0, 0, 0, 10).$$

В результате получаем

$$B_0 = \{(7, 6, 21, 10, 0, 0, 0)\},$$

$$B_1 = \{(1, 0, 1, 0, 2, 0, 0),\ (9, 2, 7, 0, 0, 10, 0),\ (7, -4, 1, 0, 0, 0, 10)\}.$$

Базис множества решений всей системы имеет вид

$$(7, 6, 21, 10),\ (1, 0, 1, 0),\ (9, 2, 7, 0),\ (7, -4, 1, 0).$$

Системы линейных неоднородных неравенств (СЛНН). СЛНН сводится к СЛОУ путем введения $p+1$ дополнительных неизвестных, где p — количество неравенств в СЛНН. Пусть имеем СЛНН

$$S' = \begin{cases} L'_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q \geq b_1, \\ L'_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q \geq b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L'_p(x) = a_{p1}x_1 + \ldots + a_{pq}x_q \geq b_p. \end{cases}$$

Этой СЛНН соответствует СЛОУ вида

$$S = \begin{cases} L'_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - y_1 - b_1x_0 = 0, \\ L'_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - y_2 - b_2x_0 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L'_p(x) = a_{p1}x_1 + \ldots + a_{pq}x_q - y_p - b_px_0 = 0. \end{cases}$$

Построим базис B множества решений СЛОУ S и его подмножества B_0 и B_1. Если в множестве B_1 нет векторов, в которых последние $p+1$ координат имеют разные знаки, то СЛНН S' совместна. Действительно, поскольку значения дополнительных неизвестных должны быть неотрицательными, то получить такие решения из векторов множества B_1 невозможно. Если же такие векторы имеются, то СЛНН совместна.

Построение базиса множества решений СЛОН без введения дополнительных неизвестных. При введении дополнительных неизвестных, как отмечалось ранее, увеличивается размерность векторов-решений, что сказывается на эффективности вычислений. Анализ процесса построения базиса множества решений СЛОН показывает, что явно вводить дополнительные p неизвестных нет необходимости, но для правильности построения базиса множества решений СЛОН необходимо вводить дополнительно всего два векторы той же размерности, что и размерность СЛОН. Объясним это на примере.

Пример 5. Рассмотрим СЛОН из примера 4:

$$S' = \begin{cases} L'_1(x) = -3x - 4y + 5z - 6u \geq 0, \\ L'_2(x) = 2x + 3y - 2z + u \geq 0, \\ L'_3(x) = x - y - z + 2u \geq 0. \end{cases}$$

Строим *TSS*-решения для первого неравенства $L'_1(x) \geq 0$:

$$(-4, 3, 0, 0),\ (5, 0, 3, 0),\ (-6, 0, 0, 3).$$

Дополним это множество двумя векторами вида $(-1, 0, 0, 0)$ и $(0, 0, 0, 0)$ и получим множество векторов

$$(-4, 3, 0, 0),\ (5, 0, 3, 0),\ (-6, 0, 0, 3),$$
$$(-1, 0, 0, 0),\ (0, 0, 0, 0).$$

Заметим, что первые три вектора составляют базис множества решений ЛОУ, соответствующего первому неравенству системы S, четвертый — частное решение первого ЛНУ этой системы, пятый — заготовка на следующее неравенство.

Следуя установленному выше порядку решений, находим значения $L_2'(x)$ на первых четырех векторах: 1, 4, -9, -2, а на нулевом векторе значению $L_2'(x)$ приписываем -1. В результате получаем уравнение $w_1 + 4w_2 - 9w_3 - 2w_4 - w_5 = 0$. Решения этого уравнения имеют вид $(4, -1, 0, 0, 0)$, $(9, 0, 1, 0, 0)$, $(2, 0, 0, 1, 0)$, $(1, 0, 0, 0, 1)$. Этим решениям соответствуют решения системы первых двух неравенств (после сокращения на их НОД):

$$(-7, 4, -1, 0),\ (14, -9, 0, -1),\ (-3, 2, 0, 0),\ (-4, 3, 0, 0).$$

Поскольку $L_3'(x) \geq 0$ — последнее неравенство в системе, то дополняем эти векторы только одним: $(-1, 0, 0, 0)$, так как заготовки на следующее неравенство делать не следует. Находим значения $L_3'(x)$ таким же образом: $-10, 21, -5, -7, -1$. В результате получаем уравнение $-10w_1 + 21w_2 - 5w_3 - 7w_4 - w_5 = 0$. Решения этого уравнения имеют вид $(21, 10, 0, 0, 0)$, $(-1, 0, 2, 0, 0)$, $(-7, 0, 0, 10, 0)$, $(-1, 0, 0, 0, 10)$, а им соответствуют решения

$$(7, 6, 21, 10),\ (1, 0, 1, 0),\ (9, 2, 7, 0, 0),\ (7, -4, 1, 0).$$

В результате получаем базис множества решений всей системы:

$$(7, 6, 21, 10),\ (1, 0, 1, 0),\ (9, 2, 7, 0),\ (7, -4, 1, 0).$$

Если проследить порядок построения базиса, то можно заметить, что решение $(7, 6, 21, 10)$ есть решением СЛОУ, которая соответствует СЛОН, а остальные решения — это частные решения СЛОН.

Резюмируя этот способ, отметим, что дополнительные векторы и значения на этих векторах фигурируют во всех неравенствах, кроме последнего. При обработке последнего неравенства к *TSS*-решениям первых $p-1$ неравенств добавляется только один вектор, имеющий первую координату -1, а остальные координаты нулевые.

СИСТЕМЫ ЛИНЕЙНЫХ ОГРАНИЧЕНИЙ В МНОЖЕСТВЕ НАТУРАЛЬНЫХ ЧИСЕЛ

Системы линейных ограничений над областью N рассматривались во многих публикациях в связи с важностью методов решения такого типа ограничений [16–22]. *TSS*-метод построения минимального порождающего множества решений (*TSS*-множества) систем линейных однородных диофантовых уравнений (СЛОДУ) был предложен в работе [1]. Напомним кратко суть этого метода и одну из модификаций, улучшающую его быстродействие.

Метод построения *TSS*-множества для СЛОДУ, используемый здесь, и алгоритм его реализации подробно описаны в работах [1, 2, 15], поэтому приведем лишь необходимые сведения.

Пусть дана СЛОДУ вида (1). Рассмотрим множество векторов канонического базиса $M_0' = \{e_1, \ldots, e_q\}$ и первое уравнение $L_1(x) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q = 0$ системы S. С помощью функции $L_1(x)$ разобьем элементы множества M_0' на три группы: $M_1^0 = \{e^0 \mid L_1(e^0) = 0\}$, $M_1^+ = \{e^+ \mid L_1(e^+) > 0\}$ и $M_1^- = \{e^- \mid L_1(e^-) < 0\}$. Очевидно, что если одно из множеств (например, $M_1^0 \cup M_1^+$ или $M_1^0 \cup M_1^-$) пусто, то уравнение $L_1(x) = 0$ не имеет нетривиальных решений в множестве натуральных чисел. Допустим, что два из множеств M_1^0, M_1^+, M_1^- непусты. Тогда рассмотрим множество

$$M_1' = M_1^0 \cup \{e_{ij} \mid e_{ij} = -L_1(e_i)e_j + L_1(e_j)e_i,\ e_j \in M_1^+, e_i \in M_1^-\}.$$

Используя функцию $L_2(x)$, разобьем элементы множества M'_1, как и множества M'_0, на три группы: $M_2^0 = \{e^0 \mid L_2(e^0) = 0\}$, $M_2^+ = \{e^+ \mid L_2(e^+) > 0\}$ и $M_2^- = \{e^- \mid L_2(e^-) < 0\}$. Допустим, что хотя бы два из этих множеств непусты. Тогда построим множество

$$M'_2 = M_2^0 \cup \{e_{ij} \mid e_{ij} = -L_2(e_i)e_j + L_2(e_j)e_i,\ e_j \in M_2^+,\ e_i \in M_2^-\}.$$

Предположим, что таким способом построено множество M'_j из множеств $M_j^0 = \{e_r^0 \mid L_j(e_r^0) = 0\}$, $M_j^+ = \{e_i^+ \mid L_j(e_i^+) > 0\}$ и $M_j^- = \{e_s^- \mid L_j(e_s^-) < 0\}$ с помощью функции $L_j(x)$ и это множество непусто. Непосредственно из этих построений вытекает следующее утверждение [1, 2].

Теорема 2. Элементы множества M'_j являются решениями системы уравнений $L_1(x) = 0 \,\&\, L_2(x) = 0 \,\&\, \ldots \,\&\, L_j(x) = 0$.

Из этой теоремы следует определение.

Определение 3. Множество M'_j назовем усеченным множеством решений системы $S' = L_1(x) = 0 \,\&\, L_2(x) = 0 \,\&\, \ldots \,\&\, L_j(x) = 0$.

Пусть $M'_j = \{e'_1, \ldots, e'_k\}$ — усеченное множество решений системы S', а M_j — множество всех ее решений. Тогда имеет место следующее утверждение.

Теорема 3. Для любого вектора $x \in M_j \setminus M'_j$ существует представление в виде неотрицательной линейной комбинации вида

$$tx = b_1 e'_1 + \ldots + b_l e'_k, \tag{8}$$

где $t, b_i \in N$, $t \neq 0$, $e'_i \in M'_j$, $i = 1, \ldots, k$.

Из этой теоремы вытекает критерий проверки совместности СЛОДУ.

Теорема 4. Система $S = L_1(x) = 0 \,\&\, L_2(x) = 0 \,\&\, \ldots \,\&\, L_{p-1}(x) = 0 \,\&\, L_p(x) = 0$ совместна тогда и только тогда, когда $M'_p \neq \varnothing$.

Заметим, что каждый вектор усеченного множества решений можно разделить на НОД его координат, если этот НОД отличен от единицы. Это позволяет уменьшить величину координат этих векторов и более эффективно проводить вычисления.

Легко заметить, что усеченные множества решений зависят от порядка расположения уравнений системы. Исключение «лишних» векторов из усеченного множества решений базируется на следующей теореме.

Теорема 5. Пусть S — СЛОДУ вида (1) и M'_p — ее усеченное множество решений, состоящее из k элементов. Тогда любой вектор x из M'_p такой, что $tx \gg e'_i \in M'_p \setminus \{x\}$, $i = 1, 2, \ldots, k-1$, $t \in N$ и $t \neq 0$, имеет представление вида

$$mx = b_1 e'_1 + b_2 e'_2 + \ldots + b_{k-1} e'_{k-1},$$

где $m \in N$, $m \neq 0$, $b_i \in N$, $e_i \in M'_p$, $i = 1, 2, \ldots, k-1$.

Из этой теоремы получаем следующую простую процедуру очистки усеченного множества решений: вектор x удаляется из усеченного множества решений, если x больше или его произведение tx больше некоторого решения из оставшихся векторов усеченного множества решений. В качестве множителя t можно использовать, в частности, максимальную координату векторов текущего усеченного множества решений. Выполнение процедуры очистки гарантирует независимость результирующего *TSS*-множества от порядка следования уравнений в СЛОДУ.

Характеристику свойств усеченного множества решений СЛОДУ, построенного таким способом, дает следующее утверждение, при этом допустим, что СЛОДУ S совместна и $M' = \{e'_1, e'_2, \ldots, e'_k\}$ — ее усеченное множество решений.

Теорема 6. 1. Векторы усеченного множества решений являются минимальными решениями СЛОДУ S, т.е. ее базисными решениями.

2. Пусть $x = (x_1, x_2, \dots, x_q)$ — минимальное решение СЛОДУ S и $M' = \{e'_1 = (\alpha_{11}, \dots, \alpha_{1q}), e'_2 = (\alpha_{21}, \dots, \alpha_{2q}), \dots, e'_k = (\alpha_{k1}, \dots, \alpha_{kq})\}$ — ее усеченное множество решений. Тогда имеет место неравенство $x' = \max\limits_i x_i \le k \cdot \max\limits_{i,j} \alpha_{ij}$, где α_{ij} — координаты векторов $e'_i \in M'$, $i = 1, \dots, k$; $j = 1, 2, \dots, q$.

3. Сложность алгоритма определения совместности СЛОДУ имеет экспоненциальную сложность по числу уравнений в системе.

Поскольку результирующее *TSS*-множество решений не зависит от порядка следования уравнений в системе, то существует возможность выбора уравнения в СЛОДУ таким образом, чтобы число промежуточных векторов на каждом шаге вычислений было минимальным. Действительно, число промежуточных векторов зависит от величины $rs + k$, где r — число положительных значений, s — число отрицательных значений, k — число нулевых значений. Вычисляя значения для всех уравнений величины $rs + k$, выбираем уравнение с минимальным значением $rs + k$ (в этом случае r, s, k равны числу положительных, отрицательных и нулевых коэффициентов в уравнении) и строим для него *TSS*-множество решений. Затем на этих векторах находим значения остальных уравнений и выбираем уравнение для комбинирования с минимальным значением $rs + k$.

Проиллюстрируем этот процесс примером.

Пример 6. Рассмотрим СЛОДУ

$$S = \begin{cases} L_1(x) = 2x_1 - 1x_2 + 3x_3 + 1x_4 - 4x_5 + 2x_6 = 0, \\ L_2(x) = 1x_1 + 0x_2 - 2x_3 - 3x_4 + 2x_5 + 1x_6 = 0, \\ L_3(x) = -3x_1 + 1x_2 + 1x_3 + 0x_4 - 1x_5 + 2x_6 = 0, \\ L_4(x) = 4x_1 + 1x_2 - 1x_3 - 2x_4 + 0x_5 + 1x_6 = 0. \end{cases}$$

Если вычислять *TSS*-множество в порядке следования уравнений в системе, то число *TSS*-решений первого уравнения составит $8 = rs + k$, где $r = 4$, $s = 2$, $k = 0$ (первый столбец), для второго уравнения таких решений будет семь (второй столбец). Здесь столбцы содержат значения на *TSS*-решениях уравнений L_2, L_3, L_4 для первого выбора и L_1, L_3, L_4 — для второго выбора.

Решения $L_1(x) = 0$	L_2	L_3	L_4
(1, 2, 0, 0, 0, 0)	1	−1	6
(0, 3, 1, 0, 0, 0)	−2	4	2
(0, 1, 0, 1, 0, 0)	−3	1	−1
(0, 2, 0, 0, 0, 1)	1	4	3
(2, 0, 0, 0, 1, 0)	4	−7	8
(0, 0, 4, 0, 3, 0)	−2	1	−4
(0, 0, 0, 4, 1, 0)	−10	−1	−8
(0, 0, 0, 0, 1, 2)	4	3	2

Решения $L_2(x) = 0$	L_1	L_3	L_4
(2, 0, 1, 0, 0, 0)	7	−5	7
(0, 1, 0, 0, 0, 0)	−1	1	1
(0, 0, 1, 0, 1, 0)	−1	1	−1
(0, 2, 1, 0, 0, 2)	7	5	1
(3, 0, 0, 1, 0, 0)	7	−9	10
(0, 0, 0, 2, 3, 0)	−10	−3	−6
(0, 0, 0, 1, 0, 3)	7	6	1

На втором шаге вычислений оптимальным будет выбор четвертого уравнения, поскольку число комбинаций составляет 10, а для других уравнений — 12. Окончательное *TSS*-множество включает два решения: $(16, 15, 89, 0, 76, 10)$ и $(2, 0, 3, 5, 7, 5)$.

Проведенные эксперименты показывают, что количество промежуточных вычислений при построении минимального порождающего множества решений СЛОДУ могут существенно уменьшаться. Например, для приведенной ниже

матрицы СЛОДУ

$$\begin{vmatrix}
-1 & -1 & 1 & -2 & 0 & -3 & -4 & -5 & 3 & -1 & 4 & -3 & -1 & -4 & 1 & 4 & 4 & 2 & 4 & -3 & 5 & 0 & 4 & 3 & 2 \\
-2 & -3 & 4 & -3 & 3 & 1 & 1 & 4 & -3 & -4 & -1 & 0 & -2 & 0 & 2 & 2 & -4 & 1 & -4 & -1 & 1 & 2 & 2 & 3 & 5 \\
2 & 3 & 2 & 0 & 3 & 2 & 5 & -4 & -5 & -3 & -3 & 3 & 3 & 5 & 0 & 2 & 1 & 5 & -3 & 0 & 2 & 5 & 2 & 4 & 1 \\
4 & -1 & 4 & -3 & -3 & -3 & 2 & 1 & 3 & 4 & -4 & 4 & 2 & 2 & -3 & -4 & -2 & 3 & -2 & 2 & -5 & 4 & 3 & 2 & 4 \\
-1 & -1 & -3 & 4 & -3 & 2 & -3 & -3 & 1 & 5 & 4 & -3 & -4 & 1 & 0 & -1 & 4 & -1 & -2 & 2 & -2 & -4 & 3 & -5 & 5 \\
3 & -3 & -1 & 3 & 4 & -3 & 1 & -3 & -2 & -1 & -3 & 4 & 3 & -3 & 4 & 3 & -5 & 0 & 2 & -1 & -4 & -3 & 1 & 2 & 4 \\
-4 & 2 & 4 & -2 & 5 & 3 & -2 & 1 & 5 & -4 & -2 & 1 & 4 & 1 & 5 & -3 & 3 & 4 & 3 & -2 & 5 & 0 & 4 & -2 & -2 \\
-1 & 3 & -1 & -4 & 0 & -4 & -4 & 0 & 3 & 1 & -3 & -1 & 3 & 1 & 5 & -1 & 4 & 0 & 4 & 5 & -4 & -3 & -1 & -3 & -2 \\
0 & -1 & -3 & 1 & 0 & 4 & -3 & -2 & 1 & -2 & 5 & 0 & 5 & -1 & 3 & -4 & -4 & 1 & -4 & 0 & -1 & -3 & -1 & 0 & -5 \\
2 & -1 & 1 & -1 & -2 & 4 & -2 & -3 & 0 & 0 & -1 & 1 & 0 & -3 & -2 & 1 & 5 & 2 & -3 & -1 & -1 & -5 & -4 & 2 & -1 \\
5 & -2 & -1 & 5 & 0 & 4 & 0 & 5 & 0 & -1 & 2 & 5 & 4 & 2 & 0 & 2 & -5 & 0 & -1 & 0 & -2 & -4 & -1 & 2 & 4 \\
3 & 3 & 4 & -4 & 0 & 4 & -3 & -1 & -3 & -4 & 3 & -3 & 1 & -5 & -3 & 2 & -4 & 4 & 0 & 3 & 1 & 0 & 2 & -2 & -2 \\
2 & -4 & 3 & 4 & 5 & -3 & 2 & 1 & 2 & -2 & -4 & -5 & 1 & 2 & 0 & 3 & 2 & 4 & 0 & 1 & -2 & 4 & 3 & -2 & 2 \\
5 & 5 & -2 & -2 & -5 & 3 & -1 & 4 & 0 & 4 & 5 & -2 & -4 & 5 & 0 & -3 & -2 & 2 & 2 & -1 & 0 & -3 & 1 & -4 & -1 \\
-4 & 1 & 3 & 1 & 4 & -2 & 0 & -1 & 0 & 2 & 4 & -3 & 3 & 2 & 2 & -2 & 0 & -3 & 3 & -3 & 0 & -1 & 5 & -5 & 2
\end{vmatrix}$$

в случае использования улучшенного *TSS*-алгоритма [15] генерируется 780 тысяч комбинаций, а его применение без улучшения генерирует 35 883 тысячи комбинаций. В результате имеем такие временные характеристики: в первом случае требуется 2493 мсек, а во втором — 123 578 мсек.

Таблица

Область	Множества	Сложность *CSP*-решения	Ссылки на публикации
Непрерывная	$\mathcal{R}$	P	[23]
	$\mathcal{Q}$	P	[23]
Дискретная	N	NP	[3, 4, 5, 16]
	Z_m	NP	[7]
	$\{0,1\}$	NP	[5]
	F_p	P	[6]
	Z	P	[8]

Оценки сложности решения *CSP* алгоритмов в перечисленных выше областях отражены в таблице.

Относительно области Z_m — кольца вычетов по модулю m — заметим, что в случае разложения модуля m на простые множители сложность решения *CSP* принадлежит классу полиномиальной сложности.

ЗАКЛЮЧЕНИЕ

Приведенные оценки временных сложностей алгоритмов можно уточнять, если прослеживать все детали процесса вычислений, происходящего в *TSS*-алгоритме. В настоящей статье мы ограничились установлением только верхних оценок временной сложности (т.е. сложностью решения в наихудшем случае) этих алгоритмов. При малых значениях модуля m сложностью вычисления НОД в полях и кольцах вычетов можно пренебречь, тогда оценка алгоритмов решения систем в таких полях упрощается. Так, например, в поле F_2, которое часто встречается в приложениях, необходимость вычисления НОД вообще отпадает.

Экспериментальные версии соответствующих алгоритмов построения предбазисов и базисов для перечисленных выше областей были реализованы в языке C^{++}. Эксперименты показали, что *TSS*-алгоритм над множеством натуральных чисел достаточно быстро работает в случае разреженных матриц систем.

СПИСОК ЛИТЕРАТУРЫ

1. Крывый С.Л. Критерий совместности систем линейных диофантовых уравнений над множеством натуральных чисел // Докл. НАНУ. — 1999. — № 5. — С. 107–112.
2. Крывый С.Л. О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в области натуральных чисел // Кибернетика и системный анализ. — 1999. — № 4. — С. 12–36.
3. Крывый С.Л., Гжывач В. Алгоритмы построения предбазиса множества решений систем линейных диофантовых ограничений в дискретных областях // Изв. Иркут. ун-та. Сер. «Математика». — 2009. — **2**, № 2. — С. 82–93.
4. Kryvyi S., Matveeva L., Grzywac W. Algorithms for building of the minimal supported set of solutions of HSLDI over the set of natural numbers // Proc. Intern. Conf. “Concurent Systems and Programming”. — Warszawa, 2005 (Sept.). — P. 281–290.
5. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях // Кибернетика и системный анализ. — 2006. — № 2. — С. 3–17.
6. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в полях вычетов // Там же. — 2007. — № 2. — С. 15–23.
7. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов // Там же. — 2007. — №5. — С. 36–43.
8. Крывый С.Л. Алгоритмы построения базиса множества решений систем линейных диофантовых уравнений в кольце целых чисел // Там же. — 2009. — № 6. — С. 36–41.
9. Донец Г.А. Решение задачи о сейфе на (0, 1)-матрицах // Там же. — 2002. — № 1. — С. 98–105.
10. Донец Г.А., Самер И.М. Альшаламе. Решение задачи о построении линейной мозаики // Теория оптимальных решений. — К.: Ин-т кибернетики им. В.М. Глушкова НАН Украины, 2005. — С. 15–24.
11. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. — 103 с.
12. Baader F., Ziekmann J. Unification theory // Handbook of logic in artificial intelligence and logic programming. — Oxford University Press, 1994. — P. 1–85.
13. Allen R., Kennedy K. Automatic translation of FORTRAN program to vector form // ACM Transactions on Programming Languages and Systems. — 1987. — **9**, N 4. — P. 491–542.
14. Creignou N., Khanna S., Sudan M. Complexity classification of boolean constraint satisfaction problems // SIAM Monographs on Discrete Mathematics and Applications: Society for Industrial and Applied Mathematics. — Philadelphia, PA. — 2001. — v. 7. — 347 p.
15. Чугаенко А.В. О реализации *TSS*-алгоритма // УСиМ. — 2007. — № 3. — С. 27–33.
16. Contejan E., Ajili F. Avoiding slack variables in the solving of linear diophantine equations and inequations // Theoretical Comp. Science. — 1997. — **173**. — P. 183–208.
17. Pottier L. Minimal solution of linear diophantine systems: bounds and algorithms // Proc. of the Fourth Intern. Conf. on Rewriting Techniques and Applications. — Como, Italy, 1991. — P. 162–173.
18. Domenjoud E. Outils pour la deduction automatique dans les theories associatives-commutatives // Thesis de Doctorat d’Universite: Universite de Nancy I. — 1991.
19. Clausen M., Fortenbacher A. Efficient solution of linear diophantine equations // J. Symbolic Computation. — 1989. — **8**, N 1, 2. — P. 201–216.
20. Romeuf J.F. A polinomial algorithm for solvin systems of two linear Diophantine equations // TCS. — 1990. — **74**, N 3. — P. 329–340.
21. Filgueiras M., Tomas A.P. A fast method for finding the basis of non-negative solutions to a linear Diophantine equation // J. Symbolic Comput. — 1995. — **19**, N 2. — P. 507–526.
22. Comon H. Constraint solving on terms: Automata techniques (Preliminary lecture notes) // Intern. Summer School on Constraints in Computational Logics: Gif-sur-Yvette, France, September 5–8. — 1999. — 22 p.
23. Bockmair A., Weispfenning V. Solving numerical constraints // Handbook of Automated Reasoning. — Elsevier Science Publishers, 2001. — P. 753–842.

Поступила 05.09.2012