Серия «Математика»
2009. Т. 2, № 2, С. 82—93

Онлайн-доступ к журналу:
http://isu.ru/izvestia

И З В Е С Т И Я
Иркутского
государственного
университета

УДК 51.681.3

Алгоритмы построения предбазиса множества решений систем линейных диофантовых ограничений в дискретных областях

С. Л. Крывый
Украина, Киев, Киевский национальный университет им. Тараса Шевченка

В. Гжывач
Польща, Ченстохов, Ченстоховский политехнический институт

Аннотация. В статье дан обзор результатов, полученных авторами в последние годы в области программирования с ограничениями (Constraint Programming) для языка ограничений линейного типа.

Ключевые слова: предбазис; базис множества решений; диофантовые ограничения; дискретные области, программирование с ограничениями

В данной работе приводится краткий обзор фактов, связанных с решением проблемы выполнимости множества ограничений, а также алгоритмов построения минимального порождающего множества решений и базиса множества решений систем линейных диофантовых уравнений в множестве целых чисел, натуральных чисел, поле и кольце Z_m вычетов по модулю простого и составного числа m. Данная работа является продолжением работ [1] – [7]. В основе предлагаемых 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 математических игр [8], криптографии [9], асоциативно-коммутативной унификации [10], распараллеливания циклов [11] и многие другие задачи.

1. Проблема выполнимости системы ограничений

Основным понятием, необходимым для формулировки проблемы выполнимости, являетсят понятие n-арного отношения, заданного на некотором множестве D. Множество всех отношений на D будет обозначаться как 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 $CSP(L)$ является решение такой комбинаторной проблемы [12]:

дано: тройка $P = (V, D, C)$, где

- V – множество переменных;
- C – некоторое множество ограничений $\{C_1, \dots, C_q\}$;
- каждое ограничение $C_i \in C$ – это пара (s_i, R_i), где
  - s_i – n-ка переменных длины n, называемая областю ограничения;
  - $R_i \in L$ – n_i-арное отношение на D, называемое отношением ограничения.

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

Множество D в этом случае называется **областью проблемы**. Множество всех решений CSP вида $P = (V, D, C)$ обозначается $Sol(P)$. Если множество D является одним из следующих множеств: Z – множество целых чисел, N – натуральных чисел, Z_m – кольцом вычетов по модулю составного числа m, F_p – полем вычетов по модулю простого числа p, то множество D в таком случае называется **дискретной областью**.

Для того, чтобы определить 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 того, допускает ли данное ограничение данную n-ку 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 легко вычислимым (*tractable*), 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 $L' \subseteq L$.

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

Рассмотрим язык линейных ограничений над дискретной областью с легко вычислимым языком ограничений.

2. Язык линейных диофантовых уравнений над кольцом целых чисел Z

Пусть D – произвольная дискретная область с бинарными операциями сложения, вычитания, умножения и двумя нульарными операциями 0 и 1. Пусть $L = L_{lin}$ – язык ограничений, состоящий из всех таких отношений на D, элементами которых являются все решения некоторой системы линейных уравнений над D.

Произвольное отношение из L_{lin}, а также произвольная проблема $CSP(L_{lin})$ могут быть представлены некоторой системой линейных уравнений над D. Рассмотрим метод и алгоритмы решения $CSP(L_{lin})$ над дискретными областями.

Системой линейных диофантовых уравнений (СЛДУ) будем называть систему вида

$$\left\{ \begin{array}{ccccccccc} L_1(x) & = & a_{11}x_1 & + & \ldots & + & a_{1q}x_q & = & b_1 \\ L_2(x) & = & a_{21}x_1 & + & \ldots & + & a_{2q}x_q & = & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ L_p(x) & = & a_{p1}x_1 & + & \ldots & + & a_{pq}x_q & = & b_p \end{array} \right. \tag{2.1}$$

где $a_{ij}, b_i \in Z$ (кольцо целых чисел), $x_i \in D$, где $D = \{Z, N, \{0,1\}, F_p, Z_m\}$ – одна из дискретных областей.

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

Пусть S – СЛОДУ и $e_1 = (1, 0, \ldots, 0, 0),\ e_2 = (0, 1, \ldots, 0, 0), \ldots, e_q = (0, 0, ..., 0, 1)$ единичные векторы из множества D^q, которые называются векторами канонического базиса множества D^q. Введем на множестве D^q отношение порядка $\ll$, которое определяется таким 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 для всех $i = 1, \ldots, q,\ x_i \leq y_i$. Ясно, что это отношение является частичным порядком и относительно этого порядка можно говорить о минимальных элементах в множестве D^q. Очевидно, что наименьшим элементом в множестве D^q есть нулевой вектор.

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

СЛОДУ S будем называть **несовместной**, если множество M состоит только лишь из тривиального решения, в противном случае она будет называться **совместной**.

TSS-метод решения СЛДУ, о котором дальше будет идти речь, и его реализация для систем уравнений над множеством натуральных чисел подробно описаны в [5, 13]. Суть этого метода состоит в комбинировании соответствующих коэффициентов системы уравнений с целью получения ее решений. Рассмотрим применение этого метода для построения множества решений систем линейных ограничений в кольце целых чисел Z.

Случай линейного однородного диофантового уравнения (ЛОДУ). Пусть дано ЛОДУ

$$L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0, \tag{2.2}$$

где $a_i, x_i \in Z,\ i = 1, \ldots, n$.

Рассмотрим множество векторов $M_0 = \{e_1, \ldots, e_n\}$ и функцию $L(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ ЛОДУ (2.2). Не ограничивая общности, предположим, что в функции $L(x)$ первым ненулевым коэффициентом будет a_1 и $a_1 > 0$. Построим множество векторов

$$B = \{e_1 = (-a_2, a_1, 0, \ldots, 0), e_2 = (-a_3, 0, a_1, 0, \ldots, 0), e_{q-1} = (-a_q, 0, 0, \ldots, 0, a_1)\} \cup M_0^0,$$

где $M_0^0 = \{e_r : L(e_r) = 0\}$, причем, если $a_i \neq 0$ и НОД$(a_i, a_1) \neq 1$, то сократим координаты такого вектора на этот НОД. Выбранный ненулевой коэффициент a_1 будем называть **основным**. Таким образом, можно считать, что все векторы в множестве B таковы, что a_i и a_1 взаимно просты. Иными словами, множество B строится путем комбинирования первого ненулевого коэффициента с остальными ненулевыми коэффициентами, взятыми с противоположными знаками, и пополнения векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (2.2). Построенное таким образом множество будем называть TSS-множеством или **предбазисом**. Очевидно, что векторы из множества B являются решениями ЛОДУ (2.2), а само множество B – замкнуто относительно сложения, вычитания и умножения на элемент из кольца Z.

Лемма 1. *Пусть $x = (c_1, c_2, \ldots, c_q)$ – некоторое решение ЛОДУ (2.2), тогда если $x \notin B$, то x представляется в виде неотрицательной линейной комбинации вида*

$$a_1x = c_2e_1 + c_3e_2 + \ldots + c_qe_{q-1},$$

где $e_i \in B, i = 1, \ldots, q-1$.

Доказательство. Если $x = (c_1, \ldots, c_q) \in M$, то вектор

$$c_2e_1 + c_3e_2 + \ldots + c_qe_{q-1} = (-c_2a_2 - c_3a_3 - \ldots - c_qa_q, c_2a_1, \ldots, c_qa_1) =$$
$$= (c_1a_1, c_2a_1, \ldots, c_qa_1) = a_1(c_1, c_2, \ldots, c_q) = a_1x$$

в силу того, что x – решение ЛОДУ (2.2), т. е. $a_1c_1 = -a_2c_2 - a_3c_3 - \ldots - a_qc_q$.

Заметим, что если некоторый вектор e_j из B является вектором канонического базиса и j-я координата вектора x равна c_j, то в представлении вектора x вектор e_j входит с коэффициентом a_1c_j. □

Из доказанной леммы вытекает такое полезное следствие.

Следствие 1. *Если среди коэффициентов ЛОДУ имеется хотя бы один коэффициент равный 1, то выбирая его в качестве основного TSS-метод строит базис B множества всех его решений.*

Пример 1. Построить TSS ЛОДУ

$$L(x) \;=\; 2x \;-\; 3y \;+\; z \;+\; 0 \;+\; v \;=\; 0.$$

Предбазис или TSS этого ЛОДУ при $a_1 = 2$ имеет вид

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

Решения ЛОДУ $x_1 = (1, 1, 1, 0, 0), x_2 = (0, 1, 2, 0, 1)$ имеют представления $2x_1 = s_1 + s_2,\ 2x_2 = s_1 + 2s_2 + s_3$.

Выбирая в качестве основного третий коэффициент, базис множества всех решений этого ЛОДУ составляют векторы

$$e_1 = (1, 0, -2, 0, 0), e_2 = (0, 1, 3, 0, 0), e_3 = (0, 0, -1, 0, 1), e_4 = (0, 0, 0, 1, 0).$$

В этом базисе векторы x_1 и x_2 имеют представление: $x_1 = e_1 + e_2,\ x_2 = e_2 + e_3$.

Случай СЛОДУ. Рассмотрим теперь СЛОДУ

$$S = \begin{cases} L_1(x) \;=\; a_{11}x_1 \;+\; \ldots \;+\; a_{1n}x_n \;=\; 0, \\ L_2(x) \;=\; a_{21}x_1 \;+\; \ldots \;+\; a_{2n}x_n \;=\; 0, \\ \quad\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_q(x) \;=\; a_{q1}x_1 \;+\; \ldots \;+\; a_{qn}x_n \;=\; 0, \end{cases} \tag{2.3}$$

где $a_{ij}, x_i \in Z,\ i = 1, \ldots, q,\ j = 1, \ldots, n$.

Построим предбазис $B_1 = \{e_1^1, e_2^1, \ldots, e_{q-1}^1\}$ для первого уравнения $L_1(x) = 0$ и вычислим значения $L_2(e_i^1) = b_i$, где $e_i^1 \in B_1, b_i \in Z$. Составим уравнение

$$b_1y_1 + \ldots + b_iy_i + \ldots + b_{q-1}y_{q-1} = 0, \tag{2.4}$$

и построим для него предбазис $B_1' = \{s_1, \ldots, s_{q-2}\}$. Векторам s_i из B_1' соответствуют векторы-решения $B_2 = \{e_1^2, \ldots, e_{q-2}^2\}$ СЛОДУ $L_1(x) = 0 \wedge L_2(x) = 0$.

Лемма 2. *Множество векторов B_2 составляет предбазис СЛОДУ $L_1(x) = 0 \wedge L_2(x) = 0$, т. е. любое решение x этой СЛОДУ представляется в виде $kx = l_1e_1^2 + \ldots + l_{q-2}e_{q-2}^2$, где $e_i^2 \in B_2, l_i \in Z,\ i = 1, \ldots, q-2,\ k \geq 1$.*

Доказательство. Пусть x – произвольное решение СЛОДУ $L_1(x) = 0 \wedge L_2(x) = 0$. Поскольку x – решение $L_1(x) = 0$, то в силу леммы 1 x можно представить в виде

$$dx = a_1e_1^1 + \ldots + a_{q-1}e_{q-1}^1,$$

где $e_i^1 \in B_1, a_i \in Z,\ i = 1, \ldots, q-1$. Тогда, в силу того, что x – решение $L_2(x) = 0$, получаем

$$L_2(dx) = a_1b_1 + \ldots + a_{q-1}b_{q-1} = 0,$$

где $b_j = L_2(e_j^1),\ j = 1, \ldots, q-1$. Следовательно, вектор $a = (a_1, \ldots, a_{q-1})$ – решение ЛОДУ (2.4) и в силу леммы 1 получаем

$$ka = d_1s_1 + \ldots + d_{q-2}s_{q-2},$$

где $s_i \in B_1', d_i \in Z,\ i = 1, \ldots, q-2$, а k – основной коэффициент этого ЛОДУ. Отсюда следует, что

$$kdx = d_1e_1^2 + \ldots + d_{q-2}e_{q-2}^2,$$

где $e_i^2 \in B_2, i = 1, \ldots, q-2$. □

С помощью математической индукции непосредственно из лемм 1 и 2 следует справедливость такой теоремы.

Теорема 1. *TSS СЛОДУ (2.3) B, построенное вышеописанным способом, является предбазисом множества всех решений этой СЛОДУ.*

Пример 2. Найдем предбазис для СЛОДУ

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

Базис для первого уравнения был построен выше в примере 1:

$$B_1 = \{e_1^1 = (1, 0, -2, 0, 0), e_2^1 = (0, 1, 3, 0, 0), e_3^1 = (0, 0, -1, 0, 1), e_4^1 = (0, 0, 0, 1, 0)\}.$$

Значения $L_2(x)$ на этих векторах равны соответственно 2, 3, 2, -1. Составляем уравнение $2y_1 + 3y_2 + 2y_3 - y_4 = 0$ и строим базис множества решений этого ЛОДУ:

$$B_1' = \{s_1 = (1, 0, 0, 2), s_2 = (0, 1, 0, 3), s_3 = (0, 0, 1, 2)\}.$$

Этим векторам соответствуют TSS-векторы (базис)

$$B_2 = \{e_1^2 = (1, 0, -2, 2, 0), e_2^2 = (0, 1, 3, 3, 0), e_3^2 = (0, 0, -1, 2, 1)\}.$$

Принимая во внимание следствие 1, результат теоремы 1 можно усилить путем введения избыточности в предбазис. Это можно сделать на основании того, что значения коэффициентов в уравнении $L_1(x) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0$ взаимно просты. Благодаря этому всегда можно добиться того, чтобы среди значений $L_1(x)$ была единица. Не ограничивая общности, будем предполагать, что НОД$(a_{11}, a_{12}, a_{13}) = 1$, т. е. первые три коэффициенты взаимно просты в $L_1(x)$. Тогда существуют числа d_1, d_2, d_3 такие, что на векторе $y = (d_1, d_2, d_3, 0, \ldots, 0)$ значение $L_1(y) = 1$. Добившись этого, вычислим значения $L_1(x)$ на векторах канонического базиса. Построим предбазис B_1, комбинируя вектор y с остальными векторами для получения предбазиса. Заметим, что векторы из B_1 имеют вид

$$\begin{gathered} e'_1 = -a_{11}y + e_1, e'_2 = -a_{12}y + e_2, e'_3 = -a_{13}y + e_3, \\ e'_4 = -a_{14}y + e_4, \ldots, e'_n = -a_{1n}y + e_n, \end{gathered}$$

где e_i – векторы канонического базиса, a_{ij} – коэффициенты в уравнении $L_1(x) = 0$. В координатной форме векторы e'_i выглядят следующим образом:

$$\begin{gathered} e'_1 = (-a_{11}d_1 + 1, -a_{11}d_2, -a_{11}d_3, 0, \ldots, 0), \\ e'_2 = (-a_{12}d_1, -a_{12}d_2 + 1, -a_{12}d_3, 0, \ldots, 0), \\ e'_3 = (-a_{13}d_1, -a_{13}d_2, -a_{13}d_3 + 1, 0, \ldots, 0), \\ e'_4 = (-a_{14}d_1, -a_{14}d_2, -a_{14}d_3, 1, \ldots, 0), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ e'_n = (-a_{1n}d_1, -a_{1n}d_2, -a_{1n}d_3, 0, \ldots, 1). \end{gathered}$$

Имеет место

Теорема 2. *TSS B_1 ЛОДУ $L_1(x) = 0$, построенное вышеописанным способом, является базисом множества всех решений этого ЛОДУ.*

Сложность алгоритма построения базиса пропорциональна величине l^3, где l – максимальное из чисел m и n, где n – число неизвестных в ЛОДУ, а m – максимальная длина двоичного представления коэффициентов ЛОДУ.

Доказательство. Пусть $x = (c_1, c_2, \ldots, c_n)$ – решение ЛОДУ $L_1(x) = 0$. Тогда вектор x имеет представление

$$\begin{gathered} x = c_1e'_1 + c_2e'_2 + c_3e'_3 + c_4e'_4 + \ldots + c_ne'_n = \\ = ([-c_1a_{11}d_1 + c_1 - c_2a_{12}d_1 - c_3a_{13}d_1 - c_4a_{14}d_1 - \ldots - c_na_{1n}d_1], \\ [-c_1a_{11}d_2 - c_2a_{12}d_2 + c_2 - c_3a_{13}d_2 - c_4a_{14}d_2 - \ldots - c_na_{1n}d_2], \\ [-c_1a_{11}d_3 - c_2a_{12}d_3 - c_3a_{13}d_3 + c_3 - c_4a_{14}d_3 - \ldots - c_na_{1n}d_3], c_4, \ldots, c_n) = \\ = (c_1, c_2, c_3, c_4, \ldots, c_n) \end{gathered}$$

в силу того, что $L(x) = a_{11}c_1 + a_{12}c_2 + \ldots + a_{1n}c_n = 0$.

Сложность данного алгоритма определяется сложностью расширенного алгоритма Эвклида, находящего вместе с НОД и линейную комбинацию, представляющую этот НОД. Известно (см. [9]), что эта сложность выражается величиной $O(m \log m)$, где m – длина двоичной записи максимального из коэффициентов ЛОДУ. Этот алгоритм применяется не более n раз и тогда имеем оценку $O(mn \log m)$. Построение базиса B_1 требует не более n^3 операций. Следовательно, общая оценка временной сложности алгоритма выражается величиной $O(l^3)$, где $l = \max(m, n)$. □

Из этой теоремы вытекает такое следствие.

Следствие 2. *Временная сложность алгоритма построения базиса множество всех решений СЛОДУ вида (2.3) пропорциональна величине $O(ql^3)$, где q – число уравнений СЛОДУ, а $l = \max(m, n)$.*

Заметим, что первые три вектора e'_1, e'_2, e'_3 в базисе B_1 линейно зависимы. Действительно, в силу того, что $a_{11}d_1 + a_{12}d_2 + a_{13}d_3 = 1$, то $d_1e'_1 + d_2e'_2 + d_3e'_3 = 0$. Действительно, используя координатное представление векторов, имеем

$$\begin{gathered} d_1e'_1 + d_2e'_2 + d_3e'_3 = (a_{12}d_1d_2 + a_{13}d_1d_3, -a_{11}d_1d_2, -a_{11}d_3, 0, \ldots, 0) + \\ +(-a_{12}d_1d_2, a_{11}d_1d_2 + a_{13}d_2d_3, -a12d_2d_3, 0 \ldots, 0) + \\ +(-a_{13}d_1d_3, -a_{13}d_2d_3, a_{11}d_1d_3 + a_{12}d_2d_3, 0 \ldots, 0) = 0. \end{gathered}$$

Таким образом один из векторов e'_1, e'_2, e'_3 можно удалить из полученного базиса решений.

3. TSS-метод решения СЛНДУ

Пусть S – СЛНДУ вида (2.1) и $b_q \neq 0$. Выполняя элиминацию свободных членов в первых $q-1$ уравнениях преобразуем исходную СЛНДУ к виду

$$S' = \left\{ \begin{array}{ccccccccc} L'_1(x) & = & a'_{11}x_1 & + & \ldots & + & a'_{1n}x_n & = & 0, \\ L'_2(x) & = & a'_{21}x_1 & + & \ldots & + & a'_{2n}x_n & = & 0, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ L'_{q-1}(x) & = & a'_{q-11}x_1 & + & \ldots & + & a'_{q-1n}x_n & = & 0, \\ L_q(x) & = & a_{q1}x_1 & + & \ldots & + & a_{qn}x_n & = & b_q. \end{array} \right. \quad (3.1)$$

Построим базис множества решений СЛОДУ, состоящей из $q-1$ первых уравнений системы (3.1). Пусть это будут векторы $\{s_1, \ldots, s_k\}$. Найдем значения $L_q(s_j) = a_j, j = 1, \ldots, k$. Для этих значений верна

Теорема 3. *СЛНДУ вида (3.1) (а вместе с ней и СЛНДУ (2.1)) совместна тогда и только тогда, когда ЛНДУ* $a_1y_1+a_2y_2+\ldots+a_ky_k=b_q$ *имеет хотя бы одно решение в множестве целых чисел.*

Доказательство. Если уравнение $a_1y_1+a_2y_2+\ldots+a_ky_k=b_q$ имеет решение $(c_1,c_2,\ldots,c_k)$, то очевидно, что вектор $s=c_1s_1+c_2s_2+\ldots+c_ks_k$ – решение СЛНДУ.

Если СЛНДУ совместна и $s=(k_1,k_2,\ldots,k_n)$ ее решение, то представим s в виде линейной комбинации через базисные векторы подсистемы, состоящей из первых $q-1$ однородных уравнений системы (3.1), т. е.

$$s=c_1s_1+c_2s_2+\ldots+c_ks_k.$$

Тогда $L_q(s)=c_1a_1+c_2a_2+\ldots+c_ks_k=b_q$ должно иметь ходя бы одно решение, поскольку s решение СЛНДУ. $\square$

Известно, что общее решение СЛНДУ имеет вид $y=x+\sum\limits_{i=1}^{k}a_ix_i$, где x – частное решение СЛНДУ, x_i – базисные решения соответствующей СЛОДУ, a_i – произвольные целые числа, а k – количество базисных решений. Таким образом, для полного решения СЛНДУ необходимо построить базис множества решений ее СЛОДУ и найти одно из решений СЛНДУ. Поиск такого решения, как следует из вышеизложенного, сводится к поиску решения уравнения $a_1y_1+a_2y_2+\ldots+a_ky_k=b_q$. Это решение можно найти, например, методом наименьшего коэффициента.

Пример 3. Проверить на совместность СЛНДУ

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

Преобразованная СЛНДУ имеет вид

$$S'=\begin{cases} L_1'(x) = 7x_1 - 5x_2 + 3x_3 + 2x_4 - x_5 = 0,\\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -2.\end{cases}$$

Базис ЛОДУ $L_1(x)'=0$ составляют векторы (здесь не нужно вычислять НОД коэффициентов, поскольку имеется коэффициент равный 1):

$$(1,0,0,0,7),(0,1,0,0,-5),(0,0,1,0,3),(0,0,0,1,2).$$

Значения $L_2(x)$ на этих векторах равны -4, 6, -2, -2. Наибольший общий делитель этих значений равен 2 и является делителем свободного члена $b_2=-2$. Следовательно, СЛНДУ имеет решение, т. е. совместна.

Частным решением данной СЛНДУ является вектор $e=(0,0,0,1,2)$, а решениями соответствующей СЛОДУ – векторы $e_1=(1,0,0,-2,3)$, $e_2=(0,0,1,-1,1), e_3=(0,1,0,3,1)$. Тогда общее решение записывается в виде $x = e + c_1e_1 + c_2e_2 + c_3e_3$, где c_1, c_2, c_3 – произвольные целые числа.

Если дана система

$$S' = \begin{cases} L'_1(x) = 7x_1 - 5x_2 + 3x_3 + 2x_4 - x_5 = 0, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -3, \end{cases}$$

то она решений не имеет в кольце целых чисел, поскольку НОД(-4, 6, -2, -2) $= 2$ не делит свободный член -3 и поэтому уравнение $-4x + 6y - 2z - 2u = -3$ не имеет решений.

Подводит итог всему сказанному выше следующее утверждение.

Теорема 4. *Язык L_{lin} линейных диофантовых уравнений над кольцом целых чисел Z является легко вычислимым в арифметической модели сложности вычислений.*

4. Заключение

Приведем краткие сведения о сложности алгоритмов решения CSP в дискретных областях, отличных от области целых чисел Z. В связи с ограниченным объёмом статьи, представим соответствующие результаты с помощью следующей таблицы:

Дискретная область	Сложность CSP	Ссылки
N	NP	[3, 4, 5]
Z_m	NP	[7]
F_p	P	[6]
Z	P	–

Относительно области Z_m – кольца вычетов по модулю m – заметим, что если имеется разложение модуля m на простые множители, то сложность решение CSP в этой области принадлежит класу полиномиальной сложности.

В заключение заметим, что приведенные оценки временных сложностей алгоритмов можно уточнять, если прослеживать все детали процесса вычислений, происходящего в TSS-алгоритме. В данной работе мы ограничиваемся тем, что устанавливаем только верхние оценки (т. е. сложность в наихудшем случае) этих алгоритмов.

Отметим также, что при малых значениях модуля p сложностью вычисления НОД в полях и кольцах вычетов можно пренебречь и 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, поэтому сложность решения

СЛОДУ и СЛНДУ в таком поле становится пропорциональна величине qn^2, где q – число уравнений, а n – число неизвестных в системе.

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, например, достаточно быстро работает в случае разреженных матриц систем.

Список литературы

1. Крывый С. Л. Критерий совместности систем линейных диофантовых уравнений над множеством натуральных чисел. / С.Л. Крывый // Доклады НАНУ. — 1999. — N 5. — С. 107 – 112.
2. Крывый С.Л. О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в области натуральных чисел. / С.Л. Крывый // ж. Кибернетика и системный анализ. — 1999. — N 4. — С. 12 – 36.
3. Крывый С.Л., Гжывач В., Хайдер Л. Алгоритм построения базиса множества решений СЛОДУ в множестве $\{0, 1\}$. / С.Л. Крывый, В. Гжывач, Л. Хайдер // Тезисы межд. конф. "Алгебра, логика, кибернетика". — Иркутск. — 2004 (август). — С. 167 –169.
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. / S. Kryvyi, L. Matveeva, W. Grzywac // In Proc. Intern. Conf. "Concurent Systems and Programming". — Warszawa. — 2005 (september). — P. 281 – 290.
5. Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях. / С. Л. Крывый // Кибернетика и системный анализ. — 2006. — N 2. — С. 3 – 17.
6. Крывый С. Л. Алгоритмы решения систем линейных диофантовы уравнений в полях вычетов. / С. Л. Крывый // Там же. — 2007. — N 2. — С. 15 – 23.
7. Крывый С. Л. Алгоритмы решения систем линейных диофантовы уравнений в кольцах вычетов. / С. Л. Крывый // Там же. — 2007. — N 5. — С. 36 – 43.
8. Донец Г. А. Решение задачи о сейфе на (0,1)-матрицах. / Г. А. Донец // Там же. — 2002. — N 1. — С. 98 – 105.
9. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. / А. В. Черемушкин // Москва: МЦНМО. — 2002. — 103 с.
10. Baader F., Ziekmann J. Unification theory / F. Baader, J. Ziekman, // Handbook of Logic in Artificial Intelligence and Logic Programming. — Oxford University Press. — 1994. – -P. 1 – 85.
11. Allen R., Kennedy K. Automatic translation of FORTRAN program to vector form / R. Allen, K. Kennedy // ACM Transactions on Programming Languages and systems. — 1987. — v. 9, N4. — P. 491 – 542.
12. Creignou N., Khanna S., Sudan M. Complexity Classification of Boolean Constraint Satisfaction Problems. / N. Creignou, S. Khanna, M. Sudan. // SIAM Monographs on Discrete Mathematics and Applications: Society for Industrial and Applied Mathematics. Philadelphia. PA. — 2001. — v. 7. — 347 p.
13. Чугаенко А.В. О реализации TSS-алгоритма. / А. Чугаенко // ж. Управляющие системы и машины. — 2007. — N 3. — С. 27 – 33. 14 – 26.

S. Kryvyi, W. Grzywac

The Algorithms for building of minimal supported solution set for systems of linear Diophantine equations over discrete domains

Abstract. This paper contains the review of the results obtained in the last years in the solution area of systems of linear Diophantine constraints over discrete domains.

Keywords: minimal supported set, basis of solution set; Diophantine constraints; discrete domains, constraint programming

Крывый Сергей Лукьянович, доктор физико-математических наук, профессор, Киевский национальный университет им. Т. Шевченко, Украина, 03187, Киев, просп. акад. Глушкова, 2,

тел.: (044)5223433, (krivoi@i.com.ua)

Гжывач Виолетта, асистент, Ченстоховский политехнический институт, факультет прикладной и теоретической информатики, Польща, Ченстохов, ул. Дамбровского, 73,

тел.: (+48-034)3250589, (wiola@icis.pcz.pl)

Kryvyi Sergii, Taras Shevchenko's University in Kiev, Ukraine, Kiev, Glushkov's prospekt, 2, professor,

Phone: (044)5223433, (krivoi@i.com.ua)

Grzywac Wioletta, Politechnical Institute of Chestochowa, Poland, Czestochowa, st. Dambrowskiego, 73, asistent,

Phone: (+38-034)3250589, (wiola@icis.pcz.pl)