ТЕОРЕТИЧНІ ОСНОВИ ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 51.681.3

Крывый С.Л.
Киевский национальный университет им. Т. Шевченко

АЛГОРИТМЫ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ В КОНТЕКСТЕ ПРОБЛЕМЫ ВЫПОЛНИМОСТИ ОГРАНИЧЕНИЙ. Ч. I

Предложены алгоритмы построения минимального порождающего множества решений систем линейных однородных уравнений в множестве натуральных чисел и базиса множества решений системы линейных однородных и неоднородных диофантовых уравнений в кольцах и полях вычетов по модулю некоторого числа. Эти алгоритмы рассматриваются в контексте решения проблемы выполнимости системы ограничений.

Запропоновано алгоритми побудови мінімальної породжуючої множини розв'язків систем лінійних однорідних рівнянь в множині натуральних чисел і базису множини розв'язків системи лінійних однорідних і неоднорідних діофантових рівнянь у кільцях і полях лишків за модулем деякого числа. Ці алгоритми розглядаються в контексті розв'язання проблеми виконуваності системи обмежень.

The algorithms for computation of minimal supported set of solutions for systems of linear Diophantine homogeneous equations over set of natural numbers and basis of systems of linear Diophantine homogeneous and inhomogeneous equations in ring and field of remainders on modulo of a number. This algorithms consider in context of solving of general constraint satisfaction problem

Ключевые слова: *диофантовые уравнения, выполнимость ограничений*

Введение

Одной из фундаментальных проблем в современном программировании с ограничениями (constraint programming – CP) является проблема определения вычислительной сложности решения задач, включающих ограничения. Существует большое количество проблем, называемых проблемами выполнимости ограничений (constraint satisfaction problems – *CSP*), являющихся *NP*-трудными [20]. Поэтому маловероятно существование общего эффективного алгоритма для решения произвольной проблемы, связанной с ограничениями. Тем не менее, во многих практических задачах возникают проблемы, решение которых вычисляется более эффективно.

Рассмотрим некоторые из решений таких проблем, в частности, проблемы выполнимости линейных диофантовых ограничений в виде уравнений [9] – [18].

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 *Zm* вычетов по модулю простого и составного числа *m*. Данная работа является продолжением работ [3] – [8]. В основе предлагаемых алгоритмов лежит *TSS*-метод построения минимального порождающего множества решений систем линейных однородных диофантовых уравнений в множестве натуральных чисел *N* [7]. К такого рода системам и методам их решений сводятся задачи математических игр [1], распознавания изображений и построение линейных мозаик [2], криптографии [9], распараллеливания циклов [12] и многие другие задачи.

1. Проблема выполнимости системы ограничений

1.1. Основные определения и обозначения

Основным понятием в дальнейшем изложении будет понятие отношения.

Определение 1. *Пусть D – некоторое множество и $n \in N$ - натуральное число. Декартовой степенью множества D называется множество D^n, состоящее из всех n-ок элементов из D, т. е.* $D_n = \{(d_1,\ldots,d_n) \mid d_i \in D, i = 1,\ldots,n\}$.

Произвольное подмножество $R \subseteq D^n$ называется n-арным отношением на множестве D.

В зависимости от мощности множества D, отношения на D могут быть конечными или бесконечными. Независимо от этого в дальнейшем будем обозначать множество отношений на D как R_D.

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

Определение 2. *Для произвольного множества D и произвольного языка ограничений L на D проблемой выполнимости ограничений CSP(L) является решение такой комбинаторной проблемы:*

дано: *тройка $P = (V, D, C)$, где*

• *V – множество переменных;*

• *C – некоторое множество ограничений $\{C_1,\ldots,C_q\}$.*

• *каждое ограничение $C_i \in C$ – это пара (s_i, R_i), где*

– *s_i – n-ка длины n, называемая областью ограничения;*

– *$R_i \in L$ – n_i-арное отношение на D, называемое отношением ограничения.*

Вопрос: существует ли решение ограничения, т. е. существует ли функция $\varphi : V \to D$ такая, что $\forall (s, R) \in C$, где $s = (\upsilon,\ldots,\upsilon_n)$, n-ка $(\varphi(\upsilon_1),\ldots,\varphi(\upsilon_n)) \in R$?

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

Определение 3 *Язык ограничений L называется легко обрабатываемым (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 $L' \subseteq L$.

Известно множество вычислительных проблем, сложность решения которых не принадлежат ни классу полиномиальной сложности, ни классу *NP*-полной сложности. Но если языки ограничений рассматриваются над областями, имеющими размер 2 или 3, то известно, что сложность их решения принадлежат одному из этих двух классов.

1.2 Примеры языков ограничений

1.2.1. Язык линейных уравнений над бесконечным полем. Пусть D – произвольное числовое поле, т. е. это алгебра вида $G = (D, \{+, -, \cdot, :, 0, 1\})$ с бинарными операциями сложения, вычитания, умножения, деления 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 и решены в полиномиальном времени [21] (например, с помощью алгоритма последовательного исключения неизвестных). Следовательно, L_{lin} является легко обрабатываемым языком.

Обобщением данного языка является язык равенств термов и проблема унификации. Пусть $D = T(V, \Omega)$ где $T(V, \Omega)$ – алгебра термов сигнатуры Ω над множеством переменных V. Предметные константы представляются нульарными функциональными символами операций из Ω.

Множество ограничений $C = \{C_1,\ldots,C_m\}$ состоит из уравнений $C_i = \{t_i = t_i'\}, i = 1,\ldots,m, t_i, t_i' \in T(V, \Omega)$.

Язык ограничений L_{unif} в этом случае состоит из множества всех решений системы уравнений $C_1 \wedge C_2 \wedge \ldots \wedge C_m$ на $T(V, \Omega)$. Это означает, что отображение φ представляет унификатор системы термов $t_1, t_1', \ldots, t_m, t_m'$, т.е. $\varphi : V \to T(V, \Omega)$ и $(\varphi(\upsilon_1),\ldots,\varphi(\upsilon_n)) = (\upsilon_1 \to u_1,\ldots,\upsilon_n \to u_m) \in R$ – унифицирующая подстановка.

1.2.1. Язык булевских ограничений. Язык ограничений над двухэлементным

множеством $D=\{d_0,d_1\}$ известен как булевский язык ограничений [22]-[24]. Используя этот язык, можно выразить стандартную форму пропозициональной проблемы выполнимости, имеющей название ВЫПОЛНИМОСТЬ в виде *CSP*, путем интерпретации элементов из *D* как ложь и истина [34].

Известен результат Шафира [33] о том, что булевский язык ограничений *L* легко обрабатываем если выполняется хотя бы одно из следующих условий:

1. каждое отношение из *L* содержит *n*-ку, в которой все компоненты равны d_0;

2. каждое отношение из *L* содержит *n*-ку, в которой все компоненты равны d_1;

3. каждое отношение из *L* определяется КНФ, где каждый дизъюнкт имеет один негативный литерал;

4. каждое отношение из *L* определяется КНФ, где каждый дизъюнкт имеет один позитивный литерал (хорновский дизъюнкт);

5. каждое отношение из *L* определяется КНФ, где каждый дизъюнкт содержит два литерала;

6. каждое отношение из *L* является множеством решений системы линейных уравнений над полем F_2 вычетов по модулю 2.

Во всех остальных случаях язык *L* является *NP*-полным. Приведенный результат известен как дихотомическая теорема Шафира. Непосредственно из этой теоремы следует, что некоторые булевские языки ограничений, содержащие единственное отношение, являются *NP*-полными. Например, для $D=\{d_0,d_1\}$ и тернарного отношения N_D, называемого «НЕ-ВСЕ-РАВНЫ» и имеющего вид

$$N_D = D^3 \setminus \{(d_0,d_0,d_0),(d_1,d_1,d_1),(d_0,d_0,d_1),$$
$$(d_0,d_1,d_0),(d_0,d_1,d_1),(d_1,d_0,d_1),(d_1,d_1,d_0)\}.$$

$CSP(N_D)$ является *NP*-полной [33].

2 Язык линейных диофантовых уравнений над полем вычетов

Последнее условие дихотомической теоремы Шафира, о которой шла речь в предыдущем разделе, обобщается на произвольное поле вычетов по модулю простого числа. Рассмотрим подробности.

Системы линейных диофантовых уравнений (СЛДУ). СЛДУ будем называть систему вида

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

где $a_{i,j}, b_i \in Z$ (множество 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 $L_i(x)$ обращает $L_i(c)\equiv b_i$ 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 $e_1=(1,0,\ldots,0,0), e_2=(0,1,\ldots,0,0),\ldots,e_q=(0,0,\ldots,0,1)$ единичные вектора из множества D^q, которые называются векторами канонического базиса множества D^q Введем на множестве D^q отношение порядка <<, которое определяется таким образом: если $x=(x_1,\ldots,x_q), y=(y_1,\ldots,y_q)\in D^q$, то $x<<y$ тогда и только тогда, когда для всех $i=1,\ldots,q$, $x_i<<y_i$. 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 **совместно**й.

Поля вычетов. Полем вычетов по модулю простого числа *p* называется алгебра $F_p=(A=\{0,1,\ldots,p-1\},\Omega=\{+,\cdot,-,-1,0,1\})$, где + и · являются бинарными ассоциативными, коммутативными и дистрибутивными операциями сложения и умножения по модулю *p*, операции – и $^{-1}$ – унарные операции взятия

противоположного и обратного элемента относительно операций + и · соответственно, 0 и 1 – нульарные операции – аддитивный нуль и мультипликативная единица. На основании законов для операций в поле F_p вытекает справедливость тождеств $(\forall x, y \in F_p)x + y = 0 \to x = -y$.

Из таких тождеств следует, что в этом поле $x = p - y$, а $-y = x - p$. Это дает возможность заменять положительное число *x* на отрицательное число $-y = x - p$ и наоборот. Элементы x и $-y$ будем называть дополнениями (x дополняет $-y$ и наоборот).

Поскольку p – простое число, то в поле F_p при $a \neq 0$ всегда разрешимо сравнение $ax \equiv b(\mathrm{mod}\, p)$, причем оно имеет единственное решение. Принимая во внимание эти свойства поля F_p, рассмотрим метод, названный *TSS*-методом [6], для решения линейных диофантовых уравнений в этом поле.

2.1 TSS-метод решения ЛОДУ

Пусть дано ЛОДУ

$$L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0 \qquad (2)$$

где $a_i, x_i \in F_p, i = 1,...,n$. Допустим, что $a \neq 0$, тогда имеет место такое простое утверждение.

Лемма 1 *Если* $c = (c_1,...,c_n)$ *– решение ЛОДУ (2) в* F_p*, то оно будет решением ЛОДУ* $a_1x_1 + \ldots - b_ix_i + \ldots + a_nx_n = 0$, *где* $-b_i$ *– дополнение коэффициента* a_i.

Рассмотрим множество векторов канонического базиса $M_0 = \{e_1,...,e_n\}$ и функцию $L_1(x) = a_1x_1 + a_2x_2 + ... + a_nx_n$ ЛОДУ (2). Заменим в функции $L(x)$ первый ненулевой коэффициент a_k его отрицательным дополнением $-b_k$ и построим множество векторов $B = \{(0,\ldots,a_j,0,\ldots,0,b_k,0,\ldots,0)\} \cup M_0$, где $M_0 = \{e_r : L_1(e_r) = 0\}, a_j \neq 0$, а b_k является *j*-й координатой в векторах из *B*. Причем если для некоторого a_i $НОД(a_i, b_k) \neq 1$ то сократим координаты такого вектора на этот общий делитель (что возможно в силу леммы 1). Таким образом, можно считать, что все векторы в множестве *B* таковы, что a_i и b_k взаимно просты. Иными словами, множество *B* строится путем комбинирования дополнения первого ненулевого коэффициента, взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополненное векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (2). Построенное таким образом множество будем называть *TSS*-множеством. Очевидно, что векторы из множества *B* являются решениями ЛОДУ (2).

Лемма 2 *Пусть* $d = (0,...,0,d_i,0,...,0,d_j,...,0)$ *– решение ЛОДУ (2), тогда*

a) если $d \in B$, *то* d *– минимальное решение ЛОДУ (2);*

b) если $d \notin B$, *то* d *представляется в виде неотрицательной линейной комбинации векторов из B.*

Теорема 1 *TSS ЛОДУ (2) B, построенное комбинированием дополнения первого ненулевого коэффициента, взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополненное векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (2), является базисом множества всех решений этого ЛОДУ.*

Сложность алгоритма пропорциональна величине l^3, *где* $l = \max(m, n)$, m *– количество разрядов числа p, а* n *– число неизвестных в ЛОДУ.*

Пример 1. Построить базис множества всех решений ЛОДУ $2x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 0$ в поле вычетов F_3.

Решение. Первый ненулевой коэффициент в данном ЛОДУ есть $a_1 = 2$, а его дополнение равно $2 - 3 = -1$. Получаем ЛОДУ вида $-x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 0$. Применяя *TSS*-метод, находим такие базисные решения:

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

Очевидными решениями данного ЛОДУ являются векторы $c_1 = (1,1,1,1,1)$ и $c_2 = (0,2,0,1,0)$. Представления этих векторов через базисные векторы имеют вид:

$c_1 = e_1 + e_2 + e_3 + e_4 = (4(\mathrm{mod}\, 3),1,1,1,1) = (1,1,1,1,1)$

$c_2 = 2e_1 + e_2 = (0,2,0,1,0).$

2.2 TSS-метод решения СЛОДУ

Пусть дана СЛОДУ *S* вида (1). Рассмотрим множество векторов канонического базиса $M_0' = \{e_1,...,e_n\}$ и первое уравнение $L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_n = 0$

системы S. Построим базис $B_1 = \{e_1,...,e_m\}$ множества всех решений этого ЛОДУ описанным выше способом. Возьмем функцию $L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n$ и рассмотрим ЛОДУ вида

$$L_2(e_1)y_1 + L_2(e_2)y_2 + ... + L_2(e_m)y_m = 0 \quad (3)$$

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

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

Лемма 3 *Множество M является базисом множества решений СЛОДУ*

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

Теорема 2 *Пусть M – TSS-множество, построенное описанным выше способом для СЛОДУ S, тогда M является базисом множества всех решений этой СЛОДУ. Сложность построения базиса пропорциональна величине ql^3, где q – число уравнений в СЛОДУ, $l = \max(m,n)$, m – количество разрядов числа p, а n – число неизвестных в СЛОДУ.*

Пример 2. Найти в поле F_3 базис множества решений СЛОДУ

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

Решение. В примере 1 был найден базис множества решений первого ЛОДУ этой системы: $e_1 = (1,1,0,0,0)$; $e_2 = (1,0,0,1,0)$; $e_3 = (2,0,0,0,1)$; $e_4 = (0,0,1,0,0)$. Находим $L_2(e_1) = 0$; $L_2(e_2) = 1$; $L_2(e_3) = 0$; $L_2(e_4) = 1$ и строим ЛОДУ $0y_1 + y_2 + 0y_3 + y_4 = 0y_1 - 2y_2 + 0y_3 + y_4 = 0$.
Базис множества решений состоит из векторов $r_1 = (1,0,0,0)$; $r_2 = (0,1,0,2)$; $r_3 = (0,0,1,0)$.
Получаем векторы множества решений для первых двух уравнений из S, соответствующие векторам r_1, r_2, r_3:
$e_1' = (1,1,0,0,0)$; $e_2' = (1,0,2,1,0)$; $e_3' = (2,0,0,0,1)$.

Находим значения $L_3(e_1') = 2$; $L_3(e_2') = 1$; $L_3(e_3') = 2$, строим ЛОДУ $2y_1 + y_2 + 2y_3 = -y_1 + y_2 + 2y_3 = 0$ и получаем его решения: $r_1 = (1,1,0)$; $r_2 = (2,0,1)$. Строим соответствующие им векторы базиса множества решений СЛОДУ S: $s_1 = (2,1,2,1,0)$; $s_2 = (1,2,0,0,1)$.

2.3 *TSS*-метод решения СЛНДУ

Случай одного линейного неоднородного диофантового уравнения (ЛНДУ). Пусть дано ЛНДУ

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b \quad (5).$$

Рассмотрим уравнение $a_1x_1 + a_2x_2 + ... + a_nx_n - bx_0 = 0$, решения которого при $x_0 = 1$ будут решениями (5). Применяя *TSS*-метод к этому ЛОДУ, получаем $s_1 = (b,0,...,a_1),...,s_n = (0,...,0,b,a_n)$.

Среди этих решений необходимо выделить такие, у которых $x_0 = 1$. Однако $x_0 \in \{a_1, a_2,...,a_n\}$ и тогда искомыми будут те решения x, которые являются решениями сравнения $a_i x \equiv 1 (\mathrm{mod}\, p)$. В силу простоты p это сравнение имеет единственное решение, причем это верно для любого $a_i \neq 0, i - 1,2,...,n$. Следовательно, можно выбрать любое $a_i \neq 0$ и для него решать уравнение. Поскольку уравнение $a_i x \equiv 1 (\mathrm{mod}\, p)$ всегда имеет решение, то и уравнение (5) тоже будет всегда иметь решение.

Пусть $x^1 = (c_1, c_2,..., c_n)$ – некоторое частное решение (5), найденное описанным выше способом, а $B = \{e_1, e_2,...,e_m\}$ – базис множества решений ЛОДУ

$$a_1x_1 + a_2x_2 + ... + a_nx_n = 0 \quad (6)$$

Лемма 4. *Произвольное решение ЛНДУ (5) представляется в виде $u = x^1 + \sum_{i=1}^{m} b_i e_i$, где x^1 – частное решение ЛНДУ (5), а $e_1,...,e_m$ – базисные векторы множества решений ЛОДУ (6), которое соответствует ЛНДУ (5).*

Пример 3. Найти в поле F_{13} общее решение ЛНДУ $2x + 3y + 5z + 6u + 4v = 7$.

Решение. Выбираем первый ненулевой коэффициент $a_1 = 2$ и строим вектор $(7,0,0,0,0,2)$. Решаем уравнение $2s \equiv 1 (\mathrm{mod}\, 13)$. Этим решением будет очевидно, $s = 7$. Тогда

вектор $x^1 = 7(7,0,0,0,0) = (10,0,0,0,0)$ будет искомым частным решением ЛНДУ.

Найдем базис множества решений ЛОДУ $2x + 3y + 5z + 6u + 4v = 0$.

С этой целью заменим, например, коэффициент 3 его дополнением -10 и построим базис множества решений ЛОДУ $2x - 10y + 5z + 6u + 4v = 0$. Этими решениями будут векторы: $e_1 = (5,1,0,0,0)$; $e_2 = (0,1,2,0,0)$; $e_3 = (0,3,0,5,0)$; $e_4 = (0,2,0,0,5)$.

Следовательно, общее решение данного ЛНДУ имеет вид:

$$x = x^1 + b_1e_1 + b_2e_2 + b_3e_3 + b_4e_4.$$

Например, при $b_1 = b_2 = b_3 = b_4 = 1$ получаем $u = (2,7,2,5,5)$.

Случай системы неоднородных диофантовых уравнений (СЛНДУ). Пусть дана СЛНДУ

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ L_q(x) = a_{q_1}x_1 + \ldots + a_{qn}x_n = b_q, \end{cases} \quad (7)$$

где $a_{ij}, b_i, x_i \in F_p$, $i = 1,..,n$, $j = 1,...,q$, $q < n$. Поскольку обе части уравнения можно умножать на число, а сами уравнения складывать и вычитать, то преобразуем S к виду (полагая, что $b_q = 0$)

$$S' = \begin{cases} L'_1(x) = a'_{11}x_1 + \ldots + a'_{1n}x_n = b'_1, \\ L'_2(x) = a'_{21}x_1 + \ldots + a'_{2n}x_n = b'_2, \\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ L'_q(x) = a'_{q_1}x_1 + \ldots + a'_{qn}x_n = b'_q, \end{cases} \quad (8)$$

Пусть $B' = \{e'_1, e'_2, ..., e'_n\}$ – базис множества решений СЛОДУ, состоящей из первых $q-1$ уравнений системы S', а $B = \{e_1, e_2, ..., e_k\}$ – базис множества решений СЛОДУ, которыйсоответствует S'. Построим уравнение $L_q(e'_1)y_1 + ... + L_q(e'_m)y_m = b_q$. Если все $L_q(e_i) = 0$, то данное уравнение не имеет решений, а вместе с ним не имеет решений и исходная СЛНДУ (в этом случае $L_q(x)$ линейно зависит от $L'_1(x),...,L'_{q-1}(x)$). Если хотя бы одно $L_q(e_i) \neq 0$, то решение всегда существует и пусть $y = (d_1,...,d_m)$ – решение этого ЛОДУ. Тогда вектор $x^1 = d_1e_1 + ... + d_me_m$ является частным решением уравнения $L_q(x) = b_q$. Следовательно, общее решение СЛОДУ S', а вместе с ней и системы S, представляется в виде

$$u = x^1 + \sum_{i=1}^{k} b_ie_i \text{, где } e_i \in B, i = 1,2,...,k.$$

Отсюда можно получить оценку временной сложности алгоритма построения общего решения СЛНДУ над F_p. Действительно, к оценке, которая приведена в теореме 1, добавляется оценка вычисления частного решения ЛОДУ. Эта оценка включает сложность решения сравнения $ax \equiv b(\mathrm{mod}\ p)$ и построение вектора, являющегося частным решением. Используя, например, способ поиска решения сравнения с помощью непрерывных дробей, получаем, что число элементарных операций, которые необходимо выполнить, не превосходит числа m – максимального числа разрядов в числе p. А построение вектора требует не более n операций. Тогда общая оценка сложности всего алгоритма выражается оценкой, приведенной в теореме 1.

Таким образом, имеет место следующее утверждение.

Теорема 3. *СЛНДУ S, все уравнения которой линейно независимы и размерность которой $q \times n$, при $q < n$, всегда совместна над полем F_p и ее общее решение имеет вид* $u = x^1 + \sum_{i=1}^{k} b_ie_i$, *где* x^1 *– некоторое частное решение S, а* e_i *– базисные векторы множества решений СЛОДУ, которая соответствует данной СЛНДУ S. Сложность построения общего решения СЛНДУ пропорциональна величине* ql^3, *где* q *– количество уравнений в системе,* $l = \max(m,n)$, m *– количество разрядов числа* p, *а* n *– число неизвестных в СЛНДУ.*

Пример 4. Найти в поле F_3 базис множества решений СЛНДУ

$$S = \begin{cases} 2x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 2; \\ x_1 + 2x_2 + 1x_3 + 0x_4 + x_5 = 1; \\ x_1 + x_2 + 2x_3 + 2x_4 + 0x_5 = 2. \end{cases}$$

Решение. СЛОДУ S' для этой системы получается путем вычитания третьего уравнения с соответствующим коэффициентом из первого и второго уравнений, т. е.

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

Базис B' для подсистемы, состоящей из первых двух уравнений, включает векторы $e'_1 = (1,0,0,0,1),\ e'_2 = (0.1.0.0.0),\ e'_3 = (0,0,1,2,2),$ Строим ЛОДУ $L_3(e'_1)y_1 + L_3(e'_2)y_2 + L_3(e'_3)y_3 = y_1 + y_2 + 0y_3 = 2$. Находим его корни путем решения сравнения $1x \equiv 2(\mathrm{mod}\,3)$: $x'_1 = (2,0,0), x'_2 = (0,2,0)$.

Выбираем один из полученных векторов, например, второй. Этому вектору соответствует частное решение $x^1 = (0,2,0,0,0)$.

Выше был найден базис множества решений СЛОДУ, которая соответствует данной СЛНДУ S: $s_1 = (2,1,2,1,0), s_2 = (1,2,0,0,1)$. Следовательно, общее решение СЛНДУ принимает вид $u = x^1 + b_1 s_1 + b_2 x_2$.

Например, при $b_1 = b_2 = 1$ получаем $u_1 = (0,2,2,1,1)$.

3. Язык линейных диофантовых уравнений над кольцом вычетов

Кольцом вычетов по модулю числа m называется алгебра $Z_m = \left(A = \{0,1,\ldots,m-1\}, \Omega = \{+,\cdot,-,^{-1},0,1\}\right)$, где + и · являются бинарными ассоциативными, коммутативными и дистрибутивными операциями сложения и умножения по модулю m, операции $-$ и $^{-1}$ есть унарные операции взятия противоположного и обратного элемента относительно операций + и соответственно, 0 и 1 – нульарные операции – аддитивный нуль и мультипликативная единица. Заметим, что операция взятия обратного элемента в кольце Z_m является частичной, поскольку для делителей нуля (а кольцо Z_m с делителями нуля) она не определена. На основании законов для операций в кольце Z_m вытекает справедливость такого тождества:

$$(\forall x, y \in Z_m)\ \ x + y = 0 \to x = -y.$$

Из тождеств следует, что в кольце Z_m $x = m - y$, а $-y = x - m$ что дает возможность заменять положительное число x на отрицательное число $-y = x - m$ и наоборот. Такие элементы x и $-y$ будем называть дополнениями (x дополняет $-y$ и наоборот).

Кольцо вычетов Z_m называется **примарным**, если модуль m является степенью простого числа p, т. е. $m = p^t$, где $t > 1,\ \ t \in N$. Поскольку m – не объязательно простое число, то в кольце Z_m при $a \neq 0$ не всегда имеет решение сравнение $ax = b(\mathrm{mod}\,m)$. Это сравнение будет иметь решение, если НОД(a,m) = 1 или НОД(a,m) = d и d – делитель числа b.

С учетом свойств кольца Z_m рассмотрим системы линейных диофантовых уравнений (СЛДУ) над этим кольцом.

Системы линейных диофантовых уравнений. СЛДУ над кольцом Z_m будем называть систему вида

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ L_q(x) = a_{r1}x_1 + \ldots + a_{rn}x_n = b_r, \end{cases} \quad (9)$$

где $a_{ij}, b_i, x_i \in Z_m,\ \ i = 1,..,n,\ \ j = 1,\ldots,r.$

3.1 *TSS*-метод решения ЛОДУ

Случай одного линейного однородного диофантового уравнения (ЛОДУ).

Пусть дано ЛОДУ $L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0$ (10), где $a_{ij}, x_i \in Z_m,\ i = 1,..,n$. Допустим, что $a_i \neq 0$, тогда имеет место такое простое утверждение.

Лемма 5 *Если* $c = (c_1,\ldots,c_n)$ *– решение ЛОДУ (10) в* Z_m*, то оно будет решением ЛОДУ* $a_1x_1 + \ldots - b_ix_i + \ldots + a_nx_n = 0$*, где* $-b_i$ *– дополнение коэффициента* a_i*, т. е.* $-b_i = a_i - m,\ i = 1,\ldots,n$ *[4].*

Рассмотрим случай ЛОДУ, которые удовлетворяют следующему условию.

Условие 1. Среди коэффициентов ЛОДУ существует коэффициент, который взаимно прост с модулем m**.**

Допустим, что в данном ЛОДУ таким коэффициентом является первый ненулевой коэффициент – коэффициент a_k, $k = 1,2,\ldots,n$. Рассмотрим множество векторов канонического базиса $M_0 = \{e_1,\ldots,e_n\}$ и функцию $L(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ ЛОДУ (10). Заменим в функции $L(x)$ первый ненулевой коэффициент a_k который взаимно прост с модулем, его отрицательным дополнением $-b_k$ и построим множество векторов $B = \{(0,\ldots,a_j,0,\ldots,0,b_k,0,\ldots,0)\} \cup M_0$, где $M_0 = \{e_r : L(e_r) = 0\},\ a_j \neq 0$, а b_k является j-й координатой в векторах из B. Причем, если

для некоторого a_i НОД$(a_i, b_k) \neq 1$, то сократим координаты такого вектора на этот общий делитель. Таким образом, можно считать, что все векторы в множестве B таковы, что a_i и b_k взаимно просты. Иными словами, множество B строится путем комбинирования дополнения произвольного ненулевого коэффициента, удовлетворяющего условию 1 и взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополненное векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (10). Построенное таким образом множество будем называть *TSS*-множеством. Очевидно, что векторы из множества B являются решениями ЛОДУ (10).

Лемма 6. *Если* $d = (0,...,0,d_i,0,...,0,d_j,0,...,0)$ *– решение ЛОДУ (10), то оно либо является элементом* B*, либо представляется в виде неотрицательной линейной комбинации векторов из* B.

Теорема 4 *Множество* B *решений ЛОДУ (10), построенное комбинированием дополнения первого ненулевого коэффициента, удовлетворяющего условию 1, взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополненное векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (10), является базисом множества всех решений этого ЛОДУ.*

Сложность алгоритма пропорциональна величине l^3*, где* $l = \max(s, n)$, $s = \log m$ *– число двоичных разрядов числа* m*, а* n *– число неизвестных в ЛОДУ.*

Следствие 1 *Если модуль* m *является простым числом, то множество* B *решений ЛОДУ (10) является базисом множества всех решений этого ЛОДУ.*

Сложность алгоритма пропорциональна величине l^3*, где* $l = \max(s, n)$, s *– число разрядов простого числа* m*, а* n *– число неизвестных в ЛОДУ [4].*

Действительно, если модуль m – простое число, то условие 1 выполняется автоматически.

Пример 5. Построить базис множества всех решений ЛОДУ $2x_1 + 5x_2 + 7x_3 + 3x_4 + 6x_5 = 0$ в кольце вычетов Z_{12}.

Решение. Выбираем ненулевой коэффициент 7, который взаимно прост с модулем 12, заменяем его дополнением -5 и получаем ЛОДУ вида $2x_1 + 5x_2 - 5x_3 + 3x_4 + 6x_5 = 0$. Применяя *TSS*-метод, получаем такие базисные решения: $e_1 = (5,0,2,0,0)$, $e_2 = (0,1,1,0,0)$, $e_3 = (0,0,3,5,0)$, $e_4 = (0,0,6,0,5)$.

Полученные решения можно редуцировать к векторам $e_1 = (5,0,2,0,0)$, $e_2 = (0,1,1,0,0)$, $e_3' = (0,0,3,1,0)$, $e_4' = (0,0,6,0,1)$, поскольку из базисных векторов как следствия получаем векторы $(0,0,0,0,2) = 10 \cdot e_4$, $(0,0,0,4,0) = 8 \cdot e_3$. Тогда вычитая эти векторы-следствия из e_3 и e_4, получаем векторы e'_3 и e_4'.

Если применить алгоритм построения базиса множества решений ЛОДУ в множестве натуральных чисел, то получаем 24 решения:

$s_1 = (1,0,10,0,0)$, $s_2 = (2,0,8,0,0)$,
$s_3 = (0,9,0,1,0)$, $s_4 = (3,0,6,0,0)$,
$s_5 = (4,0,4,0,0)$, $s_6 = (0,0,6,0,1)$,
$s_7 = (0,6,0,0,1)$, $s_8 = (5,0,2,0,0)$,
$s_9 = (1,0,4,0,1)$, $s_{10} = (0,3,0,3,0)$,
$s_{11} = (6,0,0,0,0)$, $s_{12} = (2,0,2,0,1)$,
$s_{13} = (0,3,0,1,1)$, $s_{14} = (3,0,0,2,0)$,
$s_{15} = (0,0,3,1,0)$, $s_{16} = (3,0,0,0,1)$,
$s_{17} = (2,1,0,1,0)$, $s_{18} = (0,0,0,4,0)$,
$s_{19} = (1,2,0,0,0)$, $s_{20} = (1,0,1,1,0)$,
$s_{21} = (0,0,0,2,1)$, $s_{22} = (0,1,1,0,0)$,
$s_{23} = (0,0,0,0,2)$, $s_{24} = (0,6,0,2,0)$.

Например, векторы $s_{18} = (0,0,0,4,0)$, $s_{23} = (0,0,0,0,2)$ и $s_{17} = (2,1,0,1,0)$ можно представить через базисные векторы следующим образом:

$s_{18} = 8 \cdot e_3 = (0,0,24,40,0) = (0,0,0,4,0)$,

$s_{23} = 10 \cdot e_4 = (0,0,60,0,50) = (0,0,0,0,2)$,

$s_{17} = 10e_1 + e_2 + 5e_3 = (50,0,20,0,0) + (0,1,1,0,0) +$
$+ (0,0,15,25,0) = (50,1,36,25,0) = (2,1,0,1,0)$.

Из этого примера следует, что сведение решения ЛОДУ в кольце Z_m к решению ЛОДУ в множестве натуральных чисел несет в себе много избыточности.

Случай линейного неоднородного диофантового уравнения (ЛНДУ).

Пусть дано ЛНДУ

$$a_1x_1 + ... + a_kx_k + ... + a_nx_n = b, \qquad (11)$$

у которого коэффициент a_k взаимно прост с модулем m. Найдем решение сравнения $a_k y \equiv b (\mathrm{mod}\, m)$, которое при данных условиях

будет единственным. Пусть этим числом будет c, т. е. вектор $x^1=(0,...,0,c,0,...,0)$ будет решением (11). Применяя *TSS*-метод к этому ЛОДУ, которое соответствует (11), находим базис B множества его решений.

Пусть $x^1=(c_1,c_2,...,c_n)$ – некоторое частное решение (11), найденное описанным выше способом, а $B=\{e_1,e_2,...,e_m\}$ – базис множества решений ЛОДУ

$$a_1x_1+a_2x_2+...+a_nx_n=0. \quad (12)$$

Лемма 7 *Произвольное решение ЛНДУ (11) представляется в виде* $u=x^1+\sum_{i=1}^{k}b_ie_i$, *где* x^1 – *частное решение ЛНДУ (11), а* $e_1,...,e_m$ – *базисные векторы множества решений ЛОДУ (12), которое соответствует ЛНДУ (11).*

Пример 6. Найти в кольце F_{12} общее решение ЛНДУ $2x+3y+5z+6u+4v=7$.

Решение. Выбираем ненулевой коэффициент $a_3=5$, который взаимно прост с 12. Решаем уравнение $5s\equiv 7(\mathrm{mod}\,12)$. Решением этого уравнения будет, очевидно, $s=11$. Тогда вектор $x^1=(0,0,11,0,0)$ является искомым частным решением ЛНДУ.

Найдем базис множества решений ЛОДУ $2x+3y+5z+6u+4v=0$. С этой целью заменим коэффициент 5 его дополнением -7 и построим базис множества решений ЛОДУ $2x+3y-7z+6u+4v=0$. Этими решениями будут векторы $e_1=(7,0,2,0,0)$, $e_2=(0,7,3,0,0)$, $e_3=(0,0,6,7,0)$, $e_4=(0,0,4,0,7)$.

Следовательно, общее решение данного ЛНДУ будет иметь вид $x=x^1+b_1e_1+b_2e_2+b_3e_3+b_4e_4$.

Например, при $b_1=2$, $b_2=7$, $b_3=b_4=0$ получаем $u=(2,1,0,0,0)$.

3.2 ЛОДУ над примарными кольцами

Из приведенных выше способов решения ЛОДУ и ЛНДУ вытекает возможность находить решения СЛОДУ и СЛНДУ *TSS*-методом в том случае, когда в системе имеется хотя бы одно уравнение $L_j(x)$, коэффициенты которого удовлетворяют условию 1 и из всех значений $L_i(x)$, $i\neq j$ на векторах из *TSS*-множеств, полученных к данному моменту, тоже имеется хотя бы одно, которое взаимно просто с модулем. Поясним это замечание на примере.

Пример 7. Найти в кольце Z_{12} базис множества решений СЛОДУ

$$S=\begin{cases}L_1(x)=2x_1+3x_2+8x_3+6x_4+4x_5=0,\\ L_2(x)=9x_1+7x_2+0x_3+2x_4+5x_5=0.\end{cases}$$

Решение. Выбираем второе уравнение, поскольку в нем имеется коэффициент $a_{22}=7$, который взаимно прост с модулем 12. Строим *TSS* для уравнения $9x_1-5x_2+0x_3+2x_4+5x_5=0$: $e_1=(5,9,0,0,0)$, $e_2=(0,0,1,0,0)$, $e_3=(0,2,0,5,0)$, $e_4=(0,1,0,0,1)$.

Значения $L_1(x)$ на этих векторах равны 1, 8, 0, 7. Составляем ЛОДУ $x+8y+0z+7u=0$. Коэффициент 7 этого ЛОДУ взаимно прост с модулем 12. Следовательно, решая ЛОДУ $x+8y+0z-5u=0$ *TSS*-методом, получим такие решения: (5,0,0,1), (0,5,0,8), (0,0,1,0). По ним находим базисные решения СЛОДУ *S*: $s_1=(1,10,0,0,1)$, $s_2=(0,8,5,0,8)$, $s_3=(0,2,0,5,0)$.

Следует заметить, что эту же СЛОДУ можно решать с использованием алгоритма построения базиса множества решений в множестве натуральных чисел (например, алгоритма Контежан-Деви [16]). Если применять такого типа алгоритмы, то для приведенной выше СЛОДУ он сгенерирует 46 решений, в то время как только три решения будут составлять базис множества всех решений данной СЛОДУ. Из этого следует, что *TSS*-алгоритм более предпочтителен, чем традиционные алгоритмы построения базиса множества всех решений СЛОДУ, удовлетворяющих условию 1.

ЛОДУ над примарными кольцами. Рассмотрим ЛОДУ над примарным кольцом Z_m

$$L(x)=a_1x_1+...+a_ix_i+...+a_nx_n=0, \quad (13)$$

где $a_i,x_i\in Z_m$, $m=p^{t+1}$, $t>1$, $t\in N$, $i=1,...,n$. Пусть $\mathrm{НОД}(a_1,a_2,...,a_n,m)=p^u$, тогда, сокращая (13) на p^u, получаем ЛОДУ

$$b_1x_1+b_2x_2+...+a_nx_n=0 \quad (14)$$

над примарным кольцом $Z_{m'}$, где $m'=p^v$, $k=m-u=t+1-u$ Полученное уравнение обладает тем свойством, что любое решение ЛОДУ (13) будет решением ЛОДУ (14). Обратное утверждение не имеет места. Действительно, пусть b_1 в (14) взаимно прост с модулем m'. Тогда строим *TSS* этого ЛОДУ, которое в силу теоремы 4 является базисом его множества решений: $s_1=(b_2,c,0,0,0,...,0)$, $s_2=(b_3,0,c,0,0,...,0)$, $s_3=(b_4,0,0,c,0,...,0)$, … ,

$s_{n-1}=(b_n,0,0,0,...,c)$, где $c=p^v-b_1$ – дополнение коэффициента b_1, взятое с противоположным знаком. Поскольку кольцо Z_m с делителями нуля, то очевидным решением (13) будет вектор $s_n=(p^v,0,0,...,0)$, который не выражается неотрицательной линейной комбинацией векторов из *TSS*, так как $c\cdot x\equiv 0(\bmod p^v)$ тогда и только тогда, когда $x=p^v$ силу взаимной простоты c и p^v.

Имеет место следующая теорема.

Теорема 5 *Множество TSS уравнения (14), дополненное вектором* $s_n=(p^v,0,0,...,0)$, *является базисом множества решений ЛОДУ (13).*

Общий случай ЛОДУ. Рассмотрим ЛОДУ, для которых не выполняется условие 1. Предположим, что модуль m имеет разложение на простые множители вида $m=p^cq^d$ (например, $m=12=3\cdot 4=3\cdot 2^2$) и дано ЛОДУ

$$L(x)=a_1x_1+...+a_ix_i+...+a_nx_n=0, \quad (15)$$

где $a_i,x_i\in Z_m$, $i=1,...,n$.. Построим по этому ЛОДУ два ЛОДУ

$$L_1(x)=a_1'x_1+a_2'x_2+...+a_n'x_n=0 \quad (16)$$

и

$$L_2(x)=b_1'x_1+b_2'x_2+...+b_n'x_n=0, \quad (17)$$

где $a_i'\equiv(\bmod p^c)$, $b_i'\equiv a_i(\bmod q^d)$, $i=1,...,n$.

Имеет место лемма:

Лемма 8 *ЛОДУ (16) и (17) удовлетворяют условию 1, т. е. в каждом из этих уравнений существует по крайней мере один коэффициент, который взаимно прост с модулем* p^c *и* q^d.

Отсюда вытекает, что ЛОДУ (16) и (17) удовлетворяют условию 1. Используя *TSS*-алгоритм, построим базисы множеств решений для обеих ЛОДУ. Пусть это будут множества $B_1=\{e_1,e_2,...,e_{n-1}\}$ и $B_2=\{s_1,s_2,...,s_{n-1}\}$ соответственно. Вычислим значения $c_1,c_2,...,c_{n-1}$ для $L_2(x)$ на векторах из B_1 и значения $d_1,d_2,...,d_{n-1}$ для $L_1(x)$ на векторах из B_2, а затем построим множества

$$B_1'=\{e_1'=q_1e_1,e_2'=q_2e_2,...,e_{n-1}'=q_{n-1}e_{n-1}\},$$
$$B_2'=\{s_1'=p_1s_1,s_2'=p_2s_2,...,s_{n-1}'=p_{n-1}s_{n-1}\},$$

где

$$q_i=\begin{cases}q^d, & если \quad НОД(c_i,q^d)=1;\\ \dfrac{q^d}{c_i'} & если \quad НОД(c_i,q^d)=c_i'>1;\end{cases}$$

$$p_i=\begin{cases}p^c, & если \quad НОД(d_i,p^c)=1;\\ \dfrac{p^c}{d_i'} & если \quad НОД(d_i,p^c)=d_i'>1.\end{cases}$$

Имеет место следующая теорема.

Теорема 6 *Множество* $B=B_1'\cup B_2'$ *является базисом множества всех решений ЛОДУ (15).*

Пример 8. Построить базис множества всех решений в кольце Z_{24} для ЛОДУ $2x+3y+8z+6u+4v=0$.

Решение. Разложим модуль $m=24=3\cdot 8$ и, следовательно, получим два ЛОДУ:
$L_1(x)=2x+0y+2z+0u+v=0$ в поле F_3,
$L_2(x)=2x+3y+0z+6u+4v=0$ в кольце Z_8.
Строим базисы множества решений этих ЛОДУ *TSS*-методом:
$B_1=\{(2,0,1,0,0),(0,1,0,0,0),(1,0,0,0,1),(0,0,0,1,0)\}$,
$B_2=\{(5,2,0,0,0),(0,0,1,0,0),(0,6,0,5,0),(0,4,0,0,5)\}$.

Находим значения $L_2(x)$ на векторах из B_1: 4,3,6,6, а также значения $L_1(x)$ на векторах из B_2: 1,2,0,2.

Следовательно,
$B_1'=\{(4,0,2,0,0),(0,8,0,0,0),(4,0,0,0,4),(0,0,0,4,0)\}$,
$B_2'=\{(15,6,0,0,0),(0,0,3,0,0,),(6,0,5,0,0),(0,12,0,0,15)\}$
Отсюда получаем базис множества решений исходного ЛОДУ

$$B=B_1'\cup B_2'=\left\{\begin{matrix}(4,0,2,0,0),(0,8,0,0,0),(4,0,0,0,4),\\(0,0,0,4,0),(15,6,0,0,0),(0,0,3,0,0),\\(0,6,0,5,0),(0,12,0,0,15)\end{matrix}\right\}.$$

После редукции окончательно получаем базис

$$B=\left\{\begin{matrix}(4,0,2,0,0),(0,8,0,0,0),(4,0,0,0,4),(0,0,0,4,0),\\(3,6,0,0,0),(0,0,3,0,0),(0,6,0,1,0),(0,4,0,0,3)\end{matrix}\right\}.$$

Заметим, что векторы (0,0,0,4,0) и (0,8,0,0,0) являются следствиями остальных векторов, поскольку $(0,0,0,4,0)=4\cdot(0,6,0,1,0)$, $(0,8,0,0,0)=8\cdot(0,4,0,0,3)$.

3.3 *TSS*-метод решения СЛОДУ

Из вышеприведенных теорем следует такая процедура построения базиса множества решений СЛОДУ (9). Она состоит в разбиении СЛОДУ S на две подсистемы S_1 и S_2 по модулям p^c и q^d соответственно. Каждая из этих подсистем решается отдельно, находятся вначале базисы B_1 и B_2 соответственно для S_1 и S_2, а затем базис $B=q^dB_1\cup p^cB_2$, где q^dB_1 и p^cB_2 означает умножение каждого вектора из B_1 на q^d, а из B_2 – на p^c. Проиллюстрируем это на примере.

Пример 9. Построить базис множества всех решений в кольце Z_{24} для СЛОДУ

$$S=\begin{cases}2x+3y+8z+6u+4v=0,\\4x+6y+2z+3u+2v=0,\\2x+3y+2z+2u+8v=0.\end{cases}$$

Решение. В результате разложения модуля $m=24=3\cdot 8$ получаем две СЛОДУ:

$$S_1=\begin{cases}L_{11}=2x+0y+0z+0u+1v=0,\\L_{12}=1x+0y+2z+0u+2v=0,\\L_{13}=2x+0y+2z+2u+2v=0,\end{cases}$$

и

$$S_2=\begin{cases}L_{21}=2x+3y+0z+6u+4v=0,\\L_{22}=4x+6y+2z+3u+2v=0,\\L_{23}=2x+3y+2z+2u+0v=0.\end{cases}$$

Решения СЛОДУ S_1 находим в поле F_3, а СЛОДУ S_2 – в примарном кольце Z_8.

Строим базис B_1 СЛОДУ S_1 (см. пример 4):

$B_{11}=\{(2,0,1,0,0),(0,1,0,0,0),(0,0,0,1,0),(1,0,0,0,1)\}$.

Значения L_{12} на векторах из B_{11}: 1,0,0,0. Тогда $B_{12}=\{(0,1,0,0,0),(0,0,0,1,0),(1,0,0,0,1)\}$.

Значения L_{13} на векторах из B_{12}: 0,2,1. Тогда $B_1=B_{13}=\{(0,1,0,0,0),(1,0,0,1,1)\}$.

Подставляя векторы из B_1 в уравнения СЛОДУ S_2 (для выяснения числа, на которое нужно их умножать), получаем значения для первого вектора (3,6,3) и для второго (12,9,4). Поскольку НОД(3,6,3,8)= НОД(12,9,4,8) =1, то имеем $8\cdot B_1=\{(0,8,0,0,0),(8,0,0,8,8)\}$.

Строим базис B_2 СЛОДУ S_2 (см. пример 4):

$B_{21}=\{(5,2,0,0,0),(0,0,1,0,0),(0,6,0,5,0),(0,4,0,05)\}$.

Значения L_{22} на векторах из B_{21}: 0,2,3,2. Тогда $B_{22}=\{(5,2,0,0,0),(0,4,5,2,0),(0,0,0,2,1)\}$.

Значения L_{23} на векторах из B_{22}: 0,2,4. Тогда

$B_2=B_{23}=\{(5,2,0,0,0),(0,0,2,2,3)\}\cup\{(0,0,4,0,0)\}$.

Подставляя векторы из B_2 в уравнения СЛОДУ S_1 (для выяснения числа, на которое нужно их умножать), получаем значения для первого вектора (2,5,2), для второго (7,10,14) и для третьего (8,8,8). Поскольку НОД(2,5,2,3)=НОД(7,10,14,3)=НОД(8,8,8,3)=1, то имеем $3\cdot B_2=\{(15,6,0,0,0),(0,0,6,6,9),(0,0,12,0,0)\}$.

Таким образом, после редукции базис множества решений данной СЛОДУ принимает вид

$$B=\begin{Bmatrix}(0,8,0,0,0),(8,0,0,8,8),(6,4,0,0,0),\\(0,0,0,12,6),(0,0,12,0,0)\end{Bmatrix}.$$

В общем случае, если модуль m имеет разложение, содержащее больше двух сомножителей, т. е. $m=p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$, то получаем k подсистем. Принимая во внимание, что арифметическая сложность выполнения тпераций сложения и вычитания в кольце Z_m пропорциональна s (s – максимальная разрядность рассматриваемых чисел), операций умножения и деления, как и вычисления НОД двух чисел, меньших $m-s^2$, то арифметическая сложность построения базиса множества решений СЛОДУ имеет вид:

– l^3 – решение одного ЛОДУ и решение одного промежуточного ЛОДУ;

– n^2l^3 – вычисление значений и сокращение на НОД $L(x)$.

– n^2l^3 – построение комбинаций векторов, составляющих базис множества решений ЛОДУ $(l=\max(n,s,r))$.

Таким образом, арифметическая сложность перехода от предыдущего к последующему ЛОДУ в одной подсистеме пропорциональна величине l^5, где $l=\max(n,s,r)$, $s=\log m$. Такая процедура повторяется r раз и в результате имеем $O(l^6)$, где $l=\max(n,s,k,r)$. Иными словами имеет место следующая теорема.

Теорема 7 *Множество B, построенное TSS-методом, является базисом множества решений СЛОДУ (9). Арифметическая сложность построения B пропорциональна величине* $O(l^6)$, *где* $l=\max(n,s,k,r)$.

3.4 *TSS*-метод решения СЛНДУ

Построение базиса множества решений СЛНДУ сводится к поиску частного решения ЛНДУ и базиса множества решений соответствующего ему ЛОДУ.

Процесс построения общего решения СЛНДУ включает следующие шаги:

1) $i=1$;

2) Найти частное решение x^1 ЛНДУ $L_i(x)=b_i$. Если x^1 не существует, то (СТОП: решений нет), иначе на шаг 3);

3) Построить базис $B_i=(e_{i1},e_{i2},...,e_{iw})$ ЛОДУ, которое соответствует ЛНДУ $L_i(x)=b_i$;

4) Найти значения $c=L_{i+1}(x^1)$ и $c_1=L_{i+1}(e_{i1}),...,c_w=L_{i+1}(e_{iw})$, где $e_{ij}\in B_i$, $j=1,2,...,w$;

5) Найти частное решение y^1 ЛНДУ

$$c_1y_1+...+c_wy_w=b_{i+1}-c. \qquad (18)$$

Если y^1 не существует, то (СТОП: решений нет), иначе на шаг 6);

6) Построить базис B_i' ЛОДУ, которое соответствует (18);

7) Построить базис B_{i+1} для ЛНДУ $L_{i+1}(x)=b_{i+1}$ исходя из B_i';

8) Если $i+1<r$, то ($i=i+1$; на 4)), иначе (СТОП: печать B_{i+1}).

Правильность этой процедуры следует из доказанных выше теорем и лемм. Характеристику временной сложности дает следующая теорема.

Теорема 8 *Временная сложность приведенной выше процедуры построения общего решения СЛНДУ выражается величиной* $O(l^7)$, *где* $l=\max(r,s,n,k)$.

Проиллюстрируем работу этой процедуры на примерах.

Пример 10. Найти в кольце Z_{12} общее решение СЛНДУ

$$S=\begin{cases}2x_1+3x_2+8x_3+6x_4+4x_5=8\\4x_1+3x_2+6x_3+6x_4+8x_5=6\end{cases}$$

Решение. Поскольку разложение 12 на простые множители имеет вид $m=12=3\cdot4$, то построение общего решения первого ЛНДУ системы S сводится к нахождению его частного решения и построения в кольце Z_{12} базиса ЛОДУ вида $2x_1+3x_2+8x_3+6x_4+4x_5=0$.

Очевидным решением ЛНДУ является вектор $x^1=(4,4,0,0,0)$, а построение базиса множества решений ЛОДУ в кольце Z_{12} сводится к решению двух ЛОДУ соответственно в поле F_3 и в примарном кольце Z_4 вида

$$2x_1+0x_2+2x_3+0x_4+1x_5=0,$$
$$2x_1+3x_2+0x_3+2x_4+0x_5=0.$$

Базис множества решений первого уравнения составляют векторы (2,0,1,0,0), (0,1,0,0,0), (0,0,0,1,0), (1,0,0,0,1), а базис множества решений второго уравнения составляют векторы (1,2,0,0,0), (0,2,0,1,0), (0,0,1,0,0), (0,0,0,0,1).

Значения второго уравнения на векторах из первого базиса равны: 0,3,2,2, а значения первого уравнения на векторах из второго базиса равны: 2,0,2,1. Следовательно, базис B_1 исходного ЛОДУ включает векторы (2,0,1,0,0), (0,4,0,0,0), (0,0,0,2,0), (2,0,0,0,2), (3,6,0,0,0), (0,2,0,1,0), (0,0,3,0,0), (0,0,0,0,3).

Тогда общее решение исходного ЛНДУ имеет вид $x=x^1+\sum_{i=1}^{n}a_ie_i$, где $e_i\in B_1$, $i=1,...,8$.

Подставляя полученные векторы во второе уравнение исходной СЛНДУ, получаем такие значения $L_2(x^1)=4$, а на остальных векторах соответственно 2,0,0,0,6,0,6,0. Строим уравнение (для упрощения опущены нулевые коэффициенты) $2y_1+6y_2+6y_3=6-4=2$ или $y_1+3y_2+3y_3=1$ в кольце Z_6.

Решениями полученного уравнения будут векторы (3,0,5), (3,5,0) и частное решение $y^1=(1,0,0)$. Этим векторам соответствуют такие редуцированные векторы:
$x^1=(0,0,1,0,0)$, $s_1=(3,2,3,0,0)$, $s_2=(0,0,6,0,0)$,
$s_3=(0,2,0,1,0)$, $s_4=(0,0,0,0,3)$, $s_5=(2,0,0,0,2)$.

Таким образом, общее решение исходной СЛНДУ имеет вид $x=x^1+\sum_{i=1}^{5}a_is_i$.

Пример 11. Найти в кольце Z_{12} общее решение СЛНДУ

$$S=\begin{cases}2x_1+3x_2+8x_3+6x_4+4x_5=8\\4x_1+3x_2+6x_3+6x_4+8x_5=5\end{cases}$$

Решение. Общее решение первого ЛНДУ было найдено в предыдущем примере: $x=x^1+\sum_{i=1}^{8}a_ie_i$, где $x^1=(4,4,0,0,0)$; а
$e_1=(2,0,1,0,0)$, $e_2=(0,4,0,0,0)$, $e_3=(0,0,0,2,0)$,
$e_4=(2,0,0,0,2)$, $e_5=(3,6,0,0,0)$, $e_6=(0,2,0,1,0)$,
$e_7=(0,0,3,0,0)$, $e_8=(0,0,0,0,3)$.

Подставляя эти векторы во второе уравнения СЛНДУ, получаем такие значения: $L_2(x^1)=4$, а на остальных векторах – значения 2,0,0,0,6,0,6,0. Строим уравнение (для упрощения опущены нулевые коэффициенты) $2y_1+6y_2+6y_3=5-4=1$. Полученное уравнение не имеет решений, поскольку наибольший общий делитель модуля и

коэффициентов равен 2, а 2 не делит свободный член 1. Следовательно, исходная СЛНДУ решений не имеет (несовместна).

Отметим, что приведенные алгоритмы имеют полиномиальные оценки временной сложности при условии известного разложения модуля на простые множители. Проблема разложения натурального числа на простые множители (которая называется проблемой факторизации) является одной из наиболее важных проблем теории чисел. Имеется несколько алгоритмов ее решения: алгоритмы Полларда, Полларда-Штрассена, решета числового поля [14]. Наиболее эффективным алгоритмом в настоящее время является последний из перечисленных алгоритмов, потому что в отличие от первых двух алгоритмов он ищет большие делители заданного числа. Все эти алгоритмы имеют экспоненциальные оценки временной сложности, наилучшая из которых для заданного числа n имеет вид $O\left(2^{c\sqrt{\ln n \ln\ln n}}\right)$.

Выводы

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 установлением того, 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.

Список использованных источников

1. Донец Г. А. Решение задачи о сейфе на (0,1)-матрицах // КиСА. – 2002. – № 1. – С. 98 – 105.

2. 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.

3. Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях // КиСА. – 2006. – № 2. – С. 3 – 17.

4. Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях // Кибернетика и системный анализ. – 2006. – № 2. – С. 3 – 17.

5. Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в полях вычетов // Кибернетика и системный анализ. – 2007. – № 2. – С. 15 – 23.

6. Крывый С.Л. О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в области натуральных чисел. // Кибернетика и системный анализ. – 1999. – N 4. – С. 12 – 36.

7. Крывый С. Л. Критерий совместности систем линейных диофантовых уравнений над множеством натуральных чисел // Допов. НАНУ. – 1999. – № 5. – С.107 – 112.

8. Крывый С.Л. О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в области натуральных чисел // КиСА. – 1999. – № 4. – С. 12 – 36.

9. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО. – 2002. – 103 с.

10. Чугаенко А.В. О реализации *TSS*-алгоритма. ж. Управляющие системы и машины. – 2007. – N 3. – С. 14 – 26.

11. Baader F., Ziekmann J. Uni_cation theory Handbook of Logic in Arti_cial Intelligence and Logic Programming. – Oxford University Press. – 1994. – P. 1 – 85.

12. Allen R., Kennedy K. Automatic translation of FORTRAN program to vector form // ACM Transactions on Programming Languages and systems. – 1987. – V. 9, N4. – P. 491 – 542.

13. Contejan E., Ajili F. Avoiding slack variables in the solving of linear diophantine equations and inequations // Theoretical Comp. Science. – 1997. – V. 173. – P. 183 – 208.

14. Pottier L. Minimal solution of linear diophantine systems: bounds and algorithms // In Proc. of the Fourth Intern. Conf. on Rewriting Techniques and Applications. –Como. – Italy. – 1991. – P. 162 – 173.

15. Domenjoud E. Outils pour la deduction automatique dans les theories associatives-commutatives // Thesis de Doctorat d'Universite: Universite de Nancy I. –1991.

16. Clausen M., Fortenbacher A. E_cient solution of linear diophantine equations // J.

Symbolic Computation. – 1989. – V. 8, N. 1,2. – P. 201 – 216.

17. Romeuf J. F. A polinomial Algorithm for Solvin systems of two linear Diophantine equations // TCS. – 1990. – 74, N3. – P. 329 – 340.

18. Filgueiras M.,Tomas A.P. A Fast Method for Finding the Basis of Non-negative Solutions to a Linear Diophantine Equation // J. Symbolic Computation. – 1995. – 19, N2. – P. 507 – 526.

19. 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.

20. Bulatov A. H-coloring dichotomy revisited. Theoretical Computer Science. – 2005. – V. 349. – N 1. – P. 31 – 39.

21. Bulatov A., Krokhin A., Jeavons P.G. Classifying the complexity of constraints using finite algebras // SIAM Journ. Computing. – 2005. – v. 34. – N 3. – P. 720 – 742.

22. 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.

23. Drakengren T., Jonsson P. A complete classification of tractability in Allen's algebra relative to subsets of basic relations // Artificial Intelligence. – 1998. – V. 106. – P. 205 – 219.

24. Jeavons P.G. Constructing constraints // In Proceed. 4th Intern. Conf. on Constraint Programming – CP'98 (Pisa,October 1998). – 1998. – V. 1520. – Lecture Notes in Comput. Science. : Springer-Verlag. – P. 2 – 16.

25. Jeavons P.G. On the algebraic strukture of combinatorial problems. Theoretical Computer Science. – 1998. – V. 200. – P. 185 – 204.

26. Jeavons P.G., Cohen D.A., Gyssens M. Closure properties of constraints // Journ. of the ACM. – 1997. – V. 44. – P. 527 – 548.

27. Jeavons P.G., Cohen D.A., Gyssens M. How to determine the expressive power of constraints. Constraints. – 1999. – V. 4. – P. 113 – 131.

28. Krokhin A., Jeavons P.G., Jonsson P. Reasoning about temporal relations: The tractable subalgebras of Allen's interval algebra // Journ. of the ACM. – 2003. – V. 50. – P. 591 – 640.

29. Krokhin A., Jeavons P.G., Jonsson P. Constraint satisfaction problems on intervals and lengths // SIAM Journ. On Discrete Mathematics. – 2004. – V. 17. – P. 453 – 477.

30. Nebel B., Burkert J. Reasoning about temporal relations: a maximal tractable subclass of Allen's interval algebra // Journal of the ACM. – 1995. – V. 42. – P. 43 – 66.

31. Renz J., Nebl B. On the complexity of qualitative spatial reasoning: A maximal tractable fragment of the Region Connection Calculus // Artificial Intelligence. – 1999. – V.108. – P. 69 – 123.

32. Cooper M. C., Cohen D.A., Jeavons P.G. Caracterising tractable constraints // Artificial Intelligence. – 1994. – V. 65. – P. 347 – 361.

33. Schaefer T. J. The Complexity of satisfability problems // In Propc. 10-th ACM Symposium on Theory of Computing, STOC'78. 1978. – P. 216 – 226.

34. Papadimitriou C.H. Computational complexity. Addison-Wesley. – 1994. – 462 p.

35. Poschel R., Kaluznin L.A. Funktionen und Relationenalgebren. DVW. Berlin. – 1979. – 262 p.

36. Post E.L. The two-valued iterative systems of mathematical logic. Annals Mathematical Studies. – Princeton University Press. – 1941. – 26 p.

37. Szendrei A. Clones in universal algebras // Seminares de Mathematigues Superieures. University of Montreal. – 1986. – P. 253 – 262.

Сведения об авторе:

Крывый Сергей Лукьянович – д. ф.-м. наук, профессор кафедры информационных систем Национального университета им. Т. Шевченко. Научные интересы: дискретная математика, теория автоматов сетей Петри, анализ естественноязыковых текстов.

E-mail: krivoi@i.com.ua