АЛГОРИТМЫ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ В ДИСКРЕТНЫХ ОБЛАСТЯХ

Сергей Крывый

Аннотация. *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.*

Abstract.*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.*

Keywords: *Systems of linear Diophantine constraints, minimal supported set of solutions, basis of solutions, satisfaction problem of constraints*

ACM Classification Keywords: *G 2.1 Discrete mathematics: Combinatorics*

Conference topics: *Algorithmic and Mathematical Foundations of the Artificial Intelligence*

Введение

В настоящей работе рассматривается краткий обзор алгоритмов построения минимального порождающего множества решений и базиса множества решений систем линейных диофантовых уравнений в множестве натуральных чисел, в поле и кольце Z_m вычетов по модулю простого и составного числа *m*. Данная работа является продолжением работ [Крывый, 1999] - [Крывый, 2007]. В основе предлагаемых алгоритмов лежит TSS-метод построения минимального порождающего множества решений систем линейных однородных диофантовых уравнений в множестве натуральных чисел *N* [Крывый, 1999]. К такого рода системам и методам их решений сводятся задачи математических игр [Донец, 2002], распознавания изображений [Донец,2005], криптографии [Черемушкин, 2002], распараллеливания циклов [Allen,1987], построение линейных мозаик [Донец, 2005], унификации в теориях первого порядка [Baader,1994], арифметики Пресбургера [Comon, 1999], анализ структурных свойств сетей Петри [Murata,1990] и многие другие задачи. Описываемые алгоритмы характеризуются оценками временной сложности.

Предварительные сведения

Системой линейных диофантовых констрейнтов (СЛДК) будем называть систему вида $Ax\ R\ b$, $A = |a_{ij}|$, $a_{ij}, b \in Z$ (множество целых чисел), $x \in N$, а $R \in \Omega = \{=, \leq, <, \neq, >, \geq\}$, $i = 1,2,\ldots p$, $j=1,2,\ldots,q$. Решением СЛДК 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 $L_i(x)Rb_i$ в истинное высказывание для всех i = 1,2,...,p. СЛДК называется однородной (СЛОДК)}, если все b_i равны нулю, в противном случае СЛДК называется неоднородной (СЛНДК). Если СЛОДК состоит только из уравнений, то она называется системой линейных однородных диофантовых уравнений (СЛОДУ). Если СЛНДК состоит только из уравнений, то она

называется системой линейных неоднородных диофантовых уравнений (СЛНДУ). Методы решения СЛНДУ сводятся, как известно, к решению соответствующей СЛОДУ и поэтому в дальнейшем основное внимание будет уделяться методам и алгоритмам решения СЛОДУ.

Пусть S - СЛОДУ и e_1 = *(1,0,…,0,0),* e_2 = *(0,1,…,0,0),…,* e_q = *(0,0,...,0,1)* - единичные векторы из множества N^q, которые называются векторами канонического базиса множества N^q. Введем на множестве N^q отношение порядка $\leq$, которое определяется таким образом: если $x=(x_1,...,x_q)$, $y=(y_1,...,y_q) \in N^q$ $x=(x_1,...,x_q)$, то *x* $\leq$ *y* тогда и только тогда, когда для всех *i=1,…q*, $x_i \leq y_i$. Ясно, что это отношение является частичным порядком и относительно этого порядка можно говорить о минимальных элементах в множестве N^q. Очевидно, что наименьшим элементом в множестве N^q есть нулевой вектор.

Пусть *M* - множество решений СЛОДУ *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.

Известно, что множество *B* минимальных элементов множества решений *M* системы *S* составляет базис множества *M* и если |*M*| > 1, то базис *B* всегда существует, конечен и всякий элемент из M представим в виде неотрицательной линейной комбинации векторов из B. Известно также, что процесс решения СЛНДУ или системы линейных диофантовых неравенств (СЛДН) может быть сведен к решению СЛОДУ, поэтому основное место в исследованиях уделяется СЛОДУ. Следует заметить, что в общем случае такое сведение увеличивает размерность пространства, над которым рассматривается полученная СЛОДУ, что сказывается на эффективности вычислений. Однако, имеются методы сведения, которые не увеличивают размерности пространства [Contejan, 1997].

Критерий совместности СЛОДУ

Критерий совместности СЛОДУ, используемый здесь, и алгоритм его реализации подробно описаны в работах [Крывый, 1999] и [Крывый, 1999,1], поэтому приведем лишь необходимые факты, нужные в дальнейшем, следуя этим работам.

Пусть дана СЛОДУ S = $L_1(x)=0 \wedge L_2(x)=0 \wedge ... \wedge L_p(x)=0$. Рассмотрим множество векторов канонического базиса $M_0' = \{e_1,...,e_q\}$ и первое уравнение $L_1 = a_{11}x_1 + a_{12}x_2 + ... + a_{1q}x_q$ = *0* системы *S*. С помощью функции $L_1(x)$ разобъем элементы множества M_0' на такие три группы $M_1^0 = \{e^0 \mid L_1(e^0)=0\}$, $M_1^+ = \{e^+ \mid L_1(e^+)>0\}$, $M_1^- = \{e^- \mid L_1(e^-)<0\}$ Ясно, что если одно из множеств $M_1^0 \cup M_1^+$ или $M_1^0 \cup M_1^-$ пусто, то уравнение $L_1(x)=0$ не имеет нетривиальных решений в множестве натуральных чисел. Допустим, что хотя бы два из множеств M_1^0, M_1^+, M_1^- непусты, тогда рассмотрим множество

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

Используя функцию $L_2(x)$, разобъем элементы множества $M_1^{'}$ аналогично предыдущему также на три группы $M_2^0 = \{e^0 \mid L_2(e^0)=0\}$, $M_2^+ = \{e^+ \mid L_2(e^+)>0\}$, $M_2^- = \{e^- \mid L_2(e^-)<0\}$.

Допустим, что хотя бы два из этих множеств непусты, тогда построим множество

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

Предположим, что таким способом построено множество $M_j^{'}$ из множеств $M_j^0 = \{e_r^0 \mid L_j(e_r^0) = 0\}$, $M_j^+ = \{e_i^+ \mid L_j(e_i^+) > 0\}$, $M_j^- = \{e_s^+ \mid L_j(e_s^+) < 0\}$ с помощью функции $L_j(x)$ и это множество непусто. Непосредственно из этих построений вытекает такое утверждение [Крывый, 1999].

Теорема 1. *Элементы множества* $M_j^{'}$ *есть решениями системы уравнений* $L_1(x) = 0 \wedge L_2(x) = 0 \wedge ... \wedge L_j(x) = 0$.

Определение 1. *Множество* $M_j^{'}$, *построенное выше, будем называть усеченным множеством решений системы S'* = $L_1(x) = 0 \wedge L_2(x) = 0 \wedge ... \wedge L_j(x) = 0$.

Пусть $M_j{'} = \{e_1', ..., e_k'\}$ - усеченное множество решений системы S', а M_j -- множество всех ее решений. Тогда имеет место такое утверждение.

Теорема 2. *Для всякого вектора* $x \in M_j - M_j^{'}$ *существует представление в виде неотрицательной линейной комбинации вида* $tx = b_1e_1' + b_2e_2' + ... + b_ke_k'$,, *где* $t, b \in N$, $t \neq 0$, $e_i^{'} \in M_j^{'}$, $i = 1, 2, ..., k$.

Из этой теоремы следует такой критерий совместности СЛДОДУ в множестве натуральных чисел .

Теорема 3. *СЛОДУ S* = $L_1(x) = 0 \wedge L_2(x) = 0 \wedge ... \wedge L_p(x) = 0$ *совместна тогда и только тогда, когда её усеченное множество* $M_p^{'} \neq \varnothing$.

Допустим, что СЛОДУ S совместна и $M_p{'} = \{e_1', ..., e_k'\}$ ее усеченное множество решений. Тогда имеют место такие утверждения.

Теорема 4. *Векторы из усеченного множества решений являются минимальными решениями СЛОДУ S, т.е. являются ее базисными решениями [Крывый, 1999,1].*

Теорема 5. *Пусть* $x = (x_1, ..., x_q)$ *минимальное решение СЛОДУ S и* $M' = \{e_1' = (\alpha_{11}, \alpha_{11}, ..., \alpha_{1q}), ..., e_k' = (\alpha_{k1}, \alpha_{k1}, ..., \alpha_{kq})\}$ *её усеченное множество решений. Тогда верхняя граница x' величины координат произвольного решения СЛОДУ удовлетворяет неравенству x'* = *max* $x_i \leq k \max \alpha_{ij}$.

Теорема 6. *Сложность алгоритма определения совместности СЛОДУ в общем случае имеет экспоненциальную сложность по числу уравнений в системе.*

Решение СЛДУ в кольцах и полях вычетов

Кольцом вычетов Z_m по модулю числа *m* определяется обычным образом: т. е. это алгебра с двумя нульарными операциями 0 и 1, двумя бинарными социативно-коммутативными и дистрибутивными операциями + и –. Заметим, что это кольцо имеет делители нуля. На основании законов для операций в кольце Z_m вытекает справедливость такого тождества: для всех $x, y \in Z_m$ $x + y = 0$ следует $x = -y$.

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*.

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

$L(x) = a_1x_1 + ... + a_nx_n = 0$, где $a_i, x_i \in Z_m, i = 1, 2, ..., n.$

(Условие 1): Допустим, что $a_i \neq 0$ и этот коэффициент взаимно прост с модулем *m*.

Теорема 7. *Множество B решений ЛОДУ L(x)=0, 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, 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 L(x) = 0 является базисом множества всех решений этого ЛОДУ.*

Случай линейного неоднородного диофантового уравнения (ЛНДУ). Пусть дано ЛНДУ $L(x) = a_1x_1 + ... + a_nx_n = b,$ у которого коэффициент a_k взаимно прост с модулем *m*. Найдем решение сравнения $a_k y \equiv b \pmod m$, которое при данных условиях будет единственным. Пусть этим числом будет c, т. е. вектор x = (0,…,0,c,0,…, 0) будет решением *L(x) = b*. Применяя TSS-метод к этому ЛОДУ, которое соответствует *L(x) = b* , находим базис B множества его решений.

Теорема 8. *Множество B с добавленным вектором x = (0,…,0,c,0,…, 0), найденные описанным выше способом, является базисом множества решений ЛНДУ.*

Следует заметить, что такого типа СЛОДУ можно решать с использованием алгоритма построения базиса множества решений в множестве натуральных чисел (например, алгоритма Контежан-Деви [Contejan,1997]). Если применять такого типа алгоритмы, то для приведенной выше СЛОДУ он сгенерирует большое количество решений, в то время как только несколько из них 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 $L(x) = a_1x_1 + ... + a_nx_n = 0,$ где $a_i, x_i \in Z_m, i = 1, 2, ..., n, m = p^{t+1}, t > 1, t \in N$. Пусть $НОД(a_1, a_2, ..., a_n, m) = p^u$, тогда сокращая коэффициенты на p^u, получаем ЛОДУ удовлетворяющее условию 1. Имеет место следующая теорема.

Теорема 9. *Множество TSS уравнения L(x) = 0, дополненное вектором $s = (p^v, 0, 0, ..., 0)$, является базисом множества решений ЛОДУ L(x) =0.*

Общий случай ЛОДУ. Рассмотрим ЛОДУ, для которых не выполняется условие 1. Предположим, что модуль *m* имеет разложение на простые множители вида $m = p^c q^d$ (например, *m* = 12 = 3*4 = 3* 2^2) и дано ЛОДУ $L(x) = a_1x_1 + ... + a_nx_n = 0,$ где $a_i, x_i \in Z_m, i = 1, 2, ..., n.$. Построим по этому ЛОДУ два

ЛОДУ $L_1(x) = a_1'x_1 + ... + a_n'x_n = 0,$ и $L_2(x) = b_1'x_1 + ... + b_n'x_n = 0,$ в которых коэффициенты приведены по модулям p^c и q^d. Построим базисы множеств решений B_1, B_2 для этих ЛОДУ. Имеет место следующая теорема.

Теорема 10. *Множество* $B = B_1 \cup B_2$ *является базисом множества всех решений ЛОДУ* $L(x) = a_1x_1 + ... + a_nx_n = 0$.

TSS-метод решения СЛДУ в кольцах вычетов и полях вычетов. Из вышеприведенных теорем следует такая процедура построения базиса множества решений СЛОДУ. Она состоит в разбиении СЛОДУ S на две подсистемы S' и S" по модулям p^c и q^d соответственно. Каждая из этих подсистем решается отдельно, находятся вначале базисы B' и B" соответственно для S' и S", а затем базис B = $q^d B' \cup p^c B''$, где q^d *B'* и p^c *B"* означает умножение каждого вектора из *B'* на q^d, а из *B"* - на p^c.

В общем случае, если модуль *m* имеет разложение, содержащее больше двух сомножителей, т.е. $m = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$, то получаем *k* подсистем. Принимая во внимание, что арифметическая сложность выполнения операций сложения и вычитания в кольце Z_m пропорциональна *s*, где *s* - максимальная разрядность рассматриваемых чисел; выполнения операций умножения и деления, как и вычисления НОД двух чисел, меньших *m*, - s^2, то арифметическая сложность построения базиса множества решений СЛОДУ имеет вид $O(l^5)$. Таким образом, арифметическая сложность перехода от предыдущего к последующему ЛОДУ в одной подсистеме пропорциональна величине $O(l^5)$, 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

Теорема 11. *Множество B, построенное TSS-методом, является базисом множества решений СЛОДУ* $L(x) = a_1x_1 + ... + a_nx_n = 0$. *Арифметическая сложность построения B пропорциональна величине* $O(l^6)$, *где l = max (n,s,k,r).*

TSS-метод решения СЛНДУ. Построение базиса множества решений СЛНДУ сводится к поиску частного решения ЛНДУ и базиса множества решений соответствующего ему ЛОДУ. Характеристику временной сложности дает следующая теорема.

Теорема 12. *Временная сложность приведенной выше процедуры построения общего решения СЛНДУ выражается величиной* $O(l^7)$, *где l = max (n,s,k,r).*

Заметим, 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 [Черемушкин, 2002]. 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 $O(2^{c\sqrt{\ln n \ln\ln n}})$, где *c* – константа, а *n* – число неизвестных в СЛДУ.

Очевидно, что описанные алгоритмы применимы к СЛДУ в полях вычетов, поскольку в таких полях условии 1 автоматически выполняется. А это значит, что все приведенные выше факты верны для этих полей и в случае простого модуля нет необходимости в его факторизации. Следовательно, алгоритмы решения СЛДУ в полях вычетов по модулю простого числа имеют полиномиальную оценку временной сложности и эта оценка имеет вид $O(q^2n^2)$ [Крывый, 2007].

Заключение

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 только верхних оценок (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.

Библиография

[Донец, 2002] Донец Г. А. Решение задачи о сейфе на (0,1)-матрицах//Кибернетика и системный анализ. -2002. - N 1. - С. 98--105.

[Донец, 2005] 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.

[Крывый, 2006] Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях// Кибернетика и системный анализ - 2006. - N 2. - С. 3 -- 17.

[Крывый, 2007] Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в полях вычетов.Там же. - 2007. - N 2. - С. 15 -- 23.

[Крывый, 2007,1] Крывый С. Л. Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов.Там же. - 2007. - N 6. - С. 15 -- 23.

[Крывый, 1999] Крывый С. Л. О некоторых методах решения и критериях совместности систем линейных диофантовых уравнений в области натуральных чисел. Там же. - 1999. - N 4. - С.12 -- 36.

[Крывый,1999,1] Крывый С. Л. Критерий совместности систем линейных диофантовых уравнений над множеством натуральных чисел//Доклады НАНУ. - 1999. - N 5. - С.107-112.

[Черемушкин, 2002] Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. - М.: МЦНМО. - 2002. - 103 с.

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

[Baader,1994] Baader F., Ziekmann J. Unification theory. Handbook of Logic in Artificial Intelligence and Logic Programming.-Oxford University Press. -1994. - P. 1--85.

[Allen,1987] 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.

[Contejan, 1997] Contejan E., Ajili F. Avoiding slack variables in the solving of linear diophantine equations and inequations. Theoretical Comp. Science. -1997.- 173. - P.183 -- 208.

[Pottier, 1991] 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.

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

[Clausen, 1989] Clausen M., Fortenbacher A. Efficient solution of linear diophantine equations. J. Symbolic Computation. - 1989. - 8, N 1,2, -P. 201--216.

[Romeuf, 1990] Romeuf J. F. A polinomial Algorithm for Solvin systems of two linear Diophantine equations. TCS. - 1990. - 74, N3. - P.329--340.

[Filgueiras, 1995] 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.

[Comon, 1999] 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.

[Murata, 1989] Murata T. Petri Nets: Properties, Analysis and Applications. In Proceedings of the IEEE. -1989. – v. 7.- №4. – P. 541-580.

Сведения об авторе

Крывый Сергей Лукьянович - *Институт кибернетики им. В.М.Глушкова НАН Украины; Украина, Киев.*
email: krivoi@i.com.ua