ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ МЕТОДА ТУДИКА

Зайцев Д.А.
Одесская национальная академия связи, кафедра сетей связи

Abstract

Zaitsev D.A. A theotretical grounding of the Toudic method. *A theotretical grounding of the well-known and described in the literature as heuristic Toudic method meant for a searching of the Petri-nets invariants, that is an integer nonnegative decision of a linear homogeneous diophantine equations system, is proposed. First the grounding of the one equation's decision basis is given, then the results for the whole equation's system are synthesized. To generate all solutions via Toudic's basis a linear combination is extended by special operation of reduction in common measure of vectors' component.*

Проблема решения систем линейных однородных диофантовых уравнений возникает в теории сетей Петри [1] в процессе вычисления сетевых инвариантов, а также в других областях компьютерных наук. Инварианты являются мощным инструментом для исследования структурных свойств сетей Петри. Они позволяют определять ограниченность, консервативность, необходимые условия живости и отсутствия тупиков. Эти свойства являются существенными для анализа реальных объектов [1], в особенности, коммуникационных протоколов, производственных систем, аппаратных и программных средств вычислительной техники.

Известен метод, предложенный Тудиком [2] и позволяющий находить целые неотрицательные решения системы линейных диофантовых уравнений посредством преобразований матриц. Метод представлен без формального обоснования и поэтому характеризуется в литературе [3] как эвристический. В начале мы имеем единичную матрицу, которая при завершении вычислений содержит базисные решения. В настоящее время, не смотря на асимптотически экспоненциальную сложность, метод находит широкое применение в промышленных моделирующих системах [1,3].

В математике известно множество методов для нахождения решений линейных систем на множестве рациональных чисел. Это и теоретические методы, основанные на вычислении определителей матриц, и классический метод Гаусса, а также численные методы, разрабатываемые в целях минимизации ошибок вычислений (невязок).

Если рассматривается целочисленная матрица системы и требуется найти целые решения, то требуются специфические методы. Эта группа методов основана на унимодулярных преобразованиях матриц [4] для получения нормальной формы Смита. Известны эффективные полиномиальные алгоритмы [5] основанные на последовательном решении системы в полях классов вычетов по модулям простых чисел с последующим восстановление общего решения системы в кольце целых.

В теории сетей Петри решения уравнения состояний [1] представляют собой векторы счёта допустимых последовательностей срабатываний переходов сети, и поэтому должны быть неотрицательными. Решение однородных систем требуется для нахождения сетевых инвариантов, являющихся мощным средством исследования структурных свойств сетей. Следует отметить, что множество неотрицательных целых чисел является моноидом, что затрудняет применение результатов, полученных для более сложных алгебраических структур, таких как кольца и поля.

Таким образом, имеется проблема, состоящая в построении базиса целых неотрицательных решений линейной системы уравнений. В настоящей работе эта проблема решена для однородных систем.

1. Решение одного уравнения

Начнём с построения решений для одного уравнения. Итак, имеется уравнение

$$\overline{a}\cdot\overline{x}-\overline{b}\cdot\overline{y}=0 \qquad (1)$$

где $\overline{a},\overline{x},\overline{b},\overline{y}$ это целые неотрицательные векторы, причём размерность $\overline{a},\overline{x}$ равна m, а размерность $\overline{b},\overline{y}$ равна n; $\overline{a},\overline{b}$ векторы известных коэффициентов, а $\overline{x},\overline{y}$ векторы неизвестных.

Теорема 1. Общее решение уравнения (1) в неотрицательных целых числах имеет вид $\dfrac{\overline{z}\cdot G}{k}$, где k - общий делитель компонент вектора $\overline{z}\cdot G$, $\overline{z}=(z_1^1,z_2^1,\dots,z_n^1,z_1^2,z_2^2,\dots,z_n^2,\dots,z_1^m,z_2^m,\dots,z_n^m)$ - произвольный вектор неотрицательных целых, а матрица G имеет форму:

$$G=\left|\begin{array}{cccccccc}
b_1 & 0 & .. & 0 & a_1 & 0 & .. & 0\\
b_2 & 0 & .. & 0 & 0 & a_1 & .. & 0\\
: & : & : & : & : & : & : & :\\
b_n & 0 & .. & 0 & 0 & 0 & .. & a_1\\
0 & b_1 & .. & 0 & a_2 & 0 & .. & 0\\
0 & b_2 & : & 0 & 0 & a_2 & .. & 0\\
: & : & : & : & : & : & : & ;\\
0 & b_n & .. & 0 & 0 & 0 & .. & a_2\\
 & . & & & & . & & \\
 & . & & & & . & & \\
 & . & & & & . & & \\
0 & 0 & .. & b_1 & a_m & 0 & .. & 0\\
0 & 0 & .. & b_2 & 0 & a_m & .. & 0\\
: & : & : & : & : & : & : & 0\\
0 & 0 & .. & b_n & 0 & 0 & .. & a_m
\end{array}\right|$$

Иными словами, строка матрицы G является базисным решением для пары (b_i,a_j).

Краткое описание структуры матрицы G можно представить следующим образом. Пусть $\overline{g}^l$ обозначает i-ю строку матрицы G. Тогда $\overline{g}^l, l=\overline{1,m\times n}$ имеет два ненулевых компонента:

$$g_{l,((l-1)\ div\ n)+1}=b_{((l-1)\ \mathrm{mod}\ n)+1},$$

$$g_{l,m+((l-1)\ \mathrm{mod}\ n)+1}=a_{((l-1)\ div\ n)+1}$$

Доказательство. Итак $(\overline{x},\overline{y})=\dfrac{\overline{z}\cdot G}{k}$. Пусть $(\overline{c},\overline{d})$ произвольное решение уравнения (1). Покажем, что существуют такие $k,\overline{z}$, что

$$k\cdot(\overline{c},\overline{d})=\overline{z}\cdot G \quad (2)$$

Запишем более детальное покомпонентное представление (2), выделив суммы, соответствующие переменным $\overline{c},\overline{d}$:

$$\begin{cases}\sum_i b_i\cdot z_i^j-c_j\cdot k=0, & j=\overline{1,m}\\ \sum_j a_j\cdot z_i^j-d_i\cdot k=0, & i=\overline{1,n}\end{cases} \quad (3)$$

Выполним доказательство конструктивно. Укажем конкретное решение системы (3)

$$\begin{cases}k=\overline{a}\cdot\overline{c} \quad (or \quad k=\overline{b}\cdot\overline{d})\\ z_i^j=c_j\cdot d_i, \quad j=\overline{1,m}, i=\overline{1,n}\end{cases} \quad (4)$$

Действительно, значения $k,\overline{z}$ могут быть эффективно вычислены в соответствии с (4) для произвольного решения $(\overline{c},\overline{d})$ уравнения (1).

Теперь покажем, что значения (4) являются решением уравнения (3):

$$\sum_i b_i\cdot c_j\cdot d_i-c_j\cdot\overline{a}\cdot\overline{c}=c_j\cdot\overline{b}\cdot\overline{d}-c_j\cdot\overline{a}\cdot\overline{c}=c_j\cdot(\overline{b}\cdot\overline{d}-\overline{a}\cdot\overline{c})=0, \quad j=\overline{1,m}$$
$$\sum_j a_j\cdot c_j\cdot d_i-d_i\cdot\overline{a}\cdot\overline{c}=d_i\cdot\overline{a}\cdot\overline{c}-d_i\cdot\overline{a}\cdot\overline{c}=0, \quad i=\overline{1,n}$$

Терема доказана в силу произвольности выбора решения $(\overline{c},\overline{d})$.

Удобно ввести специальную операцию над векторами с целыми неотрицательными компонентами, сокращающую значения на общий делитель компонентов. Для обозначения операции выберем угловые скобки. Итак, $\overline{y}=<\overline{x}>$ тогда и только тогда когда существует натуральное k, такое, что $k\cdot\overline{y}=\overline{x}$. Следовательно, результатом выполнения операции сокращения в общем случае является множество векторов. Заметим, что это множество всегда конечно.

Тогда решение уравнения (1) в соответствии с Теоремой 1 можно представить в форме

$$\overline{x}=<\overline{z}\cdot G>$$

<u>Теорема 2</u>. Базис решений уравнения (1), представленный в Теореме 1, является минимальным.

Доказательство. Выберем в матрице G произвольное базисное решение

$$\overline{g}_i^j=(0,...,b_i,...,0,0,...,a_j,...,0) \quad (5)$$

Покажем, что решение (5) не может быть получено из оставшихся базисных решений посредством линейной комбинации с целыми неотрицательными коэффициентами и сокращения на общий делитель.

Действительно, любое решение, которое содержит ненулевую компоненту j, содержит также некоторую ненулевую компоненту l, причём $l \neq j$, в силу построения матрицы G. Таким образом, мы не можем получить нулевое значение компоненты l с помощью операций сложения, вычитания, деления на множестве неотрицательных целых.

Таким образом, в настоящем разделе получен формальный метод решения в целых неотрицательных числах одного уравнения. Минимальный базис состоит из $m \times n$ векторов, представленных матрицей G.

2. Решение системы уравнений

Рассмотрим систему уравнений

$\bar{x} \cdot A = 0$ (6)

где A заданная матрица целых размерности $m \times n$, $\bar{x}$ целый неотрицательный вектор неизвестных. Заметим, что уравнениям системы соответствуют столбцы матрицы A.

В отличие от (1), каждое из уравнений системы (6) может содержать неизвестные с нулевыми коэффициентами. Значения таких неизвестных при решении отдельного уравнения могут быть выбраны произвольно из множества целых неотрицательных чисел. То есть такой переменной x_i соответствует отдельное базисное решение, имеющее единичное значение компоненты i; остальные компоненты базисного решения равны нулю.

Введём следующие преобразования матриц. Будем получать матрицу D из матрицы A с помощью двух элементарных преобразований:

I) Переписать строку y матрицы A в строку v матрицы D:

$\bar{l}^v \leftarrow \bar{l}^y$

II) Записать сумму строк y, z, умноженных на константы c_y, c_z, матрицы A в строку v матрицы D:

$\bar{l}^v \leftarrow c_y \cdot \bar{l}^y + c_z \cdot \bar{l}^z$

В таком случае матрица D может быть получена из матрицы A путём домножения слева на матрицу преобразований R. При этом матрица R имеет следующие ненулевые компоненты:

а) Для каждого преобразования I:

$r_{v,y} = 1$

б) Для каждого преобразования II:

$r_{v,y} = c_y$, $r_{v,z} = c_z$

Это может быть легко доказано путём детального рассмотрения представления матрицы R:

$$D = R \cdot A, \quad d_{i,j} = \sum_k r_{i,k} \cdot a_{k,j}$$

Заметим, что матрица G базисных решений уравнения (1) представляет собой матрицу преобразований II. Если же переменная входит в уравнение с нулевым коэффициентом, то её значение может быть выбрано произвольно. Этот случай соответствует преобразованиям I, а матрица преобразований переменных является единичной.

Используемый далее метод решения системы имеет некоторое сходство с методом Гаусса. Он основан на решении отдельного уравнения и подстановке полученного общего решения в оставшуюся часть системы. Процесс продолжается до тех пор, пока все уравнения не будут решены.

В начале рассмотрим решение одного, для определённости первого, уравнения системы (6). То есть мы имеем уравнение

$\overline{x} \cdot \overline{a}^1 = 0$

Построим множества индексов переменных I^+, I^0, I^- такие что

$I^+ = \{i \mid a_{i,1} > 0\},\ \ I^0 = \{i \mid a_{i,1} = 0\},\ \ I^- = \{i \mid a_{i,1} < 0\}$

Далее, в соответствии с Теоремой 1 построим матрицу решений, соответствующую преобразованиям I, II:

$$R = \begin{Vmatrix} (I^0)^I \\ \hline (I^+ \times I^-)^{II} \end{Vmatrix} = \begin{Vmatrix} E \\ \hline G \end{Vmatrix}$$

Тогда

$\overline{x} = < \overline{z} \cdot R >$ или $k \cdot \overline{x} = \overline{z} \cdot R$ (7)

Домножим систему (6) на натуральное число k и, подставив в неё выражение (7), получим:

$\overline{z} \cdot R \cdot A = 0$

или

$\overline{z} \cdot D = 0$ (8)

где $D = R \cdot A$. Следует отметить, что в результате подстановки в систему решений уравнения мы перешли от неизвестных $\overline{x}$ к новым неизвестным $\overline{z}$.

<u>Теорема 3</u>. Системы (7), (8) эквивалентны исходной системе (6).

Доказательство. Описанные выше преобразования доказывают необходимость условия теоремы. Докажем его достаточность. Заменим в (8) $\overline{z} \cdot R$ в соответствии с (7) и получим

$k \cdot \overline{x} \cdot A = 0$

Так как k натуральное число, разделим полученное уравнение на k и получим (6).
□

Рассмотрим процесс последовательного решения уравнений системы (6):

$\overline{x} = < \overline{z}^1 \cdot R^1 >$

$\overline{z}^1 \cdot R^1 \cdot A = 0$

Продолжая, таким образом, мы получим

$\overline{z}^n \cdot R^n \cdot R^{n-1} \cdots R^1 \cdot A = 0$

Обозначим

$\overline{z} := \overline{z}^n$, $R := R^n \cdot R^{n-1} \cdots R^1$

и получим

$\overline{z} \cdot R \cdot A = 0,\ R \cdot A = 0$

так как на каждом шаге мы решали одно уравнение системы, обнуляя соответствующий столбец матрицы. Таким образом, мы имеем

$\bar{z} \cdot 0 = 0$

Решением полученной системы является произвольный вектор $\bar{z}$ целых неотрицательных чисел. Тогда решение исходной системы (6) можно представить в виде

$$\bar{x} = < \bar{z} \cdot R > \text{ или } k \cdot \bar{x} = \bar{z} \cdot R \qquad (9)$$

Так как на каждом шаге в соответствии с Теоремой 3 использованы эквивалентные преобразования, описанные выкладки доказывают следующую теорему.

Теорема 4. Выражение (9) представляет собой общее решение системы (6) в целых неотрицательных числах.

Таким образом, для решения системы необходимо построить матрицу R. Матрица R содержит базисные решения системы. Заметим, что для генерации частных решений необходимо использовать как линейную комбинацию базисных решений с целыми неотрицательными коэффициентами, так и дополнительную операцию сокращения на общий делитель компонент вектора.

Далее на примере будет показано, что существуют решения, которые не могут быть получены в результате использования только линейной комбинации.

3. Описание алгоритма

Заметим, что выражение (9) можно представить в форме

$\bar{x} = < \bar{z} \cdot R \cdot E >$,

где E единичная матрица размерности $m \times m$. Рассмотрим процесс формирования матрицы R:

$R = R^n \cdot R^{n-1} \cdots R^1 \cdot E$

Таким образом, для того, чтобы вычислить матрицу R необходимо повторить все преобразования над единичной матрицей E. Заметим, что преобразования на каждом шаге удобно выполнять сразу над двумя матрицами, не сохраняя, таким образом, промежуточные матрицы преобразований. В результате описанных рассуждений мы приходим к алгоритму, представленному Тудиком в работе [2]:

Алгоритм Тудика:

Шаг 0. Положим $D := A$, $R := E$.

Шаг 1. Если $D = 0$, то *Останов*. Матрица R является искомой матрицей базисных решений системы.

Шаг 2. Если все столбцы матрицы D содержат ненулевые коэффициенты одного знака, то *Останов*. Система имеет только тривиальное решение.

Шаг 3. Выберем столбец j матрицы D с минимальным значением произведения $|I^+| \times |I^-|$, где $I^+ = \{i \mid a_{i,j} > 0\}$, $I^0 = \{i \mid a_{i,j} = 0\}$, $I^- = \{i \mid a_{i,j} < 0\}$.

Шаг 4. Построим матрицу D' следующим образом: скопируем в матрицу D' строки I^0 матрицы D, затем допишем дополнительные строки для каждой комбинации $(k,r), k \in I^+, r \in I^-$, построенные как $|a_{r,j}| \cdot \bar{l}^k + |a_{k,j}| \cdot \bar{l}^r$.

Шаг 5. Аналогичные преобразования выполним над матрицей R для получения матрицы R'.

Шаг 6. Положим $D := D', R := R'$ *и перейдём к Шагу 1.*

Отметим, что на Шаге 3 выбор столбца обеспечивает минимальное количество новых решений соответствующего уравнения. Кроме того, в соответствии с результатами раздела 3 строки матриц D и R могут быть сокращены совместно на общий делитель компонентов вектора на любом проходе алгоритма. Возможно также сокращение значений столбцов матрицы D.

Заметим, что отличительной особенностью полученных результатов является способ использования матрицы R для генерации произвольного частного решения. Линейная комбинация с целыми неотрицательными коэффициентами расширена дополнительной операцией сокращения на общий делитель компонент вектора. Так как операция деления на натуральное число не производит новые нулевые или ненулевые компоненты, то дополнительная операция сокращения на общий делитель не влияет на суппорты полученных инвариантов. Напомним, что суппортом инварианта [1,3] является множество ненулевых компонентов решения.

4. Пример вычисления инвариантов

Для иллюстрации полученных результатов решим следующую систему уравнений:

$$\begin{cases} 5\cdot x_1 + 5\cdot x_2 - 2\cdot x_3 - 2\cdot x_4 = 0 \\ 2\cdot x_1 - 5\cdot x_2 - 5\cdot x_3 - 5\cdot x_5 = 0 \\ 5\cdot x_1 + 2\cdot x_2 + 2\cdot x_3 - 2\cdot x_4 - 5\cdot x_5 = 0 \end{cases} \qquad (10)$$

В матричной форме (6) имеем следующие компоненты:

$$\overline{x} = (x_1, x_2, x_3, x_4, x_5),\ A = \begin{pmatrix} 5 & 5 & -2 & -2 & 0 \\ 2 & -5 & -5 & 0 & -5 \\ 5 & 2 & 2 & -2 & -5 \end{pmatrix}^T.$$

Запишем пару матриц (D, R):

$$\left|\begin{array}{ccc|ccccc} 5 & 2 & 5 & 1 & 0 & 0 & 0 & 0 \\ 5 & -5 & 2 & 0 & 1 & 0 & 0 & 0 \\ -2 & -5 & 2 & 0 & 0 & 1 & 0 & 0 \\ -2 & 0 & -2 & 0 & 0 & 0 & 1 & 0 \\ 0 & -5 & -5 & 0 & 0 & 0 & 0 & 1 \end{array}\right|$$

Минимальное значение произведения $\left|I^+\right| \times \left|I^-\right| = 3$ получаем для второго столбца; он будет выбран в качестве столбца j. Таким образом $j = 2$. Вычислим новые значения матриц:

$$\left|\begin{array}{ccc|ccccc} -2 & 0 & -2 & 0 & 0 & 0 & 1 & 0 \\ 35 & 0 & 29 & 5 & 2 & 0 & 0 & 0 \\ 21 & 0 & 29 & 5 & 0 & 2 & 0 & 0 \\ 25 & 0 & 15 & 5 & 0 & 0 & 0 & 2 \end{array}\right|$$

Выберем столбец $j = 1$ и получим:

$$\left|\begin{array}{ccc|ccccc} 0 & 0 & -12 & 10 & 4 & 0 & 35 & 0 \\ 0 & 0 & 16 & 10 & 0 & 4 & 21 & 0 \\ 0 & 0 & -20 & 10 & 0 & 0 & 25 & 4 \end{array}\right|$$

После обработки столбца $j = 3$ получим:

$$\left|\begin{array}{ccc|ccccc} 0 & 0 & 0 & 280 & 64 & 48 & 203 & 0 \\ 0 & 0 & 0 & 360 & 0 & 80 & 820 & 64 \end{array}\right|$$

И, наконец, сократив строки на 4, получим базисные решения системы:

$$R = \begin{pmatrix} 70 & 16 & 12 & 203 & 0 \\ 90 & 0 & 20 & 205 & 16 \end{pmatrix}.$$

Укажем вектор

$\bar{b} = (20 \quad 2 \quad 4 \quad 51 \quad 2)$

который является решением системы (10), но не может быть представлен как линейная комбинация базисных решений с целыми неотрицательными коэффициентами. С использованием операции сокращения его можно представить как:

$\bar{b} = (\bar{r}^1 + \bar{r}^2)/8$.

Аналогичным образом формируются следующие решения:

$(150,24,28,407,8) = (3 \cdot \bar{r}^1 + \bar{r}^2)/2$,

$(170,8,36,409,24) = (\bar{r}^1 + 3 \cdot \bar{r}^2)/2$,

$(130,4,28,307,20) = (4 \cdot \bar{r}^1 + 20 \cdot \bar{r}^2)/16$.

В настоящей работе представлено теоретическое обоснование метода Тудика. Метод известен как эвристический и предназначен для решения систем линейных однородных диофантовых уравнений в целых неотрицательных числах. Он широко используется в промышленных системах автоматизированного анализа свойств сетей Петри при вычислении сетевых инвариантов. Показано, что для генерации всех частных решений системы необходимо расширить линейную комбинацию базисных решений дополнительной операцией сокращения на общий делитель компонент вектора.

Литература

1. Murata T. Petri Nets: Properties, Analysis and Applications // Proc. IEEE, Vol.77, No. 4, 1989, pp. 541-580.

2. Toudic J.M. Linear Algebra Algorithms for the Structural Analysis of Petri Nets // Rev.Tech. Thomson CSF, Vol. 14, No. 1, 1982, pp. 136-156.

3. Бандман М.К., Бандман О.Л., Есикова Т.Н. Территориально-производственные комплексы: Прогнозирование процесса формирования с использованием сетей Петри.- Новосибирск. Наука, 1990.- 303с.

4. B.L.Van Der Warden, Algebra, Berlin, Heidelberg, Springer-Verlag, 1971.

5. Фрумкин М.А. Алгоритм решения систем линейных уравнений в целых числах // Исследования по дискретной оптимизации, М., Наука, 1976, с. 97-127.