Math-Net.Ru

Общероссийский математический портал

В. Г. Смирнов, Методы решения систем дискретных уравнений над кольцом целых чисел, основанные на построении графов решений, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 1, 107–126

DOI: <https://doi.org/10.4213/mvk249>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.234.156.22

26 апреля 2023 г., 13:12:27

**Методы решения систем дискретных уравнений
над кольцом целых чисел,
основанные на построении графов решений
В. Г. Смирнов**

Академия криптографии Российской Федерации, Москва

Получено 30.V.2016

Аннотация. Разрабатываются методы решения систем дискретных уравнений, основанные на их представлении с помощью графов специального вида. Доказаны утверждения о свойствах графов решений. Предложены алгоритмы построения графа решений однородной псевдоболевой системы.

Ключевые слова: системы дискретных уравнений, графы решений, алгоритмы построения решений

Methods of solution of discrete equations systems over the ring of integers based on the construction of graphs of solutions

V. G. Smirnov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. For systems of discrete equations some methods of their solution based on the representations by means of special graphs are developed. Some statements on the properties of graphs of solutions are proved. Algorithms for the construction of graphs of solutions of homogeneous pseudoboolean system are suggested.

Key words: systems of discrete equations, graphs of solutions, algorithms of construction of solution

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 1, pp. 107–126 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Введение

Аналитические методы криптографического анализа сводят задачу определения ключей шифрующих автоматов к решению систем дискретных уравнений того или иного вида. В [4–9] разрабатывались методы решения систем булевых и k -значных систем уравнений, заданных над кольцами вычетов, путем построения комбинаторного объекта, названного графом решений системы. Идея этих методов заключается в «погружении» левых частей рассматриваемой системы в модуль дискретных функций, порождаемый так называемыми *реберными функциями* графа определенного вида. По графу решений можно определить совместность системы и перебрать без повторений все ее решения.

Надо подчеркнуть, что каждая система конечных дискретных уравнений может быть «погружена» хотя бы в один модуль описываемого далее вида, а трудоемкость предлагаемых алгоритмов линейно зависит от числа вершин порождающего графа.

Усовершенствование ранее предложенных методов основано на рассмотрении систем уравнений над кольцом целых чисел и переходе от исходной системы уравнений к равносильной системе более простого вида [5].

К числу достоинств такого подхода можно отнести возможность его применения к более широкому классу систем уравнений, упрощение и сокращение трудоемкости предлагаемых алгоритмов.

В вопросах алгебраической и криптографической терминологии мы следуем [1–3]. Для замкнутости изложения далее приводятся некоторые определения из [4–9].

В разделе 1 даны исходные определения конечных дискретных функций и систем дискретных уравнений. Особое значение имеет теорема 1.1, позволяющая далее ограничиться рассмотрением систем, состоящих из однородных псевдобулевых уравнений. В разделе 2 определяются комбинаторные объекты: Δ -графы, их подграфы и замкнутые подмножества. Введено новое по сравнению с предыдущими работами понятие полного Δ -графа. Далее преимущественно рассматриваются системы уравнений, реализованные полным графом. Рассмотрены отображения Δ -графов. В разделе 3 изучается модуль дискретных функций над кольцом целых чисел, порождаемый реберными функциями соответствующего Δ -графа. В разделе 4 вводятся в рассмотрение H -системы дискретных уравнений и определяются графы их решений. Доказывается ряд утверждений о свойствах графов решений. В разделе 5 предложено три алгоритма построения графа решений однородной псевдобулевой H -системы. Рассмотрены примеры, иллюстрирующие возможности их применения. Даны некоторые оценки трудоемкости алгоритмов.

1. Конечные дискретные функции и системы дискретных уравнений

1.1. Обозначения

Введем обозначения, которые будут использоваться в дальнейшем:

Z — упорядоченное множество целых чисел,

$Z_{\geq 0}$ — упорядоченное множество целых неотрицательных чисел,

$Z_k = \{0, 1, \dots, k-1\}$, где $k \geq 2$,

$Z^n = \underbrace{Z \times \dots \times Z}_{n \text{ раз}}$,

$Z_{k_1} \times \dots \times Z_{k_n}$ — прямое произведение множеств $Z_{k_1}, \dots, Z_{k_n}$,

$m^{(n)} = (m_1, \dots, m_n) \in Z_{k_1} \times \dots \times Z_{k_n}$, если $m_i \in Z_{k_i}, i = 1, \dots, n$,

$\text{sol}(S)$ — множество решений системы уравнений S .

1.2. Конечные дискретные функции

В рамках данной работы будем придерживаться следующего определения.

О п р е д е л е н и е 1. Конечной дискретной функцией от n переменных назовем любое отображение множеств

$$f(x^{(n)}): Z_{k_1} \times \dots \times Z_{k_n} \rightarrow Z_k, \quad \text{где } k_1, \dots, k_n, k > 1.$$

Множество конечных дискретных функций указанного вида назовем *классом дискретных функций* и обозначим $D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$.

Очевидно, что при $l < k$ имеем

$$D(Z_{k_1} \times \dots \times Z_{k_n}; Z_l) \subset D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$$

и

$$D(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0}) = \bigcup_{k=1}^{\infty} D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k).$$

В используемых обозначениях множество $D(Z_2^n; Z_2)$ состоит из булевых функций от n переменных. Дискретные функции из каждого множества $D(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$, отличного от множества булевых функций, назовем *псевдобулевыми функциями*.

Через $f(N)$ обозначим множество значений, принимаемых функцией

$$f(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$$

на множестве $N \subseteq Z_{k_1} \times \dots \times Z_{k_n}$. Положим $f(Z_{k_1} \times \dots \times Z_{k_n}) = M(f)$. Через M^f , M_f обозначим максимальный и соответственно минимальный элемент множества $M(f)$.

Ограничением функции $f(x^{(n)}) \in D(Z_{k_1} \times \cdots \times Z_{k_n}; Z_k)$ на множество N назовем функцию $f(x^{(n)})|_N$ с областью определения N , для которой при всех $x^{(n)} \in N$ выполняется равенство

$$f(x^{(n)})|_N = f(x^{(n)}).$$

Множество таких $x^{(n)} \in Z_{k_1} \times \cdots \times Z_{k_n}$, что $f(x^{(n)}) = a$, обозначим $f^{-1}(a)$.

1.3. Системы дискретных уравнений

Множество систем дискретных уравнений от n неизвестных, задаваемых соотношениями вида

$$f_j(x^{(n)}) = a_j, \quad j = 1, \dots, t, \quad (1)$$

где

$$f_j(x^{(n)}) \in D(Z_{k_1} \times \cdots \times Z_{k_n}; Z_k), \quad a_j \in Z_k,$$

обозначим через $S(Z_{k_1} \times \cdots \times Z_{k_n}; Z_k)$ и назовем *классом систем дискретных уравнений*.

Положим

$$S(Z_{k_1} \times \cdots \times Z_{k_n}; Z_{\geq 0}) = \bigcup_{k=1}^{\infty} S(Z_{k_1} \times \cdots \times Z_{k_n}; Z_k).$$

Очевидно, что для совместности системы (1) необходимо выполнение условий $a_j \in M(f_j), j = 1, \dots, t$. Будем считать эти условия выполненными.

Ограничением системы S , заданной уравнениями (1), на множество $N \subseteq Z_{k_1} \times \cdots \times Z_{k_n}$, $|N| > 1$, назовем систему $S|_N$ вида

$$f(x^{(n)})|_N = a_j, \quad j = 1, \dots, t.$$

Объединением систем $S^{(1)}, S^{(2)} \in S(Z_{k_1} \times \cdots \times Z_{k_n}; Z)$ назовем систему $S^{(1)} \cup S^{(2)}$, множество уравнений которой является объединением множеств уравнений систем $S^{(1)}$ и $S^{(2)}$.

Лемма 1. Пусть $S \in S(Z_{k_1} \times \cdots \times Z_{k_n}; Z)$, $S = S^{(1)} \cup S^{(2)}$. Тогда

$$\text{sol}(S) = \text{sol}(S^{(1)})|_{\text{sol}(S^{(2)})}.$$

Доказательство следует из цепочки соотношений

$$\text{sol}(S^{(1)})|_{\text{sol}(S^{(2)})} = \text{sol}(S^{(1)}) \cap \text{sol}(S^{(2)}) = \text{sol}(S). \quad \square$$

Для каждой системы уравнений $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z)$ справедливо следующее утверждение.

Теорема 1.

1. Система уравнений $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z)$, заданная соотношениями (1), равносильна некоторой системе однородных псевдобулевых уравнений $S' \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$.
2. Каждая система псевдобулевых уравнений $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$ равносильна псевдобулевой системе, состоящей из одного дискретного уравнения.
3. Произвольная система псевдобулевых уравнений равносильна следующему уравнению $S' \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$:

$$\sum_{j=1}^t f_j(x^{(n)}) = 0. \quad (2)$$

Доказательство. 1. Рассмотрим систему уравнений $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z)$, заданную соотношениями (1). Так как уравнение $f(x^{(n)}) = a$ равносильно уравнению $f'(x^{(n)}) = b$, где $f'(x^{(n)}) = f(x^{(n)}) - M_f$, $b = a - M_f$, то исходная система уравнений равносильна системе уравнений, заданной соотношениями $f'_j(x^{(n)}) = b_j$, где $j = 1, \dots, t$, $f'_j(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$. Следовательно, можно считать, что

$$f_j(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0}), \quad j = 1, \dots, t.$$

Каждой функции $f_j(x^{(n)})$ и каждому элементу $a_j \in M(f_j)$, $j = 1, \dots, t$, поставим в соответствие псевдобулеву функцию

$$f_j^{[a_j]}(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_2),$$

определяемую следующим образом:

$$f_j^{[a_j]}(x^{(n)}) = \begin{cases} 0, & f_j(x^{(n)}) = a_j, \\ 1, & f_j(x^{(n)}) \neq a_j. \end{cases}$$

Тогда

$$f_j(x^{(n)}) = \sum_{a_j \in M(f_j)} a_j (1 - f_j^{[a_j]}(x^{(n)}))$$

и уравнение $f_j(x^{(n)}) = a_j$ равносильно уравнению $f_j^{[a_j]}(x^{(n)}) = 0$.

Так как замена каждого уравнения системы равносильным уравнением приводит к равносильной системе, то доказано, что система уравнений $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z)$, заданная соотношениями (1), равносильна системе однородных псевдоболевых уравнений

$$f_j^{[a_j]}(x^{(n)}) = 0, \quad j = 1, \dots, t, \quad (3)$$

что и является первым утверждением теоремы.

2. Второму утверждению теоремы соответствует псевдоболево уравнение

$$f(x^{(n)}) = \bigvee_{j=1}^t f_j^{[a_j]}(x^{(n)}) = 0,$$

однако надо отметить, что вычисление выражения $\bigvee_{j=1}^t f_j^{[a_j]}(x^{(n)})$ может быть весьма трудоемким.

3. Справедливость третьего утверждения теоремы вытекает из сказанного выше.

Теорема доказана. $\square$

2. Семейства Δ -графов

2.1. $\Delta(k_1, \dots, k_n)$ -графы

Рассматриваемые далее ориентированные графы могут содержать параллельные ребра, но петель не содержат.

Далее орграфы будем называть просто графами, так как в рамках данной работы это не может вызвать недоразумений.

Множества вершин и ребер графа H обозначим $V(H)$ и $E(H)$ соответственно. Через $V_{(v)}(H)$, $V^{(v)}(H)$ обозначим множества вершин графа H , смежных к вершине v и смежных из вершины v . Аналогично, через $E_{(v)}(H)$, $E^{(v)}(H)$ обозначим, соответственно, множества ребер H , входящих в вершину v и исходящих из нее. Для ребра e , ведущего из вершины v в вершину u , будем использовать обозначение (v, u) .

Для набора целых чисел $k_1, \dots, k_n$, где $n, k_i > 1$, $i = 1, \dots, n$, в [4–8] рассматривалось следующее семейство ориентированных графов.

О п р е д е л е н и е 2. Орграф H назовем Δ -графом, принадлежащим семейству

$$\Delta_n(k_1, \dots, k_n)$$

ориентированных помеченных орграфов, если выполнены следующие условия:

а) Множество $V(H)$ вершин графа H разбивается на $n + 1$ не пересекающихся подмножеств:

$$V(H) = \bigsqcup_{i=0}^n V_i(H),$$

где $V_i(H) = \{v_j^{(i)}, j = 1, \dots, h_i\}$, причем $h_0 = 1$ и $h_i \geq 1$ для $i = 1, \dots, n$.

б) Входящая степень вершины $v_0^{(0)}$ равна нулю. Входящие степени вершин графа H , отличных от $v_0^{(0)}$, положительны.

с) Из каждой вершины $v \in V_i(H)$ при $i < n$ исходит не менее одного и не более k_i ребер. Ребра, исходящие из вершин, принадлежащих множеству $V_i(H)$, ведут в вершины из множества $V_{i+1}(H)$. Исходящие степени вершин, принадлежащих множеству $V_n(H)$, равны нулю.

д) Каждое ребро $e \in E(H)$, исходящее из вершины $v \in V_i(H)$, $i < n$, имеет метку $\gamma_e \in Z_{k_{i+1}}$. Ребра, исходящие из одной вершины, имеют разные метки.

Из определения 2 следует, что каждый Δ -граф является ациклическим и корневым графом с корнем в вершине $v_0^{(0)}$. Числа $k_1, \dots, k_n$ определяют рассматриваемое семейство Δ -графов, а числа $h_0, \dots, h_n$ являются параметрами конкретного Δ -графа, причем $1 \leq h_i \leq k_i h_{i-1}$ для $i = 1, \dots, n$.

Вершины $v \in V_i(H)$ назовем вершинами i -го уровня Δ -графа H .

Ребра графа H , входящие в вершины уровня $i = 1, \dots, n$, назовем ребрами i -го уровня и обозначим $E_i(H)$. Ребро e с меткой γ , исходящее из вершины u и ведущее в вершину v , обозначим $(u, v; \gamma)$.

По построению любой путь максимальной длины (далее — *максимальный путь*) в графе $H \in \Delta_n(k_1, \dots, k_n)$ имеет длину n . Множество всех максимальных путей графа H обозначим $T(H)$.

Определим отображение $\Gamma_H: T(H) \rightarrow Z_{k_1} \times \dots \times Z_{k_n}$, при котором каждому пути $T \in T(H)$ соответствует n -последовательность $\gamma^{(n)}(T) = (\gamma_1, \dots, \gamma_n)$ меток принадлежащих ему ребер.

Образ множества $T(H)$ при отображении Γ_H обозначим $M(H)$. Очевидно, что $M(H) \subseteq Z_{k_1} \times \dots \times Z_{k_n}$ и отображение $\Gamma_H: T(H) \rightarrow M(H)$ является взаимно однозначным. Граф $H \in \Delta_n(k_1, \dots, k_n)$ назовем *полным*, если из каждой его вершины $v \in V_i(H)$, $0 \leq i < n$, исходит ровно k_{i+1} ребер. Очевидно, что $M(H) = Z_{k_1} \times \dots \times Z_{k_n}$ для полного Δ -графа.

Полный граф $H^{\min}(k_1, \dots, k_n) \in \Delta_n(k_1, \dots, k_n)$ назовем *минимальным*, если он содержит минимально возможное число вершин. В каждом семействе $\Delta_n(k_1, \dots, k_n)$ существует единственный полный минимальный граф, определяемый условиями $h_i = 1$ для $i = 1, \dots, n$, и из вершины v_j в вершину v_{j+1} ведет k_{j+1} ребер с метками из множества $Z_{k_{j+1}}$, $j = 0, \dots, n - 1$.

Граф $H^{\max}(k_1, \dots, k_n) \in \Delta_n(k_1, \dots, k_n)$ назовем *максимальным*, если он содержит максимально возможное число вершин. В каждом семействе $\Delta_n(k_1, \dots, k_n)$ существует единственный полный максимальный граф. Он является полным графом, в каждую вершину которого, кроме корневой вершины, входит ровно одно ребро. Поэтому в любую вершину максимального графа из его корня ведет единственный путь.

2.2. Отображения Δ -графов

Рассмотрим вопрос о существовании отображений, при которых образом графа $H \in \Delta_n(k_1, \dots, k_n)$ является некоторый граф $G \in \Delta_n(l_1, \dots, l_n)$, $l_i \leq k_i, i = 1, \dots, n$. Такие отображения могут быть использованы для сокращения числа вершин и меток рассматриваемых далее H -графов, что может привести, как, например, в [8], к сокращению трудоемкости решаемых задач.

О п р е д е л е н и е 3. Граф $G \in \Delta_n(l_1, \dots, l_n)$ назовем (Φ, Ψ) -образом графа $H \in \Delta_n(k_1, \dots, k_n)$, если существуют сюръективные отображения

$$\Phi: V(H) \rightarrow V(G) \quad \text{и} \quad \Psi: Z_{k_1} \times \dots \times Z_{k_n} \rightarrow Z_{l_1} \times \dots \times Z_{l_n},$$

где $\Psi(\gamma_1, \dots, \gamma_n) = (\Psi_1(\gamma_1), \dots, \Psi_n(\gamma_n))$, для которых

- 1) $\Phi(V_i(H)) = V_i(G), i = 1, \dots, n$,
- 2) если $(u, v; \gamma) \in E_i(H)$, то $(\Phi(u), \Phi(v); \Psi_i(\gamma)) \in E_i(G)$.

Если отображения Φ, Ψ инъективны, то графы H, G назовем (Φ, Ψ) -эквивалентными. Если отображение Ψ является тождественным, то граф G назовем Φ -образом графа H . Докажем следующее утверждение.

Теорема 2. При условии $l_i \leq k_i, i = 1, \dots, n$, каждый граф $G \in \Delta_n(l_1, \dots, l_n)$ является (Φ, Ψ) -образом графа $H^{\max}(k_1, \dots, k_n)$.

Доказательство состоит из двух шагов.

Первый шаг. Сначала докажем, что граф $G^{\max}(l_1, \dots, l_n)$ является образом графа $H^{\max}(k_1, \dots, k_n)$. Зададим любое сюръективное отображение

$$\Psi = (\Psi_1, \dots, \Psi_n): Z_{k_1} \times \dots \times Z_{k_n} \rightarrow Z_{l_1} \times \dots \times Z_{l_n}.$$

Если в вершину $v \in H^{\max}(k_1, \dots, k_n)$ ведет путь $T_{(v)}$ с последовательностью меток $(\gamma_1, \dots, \gamma_i)$, то положим $\Phi(v) = v'$, где $T_{(v')} = (\Psi_1(\gamma_1), \dots, \Psi_i(\gamma_i))$. Нетрудно убедиться, что построенная пара отображений удовлетворяет условиям определения 3.

Второй шаг. Покажем, что любой граф $G \in \Delta_n(l_1, \dots, l_n)$ является Φ -образом графа $G^{\max}(l_1, \dots, l_n)$. Пусть $v' \in V_i(G)$. Множество меток путей, ведущих из корня в вершину v' , обозначим $M(v')$.

Отображение Φ зададим следующим образом:

$$\Phi^{-1}(v') = \{v \in G^{\max}(l_1, \dots, l_n) | T(v) \in M(v')\}.$$

Легко проверить, что отображение Φ удовлетворяет требуемому условию.

Теорема доказана. $\square$

2.3. Δ -графы и H -замкнутые множества

О п р е д е л е н и е 4. Δ -подграфом графа $H \in \Delta_n(k_1, \dots, k_n)$ назовем каждый его подграф G , являющийся объединением непустого множества путей $T \in T(H)$, причем ребра графа сохраняют свои метки.

Очевидно, что $G \in \Delta_n(k_1, \dots, k_n)$.

Из определения 4 следует, что объединение и непустое пересечение Δ -подграфов графа H также является его Δ -подграфом.

Каждому непустому множеству $M' \subseteq M(H)$ согласно определению 4 соответствует следующий Δ -подграф графа $H \in \Delta_n(k_1, \dots, k_n)$:

$$H_{\Delta}(M') = \bigcup_{m^{(n)} \subseteq M'} \Gamma_H^{-1}(m^{(n)}).$$

Лемма 2. Пусть граф G является подграфом графа H . Равенство $G = H_{\Delta}(M')$ для некоторого множества $M' \in M(H)$ выполняется тогда и только тогда, когда:

- 1) $V_i(G) \neq \emptyset$, $i = 0, \dots, n$,
- 2) из $u \in \bigcup_{i=0}^{n-1} V_i(G)$ следует $|E^{(u)}(G)| > 0$,
- 3) из $u \in \bigcup_{i=1}^n V_i(G)$ следует $|E_{(u)}(G)| > 0$.

Действительно, при выписанных условиях каждый путь в графе G может быть продолжен до максимального пути, поэтому утверждение леммы следует из определения 4. $\square$

О п р е д е л е н и е 5. Непустое множество $M' \in M(H)$ назовем H -замкнутым множеством, если из $T \in T(H_{\Delta}(M'))$ следует, что $\Gamma_H(T) \in M'$.

Иными словами, множество $M' \subseteq M(H)$ является H -замкнутым множеством, если $M' = M(H_{\Delta}(M'))$.

Непосредственно из определения следует, что непустое пересечение H -замкнутых множеств является H -замкнутым множеством.

Лемма 3. Пусть граф G является Δ -подграфом Δ -графа H . Тогда каждое G -замкнутое множество является H -замкнутым множеством.

Утверждение леммы следует из включения $M(G) \subseteq M(H)$.

3. Пространство дискретных функций, порождаемое реберными функциями Δ -графа

3.1. Реберные функции Δ -графа

С каждым графом $H \in \Delta_n(k_1, \dots, k_n)$ свяжем следующее множество дискретных функций.

О п р е д е л е н и е 6. Реберной функцией графа H , соответствующей ребру $e \in E(H)$, назовем функцию

$$\varphi_e^H(x_1, \dots, x_n) = \begin{cases} 1, & e \in \Gamma_H^{-1}(x^{(n)}), \\ 0, & e \notin \Gamma_H^{-1}(x^{(n)}). \end{cases}$$

Множество реберных функций графа $H \in \Delta_n(k_1, \dots, k_n)$ порождает модуль над кольцом целых чисел, который обозначим $L_Z(H)$.

О п р е д е л е н и е 7. Функции $f(x^{(n)}) \in L_Z(H)$ назовем H -функциями.

Будем говорить, что H -функция реализуется графом H .

Очевидно, что $L_Z(H) \subseteq D(Z_{k_1} \times \dots \times Z_{k_n}; Z)$. Если H — максимальный граф, то $L_Z(H) = D(Z_{k_1} \times \dots \times Z_{k_n}; Z)$, т. е. максимальным графом реализуется любая функция из класса $D(Z_{k_1} \times \dots \times Z_{k_n}; Z)$.

Каждая H -функция $f(x^{(n)})$ может быть задана (вообще говоря, не однозначно) коэффициентами линейной формы:

$$f(x^{(n)}) = \sum_{e \in E(H)} c_e^f \cdot \varphi_e^H(x^{(n)}). \quad (4)$$

Коэффициент c_e^f назовем весом ребра e при задании функции $f(x^{(n)})$ соотношением (4).

Из определения 4 следует также, что

$$\varphi_e^G(x^{(n)}) = \varphi_e^H(x^{(n)})|_{M(G)}. \quad (5)$$

Поэтому для любой G -функции $f(x^{(n)})$ имеем

$$f(x^{(n)})|_{M(G)} = \sum_{e \in E(G)} c_e^f \cdot \varphi_e^G(x^{(n)}).$$

Следствие 1. Для любой H -функции $f(x^{(n)})$ и любого Δ -подграфа G графа H имеем $f(x^{(n)})|_{M(G)} \in L_Z(G)$.

Теорема 3. Если граф G является Λ -образом полного графа H , то

$$L_Z(G) \subseteq L_Z(H).$$

Доказательство. Отображение $\Lambda : V(H) \rightarrow V(G)$ индуцирует отображение $E(H) \rightarrow E(G)$, при котором $\Lambda(u, v) = (\Lambda(u), \Lambda(v))$. Отсюда для $r \in E(G)$, $e \in E(H)$ получаем:

$$\varphi_r^G(x^{(n)}) = \sum_{e \in \Lambda^{-1}(r)} \varphi_e^H(x^{(n)}),$$

что доказывает требуемое утверждение. $\square$

3.2. Веса ребер и путей в графе H , соответствующие заданию H -функции

Каждому заданию функции $f(x^{(n)})$ в виде (4) поставим в соответствие отображение $c^{(f)} : E(H) \rightarrow Z$, для которого $c^{(f)}(e) = c_e^f$. Величину c_e^f назовем *весом ребра e* при отображении $c^{(f)}$ и положим $w(e) = c^{(f)}(e)$. *Весом $\omega(c^{(f)}, T)$ непустого пути T* в графе H назовем сумму весов ребер, принадлежащих T :

$$\omega(c^{(f)}, T) = \sum_{e \in T} c_e^f.$$

Через $C^{(f)}$ обозначим множество отображений $c^{(f)}$, соответствующих всем возможным H -представлениям функции $f(x^{(n)})$.

Очевидно, что для $m^{(n)} \in M(H)$ имеем $f(m^{(n)}) = \omega(c^{(f)}, \Gamma_H^{-1}(m^{(n)}))$, а это выражение сохраняет свое значение при любом отображении $c^{(f)}$, удовлетворяющем равенству (4). Поэтому при $T \in T(H)$ для веса пути T будем использовать обозначение $\omega_f(T)$.

Через $T(u)$, $u \in V(H)$, обозначим множество путей $T \in T(H)$, для которых $u \in T$.

Рассмотрим H -функцию $f(x^{(n)})$. Для каждого числа $b \in f(M(H))$ положим

$$T_f^{(b)} = \Gamma_H^{-1}(f^{-1}(b)).$$

Пути $T \in T_f^{(b)}$ назовем b -путями функции $f(x^{(n)})$. Если $T \in T_f^{(b)}$, то исходящий из вершины u путь $T^{(u)}$ и входящий в вершину u путь $T_{(u)}$ назовем *верхним (u, b) -путем* и *нижним (u, b) -путем* соответственно.

Следующее утверждение, доказанное в [7], дает условия H -замкнутости непустого множества $f^{-1}(b)$.

Теорема 4. Множество $f^{-1}(b)$ тогда и только тогда H -замкнуто, когда для любой вершины u , удовлетворяющей условию $T(u) \cap T_f^{(b)} \neq \emptyset$, при любом отображении $c^{(f)} \in C_f$ постоянны веса как нижних, так и верхних (u, b) -путей.

Следствие 2. Для каждой H -функции $f(x^{(n)})$ множества M_f, M^f являются H -замкнутыми.

3.3. Нормализованная форма H -функции

О п р е д е л е н и е 8. Задание H -функции $f(x^{(n)})$ в виде (4) назовем ее *нормализованной формой*, если для каждой вершины $v \in \cup_{i=1}^{n-1} V_i(H)$ выполняются условия

$$\min_{e \in E^{(v)}(H)} c_e^f = 0.$$

В [7] показано, что каждая H -функция $f(x^{(n)})$ имеет единственную нормализованную форму. Трудоемкость получения нормализованной формы из любого задания функции $f(x^{(n)})$ в виде (4) пропорциональна числу $|V(H)|$. Там же приведен алгоритм получения нормализованной формы H -функции из любого ее задания в виде (4).

Задание функции $f(x^{(n)})$ нормализованной формой имеет вид

$$f(x^{(n)}) = \sum_{e \in E(H)} n_e^f \varphi_e(x^{(n)}), \quad (6)$$

где n_e^f — коэффициенты нормализованной формы.

Лемма 4. 1) Для H -функции $f(x^{(n)})$, заданной соотношением (6), имеем

$$\min(f) = \min_{e \in E_1(H)} n_e^f.$$

2) Нормализованная форма псевдобулевой функции имеет вид

$$f(x^{(n)}) = \sum_{e \in N} n_e^f \varphi_e(x^{(n)}),$$

где N — множество попарно не сравнимых ребер графа H , $n_e^f \in \mathbb{Z}_2$.

Справедливость первого утверждения леммы 4 очевидна, а справедливость второго утверждения вытекает из простого наблюдения: нормализованная форма псевдобулевой H -функции не может содержать на любом максимальном пути графа H более одного ребра веса 1, веса остальных ребер должны быть равными нулю. $\square$

4. H -системы дискретных уравнений

4.1. Исходные определения

О п р е д е л е н и е 9. Систему дискретных уравнений, заданную уравнениями (1), назовем H -системой, если выполняются условия

$$f_j(x^{(n)}) \in L_Z(H), \quad j = 1, \dots, t,$$

где $H \in \Delta_n(k_1, \dots, k_n)$.

Согласно определению H -система (1) может быть задана в виде

$$\sum_{e \in E(H)} c_e^{f_j} \cdot \varphi_e^H(x^{(n)}) = a_j, \quad j = 1, \dots, t, \quad (7)$$

где

$$\sum_{e \in E(H)} c_e^{f_j} \varphi_e^H(x^{(n)}) = f_j(x^{(n)}).$$

Лемма 5. Если система S является H -системой и граф G является Δ -подграфом графа H , то система $S|_{M(G)}$ является G -системой.

Доказательство следует из определения 9. $\square$

Согласно теореме 1 каждая система $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z)$ дискретных уравнений равносильна системе псевдобулевых уравнений вида (2). Основываясь на этом результате, далее рассматриваем только реализованные на некотором полном графе H -системы уравнений

$$f_j(x^{(n)}) = 0, \quad j = 1, \dots, t, \quad (8)$$

где $f_j(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$, и равносильное системе (8) уравнение

$$f(x^{(n)}) = \sum_{j=1}^t f_j(x^{(n)}) = 0. \quad (9)$$

О п р е д е л е н и е 10. Назовем H -систему дискретных уравнений S , для которой множество $\text{sol}(S)$ является H -замкнутым, замкнутой H -системой уравнений.

Как следует из следствия 2, система (2), равносильная псевдобулеву уравнению, является замкнутой H -системой.

О п р е д е л е н и е 11. Графом решений совместной H -системы S назовем граф

$$Q(S) = H_{\Delta}[\text{sol}(S)].$$

Из определений 10, 11 следует, что для совместной незамкнутой H -системы S граф $Q(S)$ является минимальным Δ -графом, для которого

$$M(Q(S)) \supseteq \text{sol}(S),$$

а для совместной замкнутой H -системы S имеем

$$M(Q(S)) = \text{sol}(S).$$

Теорема 5. Пусть система S является совместной H -системой дискретных уравнений. Тогда

- 1) Для любого Δ -подграфа G графа H в случае совместности системы $[S]_{M(G)}$ верно соотношение

$$Q([S]_{M(G)}) = Q(S) \cap G.$$

- 2) Если H -замкнутая система R является подсистемой совместной H -системы, то

$$Q(S) = Q([S]_{\text{sol}R}).$$

- 3) Если в условиях п. 2 система $[S]_{\text{sol}R}$ является замкнутой $H_{\Delta}(\text{sol}R)$ -системой, то система S является H -замкнутой.

Доказательство. Справедливость первого утверждения теоремы следует из цепочки соотношений

$$\begin{aligned} Q([S]_{M(G)}) &= H_{\Delta}(\text{sol}[S]_{M(G)}) = \\ &= H_{\Delta}(\text{sol}[S] \cap M(G)) = \\ &= H_{\Delta}(\text{sol}[S] \cap H_{\Delta}(M(G))) = \\ &= Q(S) \cap G. \end{aligned}$$

Второе утверждение теоремы следует из первого, если положить

$$G = H_{\Delta}(\text{sol}R),$$

так как в этом случае $Q(S) \subseteq G$.

Третье утверждение теоремы следует из определения 10, так как в рассматриваемом случае

$$M(Q(S)) = \text{sol}(S). \quad \square$$

5. Алгоритмы решения H -систем дискретных уравнений

5.1. Алгоритм решения системы дискретных уравнений путем сведения к решению дискретного уравнения

Как следует из теоремы 1, задачу построения графа решений $Q(S)$ совместной H -системы S можно свести к задаче построения графа решений дискретного уравнения, равносильного системе.

Рассмотрим однородную псевдобулеву систему уравнений, реализованную на некотором полном графе G и заданную соотношениями (8). В соответствии с леммой 4 положим

$$f_j(x^{(n)}) = \sum_{e \in N_j} n_e^{f_j} \varphi_e(x^{(n)}). \quad (10)$$

Граф решений уравнения $f(x^{(n)}) = 0$ обозначим $Q(f)$.

Алгоритм 1. Построение графа решений $Q(f)$ уравнения $f(x^{(n)}) = 0$, заданного соотношением (10).

Действие алгоритма основано на простой процедуре удаления путей из графа G .

Если для некоторого значения j имеем $n_e^{f_j} = 1$, то удаляем из графа G все пути $T \in T(e)$. Полученный граф является графом решений $Q(f)$ уравнения $f(x^{(n)}) = 0$.

Действительно, по построению $e \in E(Q(f))$ тогда и только тогда, когда в графе G любой путь имеет вес 0. Трудоемкость алгоритма зависит от параметров графа G и трудоемкости получения нормализованных форм функций, входящих в систему уравнений (8).

5.2. Последовательный алгоритм решения системы дискретных уравнений

Рассмотрим систему S псевдобулевых уравнений, реализованную на некотором полном графе G и заданную соотношениями (9).

Граф решений системы S обозначим $Q(S)$.

Алгоритм 2. Последовательный алгоритм решения системы дискретных уравнений основан на последовательном вычислении множеств

$$\bigcap_{j=1}^2 \{x^{(n)}: f_j(x^{(n)})=0\}, \bigcap_{j=1}^3 \{x^{(n)}: f_j(x^{(n)})=0\}, \dots, \bigcap_{j=1}^t \{x^{(n)}: f_j(x^{(n)})=0\},$$

Проиллюстрируем применение этого алгоритма на примере, в котором каждый список $S^{(j)}$, $j = 1, \dots, 5$, является списком решений уравнения $f_j^{[b_j]} = 0$, а значения переменных задают метки ребер некоторого (например, минимального) Δ -графа, реализующего рассматриваемую систему уравнений, из каждой вершины которого, кроме концевых вершин, исходят три ребра с метками 0, 1, 2.

Пример

Список $S^{(1)}$			Список $S^{(2)}$			Список $S^{(3)}$			Список $S^{(4)}$			Список $S^{(5)}$		
x_1	x_2	x_3	x_1	x_2	x_5	x_1	x_5	x_6	x_2	x_3	x_4	x_3	x_4	x_6
0	0	1	0	0	1	0	1	1	0	1	0	0	1	1
1	0	1	1	0	0	1	1	1	0	1	2	0	2	0
1	1	0	1	1	1	2	0	0	1	0	1	0	2	1
2	0	1	2	0	0	2	0	1	1	0	2	1	0	0
2	1	1	2	0	1	2	1	1	1	1	1	1	2	0

Последовательно вычисляем списки $\bigcap_{j=1}^l \{x^{(n)}: f_j(x^{(n)}) = 0\}$, $l = 1, \dots, 5$.

$\bigcap_{j=1}^2 \{f_j(x^{(n)})=0\}$	$\bigcap_{j=1}^3 \{f_j(x^{(n)})=0\}$	$\bigcap_{j=1}^4 \{f_j(x^{(n)})=0\}$	$\text{sol}\left(\bigcap_{j=1}^5 \{f_j(x^{(n)})=0\}\right)$
x_1, x_2, x_3, x_5	x_1, x_2, x_3, x_5, x_6	$x_1, x_2, x_3, x_4, x_5, x_6$	$x_1, x_2, x_3, x_4, x_5, x_6$
0, 0, 1, 1	0, 0, 1, 1, 1	0, 0, 1, 1, 1, 0	1, 1, 0, 1, 1, 1
1, 0, 1, 0	1, 1, 0, 1, 1	0, 0, 1, 1, 1, 2	1, 1, 0, 2, 1, 1
1, 1, 0, 1	2, 0, 1, 0, 0	1, 1, 0, 1, 1, 1	2, 0, 1, 0, 0, 0
2, 0, 1, 0	2, 0, 1, 0, 1	1, 1, 0, 2, 1, 1	2, 0, 1, 2, 0, 0
2, 0, 1, 1	2, 0, 1, 1, 1	2, 0, 1, 0, 0, 1	
		2, 0, 1, 2, 0, 1	
		2, 0, 1, 0, 1, 1	
		2, 0, 1, 2, 1, 1	

В последнем столбце находятся 4 решения рассматриваемой системы уравнений.

5.3. Алгоритм поиска решений системы дискретных уравнений, реализованной полным Δ -графом, на путях Δ -графа

Вновь рассмотрим систему S псевдобулевых уравнений, реализованную на некотором полном графе G и заданную соотношениями (9).

Аналог алгоритма бесповторного перебора путей Δ -графа, рассмотренного в [4, 5], позволяет перебрать решения системы S в лексикографическом порядке, при котором решение $(a_1, \dots, a_n)$ предшествует решению $(b_1, \dots, b_n)$, если число, соответствующее двоичной записи $[a_1, \dots, a_n]_2$, меньше числа $[b_1, \dots, b_n]_2$.

Предлагаемый алгоритм состоит из двух этапов. На первом этапе, путем вычисления одного решения, устанавливается совместность системы уравнений, а на втором этапе вычисляются ее остальные решения.

Вершину Δ -графа, из которой исходит более одного ребра, назовем *развилкой*.

1 этап. Установление совместности системы дискретных уравнений

Начиная с вершины $v_1^{(0)}$, последовательно строим путь $T \in T(G)$, выбирая на каждой развилке ребро с меткой 0. Если на некотором шаге получено ребро $e \in T$, $w(e) = 1$, то удаляем из графа G пути $T^{(e)}$, обращаемся к ближайшей лежащей ниже развилке, в которой выбираем исходящее ребро с меткой 1, и возобновляем процесс поиска решений системы. В результате, если удастся построить максимальный путь, то он будет первым по лексикографическому порядку путем $T \in \text{sol}(S)$ и совместность системы будет установлена.

2 этап. Получение следующих решений системы уравнений

Пусть очередное решение $s^{(n)} \in \text{sol}(S)$ уже получено и $v_0, \dots, v_n$ — упорядоченная последовательность вершин пути $T \in T(G)$ с последовательностью меток $s^{(n)}$. Тогда последовательностью ребер пути T будет последовательность $(v_0, s_1), \dots, (v_{n-1}, s_n)$. Выделим среди вершин пути T развилку v_i с максимальным индексом l , для которой $(v_i, 0) \in T$. Если это сделать не удастся, то вектор $\vec{s}$ — наибольший по частичной упорядоченности элемент в множестве $\text{sol}(S)$ и перебор решений завершен. Пусть развилка с требуемыми свойствами существует. Определим путь $T' \in T(G)$ с вершинами $v_0, \dots, v_i, v'_{i+1}, \dots, v'_n$. Вершины v_i и v'_{i+1} соединяет ребро $(v_i, 1)$, а далее у всех развилок пути T выбирается ребро с меткой 0. В результате будет построен следующий вектор $r^{(n)} \in \text{sol}(S)$, после чего возвращаемся к выполнению второго этапа алгоритма.

5.4. Пример решения системы булевых уравнений

Рассмотрим пример решения системы булевых уравнений в анализе фильтрующего генератора над полем $\text{GF}(2)$. Исходные данные взяты из [9], а сам пример носит чисто иллюстративный характер.

Рассматривается система булевых уравнений:

$$\begin{cases} x_1x_4 \oplus x_3 = 0 \\ x_1 \oplus x_2 \oplus x_5 = 0 \\ x_2x_5 \oplus x_4 = 1 \\ x_2 \oplus x_3 \oplus x_6 = 0 \\ x_3x_6 \oplus x_5 = 0 \\ x_3 \oplus x_4 \oplus x_7 = 0 \\ x_4x_7 \oplus x_6 = 1 \end{cases}$$

Соответствующее множество списков решений каждого уравнения приведено ниже.

Исходные списки решений отдельных уравнений системы

(X_1, L_1)	(X_2, L_2)	(X_3, L_3)	(X_4, L_4)	(X_5, L_5)	(X_6, L_6)	(X_7, L_7)
$x_1 \ x_3 \ x_4$	$x_1 \ x_2 \ x_5$	$x_2 \ x_4 \ x_5$	$x_2 \ x_3 \ x_6$	$x_3 \ x_5 \ x_6$	$x_3 \ x_4 \ x_7$	$x_4 \ x_6 \ x_7$
0 0 0	0 0 0	0 1 0	0 0 0	0 0 0	0 0 0	0 1 0
0 0 1	0 1 1	0 1 1	0 1 1	0 0 1	0 1 1	0 1 1
1 0 0	1 0 1	1 0 1	1 0 1	1 0 0	1 0 1	1 0 1
1 1 1	1 1 0	1 1 0	1 1 0	1 1 1	1 1 0	1 1 0

Предварительно полезно вычислить минимальные запреты каждого из уравнений системы (определение запретов см. в [9]). Множество минимальных запретов для уравнений системы обозначим $Z(S)$.

Перечень минимальных запретов уравнений системы

(X_1, L_1)	(X_2, L_2)	(X_3, L_3)	(X_4, L_4)
$x_1x_3 \neq 01,$ $x_3x_4 \neq 10,$ $x_1x_3x_4 \neq 101$	$x_1x_2x_5 \neq 001,$ $010, 100, 111$	$x_2x_4 \neq 00,$ $x_2x_5 \neq 00,$ $x_2x_4x_5 \neq 111$	$x_2x_3x_6 \neq 001,$ $010, 100, 111$

(X_5, L_5)	(X_6, L_6)	(X_7, L_7)
$x_3x_5 \neq 01,$ $x_5x_6 \neq 10,$ $x_1x_3x_4 \neq 101$	$x_3x_4x_7 \neq 001,$ $010, 100, 111$	$x_4x_6 \neq 00,$ $x_6x_7 \neq 00,$ $x_4x_6x_7 \neq 111$

Поиск решений системы

x_1	x_2	x_3	x_4	x_5	x_6	x_7	результат
0	0	0	0				$x_2x_4 = 00 \in Z(S)$
0	0	0	1	0	0	1	$x_1x_2 = 0 \rightarrow x_5 = 0$ $x_2x_3 = 00 \rightarrow x_6 = 0$ $x_3x_4 = 01 \rightarrow x_7 = 1$ $x^{(7)} \in \text{sol}(S)$
0	0	0	1	0	1	0	$x_2x_3x_6 = 001 \in Z(S)$
0	0	1					$x_1x_3 = 01 \in Z(S)$
0	1		0	1			$x_1x_2 = 01 \rightarrow x_5 = 1$ $x_2x_5 = 11 \rightarrow x_4 = 0$ $x_1x_5 = 01 \rightarrow x_2 = 1$ $x^{(7)} \in \text{sol}(S)$
1	0	0	1				$x_1x_3x_4 = 101 \in Z(S)$
1	0	1					$x_1x_3 = 11 \rightarrow x_4 = 1$
1	0	1	1				$x_1x_2 = 10 \rightarrow x_5 = 1$
1	0	1	1	1			$x_2x_3 = 01 \rightarrow x_6 = 1$
1	0	1	1	1	1		$x_3x_4 = 11 \rightarrow x_7 = 0$
1	0	1	1	1	1	0	$\in \text{sol}(S)$

Дальнейшая проверка показывает, что других решений нет. Таким образом, множество $\text{sol}(S)$ представлено в следующей таблице:

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	1	0	0	1
1	0	1	1	1	1	0

5.5. Замечание о сложности установления совместности системы уравнений

Рассмотрим следующую комбинаторную задачу. В урне находятся b белых шаров и c черных шаров, $b = |\text{sol}(S)|$, $b + c = 2^n$. Последовательно, случайно и равновероятно из урны извлекаются шары по одному. Появление белого шара символизирует обнаружение решения системы уравнений.

Вероятность события, заключающегося в том, что на шаге $k = 1, \dots, 2^n$ впервые будет извлечен белый шар, равна

$$P_k(b, c) = b \frac{c!(2^n - k)!}{(c - (k - 1))! 2^n!}.$$

Соответственно, математическое ожидание числа шаров до первого появления белого шара равно

$$\sum_{k=1}^{2^n} k P_k(b, c).$$

Дать более точную оценку трудоемкости алгоритма затруднительно, так как ее сокращение зависит от трудно предсказуемого процесса исключения путей графа G .

Однако очевидно, что трудоемкость рассматриваемого алгоритма меньше трудоемкости метода полного перебора.

Редакция журнала «Математические вопросы криптографии» выражает благодарность В. Г. Антипкину за тщательную подготовку статьи к публикации.

Список литературы

- [1] Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, М. : Наука, 1982, 384 с.
- [2] *Словарь криптографических терминов*, Под ред. Б. А. Погорелова, В. Н. Сачкова, М. : МЦНМО, 2006, 94 с.
- [3] Харари Ф., *Теория графов*, М. : Мир, 1973, 302 с.
- [4] Смирнов В. Г., “Эффективные алгоритмы построения графа общего решения для систем булевых уравнений”, *Труды по дискретной математике*, **5**, 2002, 227–234.
- [5] Смирнов В. Г., “Алгоритмы решения систем k -значных уравнений, использующие построение орграфа решений”, *Труды по дискретной математике*, **6**, 2002, 194–212.
- [6] Смирнов В. Г., “Методы построения графов решений для систем k -значных уравнений”, *Труды по дискретной математике*, **8**, 2004, 253–280.
- [7] Смирнов В. Г., “Методы решения систем дискретных уравнений, основанные на построении графа решений”, *Труды по дискретной математике*, **9**, 2006, 308–339.
- [8] Смирнов В. Г., “Методы решения систем квазисимметричных уравнений и их применение к анализу генераторов с управляемым движением”, *Математические вопросы криптографии*, **1:3** (2010), 67–92.
- [9] Смирнов В. Г., “Дискретные функции и разреженные системы дискретных уравнений”, *Математические вопросы криптографии*, **7:3** (2016), 93–114.