Math-Net.Ru

Общероссийский математический портал

В. Г. Смирнов, Дискретные функции и разреженные системы дискретных уравнений, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 3, 93–114

DOI: <https://doi.org/10.4213/mvk198>

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: 54.198.187.58

26 апреля 2023 г., 17:07:21

Дискретные функции и разреженные системы дискретных уравнений

В. Г. Смирнов

Академия криптографии Российской Федерации, Москва

Получено 20.IV.2015

Аннотация. Даны определения классов дискретных функций и систем дискретных уравнений. Рассмотрены аналитические способы их задания. Предложен алгоритм определения совместности разреженной системы дискретных уравнений, использующий построение пути в графе решений системы по параметрическим решениям отдельных уравнений. Приведены примеры, иллюстрирующие работу алгоритма.

Ключевые слова: дискретные функции, разреженные системы дискретных уравнений, параметрическое решение, граф решений

Discrete functions and sparse systems of discrete equations

V. G. Smirnov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Classes of discrete functions and systems of discrete equations are defined. Analytic approaches to their description are considered. We suggest an algorithm for testing the compatibility of sparse system of discrete equations. This algorithm is based on the construction of path in the graph of solutions of the system via the parametric solutions of separate equations. Some examples illustrating the realization of the algorithm are given.

Key words: discrete functions, sparse systems of discrete equations, parametric solution, graph of solutions

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 3, pp. 93–114 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

Введение

Неформальное определение m -разреженной системы состоит в том, что каждое уравнение системы, зависящей от n неизвестных, существенно зависит не более чем от $m < n$ неизвестных.

Интерес к разреженным системам дискретных уравнений вызван двумя обстоятельствами: во-первых, такие системы часто встречаются в практике криптографического анализа, и, во-вторых, существуют более эффективные, чем в общем случае, методы решения разреженных систем. В основном это связано с тем обстоятельством, что методом полного перебора можно найти решения отдельных уравнений разреженной системы, после чего возникает новый пласт задач: как по этим данным получить решения всей системы.

Разреженные системы булевых уравнений ранее рассматривались в рамках классической проблемы выполнимости (или SAT-проблемы), которая сводится к определению совместности произвольной системы булевых уравнений

$$d_i(x^{(n)}) = 1, \quad i = 1, \dots, n,$$

где функции $d_i(x^{(n)})$ являются дизъюнкциями литералов из множества $x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n$ ($[1, 2]$). Проблему выполнимости в случае, когда длина каждой дизъюнкции не превосходит m , обычно называют m -SAT задачей.

Известно, что проблема выполнимости в общей постановке является NP-полной задачей и остается такой, если длина каждой дизъюнкции не превосходит 3.

Методы решения m -SAT задач рассматривались в многочисленных работах, из которых упомянем [7–12]. Общий вывод состоит в том, что сложность решения m -SAT задачи при любом $m > 2$ имеет порядок $O(c_m)$, где $c_m < 2$, причем с ростом m константа c_m довольно быстро приближается к верхней границе.

Основными методами решения общей SAT-проблемы являются методы DPLL [3, 4] и резолюций [5, 6].

Методы, позволяющие получить список решений разреженной системы уравнений над конечным полем по спискам решений отдельных уравнений, рассматривались в [13–18] и ряде других работ.

Постановка проблемы решения разреженных систем уравнений в данной работе несколько отличает ее от упомянутых трудов, так как здесь исследуются разреженные системы произвольных дискретных уравнений.

В параграфе 1 определяются классы дискретных функций и систем дискретных уравнений, а также рассматриваются аналитические способы их задания.

В [19] было показано, что каждая дискретная функция может быть задана полиномом из кольца полиномов над полем с достаточно большим числом элементов. Здесь установлено, что любая система дискретных уравнений равносильна системе, состоящей из дискретных функций, принимающих два значения. Для них определены аналоги дизъюнктивных и конъюнктивных форм булевых функций.

Такой подход позволяет с единых позиций рассматривать разнообразные классы систем дискретных уравнений.

С каждой системой дискретных уравнений связываются *общее* (или *параметрическое*) *решение системы* (по аналогии с [20–22], где рассматриваются общие решения систем булевых уравнений), и *граф решений системы* [23, 24]. В параграфах 2, 3 устанавливаются взаимосвязи между этими понятиями и списками решений отдельных уравнений для разреженных систем дискретных уравнений.

В параграфе 4 излагается алгоритм решения разреженных систем дискретных уравнений, использующий построение общих решений уравнений системы по спискам решений и графа решений системы по общим решениям уравнений системы. В процессе работы алгоритма решается вопрос о совместности системы, а затем, продолжая построение графа решений совместной системы, можно перечислить все ее решения.

В приложениях 1 и 2 приводятся примеры, иллюстрирующие возможности применения алгоритма из параграфа 4.

1. Дискретные функции и системы дискретных уравнений

1.1. Конечные дискретные функции

Определение 1.1. *Конечной дискретной функцией* назовем любое отображение

$$f : A \rightarrow U,$$

где множество A является конечным, содержащим не менее двух элементов.

Если $A = A_1 \times \dots \times A_n$, где $n > 1$ и каждое множество $A_1, \dots, A_n$ является конечным, содержащим не менее двух элементов, то отображение f назовем *конечной дискретной функцией от n переменных*.

Множество дискретных функций при данных множествах $A_1 \times \dots \times A_n$, U обозначим $D(A_1 \times \dots \times A_n; U)$.

Очевидно, что $D(A_1 \times \dots \times A_n; U') \subseteq D(A_1 \times \dots \times A_n; U)$ при $U' \subseteq U$.

Введем обозначения:

$a^{(n)} = (a_1, \dots, a_n)$, $a^{(n)} \in A_1 \times \dots \times A_n$, если $a_i \in A_i$, $i = 1, \dots, n$,

Z — кольцо целых чисел,

$Z_{\geq 0}$ — полугруппа целых неотрицательных чисел относительно операции $+$,

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

Поскольку в определении существенны только мощности конечных множеств $A_1, \dots, A_n$, U , а их природа не имеет значения, далее полагается, что множество U не более чем счетно, $A_i = Z_k$, $i = 1, \dots, n$, и рассматриваются множество $D(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$ дискретных функций и его подмножества $D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$.

Определение 1.2.

1. Множество $D(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$ дискретных функций назовем $(k_1, \dots, k_n)$ -классом функций.
2. Множество $D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$ дискретных функций назовем $(k_1, \dots, k_n; k)$ -классом функций.

Каждую конечную дискретную функцию можно задать таблицей, в которой элементы области определения функции расположены в некотором порядке и для каждого элемента указан его образ при отображении f .

Конкретизируем табличный способ задания $(k_1, \dots, k_n; k)$ -функций. Элементы прямого произведения $Z_{k_1} \times \dots \times Z_{k_n}$ расположим в порядке следования строк в матрице $\vec{Z}_{k_1} \oplus \dots \oplus \vec{Z}_{k_n}$, обычно называемом лексикографическим порядком. Через $\vec{f}$ обозначим вектор-строку значений функции $f(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$, а через $\vec{f}^T$ — вектор-столбец ее значений, расположенных в соответствии с лексикографическим порядком следования аргументов.

1.2. Алгебры дискретных функций

Наиболее естественный путь задания операций на классах дискретных функций основан на следующих замечаниях.

1. Если на множестве $Z_{\geq 0}$ задана алгебраическая операция $*$, то ее действие может быть следующим способом распространено на каждый $(k_1, \dots, k_n)$ -класс функций: $f = f_1 * f_2$ тогда и только тогда, когда при всех $x^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}$ имеем $f(x^{(n)}) = f_1(x^{(n)}) * f_2(x^{(n)})$.

Операцию сложения чисел, определенную на множестве $Z_{\geq 0}$, распространим на $(k_1, \dots, k_n)$ -классы функций, каждый из которых становится полугруппой с операцией $+$.

2. Аналогично, действие операции, заданной на множестве Z_k , можно распространить на $(k_1, \dots, k_n; k)$ -класс функций. Так, в [19] рассмотрены некоторые свойства колец дискретных функций, полученных распространением на $(k_1, \dots, k_n; k)$ -классы функций операций кольца, заданного на множестве Z_k .

3. Если все множества Z_k замкнуты относительно операции $*$, заданной на множестве $Z_{\geq 0}$, то ее действие может быть распространено на $(k_1, \dots, k_n; k)$ -классы функций.

Зададим на множестве $Z_{\geq 0}$ линейную упорядоченность, положив $z_i < z_j$ при $i < j$, и определим двухместные операции

$$z \vee z_j = \max(z_i, z_j), \quad z_j \wedge z_j = \min(z_i, z_j).$$

Для каждого набора индексов $j_1, \dots, j_m \subseteq \{0, 1, \dots, k-1\}$, $2 \leq m \leq k-1$, по индукции получим

$$z_{j_1} \vee \dots \vee z_{j_m} = \max(z_{j_1}, \dots, z_{j_m}),$$

$$z_{j_1} \wedge \dots \wedge z_{j_m} = \min(z_{j_1}, \dots, z_{j_m}).$$

Так как множества Z_k , $k \geq 2$, замкнуты относительно указанных операций, распространим их действие на $(k_1, \dots, k_n; k)$ -классы функций.

Определим функции $x_i^{[a]}$, $\bar{x}^{[a]} \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$ для $i \in \{1, \dots, n\}$, $a \in Z_{k_i}$, положив

$$x_i^{[a]} = \begin{cases} z_{k-1}, & x_i = a, \\ z_0, & x_i \neq a, \end{cases} \quad \bar{x}_i^{[a]} = \begin{cases} z_0, & x_i = a, \\ z_{k-1}, & x_i \neq a. \end{cases}$$

По индукции получим

$$x_{i_1}^{[a_{i_1}]} \vee \dots \vee x_{i_s}^{[a_{i_s}]} = \begin{cases} z_{k-1}, & (x_{i_1}, \dots, x_{i_s}) = (a_{i_1}, \dots, a_{i_s}), \\ z_0, & (x_{i_1}, \dots, x_{i_s}) \neq (a_{i_1}, \dots, a_{i_s}), \end{cases}$$

$$\bar{x}_{i_1}^{[a_{i_1}]} \vee \dots \vee \bar{x}_{i_s}^{[a_{i_s}]} = \begin{cases} z_0, & (x_{i_1}, \dots, x_{i_s}) = (a_{i_1}, \dots, a_{i_s}), \\ z_{k-1}, & (x_{i_1}, \dots, x_{i_s}) \neq (a_{i_1}, \dots, a_{i_s}). \end{cases}$$

Легко показать, что для любой $(k_1, \dots, k_n; k)$ -функции $f(x^{(n)})$ верны тождества

$$f(x^{(n)}) = \bigvee_{a^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}} \left\{ f(a^{(n)}) \wedge (x_1^{[a_1]} \wedge \dots \wedge x_n^{[a_n]}) \right\}, \quad (1.1)$$

$$f(x^{(n)}) = \bigwedge_{d^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}} \left\{ f(d^{(n)}) \vee (\bar{x}_1^{[d_1]} \vee \dots \vee \bar{x}_n^{[d_n]}) \right\}. \quad (1.2)$$

1.3. Системы дискретных уравнений. Теорема о равносильности систем

Множество систем дискретных уравнений вида

$$f_j(x^{(n)}) = b_j, \quad j = 1, \dots, t, \quad (1.3)$$

где $f_j(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$, $b_j \in Z_k$, $j = 1, \dots, t$, обозначим $S(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$. Множество систем дискретных уравнений вида (1.3), где $f_j(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$, $b_j \in Z_{\geq 0}$, $j = 1, \dots, t$, обозначим $S(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$.

Как обычно, множество решений системы S обозначается $\text{sol}(S)$.

Множество значений $(k_1, \dots, k_n)$ -функции $f(x^{(n)})$ обозначим M_f . Очевидно, что для совместности системы (1.3) необходимо выполнение условий $b_j \in M_{f_j}$, $j = 1, \dots, t$. Будем считать эти условия выполненными.

Определение 1.3.

1. Множество $S(Z_{k_1} \times \dots \times Z_{k_n}; Z_{\geq 0})$ систем дискретных уравнений назовем $(k_1, \dots, k_n)$ -классом систем уравнений.
2. Множество $S(Z_{k_1} \times \dots \times Z_{k_n}; Z_k)$ систем дискретных уравнений назовем $(k_1, \dots, k_n; k)$ -классом систем уравнений.

Покажем, что для каждой $(k_1, \dots, k_n)$ -системы уравнений вида (1.3) существует равносильная ей $(k_1, \dots, k_n; 2)$ -система дискретных уравнений.

Каждой $(k_1, \dots, k_n)$ -функции $f(x^{(n)})$ и каждому элементу $b \in M_f$ поставим в соответствие функцию $f^{[b]}(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$, определяемую следующим образом:

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

Для $b \in Z_{\geq 0}$, $0, 1 \in Z_2$ положим $b \cdot 0 = 0$, $b \cdot 1 = b$. Тогда

$$f(x^{(n)}) = \sum_{b \in M_f} b \cdot f^{[b]}(x^{(n)}),$$

и очевидно, что уравнение $f(x^{(n)}) = b$ равносильно уравнению $f^{[b]}(x^{(n)}) = 1$.

Пример 1.1. Если функция $f(x^{(n)})$ принадлежит кольцу функций от n переменных над полем $GF(q)$, $b \in GF(q)$, то $f^{[b]}(x^{(n)}) \equiv (1 - (f(x^{(n)}) - b)^{q-1})$.

Так как замена каждого уравнения системы равносильным уравнением приводит к равносильной системе уравнений, то справедливо следующее утверждение.

Теорема 1.1. $(k_1, \dots, k_n)$ -система уравнений S , заданная соотношениями (1.3), равносильна $(k_1, \dots, k_n; 2)$ -системе, заданной уравнениями

$$g_j(x^{(n)}) = 1, \quad j = 1, \dots, t, \quad (1.4)$$

где $g_j(x^{(n)}) = f_j^{[b_j]}$.

С учетом теоремы 1.1 далее будем рассматривать алгебры, определенные на $(k_1, \dots, k_n; 2)$ -классах функций, предполагая, что на множестве Z_2 заданы операции отрицания $(\bar{x})$, дизъюнкции $(x_1 \vee x_2)$, конъюнкции $(x_1 \wedge x_2)$ или $x_1 \cdot x_2$ и сложения по mod 2: $(x_1 \oplus x_2)$, которые распространены на рассматриваемый класс дискретных функций.

Очевидны утверждения приводимого ниже следствия.

Следствие 1.1. $(k_1, \dots, k_n; 2)$ -система, заданная уравнениями (1.4), равносильна $(k_1, \dots, k_n)$ -уравнению

$$\sum_{j=1}^t g_j(x^{(n)}) = t, \quad (1.5)$$

где суммирование ведется в кольце целых чисел, и $(k_1, \dots, k_n; 2)$ -уравнениям

$$\bigwedge_{j=1}^t g_j(x^{(n)}) = 1, \quad (1.6)$$

$$\bigvee_{j=1}^t \bar{g}_j(x^{(n)}) = 0. \quad (1.7)$$

1.4. Аналоги дизъюнктивных и конъюнктивных форм в алгебре

$$D(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$$

При $k = 2$, $j \in \{1, \dots, n\}$ функции $x_i^{[a]}$, $\bar{x}^{[a]}$, определенные в разделе 1.2, связаны тождеством $\bar{x}_i^{[a]} \equiv x_i^{[a]} \oplus 1$. Поэтому для любой функции $f(x^{(n)}) \in D(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$ верны тождества, получаемые из (1.1), (1.2):

$$f(x^{(n)}) = \bigvee_{\substack{a^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}, \\ f(d^{(n)})=1}} (x_1^{[a_1]} \wedge \dots \wedge x_n^{[a_n]}), \quad (1.8)$$

$$f(x^{(n)}) = \bigwedge_{\substack{d^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}, \\ f(d^{(n)})=0}} (\bar{x}_1^{[a_1]} \vee \dots \vee \bar{x}_n^{[a_n]}). \quad (1.9)$$

Для булевых функций задание (1.8) совпадает с *совершенной дизъюнктивной нормальной формой*, задание (1.9) — с *совершенной конъюнктивной нормальной формой* функции.

По аналогии с булевым случаем выражения $x_i^{[a]}$, $\bar{x}_i^{[a]}$ назовем *литералами*, а выражения вида $l_{i_1}^{a_{i_1}} \vee \dots \vee l_{i_s}^{a_{i_s}}$ и $l_{i_1}^{a_{i_1}} \wedge \dots \wedge l_{i_s}^{a_{i_s}}$, где $l_{i_1}^{a_{i_1}}, \dots, l_{i_s}^{a_{i_s}}$ — литералы и $i_j \neq i_m$ при $j \neq m$, назовем соответственно *дизъюнктами* и *конъюнктами*.

Каждое тождество вида

$$f(x^{(n)}) = \bigvee_{C_j \in C} C_j, \quad f(x^{(n)}) = \bigwedge_{D_j \in D} D_j,$$

где C , D — некоторые множества конъюнктов (соответственно, дизъюнктов) назовем *дизъюнктивной* (соответственно, *конъюнктивной*) формой функции $f(x^{(n)})$.

2. Параметрическое решение и граф решений системы дискретных уравнений

Определение 2.1. *Параметрическим (или общим) решением совместной $(k_1, \dots, k_n)$ -системы дискретных уравнений S назовем каждое сюръективное отображение $\varphi : Z_{k_1} \times \dots \times Z_{k_n} \rightarrow \text{sol}(S)$, где*

$$\varphi(p^{(n)}) = (\varphi_1(p^{(n)}), \varphi_2(p^{(n)}), \dots, \varphi_n(p^{(n)})).$$

Из определения 2.1 следует, что для любого $p^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}$ набор значений переменных $x_i = \varphi_i(p^{(n)})$, $i = 1, \dots, n$, является решением системы S , и любое решение системы S может быть получено таким способом.

Полным $(k_1, \dots, k_n)$ -графом назовем граф $G(k_1, \dots, k_n)$, определяемый следующими условиями:

1. Граф $G(k_1, \dots, k_n)$ является корневым графом. Вершину, являющуюся корнем графа, обозначим $\nu_\emptyset$.
2. Длина каждого из максимальных путей графа $G(k_1, \dots, k_n)$ равна n .
3. Из каждой вершины графа $G(k_1, \dots, k_n)$, лежащей на расстоянии i ($1 \leq i \leq n$) от корневой вершины графа, исходит k_i ребер, помеченных метками из множества Z_{k_i} , а в каждую вершину графа $G(k_1, \dots, k_n)$, кроме корня, входит одно ребро. Множество вершин, лежащих на расстоянии i от корня графа, обозначим V_i , $i = 1, \dots, n$.
4. Ребра, исходящие из одной вершины, имеют разные метки.

Условия 2, 3 обеспечивают единственность пути, ведущего из корневой вершины в любую отличную от нее вершину графа $G(k_1, \dots, k_n)$. Используя это свойство, примем обозначение $v_{\alpha_1, \dots, \alpha_i}$ для вершины графа $G(k_1, \dots, k_n)$, в которую ведет путь с последовательностью меток $\alpha_1, \dots, \alpha_i$. Для корневой вершины примем обозначение $v_\emptyset$.

В дальнейшем будем предполагать, что множество V_i вершин уровня i графа $G(k_1, \dots, k_n)$ упорядочено в соответствии с возрастающим лексикографическим порядком соответствующей последовательности меток $\alpha_1, \dots, \alpha_i$.

Определение 2.2. Графом решений совместной системы дискретных уравнений $S \in S(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$ назовем подграф $G(S)$ графа $G(k_1, \dots, k_n)$, образованный всеми максимальными путями, n -последовательность меток которых принадлежит множеству решений системы S .

Очевидно, что каждая совместная система уравнений из класса $S(Z_{k_1} \times \dots \times Z_{k_n}; Z_2)$ имеет однозначно определенный граф решений, соответствующий определению 2.2.

В [24] дано более общее определение графа решений системы дискретных уравнений. Там же предложен алгоритм построения общего решения системы дискретных уравнений по ее графу решений.

3. Разреженные системы дискретных уравнений

3.1. Основные определения

Определение 3.1. $(k_1, \dots, k_n; 2)$ -система уравнений (1.4) называется m -разреженной, если множество существенных переменных каждого уравнения не превосходит числа $m < n$.

Каждую m -разреженную $(k_1, \dots, k_n; 2)$ -систему дискретных уравнений можно задать соотношениями

$$f_j(X_j) = 1, \quad j = 1, \dots, t, \quad (3.1)$$

где функция $f_j(X_j)$, $j = 1, \dots, t$, существенно зависит только от переменных из множества X_j , $|X_j| = m_j \leq m$, $X = \cup_{j=1}^t X_j$.

Без ущерба для общности рассуждений предположим, что выполнены следующие условия:

- 1) $|X_j| > 1$, $j = 1, \dots, t$;
- 2) подмножества $X_1, \dots, X_t$ различны;
- 3) ни одно из подмножеств $X_1, \dots, X_t$ не содержится в другом подмножестве;
- 4) отсутствуют переменные, принадлежащие только одному из подмножеств $X_1, \dots, X_t$.

Определение 3.2. Y -фрагмент $(\alpha_1, \dots, \alpha_s)$, где $Y = \{x_{i_1}, \dots, x_{i_s}\}$, назовем Y -запретным в системе S , если существует список

$$S^{(j)} = (L_j, X_j), \quad \text{где } X_j \supseteq Y,$$

и матрица L_j не содержит строки, в которой

$$x_{j_1} = \alpha_1, x_{j_2} = \alpha_2, \dots, x_{i_s} = \alpha_s.$$

Ясно, что каждый Y -фрагмент, содержащий запретный подфрагмент, Y -запретен. Запретный Y -фрагмент, не содержащий собственных запретных подфрагментов, назовем *минимальным*.

Из определения 3.2 следует, что Y -запретный фрагмент не может содержаться ни в одном Y -фрагменте решений системы S . Обратно, вектор $z^{(n)} \in Z_{k_1} \times \dots \times Z_{k_n}$ тогда и только тогда является решением системы уравнений, когда он не содержит запретных фрагментов. Поэтому удаление из ансамбля списков решений системы строк, содержащих запретные фрагменты, приводит к ансамблю списков равносильной системы уравнений.

В [13, 14] рассмотрена процедура *согласования* списков решений (X_j, L_j) , $j = 1, 2$, при $X_1 \cap X_2 \neq \emptyset$. Пусть b является $X_1 \cap X_2$ -фрагментом, пусть существует фрагмент $(a, b) \in S_1$ и не существует такого фрагмента c (может быть, и пустого), что $(b, c) \in S_2$.

Согласование списков S_1, S_2 заключается в удалении из них всех фрагментов указанного вида. Очевидно, что в описанной ситуации фрагмент b является запретным в списке S_2 , следовательно, X_1 -фрагмент (a, b) в ходе процедуры удаления запретов будет удален из всех содержащих его списков.

Следовательно, исключением минимальных запретных фрагментов, содержащихся в строках каждой матрицы L_j , автоматически достигается попарное согласование списков системы. При этом надо учитывать, что удаление запретного фрагмента может привести к появлению новых запретов.

3.4. Вычисление общего решения $(k_1, \dots, k_m; 2)$ -уравнения по списку решений

Построение общего решения разреженной $(k_1, \dots, k_n; 2)$ -системы уравнений вида (3.1) может быть трудоемким, если параметры системы велики, однако легко построить общее решение каждого уравнения $f_j(X_j) = 1$ системы (3.1) непосредственно по списку его решений.

Исходные данные: $(k_{j(1)} \times \dots \times k_{j(m_j)}; 2)$ -уравнение $f_j(X_j) = 1$ и список $S^{(j)} = (L_j, X_j)$ его решений.

Введем следующие обозначения:

$M_{j(1)}^{(j)}$ — множество значений элементов первого столбца матрицы L_j ;

$L_j(\alpha_1, \dots, \alpha_{i-1})$ — подматрица матрицы L_j , составленная из строк, в которых $x_{j(1)} = \alpha_1, \dots, x_{j(i-1)} = \alpha_{i-1}$, $i = 2, \dots, m_j$;

$M_{j(i)}^{(j)}(\alpha_1, \dots, \alpha_{i-1})$ — множество значений i -го столбца непустой матрицы $L_j(\alpha_1, \dots, \alpha_{i-1})$ (если в матрице L_j нет строк с $x_{j(1)} = \alpha_1, \dots, x_{j(i-1)} = \alpha_{i-1}$, то $L_j(\alpha_1, \dots, \alpha_{i-1}) = \emptyset$, $M_{j(i)}^{(j)}(\alpha_1, \dots, \alpha_{i-1}) = \emptyset$), $i = 2, \dots, n$;

$p_s^{\{M\}}$ — свободные переменные с областью значений $M \subset Z_{k_s}$;

$\pi_{j(1)}^{(j)}: Z_{k_{j(1)}} \rightarrow M_{j(1)}^{(j)}$ — произвольное сюръективное отображение, удовлетворяющее условию: если $\alpha \in M_{j(1)}^{(j)}$, то $\pi_{j(1)}^{(j)}(\alpha) = \alpha$;

$\pi_{j(i)}^{(j)}(\alpha_1, \dots, \alpha_{i-1}; p_{j(i)}): Z_{k_{j(i)}} \rightarrow M_{j(i)}^{(j)}(\alpha_1, \dots, \alpha_{i-1})$ — произвольное сюръективное отображение, удовлетворяющее условию: если $\alpha \in M_{j(i)}^{(j)}(\alpha_1, \dots, \alpha_{i-1})$, то $\pi_{j(i)}^{(j)}(\alpha_1, \dots, \alpha_{i-1}; \alpha) = \alpha$, $i = 2, \dots, m_j$.

Теорема 3.1. *Общее решение уравнения $f_j(X_j) = 1$ задается m_j соотношениями*

$$\begin{aligned} x_{j(1)} &= \pi_{j(1)}^{(j)}(p_{j(1)}), \\ x_{j(2)} &= \sum_{\alpha_1 \in M_{j(1)}^{(j)}} x_{j(1)}^{[\alpha_1]} \pi_{j(2)}^{(j)}(\alpha_1; p_{j(2)}), \\ x_{j(i)} &= \sum_{\substack{\alpha^{(i-1)} \in Z_{k_{j(1)}} \times \dots \times Z_{k_{j(i-1)}} \\ L(\alpha^{(i-1)}) \neq \emptyset}} x_{j(1)}^{[\alpha_1]} \dots x_{j(i-1)}^{[\alpha_{i-1}]} \pi_{j(i)}^{(j)}(\alpha^{(i-1)}; p_{j(i)}), \quad i = 3, \dots, m_j. \end{aligned} \quad (3.2)$$

Доказательство. По построению соотношения (3.2) в совокупности задают сюръективное отображение множества $Z_{k_{j(1)}} \times \dots \times Z_{k_{j(m_j)}}$ на множество строк матрицы L_j . «Треугольный» характер соотношений (3.2) позволяет привести полученное выражение общего решения к виду, указанному в определении 2.1. $\square$

3.5. Условия согласованности общих решений отдельных уравнений $(k_1, \dots, k_n; 2)$ -системы дискретных уравнений

Множество индексов j , $1 \leq j \leq t$, для которых выполняются условия $x_i \in X_j$, $i = j(s)$, обозначим $J(i, s)$. Очевидно, что

$$\begin{aligned} J(1, 1) &= \{j; x_i \in X_j\}, \quad J(1, s) = \emptyset \quad \text{при} \quad s \neq 1, \\ J(n, m_j) &= \{j; x_i \in X_j\}, \quad J(n, s) = \emptyset \quad \text{при} \quad s \neq m_j. \end{aligned}$$

Теорема 3.2 (уравнения согласованности общих решений). *Набор значений $x_1 = \alpha_1, x_2 = \alpha_2, \dots, x_n = \alpha_n$ тогда и только тогда является решением системы (3.1), когда найдутся значения $p_i \in Z_k, i = 1, 2, \dots, n$, при которых выполняются соотношения*

$$\begin{aligned} x_1 &= p_1^{\{M_1^{(j)}\}} \text{ для всех } j, \quad x_1 \in X_j, \\ x_i &= \sum_{\substack{\alpha^{(s-1)} \in Z_{k_{j(1)}} \times \dots \times Z_{k_{j(s-1)}} \\ L_j(\alpha_{j(1)}, \dots, \alpha_{j(s-1)}) \neq \emptyset}} x_{j(1)}^{[\alpha_{j(1)}]} \dots x_{j(s-1)}^{[\alpha_{j(s-1)}]} p_i^{\{M_s^{(j)}(\alpha_{j(1)}, \dots, \alpha_{j(s-1)})\}} \\ &\quad \text{для } i=2, \dots, n-1, \quad j \in J(i, s), \\ x_n &= \sum_{\substack{\alpha^{(m_j-1)} \in Z_{k_{j(1)}} \times \dots \times Z_{k_{j(m_j-1)}} \\ L_j(\alpha_{j(1)}, \dots, \alpha_{j(m_j-1)}) \neq \emptyset}} x_{j(1)}^{[\alpha_{j(1)}]} \dots x_{j(m_j-1)}^{[\alpha_{j(m_j-1)}]} p_n^{\{M_{m_j}^{(j)}(\alpha_{j(1)}, \dots, \alpha_{j(m_j-1)})\}}. \end{aligned}$$

Доказательство. Достаточность условий теоремы вытекает из того, что каждый X_j -фрагмент вектора $(\alpha_1, \alpha_2, \dots, \alpha_n)$ является, по построению, решением уравнения $f_j(X_j) = 1, j = 1, \dots, t$.

Обратно, если вектор $(\alpha_1, \alpha_2, \dots, \alpha_n)$ принадлежит множеству решений системы, то каждый его X_j -фрагмент является решением уравнения $f_j(X_j) = 1$, поэтому необходимость условий теоремы 3.2 следует из теоремы 3.1. $\square$

Набор значений переменных $x_1, x_2, \dots, x_n$ тогда и только тогда является решением системы (3.1), когда выполняются соотношения

$$\begin{aligned} x_1 &= \alpha_1 \in E_1 = \bigcap_{j, x_1 \in X_j} M_1^{(j)}, \\ x_2 &= \alpha_2 \in E_2(\alpha_1) = \left(\bigcap_{j, j(2)=1} M_1^{(j)} \right) \cap \left(\bigcap_{s=1}^2 \bigcap_{j, j(2)=s} M_s^{(j)}(\alpha_{j(1)}) \right), \\ x_i &= \alpha_i \in E_i(\alpha^{(i-1)}) = \left(\bigcap_{j, j(i)=1} M_1^{(j)} \right) \cap \left(\bigcap_{s=1}^i \bigcap_{j, j(i)=s} M_s^{(j)}(\alpha_{j(1)}, \dots, \alpha_{j(s-1)}) \right), \\ &\quad i = 3, 4, \dots, n-1, \\ x_n &= \alpha_n \in E_T(\alpha^{(n-1)}) = \bigcap_{j, x_n \in X_j} M_{m_j}^{(j)}(\alpha_{j(1)}, \dots, \alpha_{j(m_j-1)}). \end{aligned}$$

Доказательство проводится непосредственной проверкой идентичности соотношений из теоремы 3.2 и следствия 3.1.

4. Алгоритмы определения совместности и решения разреженной системы $(k_1, \dots, k_n; 2)$ -уравнений

4.1. Предварительные замечания

Рассматриваются алгоритм определения совместности и алгоритм перечисления решений разреженной системы дискретных уравнений S , заданной уравнениями (3.1).

По определению 2.2 множество решений системы S совпадает с множеством меток концевых вершин графа $G(S)$. Поэтому для установления совместности системы S достаточно построить один путь T длины n , принадлежащий графу $G(S)$.

Исходными данными для построения пути T или доказательства его отсутствия являются списки решений (X_j, L_j) , $j = 1, \dots, t$, уравнений системы и условия согласованности из теоремы 3.2, которые мы сформулируем в более удобном для описания алгоритма виде.

Предлагаемый алгоритм состоит из предварительного этапа и ряда последовательных шагов.

4.2. Алгоритм определения совместности системы уравнений (3.1)

Предварительный этап

- а) В соответствии с разделом 3.1 упорядочиваем множество неизвестных и уравнений системы.
- б) Попарно согласуем списки решений.
- с) Вычисляем общие решения отдельных уравнений системы (3.1) и получаем условия согласованности общих решений отдельных уравнений. Полагаем $\nu_\emptyset \in T$.

Шаг 1. Вычисляем множество E_1 возможных меток ребер графа $G(S)$, исходящих из вершины $\nu_\emptyset$.

Если $|E_1| = 0$, то система (3.1) несовместна. Если $|E_1| > 0$, полагаем $\nu_{\alpha_1} \in T$, где α_1 — минимальная метка в множестве E_1 , после чего метка α_1 удаляется из множества E_1 (обозначение множества при этом не меняется). Если после удаления метки оказывается, что $|E_1| \neq 0$, помечаем вершину $\nu_\emptyset$ знаком *развилки*.

Шаг 2. Вычисляем множество $E_2(\alpha_1)$ возможных меток ребер графа $G(S)$, исходящих из вершины ν_{α_1} .

Если $|E_2(\alpha_1)| = 0$ и вершина $\nu_{\emptyset}$ является развилкой, то возвращаемся к шагу 1. Если при всех $\alpha_1 \in E_1$ имеем $E_2(\alpha_1) = \emptyset$, то система (3.1) несовместна. В противном случае полагаем $\nu_{\alpha_1, \alpha_2} \in T$, где α_2 — минимальная метка в множестве $E_2(\alpha_1)$, для которой $E_2(\alpha_1) \neq \emptyset$, после чего метка α_2 удаляется из множества $E_2(\alpha_1)$ (обозначение множества при этом не меняется). Если после удаления метки $|E_2(\alpha_1)| \neq 0$, помечаем вершину ν_{α_1, α_2} знаком развилки.

.....

Шаг $i = 3, \dots, n-1$. Вычисляем множество $E_i(\alpha^{(i-1)})$ возможных меток ребер графа $G(S)$, исходящих из вершины $\nu_{\alpha^{(i-1)}}$. Если $|E_i(\alpha^{(i-1)})| = 0$, то возвращаемся к шагу l , где $0 < l < i$ и l — максимальное число, при котором вершина $\nu_{\alpha^{(l)}}$ является развилкой. Если $|E_i(\alpha^{(i-1)})| = 0$ и среди вершин $\nu_{\alpha^{(l)}}$, $l < i$, нет развилок, то система (3.1) несовместна.

Если $|E_i(\alpha^{(i-1)})| > 0$, то полагаем $\nu_{\alpha^{(i-1)}} \in T$, где α_{i-1} — минимальная метка в множестве $E_i(\alpha^{(i-1)})$, после чего метка α_{i-1} удаляется из множества $E_i(\alpha^{(i-1)})$ (обозначение множества при этом не меняется). Если после удаления метки $|E_i(\alpha^{(i-1)})| \neq 0$, помечаем вершину $\nu_{\alpha^{(i-1)}}$ знаком развилки.

.....

Шаг n . Вычисляем множество $E_n(\alpha^{(n-1)})$ возможных меток ребер графа $G(S)$, исходящих из вершины $\nu_{\alpha^{(n-1)}}$. Если $|E_n(\alpha^{(n-1)})| = 0$, то возвращаемся к шагу l , где $0 < l < n$ и l — максимальное число, при котором вершина $\nu_{\alpha^{(l-1)}}$ является развилкой.

Если $|E_n(\alpha^{(n-1)})| > 0$, то для всех меток $\alpha_n \in E_n(\alpha^{(n-1)})$ имеем $\alpha^{(n)} \in \text{sol}(S)$.

После получения одного решения совместной системы уравнений вида (3.1) работа алгоритма 4.2 может быть продолжена вплоть до перечисления всех решений системы уравнений.

4.3. К оценке сложности алгоритма 4.1

В алгоритме реализуются аналоги принципов и приемов, заложенных в алгоритме DPLL [3, 4], методе резолюций [5, 6] и методе согласования [13, 14, 16].

Алгоритм DPLL основан на следующих принципах.

1. Правило единичного дизъюнкта.
2. Стратегия распространения булевых ограничений (ВСП-стратегия).
3. Разбор конфликтов (бэктрекинг и бэкджампинг).

Аналоги этих принципов очевидным образом реализуются в ходе работы алгоритма 4.2. Так, бэкджампингу соответствует спуск до первой развилки при возникновении конфликтной ситуации.

В основе метода резолюций лежат поиск контрарных дизъюнктов и построение их резольвент, для чего используется метод исключения неизвестных. Понятие контрарных дизъюнктов может быть распространено на разреженные системы дискретных уравнений. Конфликты, порождаемые контрарными дизъюнктами, автоматически учитываются и разрешаются в ходе работы алгоритма.

Метод согласования используется на предварительном этапе алгоритма 4.1 для сокращения списков решений.

В [18] приведена оценка средней трудоемкости алгоритма построения всех решений 3-разреженной системы уравнений над конечным полем, использующего операцию «склеивания» списков решений.

Вопрос о средней трудоемкости алгоритма 4.1 требует дальнейшего изучения. Отметим, что его трудоемкость сокращается с увеличением числа решений системы.

Список литературы

- [1] Cook S., "The complexity of theorem-proving procedures". In: "Proc. 3rd Ann. ACM Symp. Theory of Computing", New York: ACM, 1971, 151–158
- [2] Гэри М., Джонсон Д., *Вычислительные машины и труднорешаемые задачи*, М.: Мир, 1982, 416 с.
- [3] Davis M., Putnam H., "A computing procedure for quantification theory", *J. ACM*, 7:3 (1960), 201–215.
- [4] Davis M., Logemann G., Loveland D., "A machine program for theorem proving", *Comm. ACM*, 5:7 (1962), 394–397.
- [5] Робинсон Дж., "Машинно-ориентированная логика, основанная на принципе резолюции", *Киберн. сборник. Новая серия*, 7 (1970), 194–218.

- [6] Чень Ч., Ли Р., *Математическая логика и автоматическое доказательство теорем*, М.: Наука, 1983, 360 с.
- [7] Rolf D., *Improved bound for the PPSZ/Schöning-algorithm for 3-SAT*, Electr. Colloq. Comput. Complexity (ECCC), Report 159 (2005), 11 с.
- [8] Dantsin E., Goerd A., Hirsch E. A., Kannan R., Kleinberg J., Papadimitriou C., Raghavan P., Schöning U., “A deterministic $(2 - 2/(k+1))^n$ algorithm for k -SAT, based on local search”, *Theor. comput. science*, **289**:1 (2002), 69–83.
- [9] Brüggemann T., Kern W., “An improved local search algorithm for 3-SAT”, *Theor. comput. science*, **329**:1–3 (2004), 303–313.
- [10] Scheder D., “Guided search and a faster deterministic algorithm for 3-SAT”, *Lect. Notes Comput. Sci.*, **4957**, 2008, 60–71.
- [11] Scheder D., *Algorithms and Extremal Properties of SAT and CSP*, diss. for the degree of Doctor of Sciences, Zurich: Swiss Federal Inst. Technol., 2011, 123 с.
- [12] Monien B., Speckenmeyer E., “Solving satisfiability in less than 2^n steps”, *Discr. Appl. Math.*, **10**:3 (1985), 287–295.
- [13] Raddum H., Semaev I., *New technique for solving sparse equation systems*, Cryptology ePrint Archive, 2006/475.
- [14] Semaev I., “On solving sparse algebraic equations over finite fields”, *Des., Codes and Cryptogr.*, **49**:1–3 (2008), 47–60.
- [15] Semaev I., Mikuš M., “Methods to solve algebraic equations in cryptanalysis”, *Tatra Mt. Math. Publ.*, **45** (2010), 107–136.
- [16] Semaev I., “Improved agreeing-gluing algorithm. 2nd Int.”, *Math. in Comput. Sci.*, **7** (2010), 321–339.
- [17] Semaev I., “Sparse Boolean equations and circuit lattices”, *Des., Codes Cryptogr.*, **59**:1 (2011), 349–364.
- [18] Semaev I., “MaxMinMax problem and sparse equations over finite fields”, *Des., Codes Cryptogr.*, **79**:2 (2016), 383–404.
- [19] Смирнов В. Г., “Полиномиальные представления дискретных функций”, *Труды по дискретной математике*, **11**, М.: Физматлит, 2008, 119–137.
- [20] Löwenheim L., “Über die auflösung von Gleichungen im logischen Gebietkalkül”, *Math. Ann.*, **68**:2 (1910), 169–207.
- [21] Scala H., “The general solution of an arbitrary Boolean equation”, *Amer. Math. Monthly*, **74**:9 (1967), 1074–1077.
- [22] Deschamps J. P., “Parametric solutions of boolean equations”, *Discrete Math.*, **3**:4 (1972), 333–342.
- [23] Смирнов В. Г., “Эффективные алгоритмы построения графа общего решения для систем булевых уравнений”, *Труды по дискретной математике*, **5**, М.: Физматлит, 2002, 227–234.
- [24] Смирнов В. Г., “Методы решения систем дискретных уравнений, основанные на построении графа решений”, *Труды по дискретной математике*, **9**, М.: Гелиос АРВ, 2006, 308–339.

Приложение 1. Пример решения разреженной $(k_1, \dots, k_n; 2)$ -системы уравнений по общим решениям отдельных уравнений системы

Ниже приведено упорядоченное множество списков решений $Z_3 \times Z_2 \times Z_2 \times Z_3 \times Z_2 \times Z_2$ -системы дискретных уравнений.

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 0	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

В ходе попарного согласования списков из списка $S^{(1)}$ удаляется строка, содержащая запретный фрагмент $(x_1, x_2) = (2, 1)$, из списка $S^{(4)}$ удаляется строка, содержащая запретный фрагмент $(x_3, x_4) = (1, 1)$, из списка $S^{(2)}$ удаляется строка, содержащая запретный фрагмент $(x_1, x_5) = (1, 0)$. В результате становится запретным фрагмент $(x_1, x_2) = (1, 0)$, который удаляется из списка $S^{(1)}$. Попарно согласованный ансамбль списков приведен ниже.

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 1 0	1 1 1	1 1 1	0 1 2	0 2 0
2 0 1	2 0 0	2 0 0	1 0 1	0 2 1
	2 0 1	2 0 1	1 0 2	1 0 0
		2 1 1		1 2 0

Используя теорему 3.1, вычислим общие решения уравнений системы.

$$\text{Список } S^{(1)}: x_1 = p_1^{\{0,1,2\}}, \quad x_2 = x_1^{[1]}, \quad x_3 = x_1^{[0]} + x_1^{[2]}.$$

$$\text{Список } S^{(2)}: x_1 = p_1^{\{0,1,2\}}, \quad x_2 = x_1^{[1]}, \quad x_5 = x_1^{[0]} + x_1^{[1]} + x_1^{[2]} \cdot p_5^{\{0,1\}}.$$

$$\text{Список } S^{(3)}: x_1 = p_1^{\{0,1,2\}}, \quad x_5 = x_1^{[0]} + x_1^{[1]} + x_1^{[2]} \cdot p_5^{\{0,1\}}, \quad x_6 = x_5^{[1]} + x_1^{[2]} \cdot x_5^{[0]} \cdot p_6^{\{0,1\}} + x_1^{[2]} \cdot x_5^{[1]}.$$

$$\text{Список } S^{(4)}: x_2 = p_2^{\{0,1\}}, \quad x_3 = x_2^{[0]}, \quad x_4 = x_3^{[0]} \cdot p_4^{\{1,2\}} + x_3^{[1]} \cdot p_4^{\{0,2\}}.$$

$$\text{Список } S^{(5)}: x_3 = p_3^{\{0,1\}}, \quad x_4 = x_3^{[0]} \cdot p_4^{\{1,2\}} + x_3^{[1]} \cdot p_4^{\{0,2\}}, \quad x_6 = x_4^{[1]} + x_3^{[0]} x_4^{[2]} \cdot p_6^{\{0,1\}}.$$

По теореме 3.2 условия согласованности общих решений задаются соотношениями

$$\begin{aligned}x_1 &= p_1^{\{0,1,2\}}, \\x_2 &= x_1^{[1]}, \\x_3 &= x_1^{[0]} + x_1^{[2]} = x_2^{[0]}, \\x_4 &= x_3^{[0]} \cdot p_4^{\{1,2\}} + x_3^{[1]} \cdot p_4^{\{0,2\}}, \\x_5 &= x_1^{[0]} + x_1^{[1]} + x_1^{[2]} \cdot p_5^{\{0,1\}}, \\x_6 &= x_5^{[1]} + x_1^{[2]} \cdot x_5^{[0]} \cdot p_6^{\{0,1\}} + x_1^{[2]} \cdot x_5^{[1]} = x_4^{[1]} + x_3^{[0]} x_4^{[2]} \cdot p_6^{\{0,1\}}.\end{aligned}$$

Переменная, значение которой в ходе работы алгоритма не определилось однозначно, назовем развилкой, которую отметим знаком $\vee$.

Схематически процесс построения путей в графе решений представлен в табл. 1.

Таблица 1. Построение путей в графе решений

NN	x_1	x_2	x_3	x_4	x_5	x_6	Результат
1	$0\vee$	0	1	$0\vee$	1	$\mathbf{1} = 0!$	$\times$
2	$0\vee$	0	1	2	1	$\mathbf{1} = 0!$	$\times$
3	$1\vee$	1	0	$1\vee$	1	1	$\in \text{sol}(S)$
4	$1\vee$	1	0	2	1	1	$\in \text{sol}(S)$
5	2	0	1	$0\vee$	$0\vee$	0	$\in \text{sol}(S)$
6	2	0	1	$0\vee$	1	$\mathbf{1} = 0!$	$\times$
7	2	0	1	2	$0\vee$	0	$\in \text{sol}(S)$
8	2	0	1	2	1	$\mathbf{0} = 1!$	$\times$

В последней строке нет развилок, следовательно, перебор закончен. Найдено четыре решения рассматриваемой системы уравнений.

Приложение 2. Пример применения алгоритма 4.1 для решения разреженной системы булевых уравнений

Рассмотрим пример решения разреженной системы булевых уравнений в анализе фильтрующего генератора над полем $GF(2)$. Пример имеет чисто иллюстративный характер.

Предполагается, что в рассматриваемой схеме рекуррентная зависимость имеет вид $x_{i+4} = x_i \oplus x_{i+1}$, фильтрующая функция известна: $f(x^{(4)}) = x_1 \cdot x_4 \oplus x_2$, ключом задается начальное заполнение (x_1, x_2, x_3, x_4) регистра сдвига. Требуется определить ключ по известной выходной последовательности $\gamma_1 = 0, \gamma_2 = 1, \gamma_3 = 0, \gamma_3 = 4$.

Разреженная система булевых уравнений, к решению которой сводится поставленная задача, имеет следующий вид:

$$\begin{aligned}x_1 \cdot x_4 \oplus x_3 &= 0, \\x_1 \oplus x_2 \oplus x_5 &= 0, \\x_2 \cdot x_5 \oplus x_4 &= 1, \\x_2 \oplus x_3 \oplus x_6 &= 0, \\x_3 \cdot x_6 \oplus x_5 &= 0, \\x_3 \oplus x_4 \oplus x_7 &= 0, \\x_4 \cdot x_7 \oplus x_6 &= 1.\end{aligned}$$

Соответствующее множество списков решений системы уравнений приведено ниже.

Исходные списки решений 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

Предварительный этап

а) Вычисляем частоты вхождения переменных в уравнения системы:

$$\begin{aligned}v(x_1) &= 2, & v(x_2) &= 3, & v(x_3) &= 4, & v(x_4) &= 4, \\v(x_5) &= 3, & v(x_6) &= 3, & v(x_7) &= 2.\end{aligned}$$

Полагаем $y_1 \equiv x_3$, $y_2 \equiv x_4$, $y_3 \equiv x_2$, $y_4 \equiv x_5$, $y_5 \equiv x_6$, $y_6 \equiv x_1$, $y_7 \equiv x_7$.

б) Упорядочиваем уравнения системы:

$$\begin{aligned}y_2 \cdot y_6 \oplus y_1 &= 0, \\y_1 \oplus y_2 \oplus y_7 &= 0, \\y_1 \oplus y_3 \oplus y_5 &= 0, \\y_1 \cdot y_5 \oplus y_4 &= 0, \\y_3 \cdot y_4 \oplus y_2 &= 1, \\y_2 \cdot y_7 \oplus y_5 &= 1, \\y_3 \oplus y_4 \oplus y_6 &= 0.\end{aligned}$$

Ниже приведен упорядоченный ансамбль списков решений уравнений системы.

(Y_1, L_1)	(Y_2, L_2)	(Y_3, L_3)	(Y_4, L_4)	(Y_5, L_5)	(Y_6, L_6)	(Y_7, L_7)
y_1, y_2, y_6	y_1, y_2, y_7	y_1, y_3, y_5	y_1, y_4, y_5	y_2, y_3, y_4	y_2, y_5, y_7	y_3, y_4, y_6
0 0 0	0 0 0	0 0 0	0 0 0	0 1 1	0 1 0	0 0 0
0 0 1	0 1 1	0 1 1	0 0 1	1 0 0	0 1 1	0 1 1
0 1 0	1 0 1	1 0 1	1 0 0	1 0 1	1 0 1	1 0 1
1 1 1	1 1 0	1 1 0	1 1 1	1 1 0	1 1 0	1 1 0

с) Попарно согласовываем списки решений:

$Y_1 \cap Y_2 = \{y_1, y_2\}$. Исключаем запрет $(y_1, y_2) = (0, 1)$ списка S_1 из списка S_2 .

$Y_2 \cap Y_6 = \{y_2, y_7\}$. Исключаем запрет $(y_2, y_7) = (0, 1)$ измененного списка S_2 из списка S_6 .

Получили попарно согласованный список решений, представленный ниже.

S_1	S_2	S_3	S_4	S_5	S_6	S_7
y_1, y_2, y_6	y_1, y_2, y_7	y_1, y_3, y_5	y_1, y_4, y_5	y_2, y_3, y_4	y_2, y_5, y_7	y_3, y_4, y_6
0 0 0	0 0 0	0 0 0	0 0 0	0 1 1	0 1 0	0 0 0
0 0 1	0 1 1	0 1 1	0 0 1	1 0 0	1 0 1	0 1 1
0 1 0	1 1 0	1 0 1	1 0 0	1 0 1	1 1 0	1 0 1
1 1 1		1 1 0	1 1 1	1 1 0		1 1 0

д) Общие решения уравнений системы:

- 1) $y_1 = p_1, \quad y_2 = y_1^{[0]} \cdot p_2 + y_1^{[1]}, \quad y_6 = y_1^{[0]} \cdot y_2^{[0]} \cdot p_6 + y_1^{[1]},$
- 2) $y_1 = p_1, \quad y_2 = y_1^{[0]} \cdot p_2 + y_1^{[1]}, \quad y_7 = y_1 \oplus y_2,$
- 3) $y_1 = p_1, \quad y_3 = p_3, \quad y_5 = y_1 \oplus y_3,$
- 4) $y_1 = p_1, \quad y_4 = y_1^{[1]} \cdot p_4, \quad y_5 = p_5,$
- 5) $y_2 = p_2, \quad y_3 = y_2^{[0]} + y_2^{[1]} \cdot p_3, \quad y_4 = y_2^{[0]} \cdot y_3^{[1]} + y_2^{[1]} \cdot y_3^{[0]} \cdot p_4,$
- 6) $y_2 = p_2, \quad y_5 = y_2^{[0]} + y_2^{[1]} \cdot p_5, \quad y_2^{[1]} \cdot y_5^{[0]},$
- 7) $y_3 = p_3, \quad y_4 = p_4, \quad y_6 = y_3 \oplus y_4.$

е) Условия согласованности общих решений:

- 1) $y_1 = p_1,$
- 2) $y_2 = y_1^{[0]} \cdot p_2 + y_1^{[1]},$
- 3) $y_3 = y_2^{[0]} + y_2^{[1]} \cdot p_3,$
- 4) $y_4 = y_1 p_4 = y_2^{[0]} \cdot y_3^{[1]} + y_2^{[1]} \cdot y_3^{[0]} \cdot p_4,$
- 5) $y_5 = y_1 \oplus y_3 = y_2^{[0]} + y_2^{[1]} \cdot p_5,$
- 6) $y_6 = y_1^{[0]} \cdot y_2^{[0]} \cdot p_6 + y_1^{[1]} = y_3 \oplus y_4,$
- 7) $y_7 = y_1 \oplus y_2 = y_2^{[1]} \cdot y_5^{[0]}.$

Схематически процесс построения путей в графе решений представлен в табл. 2.

Таблица 2. Построение путей в графе решений

NN	y_1	y_2	y_3	y_4	y_5	y_6	y_7	результат
1	$0\vee$	$0\vee$	1	$0 = 1\times$				$\times$
2	$0\vee$	1	$0\vee$	$0\vee$	0	0	1	$\in \text{sol}(S)$
3	$0\vee$	1	$0\vee$	1	0	$0 = 1\times$		$\times$
4	$0\vee$	1	1	0	1	$0 = 1\times$		$\times$
5	1	1	$0\vee$	$0\vee$	1	$0 = 1\times$		$\times$
6	1	1	$0\vee$	1	1	1	0	$\in \text{sol}(S)$
7	1	1	1	0	$0 = 1\times$			$\times$

В последней строке нет развилок, следовательно, перебор закончен. Найдено два решения рассматриваемой системы уравнений. В исходных переменных решения системы уравнений приведены в следующей таблице.

Таблица 3. Решения системы уравнений

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