МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2023 Т. 14 № 1 С. 115–130

УДК 519.712.41+519.719.2 DOI https://doi.org/10.4213/mvk434

Об одном методе построения следствий специального вида для систем булевых уравнений

А. В. Тарасов

ООО «Центр сертификационных исследований», Москва

Получено 12.V.2022

Аннотация. Излагается подход к решению систем булевых уравнений, основанный на использовании биюнктивных имплицент. Предложен базовый алгоритм нахождения таких имплицент и рассмотрен вопрос об одновыполнимости построенной системы.

Ключевые слова: булева функция, система булевых уравнений, биюнктивные функции

On a method to construct special type corollaries for systems of Boolean equations

A. V. Tarasov

LLC «Sertification Research Center», Moscow

Abstract. We describe an approach to solve systems of Boolean equations by means of bijunctive implicents. We suggest a basic algorithm to find such implicents and discuss the question on the uniqueness of feasibility of the constructed system.

Keywords: Boolean function, system of Boolean equations, bijunctive function

Citation: Matematicheskie Voprosy Kriptografii, 2023, v. 14, № 1, pp. 115–130 (Russian)
© Академия криптографии Российской Федерации, 2023 г.

Обозначения и определения

$P = GF(2)$ — поле из двух элементов,

$V_n = P^n$ — пространство двоичных векторов длины n,

$0_n, 1_n$ — нулевой и единичный векторы длины n,

$\mathcal{F}_2(n)$ — множество булевых функций от n переменных,

$E_f = \{(\alpha_1, \ldots, \alpha_n) \in V_n : \quad f(\alpha_1, \ldots, \alpha_n) = 1\}$ — множество выполняющих векторов функции $f \in \mathcal{F}_2(n)$,

для двоичной переменной x положим:

$$x^a = \begin{cases} x, & \text{если } a = 1, \\ \overline{x}, & \text{если } a = 0, \end{cases}$$

$\mathcal{R} = P[x_1, \ldots, x_n]/I_0$ — факторкольцо кольца многочленов над $GF(2)$ от переменных $x_1, \ldots, x_n$ по идеалу $I_0 = (x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n)_{P[x_1,\ldots,x_n]}$, изоморфное кольцу $(\mathcal{F}_2(n), \oplus, \cdot)$,

$\|\alpha\|$ — вес вектора $\alpha \in V_n$,

$\|f\| = |E_f|$ — вес функции f (если $f \in \mathcal{F}_2(n)$, $\|f\| = 2^{n-1}$, то функцию f называют *сбалансированной*),

$\deg f$ — степень многочлена Жегалкина функции $f \in F_2(n)$,

$RM(k, n) = \{f \in F_2(n) : \deg f \leqslant k\}$ — код Рида – Маллера порядка k, $0 \leqslant k \leqslant n$,

$N_k = 1 + n + \binom{n}{2} + \ldots + \binom{n}{k}$ — размерность $RM(k, n)$, $0 \leqslant k \leqslant n$.

Импликантой булевой функции f называется такая не равная константе булева функция g, что для любого значения набора переменных $(x_1, \ldots x_n) \in V_n$

$$f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n),$$

иными словами, $E_f \subseteq E_g$.

Аннигилятором функции f называется множество

$$Ann(f) = \{g \in \mathcal{F}_2(n) \ : fg \equiv 0\}.$$

Порядком алгебраической иммунности (*алгебраической иммунностью*) булевой функции $f \in \mathcal{F}_2(n)$ называется величина

$$AI(f) = \min\left\{\deg g \colon fg \equiv 0 \ \text{ или } \ \overline{f}g \equiv 0\right\}.$$

Введем основные классы булевых функций, важные для дальнейшего изложения. Булева функция $f(x_1, \ldots, x_n)$ называется:

1) 0-*выполнимой* (0-S), если $f(0, \ldots, 0) = 1$,

2) 1-*выполнимой* (1-S), если $f(1, \ldots, 1) = 1$,

3) *биюнктивной* (Bi), если $f \equiv 1$ или существует представление функции f в виде 2-КНФ

$$f(x_1, \ldots, x_n) \equiv \bigwedge_{i=1}^{t} \left(x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}} \right), \tag{1}$$

4) слабо положительной (WP), если $f \equiv 1$ или существует представление f в виде следующей КНФ:

$$f(x_1, \ldots, x_n) \equiv \bigwedge_{i=1}^{t} (x_{s_{i1}}^{a_i} \vee x_{s_{i2}} \vee \ldots \vee x_{s_{ik_i}}, \tag{2}$$

5) *слабо отрицательной* (WN), если $f \equiv 1$ или существует представление f в виде следующей КНФ:

$$f(x_1, \ldots, x_n) \equiv \bigwedge_{i=1}^{t} (x_{s_{i1}}^{a_i} \vee \overline{x}_{s_{i2}} \vee \ldots \vee \overline{x}_{s_{ik_i}}), \tag{3}$$

6) *мультиаффинной* (A), если $f \equiv 1$ или существует представление f в виде формулы

$$f(x_1, \ldots, x_n) \equiv \bigwedge_{i=1}^{t} l_i(x_1, \ldots, x_n), \tag{4}$$

где $l_i(x_1, \ldots, x_n), i = \overline{1, t}$, — аффинные функции.

Классы функций $0-S$, $1-S$, Bi, WP, WN, A называются *классами Шефера*.

Введение

Известно ([1]), что классы функций Bi, WP, WN, A порождают полиномиально решаемые классы систем булевых уравнений. Поэтому возникает задача изучения возможности использования функций из этих классов при анализе систем булевых уравнений, порождаемых функционированием различных криптографических узлов. Одним из способов их использования является применение биюнктивных функций в методе имплицент, идея которого принадлежит С. Н. Сумарокову. Данная идея получила развитие в виде разного вида алгебраических атак (см., например, [2–5]), состоящих, как правило, в поиске следствий исходной системы, имеющих более низкую алгебраическую степень.

Идея излагаемого метода близка к идее алгебраической атаки, однако целью метода является построение следствий исходной системы

уравнений, лежащих в классах Bi, WP, WN, A. Для реализации метода можно использовать методы, основанные на построении базисов Грёбнера, и методы, основанные на применении методов линейной алгебры. В статье рассматривается второй класс методов.

1. Основная идея метода построения биюнктивных следствий

Основная идея метода построения биюнктивных следствий для систем булевых уравнений состоит в следующем.

Рассмотрим произвольную систему булевых уравнений S вида

$$\{f_i(\overline{x}) = \gamma_i, \quad i = \overline{1,t}. \tag{5}$$

Множество решений системы S вида (5) обозначим $Sol(S)$. Ясно, что $Sol(S) \subset V_n$.

Импликентой системы (5) назовем любую такую функцию $g \in F_2(n)$, что из условия $\alpha \in Sol(S)$ следует $\alpha \in E_g$. Основная идея метода импликент состоит в построении по системе (5) такой системы уравнений S_1, что

$$Sol(S) \subset Sol(S_1) \tag{6}$$

и система S_1 решается эффективнее, чем система S (например, лежит в классе полиномиально решаемых систем уравнений [1]). В данных условиях метод решения системы S состоит в построении системы S_1, ее решении, переборе векторов $\alpha \in Sol(S_1)$ и подстановке их в систему (5). В результате получим множество $Sol(S)$.

Для описания основного алгебраического подхода к решению системы уравнений будем считать, что в исходной системе S правые части $\gamma_1 = \ldots = \gamma_t = 0$, т. е. система S имеет вид

$$\{f_i(\overline{x}) = 0, \quad i = \overline{1,t}. \tag{7}$$

В системе S_1, которую мы намерены построить, правые части тоже будут нулевыми:

$$\{g_j(\overline{x}) = 0, \quad j = \overline{1,m}. \tag{8}$$

В этом случае функции $g_1, \ldots, g_m$ будем называть *следствиями* системы (7). Соответственно, функции $\overline{g}_1, \ldots, \overline{g}_m$ будут импликентами системы (7). В соответствии с [2] для выполнения включения (6) необходимо и достаточно, чтобы выполнялось условие $J_1 \subset J$, где

$J_1 = (g_1, \ldots, g_m)_{\mathcal{R}}$, $J = (f_1, \ldots, f_t)_{\mathcal{R}}$ — соответствующие идеалы кольца $\mathcal{R}$.

Поскольку одним из наиболее трудоемких этапов алгоритма решения является перебор векторов из множества $Sol(S_1)$, важной задачей является нахождение как можно большего числа следствий системы (7), т. е. получение максимально возможного числа уравнений в системе (8).

Рассмотрим следующий метод проверки условия $g \in J$ для произвольной функции $g \in \mathcal{F}_2(n)$. Будем считать, что все рассматриваемые функции заданы многочленами Жегалкина. Заметим, что, в силу конечности кольца $\mathcal{R}$, условие $g \in J$ равносильно условию существования таких функций $h_1, \ldots, h_t \in F_2(n)$, что

$$g = h_1 f_1 \oplus \ldots \oplus h_t f_t. \tag{9}$$

Другими словами, $(h_1, \ldots, h_t)$ — решение линейного уравнения

$$(f_1, \ldots, f_t)\, z^{\downarrow} = g \tag{10}$$

в кольце $\mathcal{R}$.

Пусть $k = \max\{\deg f_i,\ i = \overline{1,t}\}$. Представим функции $f_1, \ldots, f_t,\ g$ в виде векторов-столбцов, состоящих из коэффициентов при мономах многочленов Жегалкина. Обозначим их через $f_1^{\downarrow}, \ldots, f_t^{\downarrow},\ g^{\downarrow}$ соответственно. Матрицу коэффициентов $(f_1^{\downarrow}, \ldots, f_t^{\downarrow})$ обозначим через F_0. Без ограничения общности будем считать, что столбцы этой матрицы линейно независимы. Матрица F_0 содержит N_k строк и t столбцов.

Для простоты изложения будем считать, что $\deg g \leqslant k$ (в противном случае просто увеличим k до значения $\deg g$). Предлагается следующий алгоритм проверки условия $g \in J$, использующий идеи, лежащие в основе XL-метода [6].

Алгоритм 1. ***Вход:*** *многочлены Жегалкина функций $f_1, \ldots, f_t,\ g$, представленные в виде вектор-столбцов.*

Выход: *ответ «Да», если $g \in J$, и «Нет» в противном случае.*

Метод.

1) *Положим $d = 0, t_0 = t$. (Окончательным значением d будет максимальная степень функций $(h_1, \ldots, h_t)$.)*

2) *При $k = 0$ рассматривается вариант, когда вектор $(h_1, \ldots, h_t)$ состоит из констант ($\deg h_i = 0, i = \overline{1,t}$). Если такой вектор*

существует, то он является решением системы линейных уравнений

$$F_0 z^{\downarrow} = g^{\downarrow} \tag{11}$$

над полем P, где F_0 — матрица, составленная из столбцов $f_1, \ldots, f_t$. Для проверки совместности системы (11) *матрица $(F_0, g^{\downarrow})$ приводится к специальному ступенчатому виду и применяется критерий Кронекера – Капелли. Если система* (11) *совместна, то алгоритм заканчивает работу с ответом «Да».*

3) *Если система* (11) *несовместна, то увеличиваем d на единицу и по матрице F_{d-1} строим матрицу F_d, добавив столбцы функций $x_l\ f_i,\ l = \overline{1,n},\ i = \overline{1,t}$, соответствующим образом увеличив размеры системы. Получим систему линейных уравнений вида*

$$F_d \cdot z^{\downarrow} = g^{\downarrow}, \tag{12}$$

где F_d — матрица, содержащая N_{k+d} строк и $t_d \leqslant t_{d-1} + nt_{d-1}$ столбцов (при ее построении удаляем линейно зависимые столбцы). Далее рассматриваем вопрос о разрешимости системы (12) *аналогично п.* 2.

4) *Повторяем п.* 3 *до получения положительного ответа или пока минимальная степень d функции из матрицы F_k не достигнет n. В этом случае при несовместности системы* (12) *алгоритм выдает ответ «Нет».*

Очевидно следующее утверждение.

Утверждение 2. *Алгоритм* 1 *сделает ровно d шагов тогда и только тогда, когда существуют $h_1, \ldots, h_t \in \mathcal{F}_2(n)$, удовлетворяющие* (9), *для которых $d = \max\{\deg h_i,\ i = \overline{1,t}\}$, и это значение минимально по всем наборам функций $h_1, \ldots, h_t$, для которых верно* (9).

Пример 1. Приведем пример, иллюстрирующий работу данного алгоритма в одном из простейших случаев. В качестве исходной системы рассмотрим систему из одного уравнения:

$$x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1 = 0. \tag{13}$$

Решениями данного уравнения являются все трехмерные векторы веса, не меньшего 2. Покажем, что функции $x_1 \vee x_2,\ \ x_1 \vee x_3,\ \ x_2 \vee x_3$ являются имплицентами уравнения (13). Достаточно показать, что функции

$g_1 = \overline{x_1 \vee x_2}$, $g_2 = \overline{x_1 \vee x_3}$, $g_3 = \overline{x_2 \vee x_3}$ лежат в идеале кольца $\mathcal{R}$, порожденном функцией $f = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1$. Выпишем многочлены указанных функций:

$$\overline{x_1 \vee x_2} = x_1x_2 \oplus x_1 \oplus x_2 \oplus 1,$$

$$\overline{x_1 \vee x_3} = x_1x_3 \oplus x_1 \oplus x_3 \oplus 1,$$

$$\overline{x_2 \vee x_3} = x_2x_3 \oplus x_2 \oplus x_3 \oplus 1.$$

Положим $d = 0$ и составим расширенную матрицу системы $A_0 = (f^{\downarrow},\ g_1^{\downarrow},\ g_2^{\downarrow},\ g_3^{\downarrow})$:

$$A_0 = \begin{bmatrix} & f^{\downarrow} & g_1^{\downarrow} & g_2^{\downarrow} & g_3^{\downarrow} \\ x_1x_2 & 1 & 1 & 0 & 0 \\ x_1x_3 & 1 & 0 & 1 & 0 \\ x_2x_3 & 1 & 0 & 0 & 1 \\ x_1 & 0 & 1 & 1 & 0 \\ x_2 & 0 & 1 & 0 & 1 \\ x_3 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Легко видеть, что $\mathtt{rank} A_0 = 3$, но столбцы 2, 3 и 4 не выражаются линейно через столбец 1. Умножая функцию f на переменные x_1, x_2, x_3, получим функции из идеала $J = (f)_{\mathcal{R}}$:

$$f_1 = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1,$$

$$f_2 = x_1x_2x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2,$$

$$f_3 = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3.$$

Результирующая матрица $A_1 = \left(f_1^{\downarrow}, f_2^{\downarrow}, f_3^{\downarrow}, f^{\downarrow},\ g_1^{\downarrow},\ g_2^{\downarrow},\ g_3^{\downarrow}\right)$ имеет вид:

$$A_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Несложными вычислениями легко показать, что последние три столбца матрицы линейно выражаются через предыдущие, следовательно, $g_1, g_2,\ g_3 \in J$, причем

$$g_1 = f_1 \oplus f_2 \oplus f = (x_1 \oplus x_2 \oplus 1)f,$$

$$g_2 = f_1 \oplus f_3 \oplus f = (x_1 \oplus x_3 \oplus 1)f,$$

$$g_3 = f_2 \oplus f_3 \oplus f = (x_2 \oplus x_3 \oplus 1)f.$$

Таким образом, $g_1, g_2,\ g_3 \in J$.

2. Применение метода к системам уравнений итеративного вида

Рассмотрим систему уравнений следующего вида:

$$\left\{ f(\overline{x}A^{i-1}) = \gamma_i\ , \quad i = \overline{1,t}, \right. \tag{14}$$

где $f(x_1, \ldots, x_n)$ — булева функция от n переменных, $\deg f = k$, A — невырожденное линейное преобразование. Такие системы описывают, в частности, функционирование фильтрующих и комбинирующих генераторов. При достаточно больших t совместная система (14) имеет, как правило, единственное решение $\overline{x} = (c_1, \ldots, c_n)$, а значит, следствием этой системы является функция вида $x_1^{c_1} \ldots x_n^{c_n}$. Данная функция лежит в классах Bi, WP, WN. Поэтому имеет смысл проводить поиск следствий в каждом из указанных классов функций. В настоящей работе рассматривается поиск следствий в классе биюнктивных функций.

Систему (14) перепишем в виде

$$\{ f_i\,(\overline{x}) = 0, \quad i = \overline{1,t}, \tag{15}$$

где $f_i(\overline{x}) = f(\overline{x}A^{i-1}) \oplus \gamma_i$. Поскольку $\deg f = k$, то $f_1, \ldots, f_t \in RM(k,n)$. Без ограничения общности будем считать, что функции $f_1, \ldots, f_t$ линейно независимы как элементы соответствующего кода Рида–Маллера. Будем предполагать, что число уравнений t близко к числу неизвестных n, поскольку при значительном объеме материала ($t \sim n^k$) существует ряд методов, основанных на формальной линеаризации, дающих приемлемый результат.

Основными свойствами системы (15) являются следующие:

— система (15) совместна по построению,

— алгебраические степени функций $f_i, \quad i = \overline{1,t}$, совпадают и равны k,

— спектры Фурье и Уолша – Адамара функций $f_i,\ i = \overline{1,t}$, различаются перестановками, задаваемыми степенями линейного преобразования A и знаками, зависящими от соответствующих битов выходной последовательности,

— носители спектров Фурье и Уолша – Адамара функций $f_i,\ i = \overline{1,t}$ (т. е. множества векторов, которым соответствуют ненулевые коэффициенты) лежат в подпространствах, задаваемых точками съема фильтрующей функции и матрицей линейного преобразования. Этот факт особенно актуален в случае, когда исходная функция имеет достаточно много несущественных переменных.

Рассмотрим применение изложенного в разделе 2 метода к системам вида (15).

В множестве биюнктивных функций выберем множество *элементарных* биюнктивных функций, т. е. функций вида $x_i^a \vee x_j^b,\ 1 \leqslant i < j \leqslant n,\ a, b \in \{0, 1\}$, среди которых и будем искать имплиценты. Таких функций всего $m = 2n(n-1)$.

Обозначим их через $g_1, \ldots, g_m$ и положим

$$K = \{g_1, \ldots, g_m\}\,,\ \overline{K} = \{\overline{g}_1, \ldots, \overline{g}_m\}\,.$$

Основная идея предлагаемого алгоритма, развивающего идею алгоритма 1, состоит в поиске многочленов Жегалкина функций из множества $\overline{K}$ в идеале, порожденном многочленами функций $f_1, \ldots, f_t$.

Алгоритм 3.

Вход: *Набор функций* $f_i, \quad i = \overline{1,t}$, *и множество функций* K, *заданных многочленами Жегалкина.*

Выход: *Набор функций из множества* K, *являющихся следствиями системы* (15).

Метод.

1) *Для многочленов Жегалкина функций системы* (15) *и функций* $\overline{g}_1, \ldots, \overline{g}_m$ *построим матрицу* A_0 *с* N_k *строками и* $t + m$ *столбцами*:

$$A_0 = \left(f_1^{\downarrow}, \ldots, f_t^{\downarrow}, \overline{g}_1^{\downarrow}, \ldots, \overline{g}_m^{\downarrow}\right) = (F,\ G)\,. \tag{16}$$

2) *Приводим матрицу* A_0 *строчными преобразованиями к специальному ступенчатому виду. Получаем матрицу* $S_0 = (B_0, C_0)$, *где матрицы* B_0, C_0 *составлены из, соответственно, первых* t *и последних* m *столбцов матрицы* S_0. *Обозначим* $r_0 = \texttt{rank}\ B_0$.

3) *В матрице* C_0 *выбираем те столбцы, у которых последние* $N_k - r_0$ *элементов равны* 0. *Если столбец соответствует функции* $\overline{g}_j$, *то* g_j — *имплицента системы* (15). *Запоминаем такие функции и удаляем соответствующие столбцы из матрицы* A_0. *Число оставшихся столбцов обозначим через* m_1.

4) *Методом, аналогичным шагу* 2 *алгоритма* 1, *строим матрицу* A_1 *с* N_{k+1} *строками и* $t + m_1$ *столбцами и для этой матрицы выполняем шаги* 2–3 *алгоритма, т. е. строим матрицу* $S_1 = (B_1, C_1)$ *и обозначаем* $r_1 = \texttt{rank}\ B_1$.

5) *Повторяем шаги* 2–5 *необходимое число раз, пока не получим требуемое число имплицент.*

Исследуем некоторые свойства матриц, участвующих в описании алгоритма.

Утверждение 4. *Верно равенство*

$$\texttt{rank}\ G = \binom{n}{2} + n + 1 = N_2.$$

Доказательство. Рассмотрим многочлены Жегалкина функций, входящих в матрицу G. Для $1 \leqslant i < j \leqslant n$ эти многочлены имеют вид

$$x_i x_j \oplus a x_i \oplus b x_j \oplus ab,\ \ a, b \in \{0, 1\}.$$

Ранг подсистемы соответствующих столбцов равен 4. Преобразованиями столбцов эта система приводится к виду $x_i x_j,\ x_i, x_j, 1$. В результате получаем столбцы, соответствующие многочленам Жегалкина функций

$$1, x_1, \ldots, x_n, x_1 x_2, \ldots,\ x_{n-1} x_n,$$

которые, очевидно, линейно независимы. Дальнейшие рассуждения очевидны. □

Следствие 5. *Если* $k = \deg f = 2$, *то*

$$\texttt{rank}\ A_0 = N_2.$$

Доказательство следует из утверждения 4 и того факта, что $\dim RM(2, n) = N_2$.

Утверждение 6. *Пусть для функции f, порождающей систему* (15), *выполняется неравенство $AI(f) > l$. Тогда верно неравенство*

$$\texttt{rank}\ B_l \geqslant N_l. \tag{17}$$

Доказательство. Достаточно показать, что в матрице B_l, порождаемой алгоритмом 3, найдется N_l линейно независимых столбцов.

По построению системы (15) для функций $f_1, \ldots, f_t$ выполняются равенства $AI(f_i) = AI(f)$, $i = \overline{1,t}$. Поэтому $AI(f_i) > l$, $i = \overline{1,t}$, и достаточно провести рассуждения для функции f_1.

По построению матрицы B_l в ней есть столбцы, соответствующие всем функциям вида mf_1, $\deg m \leqslant l$, и таких столбцов в точности N_l. Предположим, что они линейно зависимы. Тогда существует нетривиальное линейное соотношение вида

$$\sum_{m\colon \deg m \leqslant l} a_m \cdot (mf_1)^{\downarrow} = 0,$$

откуда следует, что

$$f_1 \cdot \left(\sum_{m\colon \deg m \leqslant l} a_m m \right) \equiv 0.$$

Это означает, что функция $h = \sum_{m\colon \deg m \leqslant l} a_m m$, $\deg h \leqslant l$, является аннигилятором функции f_1, что противоречит условию $AI\,(f_1) > l$. $\square$

Следствие 7. *В условиях утверждения* 6 *выполняется неравенство* $|J| \geqslant 2^{N_l}$.

3. Размер системы следствий для достижения одновыполнимости

Систему уравнений, имеющую единственное решение, будем называть одновыполнимой. Рассмотрим вопрос о числе имплицент, необходимом для того, чтобы полученная система вида (8) имела единственное решение при условии, что исходная система одновыполнима. Основными свойствами систем-следствий являются следующие:

— системы совместны,

— все уравнения различны.

Утверждение 8. *Пусть S — совместная система уравнений вида*

$$\left\{ x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}} = 1, \quad i = \overline{1,w}, \right. \tag{18}$$

от n неизвестных. Если $w \leqslant n$, то система S имеет не менее двух решений.

Доказательство. Достаточно доказать утверждение для случая $w = n$. Положим

$$f(x_1, \ldots, x_n) = \bigwedge_{i=1}^{n} (x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}}). \tag{19}$$

Тогда, по условию утверждения, $f \not\equiv 0$. Покажем, что $\|f\| \geqslant 2$. Построим граф 2-КНФ из правой части (19):

$$G = (V, D), \ V = \{x_1, \ldots, x_n, \ \overline{x}_1, \ldots, \overline{x}_n\},$$

$$D = \{(x_{s_{i1}}^{a_{i1} \oplus 1}, x_{s_{i2}}^{a_{i2}}), (x_{s_{i2}}^{a_{i2} \oplus 1}, x_{s_{i1}}^{a_{i1}}), \ i = \overline{1, n}\}.$$

Таким образом, в графе G в точности $2n$ вершин и $2n$ дуг. Пары вершин вида x_i, $\overline{x}_i$ будем далее называть *контрарными*. В дальнейшем, при необходимости, данный граф будем рассматривать как неориентированный граф. При этом будем особо оговаривать наличие ориентированных и неориентированных цепей и циклов.

Рассмотрим разбиение графа G на компоненты связности (как неориентированного графа):

$$G = H_1 + H_2 + \ldots + H_l.$$

Обозначим также $H_i = (V_i, \ D_i), \ i = 1, 2, \ldots, l$. Положим, далее,

$$n_i = |V_i|, \ m_i = |D_i|, \ i = \overline{1, l}.$$

Тогда $m_i \geqslant n_i - 1, \ i = \overline{1, l}$, и выполняются соотношения

$$n_1 + \ldots + n_l = n, m_1 + \ldots + m_l = w. \tag{20}$$

Как отмечено в [6], для каждой компоненты связности $H_i = (V_i, \ D_i)$ выполнено в точности одно из условий: либо $V_i = \overline{V}_i$ и множество вершин состоит из пар контрарных вершин, либо в множестве V_i нет пар контрарных вершин и тогда существует такая компонента $H_j = (V_j, \ D_j)$, что $V_j = \overline{V}_i$, а множество D_j состоит из всех таких дуг вида $(\overline{v}, \overline{u})$, что $(u, v) \in V_i$. Такие компоненты связности назовем взаимно обратными. Ясно, что пара взаимно обратных компонент соответствует одному и тому же набору элементарных дизъюнкций в 2-КНФ вида (19).

В этом случае функцию f можно представить в виде произведения вида

$$f = f_1 \cdot \ldots \cdot f_k, \tag{21}$$

где f_i — функции, соответствующие компонентам связности, зависящие от n_i переменных, т. е. наборы переменных этих функций не пересекаются.

Заметим, что если в графе G есть изолированные вершины, то утверждение очевидным образом верно, поскольку в этом случае функция f ненулевая и имеет несущественные переменные. Аналогичные рассуждения проводятся в случае, когда произвольная функция f_i имеет несущественные переменные. Поэтому в дальнейшем считаем, что каждая функция f_i существенно зависит от всех n_i переменных.

Далее считаем, что $n_i \geqslant 2$, $i = 1, 2, \ldots, l$. Для доказательства утверждения достаточно доказать, что $\|f_i\| \geqslant 2$ для некоторого $i \in \overline{1, l}$. Выберем компоненту H_1. Сначала будем считать, что эта компонента не содержит пары контрарных вершин. Рассмотрим ряд случаев.

1) Пусть $m_1 = n_1 - 1$. Тогда граф H_1 является ориентацией некоторого дерева, т. е. ацикличен. Сначала покажем, что этот граф не содержит контрарных вершин. В самом деле, пусть в нем есть неориентированная цепь вида $z_1 z_2 \ldots z_{s-1} \overline{z}_1$, где $z_1, z_2, \ldots, z_{s-1} \in V$. Тогда в нем есть неориентированная цепь вида $z_1 \overline{z}_{s-1} \ldots \overline{z}_2 \overline{z}_1$. Таким образом в графе H_1 есть неориентированный цикл, что противоречит условию пункта. Таким образом, в компоненте нет пар контрарных вершин и, с точностью до навешивания отрицаний, можно считать, что $f_1 \in WP \cap WN$. Далее воспользуемся результатами работы [7]. Если $r = r(f_1)$ — глубина функции f_1, то

$$\|f_1\| \geqslant (r + l + 1) \cdot 2^q - r = (2^q - 1) \cdot r + (l + 1) \cdot 2^q,$$

где $q = \left\lfloor \frac{n_1}{r+1} \right\rfloor$, а l — остаток от деления n_1 на $r+1$. При $q \geqslant 1$ получаем, что $2^q \geqslant 2$ и $\|f_1\| \geqslant 2$. Случай $q = 0$ невозможен, поскольку $n_1 \geqslant r + 1$ по определению глубины функции. В итоге $\|f\| \geqslant \|f_1\| = n_1 \geqslant 2$, что и требовалось.

2) Пусть $m_1 \geqslant n_1 + 1$. Тогда, в силу (20), существует такая компонента связности H_i, что $m_i = n_i - 1$. В этом случае попадаем в условия случая 1.

3) Случай $m_1 = n_1$: тогда граф содержит единственный неориентированный цикл.

Предположим, что орграф H_1 ацикличен (как орграф) и не содержит пары контрарных вершин. Тогда, повторяя рассуждения предыдущего пункта, получаем, что $\|f_1\| \geqslant 2$.

Пусть теперь орграф H_1 не содержит пар контрарных вершин, но содержит орцикл. Если он сам является циклом, то очевидно, что $\|f_1\| = 2$. Если нет, то рассмотрим его конденсацию и соответствующую ей функцию h. В этом случае функция h существенно зависит не менее чем от 2 переменных, граф ее 2-КНФ ацикличен и $r(h) \geqslant 1$. Тогда, повторяя рассуждения предыдущего пункта, получаем, что $\|f_1\| \geqslant 2$.

Пусть теперь орграф H_1 содержит пару контрарных вершин. Следовательно, множество V_1 состоит из пар контрарных вершин. В силу того что $\|f_1\| \not\equiv 0$, ни одна пара контрарных вершин не лежит на орцикле (см. [6]). В частности, он сам не является орциклом. Покажем, что он ацикличен.

Пусть в графе H_1 есть орцикл вида $x_1 u_1 \dots u_p x_1$. Тогда есть и орцикл $\overline{x}_1 \overline{u}_p \dots \overline{u}_1 \overline{x}_1$ и эти орциклы различны, что противоречит единственности неориентированного цикла. Поэтому H_1 ацикличен.

Теперь заметим, что если вершина u лежит на неориентированном цикле, то и вершина $\overline{u}$ также лежит на неориентированном цикле. Кроме того, цикломатическое число этого графа равно 1. Следовательно, в нем есть единственный цикл, поэтому его длина четная и он состоит из пар контрарных вершин. Остальные вершины находятся на подходах к этому циклу.

Рассмотрим случай, когда граф H_1 образует единственный неориентированный цикл. Без ограничения общности считаем, что x_1 — начальная вершина и, соответственно, $\overline{x}_1$ — конечная. Далее, считаем, что неориентированная цепь из x_1 в $\overline{x}_1$ имеет вид $x_1 x_2 \dots x_{n_1} \overline{x}_1$. Соответственно, вторая цепь цикла имеет вид $x_1 \overline{x}_{n_1} \dots \overline{x}_2 \overline{x}_1$. Покажем, что независимо от ориентации дуг $\|f_1\| \geqslant 2$. Рассмотрим граф подфункции $g(x_2, \dots, x_{n_1}) = (f_1)_1^0$, полученной фиксацией значения $x_1 = 0$. Граф 2-КНФ этой функции получается путем исключения вершин x_1и $\overline{x}_1$ из графа H_1 и содержит не менее одной пары контрарных вершин. Кроме того, он представляет собой две взаимно обратные орцепи. Поэтому $g \in WP \cap WN$, компоненты связности полученного графа не содержат пар контрарных вершин и содержат по $n_1 - 2$ дуг. По ранее доказанному $\|g\| \geqslant 2$. Далее осталось заметить, что при $x_1 = 0$ дизъюнкты принимают значение 1. Поэтому $\|f_1\| \geqslant 2$.

Рассмотрение оставшегося случая (когда H_1 есть цикл с подходами) легко провести методом математической индукции по числу нециклических вершин. $\square$

Утверждение 9. *Пусть S — совместная система уравнений вида*

$$\left\{x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}} \right. = 1, \quad i = \overline{1, w}, \tag{22}$$

от n неизвестных. Если $w \geqslant 3 \cdot \binom{n-1}{2} + 2n - 1$, то система S имеет единственное решение.

Идея доказательства данного утверждения была предложена А. А. Чернышовым.

Доказательство. Сначала заметим, что существует не одновыполнимая система из $w_0 = 3 \cdot \binom{n-1}{2} + 2n - 2$ уравнений. Построим систему следующего вида:

$$\begin{cases} x_i \vee x_j = 1, & 1 \leqslant i < j \leqslant n-1, \\ x_i \vee \overline{x}_j = 1, & 1 \leqslant i < j \leqslant n-1, \\ \overline{x}_i \vee x_j = 1, & 1 \leqslant i < j \leqslant n-1, \\ x_i \vee x_n = 1, & 1 \leqslant i \leqslant n-1, \\ x_i \vee \overline{x}_n = 1, & 1 \leqslant i \leqslant n-1. \end{cases} \tag{23}$$

Решениями этой системы являются, очевидно, векторы $(1, 1, \ldots, 1, 1)$ и $(1, 1, \ldots, 1, 0)$. Таким образом, система (23) не одновыполнима. Покажем, что любая совместная система из $w_0 + 1$ уравнений одновыполнима. Далее без ограничения общности будем считать, что одним из решений системы является вектор $1_n = (1, 1, \ldots, 1)$. Поэтому в системе (22) в левых частях уравнений по крайней мере одно неизвестное взято без отрицания.

Пусть система имеет не менее двух решений, одно из которых есть вектор 1_n, а второе — некоторый вектор $\alpha = (a_1, \ldots, a_n)$. Оценим максимальное число уравнений, которым удовлетворяют векторы 1_n и α. Соответственно, если решений больше двух, то число уравнений будет не больше полученного числа.

Пусть $\|1_n \oplus \alpha\| = k,\ 1 \leqslant k \leqslant n$. Без ограничения общности считаем, что в векторе α компоненты $a_1 = \ldots = a_k = 0$, $a_{k+1} = \ldots = a_n = 1$. Найдем все элементарные дизъюнкции вида $x_i^a \vee x_j^b$, для которых векторы 1_n и α являются выполняющими.

1) При $k + 1 \leqslant i < j \leqslant n$ оба вектора являются выполняющими для элементарных дизъюнкций $x_i \vee x_j,\ x_i \vee \overline{x}_j,\ \ \overline{x}_i \vee x_j$. Всего $3 \cdot \binom{n-k}{2}$ вариантов.

2) При $1 \leqslant i \leqslant k < j \leqslant n$ получаем дизъюнкции вида $x_i \vee x_j,\ \overline{x}_i \vee x_j$, что дает $2k(n-k)$ вариантов.

3) При $1 \leqslant i < j \leqslant k$ — дизъюнкции вида $x_i \vee \overline{x}_j$, $\overline{x}_i \vee x_j$, что дает $2 \cdot \binom{k}{2}$ вариантов.

В сумме получаем величину

$$3 \cdot \binom{n-1}{2} + 2k\,(n-k) + 2 \cdot \binom{k}{2} = \frac{1}{2}\left(k^2 + (1-2n)\,k + 3n^2 - 3n\right).$$

Легко видеть, что эта функция при $1 \leqslant k \leqslant n$ принимает максимальное значение при $k = 1$, равное w_0. Значит, система из $w_0 + 1$ уравнений имеет не более одного решения. Поскольку система совместна, она является одновыполнимой. □

Заключение

В работе предложен алгебраический подход к построению биюнктивных следствий для систем булевых уравнений. Подход допускает развитие в сторону построения слабо положительных, слабо отрицательных и мультиаффинных следствий, равно как и любого множества потенциальных следствий, если только размер этого множества ограничен полиномом от n. Например, можно искать слабо положительные следствия, зависящие от не более чем k переменных. Поэтому предложенная идея представляется перспективной.

Список литературы

[1] Горшков С.П., Тарасов А.В., *Сложность решения систем булевых уравнений*, М.: Курс, 2017, 192 с.

[2] Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В., *Булевы функции в теории кодирования и криптологии*, М.: ЛЕНАНД, 2015, 576 с.

[3] Courtois N., Meier W., “Algebraic attacks on stream ciphers with linear feedback”, EUROCRYPT’2003, Lect. Notes Comput. Sci., **2656**, 2003, 345–359.

[4] Courtois N., “Fast algebraic attacks on stream ciphers with linear feedback”, CRYPTO’2003, Lect. Notes Comput. Sci., **2729**, 2003, 176–194.

[5] Chen J.-M., Yang B.-Y., “All in the XL family: theory and practice”, ICISC 2004, Lect. Notes Comput. Sci., **3506**, 2005, 67–86.

[6] Данцин Е.Я., “Алгоритмика задачи выполнимости”, *Вопросы кибернетики*, **131**, 1987, 7–29.

[7] Тарасов А.В., “Булевы биюнктивные функции, графы 2-КНФ и их порядковые функции. Оценки веса биюнктивной функции с заданным числом слоев”, *Математические вопросы криптографии*, **12**:1 (2021), 83–95.