Математические структуры и моделирование
2024. № 1 (69). С. 5–17

УДК 519.65:519.85:512.563
DOI 10.24147/2222-8772.2024.1.5-17

ОБ ОДНОМ ПРИВЕДЕНИИ СИСТЕМЫ БУЛЕВЫХ УРАВНЕНИЙ К ЭКВИВАЛЕНТНОЙ СИСТЕМЕ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ

Д.Н. Баротов[1]
старший преподаватель, e-mail: DNBarotov@fa.ru
Р.Н. Баротов[2]
докторант, e-mail: ruzmet.tj@mail.ru

[1]Финансовый университет при Правительстве Российской Федерации, Москва, Россия

[2]Худжандский государственный университет имени академика Б. Гафурова, Худжанд, Таджикистан

Аннотация. В данной работе исследуется задача конструирования специального продолжения булевой функции на всё пространство $\mathbb{R}^n$, благодаря которому без добавления каких-либо ограничений система m булевых уравнений преобразуется в эквивалентную систему m полиномиальных уравнений. В результате исследования для любой булевой функции $f_b(x_1, x_2, \ldots, x_n)$ конструируется соответствующая бесконечно дифференцируемая рациональная функция $f_s(x_1, x_2, ..., x_n)$ такая, что

$$f_s(x_1, x_2, ..., x_n) \in \{0,1\} \Longleftrightarrow \begin{cases} (x_1, x_2, ..., x_n) \in \{0,1\}^n \\ f_b(x_1, x_2, ..., x_n) = f_s(x_1, x_2, ..., x_n) \end{cases}.$$

Благодаря конструированной функции $f_s(x_1, x_2, ..., x_n)$, во-первых, без добавления каких-либо ограничений произвольная система m булевых уравнений преобразуется в эквивалентную систему m рациональных уравнений, во-вторых, решение преобразованной эквивалентной системы рациональных уравнений сводится к задаче численной минимизации некоторой бесконечно-дифференцируемой целевой функции, решаемой методами оптимизации, и к эквивалентной системе полиномиальных уравнений, решаемой и анализируемой алгоритмом F4.

Ключевые слова: продолжение булевой функции, система булевых уравнений, глобальная оптимизация, алгоритм F4, SAT.

Введение

Система булевых уравнений была важной темой исследований на протяжении почти двух столетий, и её значимость и сегодня трудно переоценить. Решение булевых уравнений проникает во многие области современной науки, такие как логическое проектирование, биология, грамматика, химия, право, медицина, спектроскопия и теория графов [1]. Многие важные задачи исследования операций можно

свести к задаче решения системы булевых уравнений. Ярким примером является задача коалиционной игры n лиц с отношением доминирования между различными стратегиями [2]. Решения булевых уравнений также служат важным инструментом при обработке псевдобулевых уравнений и неравенств и связанных с ними задач целочисленного линейного программирования [2]. В последние годы ещё одной важной и перспективной областью, в которой применяется решение системы булевых уравнений, является алгебраический криптоанализ. Для конкретного шифра алгебраический криптоанализ состоит из двух этапов: преобразовать шифр в систему полиномиальных уравнений (обычно над булевым кольцом) и решить полученную систему полиномиальных уравнений [3]. Одно из первых успешных применений решение системы булевых уравнений было продемонстрировано в работе [4]. Поэтому, с одной стороны, совершенствуются существующие методы и алгоритмы, с другой стороны, разрабатывается и адаптируется множество новых направлений и алгоритмов решения систем булевых уравнений [5–11]. Одним из таких направлений является преобразование системы булевых уравнений в систему уравнений над полем действительных чисел, поскольку в этой области известно множество методов и алгоритмов решения систем. Суть этого направления состоит в том, что система булевых уравнений преобразуется в систему уравнений над полем действительных чисел и решение ищется на множестве действительных чисел. В свою очередь преобразованная система может быть сведена к задаче численной оптимизации, что позволяет применять, анализировать и комбинировать такие методы, как алгоритм наискорейшего спуска, метод Ньютона и алгоритм координатного спуска [11–20]. Существует множество способов преобразования системы булевых уравнений в систему уравнений над полем действительных чисел [11–22]. Но одна из основных проблем, возникающих при применении этих методов, заключается в том, что преобразованная система уравнений на множестве действительных чисел может иметь множество посторонних решений, что усложняет их практическое использование [16, 18].

В настоящей работе немного уточняется результат, приведённый в [19], а именно конструируется «подходящее» продолжение (определение будет дано ниже) произвольной булевой функции на всё пространство $\mathbb{R}^n$, благодаря которому доказывается, что без добавления каких-либо ограничений система m булевых уравнений и преобразованная система m рациональных уравнений на множестве действительных чисел будут эквивалентны, т. е. проблема посторонних решений полностью решается. Также доказывается, что на основе предъявленного подходящего продолжения булевой функции $f(x_1, x_2, ..., x_n)$ можно конструировать новую функцию, которая также является подходящим продолжением на $\mathbb{R}^n$ функции $f(x_1, x_2, ..., x_n)$.

1. Используемые определения и обозначения

Пусть $\mathbb{B}^n = \{(b_1, b_2, \ldots, b_n) : b_1, b_2, \ldots, b_n \in \{0, 1\}\}$ – множество всевозможных двоичных слов (булевых векторов) длины n.

Определение 1. Функцию вида $f_b : \mathbb{B}^n \to \mathbb{B}$ назовём булевой функцией.

Пусть $supp(f_b) = \{(b_1, b_2, ..., b_n) \in \mathbb{B}^n : f_b(b_1, b_2, ..., b_n) = 1\}$ – носитель булевой

функции $f_b(x_1, x_2, ..., x_n)$, т. е. множество всех булевых векторов, на которых булева функция $f_b(x_1, x_2, ..., x_n)$ принимает значение 1.

Пусть $and_b(b_1, b_2, ..., b_n) = b_1 \wedge b_2 \wedge ... \wedge b_n$ – логическое произведение булевых переменных $b_1, b_2, ..., b_n$.

Пусть $xor_b(b_1, b_2, ..., b_n) = b_1 \oplus b_2 \oplus ... \oplus b_n$ – логическая сумма (сумма по модулю 2) булевых переменных $b_1, b_2, ..., b_n$.

Определение 2. Функцию вида $f_r : \mathbb{R}^n \to \mathbb{R}$ назовём продолжением на $\mathbb{R}^n$ булевой функции $f_b(x_1, x_2, ..., x_n)$, если

$$f_r(b_1, b_2, ..., b_n) = f_b(b_1, b_2, ..., b_n) \quad \forall (b_1, b_2, ..., b_n) \in \mathbb{B}^n.$$

Определение 3. Функцию вида $f_s : \mathbb{R}^n \to \mathbb{R}$ назовём подходящим продолжением на $\mathbb{R}^n$ булевой функции $f_b(x_1, x_2, ..., x_n)$, если $f_s(x_1, x_2, ..., x_n) \in C^\infty(\mathbb{R}^n)$ и

$$f_s(x_1, x_2, ..., x_n) \in \{0, 1\} \iff \begin{cases} (x_1, x_2, ..., x_n) \in \{0, 1\}^n \\ f_b(x_1, x_2, ..., x_n) = f_s(x_1, x_2, ..., x_n) \end{cases}.$$

2. Конструирование подходящих продолжений булевых функций

В этом разделе мы сначала построим подходящее продолжение для элементарных функций $and_b(b_1, b_2, ..., b_n)$ и $xor_b(b_1, b_2, ..., b_n)$, а затем на его основе построим продолжение для произвольной булевой функции. С этой целью обоснуем справедливость следующих двух лемм.

Лемма 1. *Для булевой функции $and_b(b_1, b_2, ..., b_n)$ функция вида*

$$and_s(x_1, x_2, \ldots, x_n) = \prod_{k=1}^{n} \frac{x_k^2}{2x_k^2 - 2x_k + 1} + \frac{1}{n} \cdot \sum_{k=1}^{n} \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} \qquad (1)$$

является подходящим продолжением на $\mathbb{R}^n$.

Доказательство. Действительно, предъявленная функция $and_s(x_1, x_2, \ldots, x_n)$ является подходящим продолжением на $\mathbb{R}^n$, для этого достаточно проверить справедливость следующих свойств:

$$(a) \quad 0 \leqslant and_s(x_1, x_2, \ldots, x_n) \leqslant 1, \quad \forall (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n.$$

$$(b) \quad \text{Если } (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n, \text{ то } and_s(x_1, x_2, \ldots, x_n) \in \mathbb{B} = \{0, 1\}.$$

$$(c) \quad and_s(x_1, x_2, \ldots, x_n) = 0 \iff (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n \backslash \{(1, 1, \ldots, 1)\}.$$

$$(d) \quad and_s(x_1, x_2, \ldots, x_n) = 1 \iff (x_1, x_2, \ldots, x_n) = (1, 1, \ldots, 1).$$

(a) Первое неравенство, которое находится слева, очевидно, так как

$$\frac{x_k^2}{2x_k^2 - 2x_k + 1} \geqslant 0 \;\; \frac{(x_k^2 - x_k)^2}{(2x_k^2 - 2x_k + 1)^2} \geqslant 0, \;\; \forall x_k \in \mathbb{R} \text{ и } \forall k \in \{1, 2, \ldots, n\}$$

и, следовательно,

$$and_s\left(x_1,x_2,\ldots,x_n\right)=\prod_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}\geqslant 0.$$

Теперь докажем второе неравенство, которое находится справа. Для этого в процессе пользуемся в том числе неравенством между средним арифметическим и средним геометрическим.

$$and_s\left(x_1,x_2,\ldots,x_n\right)=\frac{x_1^2}{2x_1^2-2x_1+1}\cdot\frac{x_2^2}{2x_2^2-2x_2+1}\cdot\ldots\cdot\frac{x_n^2}{2x_n^2-2x_n+1}+$$

$$+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=$$

$$=\left(\sqrt[n]{\frac{x_1^2}{2x_1^2-2x_1+1}\cdot\frac{x_2^2}{2x_2^2-2x_2+1}\cdot\ldots\cdot\frac{x_n^2}{2x_n^2-2x_n+1}}\right)^n+$$

$$+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}\leqslant$$

$$\leqslant\left(\frac{1}{n}\cdot\left(\frac{x_1^2}{2x_1^2-2x_1+1}+\frac{x_2^2}{2x_2^2-2x_2+1}+\ldots+\frac{x_n^2}{2x_n^2-2x_n+1}\right)\right)^n+$$

$$+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}\leqslant$$

$$\leqslant\frac{1}{n}\cdot\left(\frac{x_1^2}{2x_1^2-2x_1+1}+\frac{x_2^2}{2x_2^2-2x_2+1}+\ldots+\frac{x_n^2}{2x_n^2-2x_n+1}\right)+$$

$$+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=$$

$$=\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{x_k^2\cdot\left(2x_k^2-2x_k+1\right)}{\left(2x_k^2-2x_k+1\right)^2}+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{x_k^2\cdot\left(2x_k^2-2x_k+1\right)-x_k^4}{\left(2x_k^2-2x_k+1\right)^2}=$$

$$=\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{2\cdot x_k^2\left(2x_k^2-2x_k+1\right)-x_k^4}{\left(2x_k^2-2x_k+1\right)^2}=\frac{1}{n}\cdot$$

$$\sum_{k=1}^{n}\frac{2\cdot x_k^2\left(2x_k^2-2x_k+1\right)-x_k^4-\left(2x_k^2-2x_k+1\right)^2}{\left(2x_k^2-2x_k+1\right)^2}+\frac{1}{n}\cdot$$

$$\sum_{k=1}^{n}\frac{\left(2x_k^2-2x_k+1\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=-\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-2x_k+1\right)^2}{\left(2x_k^2-2x_k+1\right)^2}+\frac{n}{n}\leqslant 1,\quad\forall\left(x_1,x_2,\ldots,x_n\right)\in\mathbb{R}^n.$$

(b) Если $\left(x_1,x_2,\ldots,x_n\right)\in\mathbb{B}^n$, то $x_k\in\mathbb{B},\forall k\in\{1,2,\ldots,n\}$. Отсюда

$$\frac{x_k^2}{2x_k^2-2x_k+1}=\frac{x_k^2}{2x_k\cdot\left(x_k-1\right)+1}=\frac{x_k}{0+1}=x_k\in\mathbb{B},$$

$$\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=\frac{\left(x_k(x_k-1)\right)^2}{\left(2x_k(x_k-1)+1\right)^2}=\frac{0^2}{(0+1)^2}=0\in\mathbb{B},\quad \forall k\in\{1,2,\ldots,n\}.$$

Следовательно,

$$\prod_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=and_s\left(x_1,x_2,\ldots,x_n\right)\in\mathbb{B}.$$

(c) Действительно,

$$and_s\left(x_1,x_2,\ldots,x_n\right)=\prod_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=0\iff$$

$$\iff\begin{cases}\prod\limits_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}=0\\ \sum\limits_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=0\end{cases}\iff\begin{cases}\prod\limits_{k=1}^{n}x_k^2=0\\ \sum\limits_{k=1}^{n}\left(x_k^2-x_k\right)^2=0\end{cases}\iff$$

$$\iff\begin{cases}x_1\cdot x_2\cdot\ldots\cdot x_n=0\\ x_1^2-x_1=0\\ x_2^2-x_2=0\\ \ldots\quad\ldots\quad\ldots\\ x_n^2-x_n=0\end{cases}\iff\left(x_1,x_2,\ldots,x_n\right)\in\mathbb{B}^n\setminus\{(1,1,\ldots,1)\}.$$

(d) Действительно, в силу (a)

$$and_s\left(x_1,x_2,\ldots,x_n\right)=\prod_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}+\frac{1}{n}\cdot\sum_{k=1}^{n}\frac{\left(x_k^2-x_k\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=1\iff$$

$$\iff\begin{cases}\sum\limits_{k=1}^{n}\frac{\left(x_k^2-2x_k+1\right)^2}{\left(2x_k^2-2x_k+1\right)^2}=0\\ -\frac{1}{n}\cdot\sum\limits_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}+\prod\limits_{k=1}^{n}\frac{x_k^2}{2x_k^2-2x_k+1}=0\end{cases}\iff$$

$$\iff\begin{cases}\left(x_k^2-2x_k+1\right)^2=0,\quad\forall k\in\{1,2,\ldots,n\}\\ \frac{x_i^2}{2x_i^2-2x_i+1}=\frac{x_j^2}{2x_j^2-2x_j+1},\quad\forall i,j\in\{1,2,\ldots,n\}\end{cases}\iff$$

$$\iff\left(x_1,x_2,\ldots,x_n\right)=(1,1,\ldots,1).$$

Лемма подробно доказана. ■

Замечание 1. Нет свойства единственности подходящего продолжения на $\mathbb{R}^n$ булевой функции $and_b(b_1,b_2,...,b_n)$, поскольку, например, если $and_s\left(x_1,x_2,\ldots,x_n\right)$ подходящее продолжение булевой функции $and_b(b_1,b_2,...,b_n)$, то $\left(and_s(x_1,x_2,\ldots,x_n)\right)^2$ также является подходящим продолжением на $\mathbb{R}^n$ функции $and_b(b_1,b_2,...,b_n)$.

Лемма 2. *Для булевой функции* $xor_b(b_1, b_2, ..., b_n)$ *функция вида*

$$xor_s(x_1, x_2, \ldots, x_n) = \frac{1}{2} - \frac{1}{2} \cdot \prod_{k=1}^{n} \frac{2 - 4x_k}{1 + (1 - 2x_k)^2} \tag{2}$$

является подходящим продолжением на $\mathbb{R}^n$.

Доказательство. Действительно, представленная функция $xor_s(x_1, x_2, \ldots, x_n)$ является подходящим продолжением на $\mathbb{R}^n$, для этого достаточно показать справедливость следующих свойств:

$$(a) \quad 0 \leqslant xor_s(x_1, x_2, \ldots, x_n) \leqslant 1, \quad \forall (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n.$$

$$(b) \quad xor_s(x_1, x_2, \ldots, x_n) \in \mathbb{B} \iff (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n.$$

(c) $xor_s(x_1, x_2, \ldots, x_n) = 0 \iff (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$ и $(x_1 + x_2 + \ldots + x_n)$ – чётно.

(d) $xor_s(x_1, x_2, \ldots, x_n) = 1 \iff (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$ и $(x_1 + x_2 + \ldots + x_n)$ – нечётно.

(a) Действительно, так как очевидно, что $(-2x_k)^2 \geqslant 0$ и $(2 - 2x_k)^2 \geqslant 0, \ \forall x_k \in \mathbb{R}$. Из этих неравенств следует

$$-1 \leqslant \frac{2 - 4x_k}{1 + (1 - 2x_k)^2} \leqslant 1, \quad \forall x_k \in \mathbb{R}.$$

Теперь легко заметить, что из последнего неравенства следует, что

$$-1 \leqslant \frac{2 - 4x_1}{1 + (1 - 2x_1)^2} \cdot \frac{2 - 4x_2}{1 + (1 - 2x_2)^2} \cdot \ldots \cdot \frac{2 - 4x_n}{1 + (1 - 2x_n)^2} \leqslant 1, \ \ \forall (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n.$$

Отсюда в силу (2) получим

$$0 \leqslant xor_s(x_1, x_2, \ldots, x_n) \leqslant 1, \quad \forall (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n.$$

(b) Сначала докажем в одну сторону, если $(x_1, x_2, \ldots, x_n) \in \mathbb{B}^n$, то

$$\frac{2 - 4x_k}{1 + (1 - 2x_k)^2} \in \{-1, 1\}, \quad \forall k \in \{1, 2, \ldots, n\}$$

и, следовательно,

$$-\frac{1}{2} \cdot \frac{2 - 4x_1}{1 + (1 - 2x_1)^2} \cdot \frac{2 - 4x_2}{1 + (1 - 2x_2)^2} \cdot \ldots \cdot \frac{2 - 4x_n}{1 + (1 - 2x_n)^2} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}.$$

Отсюда в силу (2) получим

$$xor_s(x_1, x_2, \ldots, x_n) \in \mathbb{B} = \{0, 1\}, \quad \forall (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n.$$

Теперь докажем в обратную сторону, если $xor_s(x_1, x_2, \ldots, x_n) \in \{0, 1\}$, то в силу (2)

$$\frac{2 - 4x_1}{1 + (1 - 2x_1)^2} \cdot \frac{2 - 4x_2}{1 + (1 - 2x_2)^2} \cdot \ldots \cdot \frac{2 - 4x_n}{1 + (1 - 2x_n)^2} \in \{-1, 1\}.$$

Переходя к модулям, получим

$$\left|\frac{2-4x_1}{1+(1-2x_1)^2}\cdot\frac{2-4x_2}{1+(1-2x_2)^2}\cdot\ldots\cdot\frac{2-4x_n}{1+(1-2x_n)^2}\right|=1.$$

Отсюда

$$\left|\frac{2-4x_k}{1+(1-2x_k)^2}\right|=1,\quad \forall k\in\{1,2,\ldots,n\}.$$

Заметим, что из последнего равенства следует

$$x_k\in\{0,1\},\quad \forall k\in\{1,2,\ldots,n\}$$

и, следовательно,

$$(x_1,x_2,\ldots,x_n)\in\mathbb{B}^n.$$

(c) Сначала докажем в одну сторону, если $xor_s(x_1,x_2,\ldots,x_n)=0$, то из пункта (b) следует, что $(x_1,x_2,\ldots,x_n)\in\mathbb{B}^n$. Заметим, что если $(x_1,x_2,\ldots,x_n)\in\mathbb{B}^n$, то

$$\frac{2-4x_k}{1+(1-2x_k)^2}=\frac{2-4x_k}{1+(\pm1)^2}=1-2x_k=(-1)^{x_k},\quad \forall k\in\{1,2,\ldots,n\}$$

и, следовательно,

$$\begin{aligned}0=\frac{1}{2}-\frac{1}{2}\cdot\frac{2-4x_1}{1+(1-2x_1)^2}\cdot\frac{2-4x_2}{1+(1-2x_2)^2}\cdot\ldots\cdot\frac{2-4x_n}{1+(1-2x_n)^2}=\\ =\frac{1}{2}-\frac{1}{2}\cdot\frac{2-4x_1}{1+(\pm1)^2}\cdot\frac{2-4x_2}{1+(\pm1)^2}\cdot\ldots\cdot\frac{2-4x_n}{1+(\pm1)^2}=\\ =\frac{1}{2}-\frac{1}{2}\cdot(1-2x_1)\cdot(1-2x_2)\cdot\ldots\cdot(1-2x_n)=\\ =\frac{1}{2}-\frac{1}{2}\cdot(-1)^{x_1}\cdot(-1)^{x_2}\cdot\ldots\cdot(-1)^{x_n}=\frac{1}{2}-\frac{1}{2}\cdot(-1)^{x_1+x_2+\ldots+x_n}.\end{aligned}$$

Отсюда получим, что $(x_1+x_2+\ldots+x_n)$ – чётно.
Теперь докажем в обратную сторону, если $(x_1,x_2,\ldots,x_n)\in\mathbb{B}^n$ и $(x_1+x_2+\cdots+x_n)$ – чётно, то

$$\begin{aligned}0=\frac{1}{2}-\frac{1}{2}\cdot(-1)^{x_1+x_2+\ldots+x_n}=\frac{1}{2}-\frac{1}{2}\cdot(-1)^{x_1}\cdot(-1)^{x_2}\cdot\ldots\cdot(-1)^{x_n}=\\ =\frac{1}{2}-\frac{1}{2}\cdot(1-2x_1)\cdot(1-2x_2)\cdot\ldots\cdot(1-2x_n)=\\ =\frac{1}{2}-\frac{1}{2}\cdot\frac{2-4x_1}{1+(\pm1)^2}\cdot\frac{2-4x_2}{1+(\pm1)^2}\cdot\ldots\cdot\frac{2-4x_n}{1+(\pm1)^2}=\\ =\frac{1}{2}-\frac{1}{2}\cdot\frac{2-4x_1}{1+(1-2x_1)^2}\cdot\frac{2-4x_2}{1+(1-2x_2)^2}\cdot\ldots\cdot\frac{2-4x_n}{1+(1-2x_n)^2}=xor_s(x_1,x_2,\ldots,x_n).\end{aligned}$$

(d) Справедливость этого пункта следует из пунктов (b) и (c). Лемма подробно доказана. ■

Замечание 2. Нет свойства единственности подходящего продолжения на $\mathbb{R}^n$ булевой функции $xor_b(b_1,b_2,...,b_n)$. Обоснование этого аналогично обоснованию замечания 1.

3. Конструирование подходящего продолжения произвольной булевой функции

В этом разделе на основе (1) и (2) построим подходящее продолжение для произвольной булевой функции $f_b(b_1, b_2, ..., b_n)$.

Теорема 1. *Для произвольной булевой функции $f_b(b_1, b_2, ..., b_n)$ функция вида*

$$f_s(x_1, x_2, ..., x_n) =$$

$$= \frac{1}{2} - \frac{1}{2} \cdot \prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \frac{2 - 4 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)}{1 + \left(1 - 2 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)\right)^2} \qquad (3)$$

является подходящим продолжением на $\mathbb{R}^n$, где $x_k^{b_k} = (2b_k - 1) \cdot x_k + 1 - b_k$.

Доказательство. Легко заметить, что предъявленная функция $f_s(x_1, x_2, ..., x_n) \in C^\infty(\mathbb{R}^n)$. В силу теоремы 2 из [21] и формы СДНФ справедливо следующее вспомогательное тождество:

$$f_b(x_1, x_2, ..., x_n) = \bigoplus_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1, b_2, ..., b_n) \wedge x_1^{b_1} \wedge x_2^{b_2} \wedge ... \wedge x_n^{b_n}. \qquad (4)$$

Остаётся доказать, что

$$\forall b \in \{0, 1\}, \quad f_s(x_1, x_2, \ldots, x_n) = b \Longleftrightarrow (x_1, x_2, \ldots, x_n) \in \mathbb{B}^n \text{ и } f_b(x_1, x_2, \ldots, x_n) = b.$$

Сначала докажем в одну сторону, пусть $f_s(x_1, x_2, \ldots, x_n) = b \in \{0, 1\}$. Тогда в силу леммы 2 имеем $and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right) \in \{0, 1\}, \quad \forall (b_1, b_2, ..., b_n) \in \mathbb{B}^n$. Тогда в силу леммы 1 имеем $\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right) \in \mathbb{B}^{n+1}, \quad \forall (b_1, b_2, ..., b_n) \in \mathbb{B}^n$. Отсюда следует, что $(x_1, x_2, ..., x_n) \in \mathbb{B}^n$. В таком случае

$$and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right) =$$

$$= f_b(b_1, b_2, ..., b_n) \cdot ((2b_1 - 1) \cdot x_1 + 1 - b_1) \cdot ((2b_2 - 1) \cdot x_2 + 1 - b_2) \cdot$$

$$\cdot ... \cdot ((2b_n - 1) \cdot x_n + 1 - b_n) = f_b(b_1, b_2, ..., b_n) \cdot \prod_{k=1}^{n} (b_k \cdot x_k + (1 - b_k) \cdot (1 - x_k)) =$$

$$= f_b(b_1, b_2, ..., b_n) \wedge \bigwedge_{k=1}^{n} \left(b_k \cdot x_k + \overline{b_k} \cdot \overline{x_k}\right) = f_b(b_1, b_2, ..., b_n) \wedge \bigwedge_{k=1}^{n} x_k^{b_k}, \quad \forall (b_1, b_2, ..., b_n) \in \mathbb{B}^n$$

и, следовательно,

$$\frac{2 - 4 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)}{1 + \left(1 - 2 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)\right)^2} =$$

$$= \frac{2 - 4 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)}{1 + (\pm 1)^2} =$$

$$= 1 - 2 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right) =$$

$$= 1 - 2 \cdot f_b(b_1, b_2, ..., b_n) \wedge \bigwedge_{k=1}^{n} x_k^{b_k} = (-1)^{f_b(b_1,b_2,...,b_n) \wedge \bigwedge\limits_{k=1}^{n} x_k^{b_k}}.$$

Отсюда

$$f_s(x_1, x_2, ..., x_n) = \frac{1}{2} - \frac{1}{2} \cdot \prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} (-1)^{f_b(b_1,b_2,...,b_n) \wedge \bigwedge\limits_{k=1}^{n} x_k^{b_k}} =$$

$$= \frac{1}{2} - \frac{1}{2} \cdot (-1)^{\sum\limits_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1,b_2,...,b_n) \wedge \bigwedge\limits_{k=1}^{n} x_k^{b_k}} =$$

$$= \left(\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1, b_2, ..., b_n) \wedge \bigwedge_{k=1}^{n} x_k^{b_k}\right) \mod 2 =$$

$$= \bigoplus_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1, b_2, ..., b_n) \wedge x_1^{b_1} \wedge x_2^{b_2} \wedge ... \wedge x_n^{b_n}.$$

В силу тождества (4) справедливо

$$\bigoplus_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1, b_2, ..., b_n) \wedge x_1^{b_1} \wedge x_2^{b_2} \wedge ... \wedge x_n^{b_n} = f(x_1, x_2, ..., x_n) = b.$$

Теперь докажем в другую сторону, пусть $(x_1, x_2, ..., x_n) \in \mathbb{B}^n$ и $f(x_1, x_2, ..., x_n) = b$. Тогда

$$b = f(x_1, x_2, ..., x_n) = \bigoplus_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1, b_2, ..., b_n) \wedge x_1^{b_1} \wedge x_2^{b_2} \wedge ... \wedge x_n^{b_n} =$$

$$= \left(\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1, b_2, ..., b_n) \wedge \bigwedge_{k=1}^{n} x_k^{b_k}\right) \mod 2 = \frac{1}{2} - \frac{1}{2}\cdot$$

$$(-1)^{\sum\limits_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} f_b(b_1,b_2,...,b_n) \wedge \bigwedge\limits_{k=1}^{n} x_k^{b_k}} = \frac{1}{2} - \frac{1}{2} \cdot \prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} (-1)^{f_b(b_1,b_2,...,b_n) \wedge \bigwedge\limits_{k=1}^{n} x_k^{b_k}} =$$

$$= \frac{1}{2} - \frac{1}{2} \cdot \prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \left(1 - 2 \cdot f_b(b_1, b_2, ..., b_n) \wedge \bigwedge_{k=1}^{n} x_k^{b_k}\right) =$$

$$= \frac{1}{2} - \frac{1}{2} \cdot \prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \frac{2 - 4 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)}{1 + (\pm 1)^2} =$$

$$= \frac{1}{2} - \frac{1}{2} \cdot \prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \frac{2 - 4 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)}{1 + \left(1 - 2 \cdot and_s\left(f_b(b_1, b_2, ..., b_n), x_1^{b_1}, x_2^{b_2}, ..., x_n^{b_n}\right)\right)^2}.$$

В силу (3) справедливо

$$\frac{1}{2}-\frac{1}{2}\cdot\prod_{(b_1,b_2,...,b_n)\in\mathbb{B}^n}\frac{2-4\cdot and_s\left(f_b(b_1,b_2,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)}{1+\left(1-2\cdot and_s\left(f_b(b_1,b_2,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)\right)^2}=$$

$$=f_s(x_1,x_2,...,x_n)=b.$$

Теорема доказана. ■

Замечание 3. Нет свойства единственности подходящего продолжения на $\mathbb{R}^n$ булевой функции $f_b(b_1,b_2,...,b_n)$. Обоснование этого аналогично обоснованию замечания 1, т. е. благодаря одному конструированному подходящему предложению можно построить бесконечное количество новых подходящих предложений.

Рассмотрим произвольную систему булевых уравнений вида

$$\begin{cases}p_1(x_1,x_2,...,x_n)=0\\p_2(x_1,x_2,...,x_n)=0\\p_3(x_1,x_2,...,x_n)=0\\\dots\quad\dots\quad\dots\\p_m(x_1,x_2,...,x_n)=0\end{cases}. \tag{5}$$

Трансформируем систему (5) в соответствующую систему подходящих уравнений вида

$$\begin{cases}p_{s1}(x_1,...,x_n)=\frac{1}{2}-\frac{1}{2}\cdot\prod\limits_{(b_1,...,b_n)\in\mathbb{B}^n}\frac{2-4\cdot and_s\left(p_1(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)}{1+\left(1-2\cdot and_s\left(p_1(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)\right)^2}=0\\p_{s2}(x_1,...,x_n)=\frac{1}{2}-\frac{1}{2}\cdot\prod\limits_{(b_1,...,b_n)\in\mathbb{B}^n}\frac{2-4\cdot and_s\left(p_2(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)}{1+\left(1-2\cdot and_s\left(p_2(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)\right)^2}=0\\p_{s3}(x_1,...,x_n)=\frac{1}{2}-\frac{1}{2}\cdot\prod\limits_{(b_1,...,b_n)\in\mathbb{B}^n}\frac{2-4\cdot and_s\left(p_3(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)}{1+\left(1-2\cdot and_s\left(p_3(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)\right)^2}=0\\\dots\qquad\qquad\dots\qquad\qquad\qquad\qquad\qquad\qquad\dots\\p_{sm}(x_1,...,x_n)=\frac{1}{2}-\frac{1}{2}\cdot\prod\limits_{(b_1,...,b_n)\in\mathbb{B}^n}\frac{2-4\cdot and_s\left(p_m(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)}{1+\left(1-2\cdot and_s\left(p_m(b_1,...,b_n),x_1^{b_1},x_2^{b_2},...,x_n^{b_n}\right)\right)^2}=0\end{cases}. \tag{6}$$

В свою очередь, для системы (6) построим целевую функцию вида

$$tf_s(x_1,x_2,...,x_n)=\sum_{k=1}^{m}p_{sk}(x_1,x_2,...,x_n). \tag{7}$$

Теперь установим связь между (5), (6) и (7) в виде утверждения и приведём соответствующее доказательство.

Утверждение 1. *В $\mathbb{R}^n$ системы (5) и (6) эквивалентны, причём $(x_1,x_2,...,x_n)$ будет решением систем (5) и (6) тогда и только тогда, когда $tf_s(x_1,x_2,...,x_n)=0$.*

Доказательство. В одну сторону очевидно, так как функция $p_{sk}(x_1, x_2, ..., x_n)$ является одним из продолжений булевой функции $p_k(x_1, x_2, ..., x_n)$, $\forall k \in \{1, 2, ..., m\}$ и, следовательно, множество решений системы (5) является подмножеством множества решений системы (6).

В другую сторону, пусть $(r_1, r_2, ..., r_n) \in \mathbb{R}^n$ произвольное решение системы (6). Тогда в силу лемм 1, 2 и теоремы 1 $(r_1, r_2, ..., r_n) \in \mathbb{B}^n$ и, следовательно, $(r_1, r_2, ..., r_n)$ является решением системы (5), так как $p_{sk}(r_1, r_2, ..., r_n) = p_k(r_1, r_2, ..., r_n), \ \forall k \in \{1, 2, ..., m\}$. Следовательно, множество решений системы (6) в $\mathbb{R}^n$ является подмножеством множества решений системы (5).

В силу лемм 1, 2 и теоремы 1 справедливо неравенство

$$0 \leqslant p_{sk}(x_1, x_2, ..., x_n) \leqslant 1, \quad \forall k \in \{1, 2, ..., m\} \quad \text{и} \quad \forall (x_1, x_2, ..., x_n) \in \mathbb{R}^n$$

и, следовательно, $(x_1, x_2, ..., x_n)$ будет решением систем (5) и (6) $\iff$ $tf_s(x_1, x_2, ..., x_n) = 0$. Утверждение доказано. ■

Замечание 4. Система рациональных уравнений (6) путём умножения на общий знаменатель элементарно может быть сведена к эквивалентной системе полиномиальных уравнений вида

$$\begin{cases} h_1(x_1, x_2, ..., x_n) = 0 \\ h_2(x_1, x_2, ..., x_n) = 0 \\ h_3(x_1, x_2, ..., x_n) = 0 \\ \dots \quad \dots \quad \dots \\ h_m(x_1, x_2, ..., x_n) = 0 \end{cases}, \tag{8}$$

где многочлен $h_k(x_1, x_2, ..., x_n)$ равен числителю несократимой дроби, равной $p_{sk}(x_1, x_2, ..., x_n), \quad \forall k \in \{1, 2, ..., m\}$. В свою очередь, система (8) может быть проанализирована и решена алгоритмом F4 [8, 9].

Заключение

В результате исследования построено $f_s(x_1, x_2, ..., x_n)$ – подходящее, т. е. специальное бесконечно дифференцируемое рациональное продолжение на всё пространство $\mathbb{R}^n$ произвольной булевой функции $f_b(x_1, x_2, ..., x_n)$, имеющее следующее важное свойство

$$f_s(x_1, x_2, ..., x_n) \in \{0, 1\} \iff \begin{cases} (x_1, x_2, ..., x_n) \in \{0, 1\}^n \\ f_b(x_1, x_2, ..., x_n) = f_s(x_1, x_2, ..., x_n) \end{cases}.$$

Благодаря этому аргументировано, что система m булевых уравнений без добавления каких-либо ограничений может быть трансформирована в эквивалентную систему m рациональных уравнений, т. е. для таких задач проблема посторонних решений, возникающих при трансформации систем, полностью решена. Также доказано, что на основе предъявленного подходящего продолжения булевой функции $f_b(x_1, x_2, ..., x_n)$ можно конструировать новую функцию, которая также является подходящим продолжением на $\mathbb{R}^n$ функции $f_b(x_1, x_2, ..., x_n)$.

Полученный результат также может быть применён при решении систем уравнений, заданных одновременно как математическими, так и логическими операциями.

Литература

1. Brown F.M. Boolean Reasoning: The logic of Boolean Equations. Boston: Kluwer Academic Publishers, 1990.
2. Hammer P.L., Rudeanu S. Boolean Methods in Operations Research and Related Areas. Berlin: Springer Verlag, 1968.
3. Bard G.V. Algorithms for Solving Linear and Polynomial Systems of Equations over Finite Fields, with Applications to Cryptanalysis.College Park, MD, USA: University of Maryland, 2007.
4. Faugere J.C., Joux A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases // Annual International Cryptology Conference. Berlin; Heidelberg: Springer, 2003. P. 44–60.
5. Armknecht F. Improving Fast Algebraic Attacks // International Workshop on Fast Software Encryption. Berlin; Heidelberg, Germany: Springer, 2004. P. 65–82.
6. Bardet M., Faugère J.-C., Salvy B., Spaenlehauer P.-J. On the complexity of solving quadratic boolean systems // J. Complex. 2013. Vol. 29. P. 53–75. DOI: 10.1016/j.jco.2012.07.001.
7. Courtois N. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback // CRYPTO 2003 / Ed. D. Boneh. Berlin; Heidelberg, Germany: Springer, 2003. P. 176–174. (Lecture Notes in Computer Science, vol. 2729.)
8. Faugere J.C. A new efficient algorithm for computing Gröbner bases (F4) // J. Pure Appl. Algebra. 1999. Vol. 139. P. 61–88. DOI: 10.1016/S0022-4049(99)00005-5.
9. Faugere J.C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5) // Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Lille, France, 7–10 July 2002. P. 75–83.
10. Liu M., Lin, D., Pei D. Fast algebraic attacks and decomposition of symmetric Boolean functions // IEEE Trans. Inf. Theory. 2011. Vol. 57. P. 4817–4821. DOI: 10.1109/TIT.2011.2145690.
11. Abdel-Gawad A.H., Atiya A.F., Darwish N.M. Solution of systems of Boolean equations via the integer domain // Inform. Sci. 2010. Vol. 180. P. 288–300. DOI: 10.1016/j.ins.2009.09.010.
12. Gu J. How to Solve Very Large-Scale Satisfiability (VLSS) Problems: Technical Report UCECETR-90-002. Calgary, AB, Canada: University of Calgary, 1990.
13. Gu J. On optimizing a search problem // Artificial Intelligence Methods and Applications / Ed. N.G. Bourbakis. Singapore: World Scientific Publishers, 1992.
14. Gu J. Global optimization for satisfiability (SAT) problem // IEEE Trans. Knowl. Data Eng. 1994. Vol. 6. P. 361–381. DOI: 10.1109/69.334864.
15. Gu J., Gu Q., Du D. On optimizing the satisfiability (SAT) problem // J. Comput. Sci. Technol. 1999. Vol. 14. P. 1–17. DOI: 10.1007/BF02952482.
16. Баротов Д.Н., Музафаров Д.З., Баротов Р.Н. Об одном методе решения систем булевых алгебраических уравнений // Современная математика и концепции инновационного математического образования. 2021. Т. 8, № 1. С. 17–23.
17. Barotov D., Osipov A., Korchagin S., Pleshakova E., Muzafarov D., Barotov R., Serdechnyy D. Transformation Method for Solving System of Boolean Algebraic Equations // Mathematics. 2021. Vol. 9. Art. 3299. DOI: 10.3390/math9243299.
18. Barotov D.N., Barotov, R.N. Polylinear Transformation Method for Solving Systems of Logical Equations // Mathematics. 2022. Vol. 10. Art. 918. DOI: 10.3390/math10060918.

19. Barotov D.N., Barotov R.N., Soloviev V., Feklin V., Muzafarov D., Ergashboev T., Egamov K. The Development of Suitable Inequalities and Their Application to Systems of Logical Equations // Mathematics. 2022. Vol. 10. Art. 1851. DOI: 10.3390/math10111851.
20. Barotov D.N. Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution // Mathematics. 2022. Vol. 10. Art. 2097. DOI: 10.3390/math10122097.
21. Баротов Д.Н., Баротов Р.Н. Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения // Вычислительные методы и программирование. 2023. № 24. С. 10–23. DOI: 10.26089/NumMet.v24r102.
22. Баротов Д.Н. Выпуклое продолжение булевой функции и его приложения // Дискретный анализ и исследование операций. 2024. Т. 31, № 1. С. 5–21. (Принята в печать)

ON THE REDUCTION OF A SYSTEM OF BOOLEAN EQUATIONS TO AN EQUIVALENT SYSTEM OF POLYNOMIAL EQUATIONS

D.N. Barotov[1]
Assistant Professor, e-mail: DNBarotov@fa.ru
R.N. Barotov[2]
Doctoral Student, e-mail: ruzmet.tj@mail.ru

[1]Financial University under the Government of the Russian Federation, Moscow, Russia
[2]Khujand State University named after Academician Bobojon Gafurov, Khujand, Tajikistan

Abstract. In this paper, we study the problem of constructing a special continuation of a Boolean function to the entire space $\mathbb{R}^n$, thanks to which, without adding any restrictions, a system of m Boolean equations is transformed into an equivalent system of m polynomial equations. As a result of the study, for any Boolean function $f_b(x_1, x_2, ..., x_n)$, a corresponding infinitely differentiable rational function $f_s(x_1, x_2, ..., x_n)$ is constructed such that

$$f_s(x_1, x_2, ..., x_n) \in \{0, 1\} \Longleftrightarrow \begin{cases} (x_1, x_2, ..., x_n) \in \{0, 1\}^n \\ f_b(x_1, x_2, ..., x_n) = f_s(x_1, x_2, ..., x_n) \end{cases}.$$

Thanks to the constructed function $f_s(x_1, x_2, ..., x_n)$, firstly, without adding any restrictions, an arbitrary system of m Boolean equations is transformed into an equivalent system of m rational equations, and secondly, the solution of the transformed an equivalent system of rational equations is reduced to the problem of numerical minimization of some infinitely differentiable target function, solved by optimization methods, and to an equivalent system of polynomial equations, solved and analyzed by the F4 algorithm.

Keywords: continuation of a Boolean function, system of Boolean equations, global optimization, F4 algorithm, SAT.

Дата поступления в редакцию: 16.11.2023