АЛГЕБРО-ЛОГИЧЕСКИЕ МЕТОДЫ В ИНФОРМАТИКЕ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ALGEBRAIC AND LOGICAL METHODS IN COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE

Серия «Математика»
2024. Т. 49. С. 105—123

Онлайн-доступ к журналу:
http://mathizv.isu.ru

ИЗВЕСТИЯ
Иркутского
государственного
университета

Научная статья

УДК 512.563+519.853.3
MSC 06E30, 90C25, 46N10
DOI https://doi.org/10.26516/1997-7670.2024.49.105

Вогнутые продолжения булевых функций и некоторые их свойства и приложения

Д. Н. Баротов[1]✉

[1] Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
✉ DNBarotov@fa.ru

Аннотация. Доказывается, что для любой булевой функции от n переменных существует бесконечно много функций, каждая из которых является её вогнутым продолжением на n-мерный единичный куб. Для произвольной булевой функции от n переменных построена вогнутая функция, являющаяся минимумом среди всех её вогнутых продолжений на n-мерный единичный куб. Доказано, что эта вогнутая функция на n-мерном единичном кубе непрерывна и единственна. Благодаря полученным результатам, в частности, конструктивно доказано, что задача решения системы булевых уравнений может быть сведена к задаче численной максимизации целевой функции, любой локальный максимум которой в искомой области является глобальным максимумом, тем самым проблема локальных максимумов для таких задач полностью решена.

Ключевые слова: вогнутое продолжение булевой функции, булева функция, вогнутая функция, глобальная оптимизация, локальный экстремум

Ссылка для цитирования: Баротов Д. Н. Вогнутые продолжения булевых функций и некоторые их свойства и приложения // Известия Иркутского государственного университета. Серия Математика. 2024. Т. 49. С. 105–123.
https://doi.org/10.26516/1997-7670.2024.49.105

Research article

Concave Continuations of Boolean Functions and Some of Their Properties and Applications

Dostonjon N. Barotov[1]✉

[1] Financial University under the Government of the Russian Federation, Moscow, Russian Federation
✉ DNBarotov@fa.ru

Abstract. In this paper, it is proved that for any Boolean function of n variables, there are infinitely many functions, each of which is its concave continuation to the n-dimensional unit cube. For an arbitrary Boolean function of n variables, a concave function is constructed, which is the minimum among all its concave continuations to the n-dimensional unit cube. It is proven that this concave function on the n-dimensional unit cube is continuous and unique. Thanks to the results obtained, in particular, it has been constructively proved that the problem of solving a system of Boolean equations can be reduced to the problem of numerical maximization of a target function, any local maximum of which in the desired domain is a global maximum, and, thus, the problem of local maxima for such problems is completely solved.

Keywords: concave continuation of a Boolean function, Boolean function, concave function, global optimization, local extremum.

For citation: Barotov D. N. Concave Continuations of Boolean Functions and Some of Their Properties and Applications. *The Bulletin of Irkutsk State University. Series Mathematics*, 2024, vol. 49, pp. 105–123. (in Russian)
https://doi.org/10.26516/1997-7670.2024.49.105

1. Введение

Система булевых уравнений была важной темой исследований на протяжении почти двух столетий, и ее значимость трудно переоценить. Решение булевых уравнений проникает во многие области современной науки, такие как логическое проектирование, биология, грамматика, химия, право, медицина, спектроскопия и теория графов [14]. 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 [23]. Решения булевых уравнений также служат важным инструментом при обработке псевдобулевых уравнений, неравенств и связанных с ними задач целочисленного линейного программирования [23]. В последние годы еще одной важной и перспективной областью, в которой применяется решение системы булевых уравнений, является алгебраический криптоанализ, особенно применяется при анализе и

взломе блочных шифров, поскольку их можно свести к задаче решения крупномасштабной системы булевых уравнений [7–9; 15–17]. Одно из первых успешных применений решения системы булевых уравнений в криптографической задаче было продемонстрировано в [16]. В связи с этим, с одной стороны, совершенствуются существующие методы и алгоритмы, с другой стороны, разрабатывается и адаптируется множество новых направлений исследования и алгоритмов решения систем булевых уравнений [6; 7; 9; 15; 17; 18; 25]. 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 [4; 10; 12; 19–22], либо к MILP или QUBO, решаемой классическими алгоритмами дискретной оптимизации или квантовыми алгоритмами [26], либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [6], либо к эквивалентной системе полиномиальных уравнений, решаемой и анализируемой символьными методами [13; 16–18].

Существует множество способов преобразования системы булевых уравнений к задаче непрерывной оптимизации, поскольку принципиальное отличие таких методов от «переборных» алгоритмов локального поиска состоит в том, что на каждой итерации алгоритма сдвиг по градиенту (антиградиенту) производится одновременно по всем переменным [1–3; 5; 11]. Но одна из основных проблем, возникающих при применении этих методов, заключается в том, что оптимизируемая целевая функция в искомой области может иметь множество локальных экстремумов, что существенно усложняет их практическое использование [2; 3; 10–12; 19]. В [3; 11] аргументировано, что полилинейное продолжение булевой функции также играет важную роль в уменьшении числа локальных минимумов целевой функции. По этой тематике недавно в [3] были найдены явные формы полилинейных продолжений произвольных функций, заданных на множестве вершин n-мерного единичного куба, произвольного куба и параллелепипеда, и в каждом конкретном случае доказана единственность соответствующего полилинейного продолжения.

На основании вышеизложенной мотивации в данной статье исследуются существование и единственность вогнутого продолжения произвольной булевой функции на множество $[0, 1]^n$. В результате исследования получены некоторые теоретические результаты, а именно, во-

первых, для любой булевой функции явно строится её вогнутое продолжение на $[0,1]^n$. Также благодаря построенному продолжению на $[0,1]^n$ конструктивно доказывается, что для любой булевой функции существует бесконечно много функций, каждая из которых является её вогнутым продолжением на $[0,1]^n$. Во-вторых, для любой булевой функции строится её специальное вогнутое продолжение, являющееся минимумом среди всех её вогнутых продолжений на $[0,1]^n$, а также доказывается единственность и непрерывность такого специального продолжения. На основе полученных результатов также конструктивно аргументируется, что задача решения системы булевых уравнений может быть сведена к задаче максимизации целевой функции, любой локальный максимум которой в искомой области является глобальным максимумом.

2. 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,
$\mathbb{K}^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in [0,1]\}$ — n-мерный куб, натянутый на булевы векторы длины n.

Пусть $int(\mathbb{K}^n) = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in (0,1)\}$ — множество внутренних точек куба $\mathbb{K}^n$.

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

Пусть $and_{(b_1,b_2,\ldots,b_n)}(x_1, x_2, \ldots, x_n) = x_1^{b_1} \wedge x_2^{b_2} \wedge \ldots \wedge x_n^{b_n}$ – конъюнкция литералов $x_1^{b_1}, x_2^{b_2}, \ldots, x_n^{b_n}$, где $x_k^{b_k} = \begin{cases} \overline{x_k}, & \text{если } b_k = 0 \\ x_k, & \text{если } b_k = 1 \end{cases}$.

Пусть $or_{(b_1,b_2,\ldots,b_n)}(x_1, x_2, \ldots, x_n) = x_1^{b_1} \vee x_2^{b_2} \vee \ldots \vee x_n^{b_n}$ – дизъюнкция литералов $x_1^{b_1}, x_2^{b_2}, \ldots, x_n^{b_n}$.

Пусть $\mathbf{\Lambda}(x_1, x_2, \ldots, x_n) = \Bigg\{ \left(\lambda_{(0,0,\ldots,0)}, \lambda_{(0,0,\ldots,1)}, \ldots, \lambda_{(1,1,\ldots,1)}\right) \in \mathbb{K}^{2^n} :$

$$\sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)} \cdot (b_1, b_2, \ldots, b_n, 1) = (x_1, x_2, \ldots, x_n, 1) \Bigg\}$$

— множество весовых коэффициентов, используемых для представления точки $(x_1, x_2, \ldots, x_n)$ как выпуклой комбинации вершин куба $\mathbb{K}^n$.

Определение 2. *Функцию вида $f : \mathbb{K}^n \to \mathbb{R}$ назовём вогнутой функцией на $\mathbb{K}^n$, если для любых $x, y \in \mathbb{K}^n$ и любого $\alpha \in [0,1]$ выполняется*

$$f(\alpha \cdot x + (1-\alpha) \cdot y) \geq \alpha \cdot f(x) + (1-\alpha) \cdot f(y).$$

Определение 3. *Функцию вида* $f_{CC} : \mathbb{K}^n \to \mathbb{R}$ *назовём вогнутым продолжением на* $\mathbb{K}^n$ *булевой функции* $f_B : \mathbb{B}^n \to \mathbb{B}$, *если она на* $\mathbb{K}^n$ *вогнутая и*

$$f_{CC}(b_1, b_2, \ldots, b_n) = f_B(b_1, b_2, \ldots, b_n) \quad \forall (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n.$$

Определение 4. *Функцию вида* $f_{BD} : \mathbb{K}^n \to \mathbb{R}$ *назовём минимумом среди всех вогнутых продолжений на* $\mathbb{K}^n$ *булевой функции* $f_B : \mathbb{B}^n \to \mathbb{B}$, *если она является вогнутым продолжением на* $\mathbb{K}^n$ *булевой функции* f_B *и для любого* $f_{CC}(x_1, x_2, ..., x_n)$ – *вогнутого продолжения на* $\mathbb{K}^n$ *булевой функции* f_B *и любой* $(x_1, x_2, ..., x_n) \in \mathbb{K}^n$ *выполняется*

$$f_{BD}(x_1, x_2, ..., x_n) \leq f_{CC}(x_1, x_2, ..., x_n).$$

3. Количество вогнутых продолжений булевой функции

В этом разделе конструктивно докажем, что для любой булевой функции $f_B : \mathbb{B}^n \to \mathbb{B}$ существует бесконечно много функций, каждая из которых является её вогнутым продолжением на $\mathbb{K}^n$.

Утверждение 1. *Для любой булевой функции* $f_B(x_1, x_2, \ldots, x_n)$ *соответствующая вещественная функция вида* $f_{CC}(x_1, x_2, \ldots, x_n) =$

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

$$\left. - \left| 1 - f_B(b_1, b_2, ..., b_n) + \sum_{k=1}^{n} ((2b_k - 1)x_k - b_k) \right| \right] \qquad (3.1)$$

является её вогнутым продолжением на $\mathbb{K}^n$.

Доказательство. Действительно, для этого достаточно показать справедливость следующих свойств:

i) $f_{CC}(a_1, a_2, ..., a_n) = f_B(a_1, a_2, ..., a_n) \quad \forall (a_1, a_2, ..., a_n) \in \mathbb{B}^n.$

ii) Функция $f_{CC}(x_1, x_2, ..., x_n)$ на множестве $\mathbb{K}^n$ вогнутая.

i) Действительно,

$$f_{CC}(a_1, a_2, ..., a_n) = 1 + \sum_{(b_1, b_2, ..., b_n) \in \mathbb{B}^n} \frac{1}{2} \cdot \left[f_B(b_1, b_2, ..., b_n) - 1 + \right.$$

$$\sum_{k=1}^{n} ((-2b_k + 1)a_k + b_k) - \left| 1 - f_B(b_1, b_2, ..., b_n) + \sum_{k=1}^{n} ((2b_k - 1)a_k - b_k) \right| \Bigg] =$$

$$1+\frac{1}{2}\cdot\Bigg[f_B(a_1,a_2,...,a_n)-1+\sum_{k=1}^{n}((-2a_k+1)a_k+a_k)-\Bigg|1-f_B(a_1,a_2,...,a_n)+$$

$$\sum_{k=1}^{n}((2a_k-1)a_k-a_k)\Bigg|\Bigg]+\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n\setminus(a_1,a_2,...,a_n)}\frac{1}{2}\cdot\Bigg[f_B(b_1,b_2,...,b_n)-1+$$

$$\sum_{k=1}^{n}((-2b_k+1)a_k+b_k)-\Bigg|1-f_B(b_1,b_2,...,b_n)+\sum_{k=1}^{n}((2b_k-1)a_k-b_k)\Bigg|\Bigg]=$$

$$1+\frac{1}{2}\cdot\Bigg[f_B(a_1,a_2,...,a_n)-1+0-\Bigg|1-f_B(a_1,a_2,...,a_n)+0\Bigg|\Bigg]+$$

$$\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n\setminus(a_1,a_2,...,a_n)}\frac{1}{2}\cdot\Bigg[f_B(b_1,b_2,...,b_n)-1+$$

$$\sum_{k=1}^{n}((-2b_k+1)a_k+b_k)+1-f_B(b_1,b_2,...,b_n)+\sum_{k=1}^{n}((2b_k-1)a_k-b_k)\Bigg]=$$

$$1+f_B(a_1,a_2,...,a_n)-1+\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n\setminus(a_1,a_2,...,a_n)}0=f_B(a_1,a_2,...,a_n).$$

ii) Видно, что $F(L(x_1,x_2,...,x_n))\equiv\frac{1}{2}\cdot\Bigg[f_B(b_1,b_2,...,b_n)-1+$

$\sum\limits_{k=1}^{n}((-2b_k+1)x_k+b_k)-\Bigg|1-f_B(b_1,b_2,...,b_n)+\sum\limits_{k=1}^{n}((2b_k-1)x_k-b_k)\Bigg|\Bigg]$, где $F(y)=\frac{1}{2}\cdot(-1+y-|1-y|)$, $L(x_1,x_2,...,x_n)=f_B(b_1,b_2,...,b_n)+\sum\limits_{k=1}^{n}((-2b_k+1)x_k+b_k)$. Теперь легко видеть, что из вогнутости функции $F(y)$ и линейности функции $L(x_1,x_2,...,x_n)$ следует вогнутость суперпозиции $F(L(x_1,x_2,...,x_n))$. Следовательно, функция $f_{CC}(x_1,x_2,\ldots,x_n)$, определённая формулой (3.1), на $\mathbb{K}^n$ вогнута. □

Замечание 1. Нетрудно заметить, что построенное вогнутое продолжение вида (3.1) булевой функции $f_B(x_1,x_2,...,x_n)$, вообще говоря, не является минимумом. В качестве иллюстрирующего примера можно привести булеву функцию вида $f_B(x_1,x_2)=(x_1\vee x_2)\wedge(x_1\vee\overline{x_2})$.

Теорема 1. *Для любой булевой функции $f_B(x_1,x_2,...,x_n)$ существует бесконечно много функций, каждая из которых является её вогнутым продолжением на $\mathbb{K}^n$.*

Доказательство. Существование. Согласно утверждению 1 для любой булевой функции $f_B(x_1,x_2,...,x_n)$ соответствующая вещественная функция $f_{CC}(x_1,x_2,\ldots,x_n)$, определённая формулой (3.1), является её вогнутым продолжением на $\mathbb{K}^n$.

Бесконечность. Докажем от противного: пусть имеется конечное множество $S_{CC} = \{g_1(x_1, x_2, ..., x_n), g_2(x_1, x_2, ..., x_n), ..., g_N(x_1, x_2, ..., x_n)\}$ вогнутых продолжений булевой функции $f_B(x_1, x_2, ..., x_n)$ на $\mathbb{K}^n$. Тогда

$$\exists N_0 \in \{1, , 2, ..., N\} : \quad g_{N_0}\left(\frac{1}{2}, \frac{1}{2}, ..., \frac{1}{2}\right) \geq$$

$$g_k\left(\frac{1}{2}, \frac{1}{2}, ..., \frac{1}{2}\right) \quad \forall k \in \{1, 2, ..., N\}. \tag{3.2}$$

Теперь рассмотрим специальную функцию вида $g_{new}(x_1, x_2, ..., x_n) =$

$$g_{N_0}(x_1, x_2, ..., x_n) + A \cdot \min(x_1, 1 - x_1, x_2, 1 - x_2, ..., x_n, 1 - x_n), \tag{3.3}$$

где A — любое положительное число. Докажем, что вещественная функция $g_{new}(x_1, x_2, ..., x_n)$ также является вогнутым продолжением булевой функции $f_B(x_1, x_2, ..., x_n)$ на $\mathbb{K}^n$. Для этого достаточно показать справедливость следующих свойств:

$i)$ $g_{new}(a_1, a_2, ..., a_n) = f_B(a_1, a_2, ..., a_n) \quad \forall (a_1, a_2, ..., a_n) \in \mathbb{B}^n$.

$ii)$ Функция $g_{new}(x_1, x_2, ..., x_n)$ на множестве $\mathbb{K}^n$ вогнутая.

$i)$ Действительно, $\forall (a_1, a_2, ..., a_n) \in \mathbb{B}^n$ выполнено $g_{new}(a_1, a_2, ..., a_n) =$

$$g_{N_0}(a_1, a_2, ..., a_n) + A \cdot \min(a_1, 1 - a_1, a_2, 1 - a_2, ..., a_n, 1 - a_n) =$$

$$g_{N_0}(a_1, a_2, ..., a_n) + A \cdot 0 = g_{N_0}(a_1, a_2, ..., a_n) = f_B(a_1, a_2, ..., a_n),$$

так как, во-первых, $g_{N_0}(x_1, x_2, ..., x_n)$ — одно из вогнутых продолжений булевой функции $f_B(x_1, x_2, ..., x_n)$ на $\mathbb{K}^n$, во-вторых, $a_k \in \{0, 1\} \quad \forall k \in \{1, 2, ..., n\}$ и, следовательно,

$$\min(a_1, 1 - a_1, a_2, 1 - a_2, ..., a_n, 1 - a_n) = 0 \quad \forall (a_1, a_2, ..., a_n) \in \mathbb{B}^n.$$

$ii)$ Хорошо известно, что минимум набора линейных функций является вогнутой функцией, следовательно, $\min(x_1, 1 - x_1, x_2, 1 - x_2, ..., x_n, 1 - x_n)$ является вогнутой функцией. Отсюда в силу $A > 0$ и вогнутости $g_{N_0}(x_1, x_2, ..., x_n)$ получаем вогнутость функции $g_{new}(x_1, x_2, ..., x_n)$ на $\mathbb{K}^n$ как сумму двух вогнутых функций.

Теперь покажем, что $\forall (x_1, x_2, ..., x_n) \in int\,(\mathbb{K}^n)$ справедливо

$$g_{new}(x_1, x_2, ..., x_n) > g_{N_0}(x_1, x_2, ..., x_n). \tag{3.4}$$

Действительно, если $(x_1, x_2, ..., x_n) \in int\,(\mathbb{K}^n)$, то $\min(x_1, 1 - x_1, x_2, 1 - x_2, ..., x_n, 1 - x_n) > 0$, так как $0 < x_k < 1 \ \ \forall k \in \{1, 2, ..., n\}$. Следовательно, в силу (3.3) выполняется неравенство (3.4). Из (3.4), в частности, следует, что

$$g_{new}\left(\frac{1}{2}, \frac{1}{2}, ..., \frac{1}{2}\right) > g_{N_0}\left(\frac{1}{2}, \frac{1}{2}, ..., \frac{1}{2}\right).$$

Следовательно, $g_{new}(x_1, x_2, ..., x_n)$ — предъявленное вогнутое продолжение на $\mathbb{K}^n$ булевой функции $f_B(x_1, x_2, ..., x_n)$ не принадлежит множеству S_{CC}. Получили противоречие. □

Замечание 2. Теорема 1 также доказывает, что для любой булевой функции $f_B(x_1, x_2, ..., x_n)$ не существует максимального вогнутого продолжения на $\mathbb{K}^n$.

4. Вогнутое продолжение произвольной булевой функции

В этом разделе конструируем $f_{BD}(x_1, x_2, ..., x_n)$ — вогнутое продолжение на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \ldots, x_n)$, которое также является минимумом среди всех вогнутых продолжений на $\mathbb{K}^n$ булевой функции $f_B(x_1, x_2, \ldots, x_n)$. Также докажем его единственность и непрерывность.

С этой целью обоснуем справедливость следующей вспомогательной леммы.

Лемма 1. *Для любого $(b_1, b_2, ..., b_n) \in \mathbb{B}^n$ множество $\mathbf{\Lambda}(b_1, b_2, ..., b_n)$ состоит из одного элемента, в котором на месте $\lambda_{(b_1,b_2,...,b_n)}$ стоит единица, а на остальных местах стоят нули.*

Доказательство. Рассмотрим три случая.

Случай 1. Пусть $(b_1, b_2, ..., b_n) = (0, 0, ..., 0)$. Тогда согласно приведенному выше обозначению $\mathbf{\Lambda}(b_1, b_2, ..., b_n) =$

$$\mathbf{\Lambda}(0,0,...,0) = \Bigg\{ \left(\lambda_{(0,0,...,0)}, \lambda_{(0,0,...,1)}, ..., \lambda_{(1,1,...,1)}\right) \in \mathbb{K}^{2^n} :$$

$$\sum_{(a_1,a_2,...,a_n)\in\mathbb{B}^n} \lambda_{(a_1,a_2,...,a_n)} \cdot (a_1, a_2, ..., a_n) = (0, 0, ..., 0) \text{ и}$$

$$\sum_{(a_1,a_2,...,a_n)\in\mathbb{B}^n} \lambda_{(a_1,a_2,...,a_n)} = 1 \Bigg\}.$$ Приравняв покоординатно, получим

$$\lambda_{(a_1,a_2,...,a_n)} = \begin{cases} 1, & \text{если } (a_1, a_2, ..., a_n) = (0, 0, ..., 0) \\ 0, & \text{если } (a_1, a_2, ..., a_n) \in \mathbb{B}^n \setminus \{(0, 0, ..., 0)\} \end{cases}.$$

Действительно, если предположить

$$\exists (a_1^*, a_2^*, ..., a_n^*) \in \mathbb{B}^n \setminus \{(0, 0, ..., 0)\} : \lambda_{(a_1^*,a_2^*,...,a_n^*)} > 0,$$

то хотя бы одна координата вектора

$$\sum_{(a_1,a_2,...,a_n)\in\mathbb{B}^n} \lambda_{(a_1,a_2,...,a_n)} \cdot (a_1, a_2, ..., a_n)$$

будет положительна и, следовательно, он не будет равен $(0,0,...,0)$.

Случай 2. Пусть $(b_1,b_2,...,b_n)=(1,1,...,1)$. Тогда

$$\mathbf{\Lambda}(1,1,...,1)=\Bigg\{\left(\lambda_{(0,0,...,0)},\lambda_{(0,0,...,1)},...,\lambda_{(1,1,...,1)}\right)\in\mathbb{K}^{2^n}:$$

$$\sum_{(a_1,a_2,...,a_n)\in\mathbb{B}^n}\lambda_{(a_1,a_2,...,a_n)}\cdot(a_1,a_2,...,a_n)=(1,1,...,1)\text{ и}$$

$$\sum_{(a_1,a_2,...,a_n)\in\mathbb{B}^n}\lambda_{(a_1,a_2,...,a_n)}=1\Bigg\}.$$

Приравняв k-е координаты обеих частей, заметим, что

$$\lambda_{(a_1,a_2,...,a_{k-1},0,a_{k+1},...,a_n)}=0\quad\forall(a_1,a_2,...,a_{k-1},a_{k+1},...,a_n)\in\mathbb{B}^{n-1}$$

и, следовательно, в силу произвольности $k\in\{1,2,...,n\}$ справедливо

$$\lambda_{(a_1,a_2,...,a_n)}=\begin{cases}1, & \text{если } (a_1,a_2,...,a_n)=(1,1,...,1)\\ 0, & \text{если } (a_1,a_2,...,a_n)\in\mathbb{B}^n\setminus\{(1,1,...,1)\}\end{cases}.$$

Случай 3. Пусть $(b_1,b_2,...,b_n)\in\mathbb{B}^n\setminus\{(0,0,...,0),(1,1,...,1)\}$. Тогда существуют числа $p,q\in\mathbb{N}$ и множества $\{i_1,i_2,...,i_p\},\{j_1,j_2,..,j_q\}$ такие, что

$$\{i_1,i_2,...,i_p\}\cup\{j_1,j_2,..,j_q\}=\{1,2,...,n\}\text{ и }b_k=\begin{cases}0,\text{ если } k\in\{i_1,i_2,...,i_p\}\\ 1,\text{ если } k\in\{j_1,j_2,..,j_q\}.\end{cases}$$

Теперь, во-первых, исходя из рассуждения, аналогичного рассуждению в случае 1, получим, что если хотя бы одна из этих $a_{i_1},a_{i_2},...,a_{i_p}$ координат вектора $(a_1,a_2,...,a_n)$ равна единице, то $\lambda_{(a_1,a_2,...,a_n)}=0$, во-вторых, исходя из рассуждения, аналогичного рассуждению в случае 2, получим, что если хотя бы одна из этих $a_{j_1},a_{j_2},...,a_{j_q}$ координат вектора $(a_1,a_2,...,a_n)$ равна нулю, то $\lambda_{(a_1,a_2,...,a_n)}=0$. Отсюда

$$\lambda_{(a_1,a_2,...,a_n)}=\begin{cases}1, & \text{если } (a_1,a_2,...,a_n)=(b_1,b_2,...,b_n)\\ 0, & \text{если } (a_1,a_2,...,a_n)\neq(b_1,b_2,...,b_n)\end{cases}.$$

□

Пусть теперь задана произвольная булева функция $f_B(x_1,x_2,\ldots,x_n)$. Конструируем соответствующую ей вещественную функцию вида

$$f_{BD}(x_1,x_2,\ldots,x_n)=$$

$$\max_{\left(\lambda_{(0,0,...,0)},...,\lambda_{(1,1,...,1)}\right)\in\mathbf{\Lambda}(x_1,x_2,...,x_n)}\left[\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n}\lambda_{(b_1,b_2,...,b_n)}\cdot f_B(b_1,b_2,...,b_n)\right].\tag{4.1}$$

В силу компактности непустого множества $\mathbf{\Lambda}(x_1, x_2, \ldots, x_n), (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$, непрерывности функции

$$s\left(\lambda_{(0,0,\ldots,0)}, \ldots, \lambda_{(1,1,\ldots,1)}\right) = \sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)} \cdot f_B(b_1, b_2, \ldots, b_n)$$

и теоремы Вейерштрасса в любой точке $(x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$ функция $f_{BD}(x_1, x_2, \ldots, x_n)$ корректно определена и также непрерывна на $\mathbb{K}^n$.

Далее сформулируем и докажем теорему, утверждающую, что для любой булевой функции $f_B(x_1, x_2, \ldots, x_n)$ функция $f_{BD}(x_1, x_2, \ldots, x_n)$ является единственным минимумом среди всех её вогнутых продолжений на $\mathbb{K}^n$.

Теорема 2. *Для произвольной булевой функции $f_B(x_1, x_2, \ldots, x_n)$ функция $f_{BD}(x_1, x_2, \ldots, x_n)$, определённая формулой* (4.1)*, является единственным минимумом среди всех её вогнутых продолжений на $\mathbb{K}^n$.*

Доказательство. Сначала покажем, что если $g_{CC}(x_1, x_2, \ldots, x_n)$ – произвольное вогнутое продолжение булевой функции $f_B(x_1, x_2, \ldots, x_n)$ на $\mathbb{K}^n$, то

$$g_{CC}(x_1, x_2, \ldots, x_n) \geq f_{BD}(x_1, x_2, \ldots, x_n) \quad \forall (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n. \quad (4.2)$$

Пусть $(x_1^*, x_2^*, \ldots, x_n^*) \in \mathbb{K}^n$. Тогда в силу выпуклости множества $\mathbb{K}^n$

$$\exists \lambda_{(0,0,\ldots,0)}, \lambda_{(0,0,\ldots,1)}, \ldots, \lambda_{(1,1,\ldots,1)} :$$

$$\left(\lambda_{(0,0,\ldots,0)}, \lambda_{(0,0,\ldots,1)}, \ldots, \lambda_{(1,1,\ldots,1)}\right) \in \mathbf{\Lambda}(x_1^*, x_2^*, \ldots, x_n^*),$$

т. е. такие, что

$$\sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)} \cdot (b_1, b_2, \ldots, b_n) = (x_1^*, x_2^*, \ldots, x_n^*)$$

и

$$\lambda_{(b_1,b_2,\ldots,b_n)} \geq 0, \qquad \sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)} = 1.$$

В силу вогнутости функции $g_{CC}(x_1, x_2, \ldots, x_n)$ и неравенства Йенсена [24] получим

$$g_{CC}(x_1^*, x_2^*, \ldots, x_n^*) = g_{CC}\left(\sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)} \cdot (b_1, b_2, \ldots, b_n)\right) \geq$$

$$\sum_{(b_1,b_2,\ldots,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,\ldots,b_n)} \cdot g_{CC}(b_1, b_2, \ldots, b_n) =$$

$$\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,...,b_n)} \cdot f_B(b_1,b_2,...,b_n)$$

$$\forall \left(\lambda_{(0,0,...,0)}, \lambda_{(0,0,...,1)}, ..., \lambda_{(1,1,...,1)}\right) \in \mathbf{\Lambda}(x_1^*, x_2^*, ..., x_n^*).$$

В частности,

$$g_{CC}(x_1^*, x_2^*, ..., x_n^*) \geq f_{BD}(x_1^*, x_2^*, ..., x_n^*) =$$

$$\max_{\left(\lambda_{(0,0,...,0)},...,\lambda_{(1,1,...,1)}\right)\in\mathbf{\Lambda}(x_1^*,x_2^*,...,x_n^*)} \left[\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,...,b_n)} f_B(b_1,b_2,...,b_n)\right].$$

В силу произвольности $(x_1^*, x_2^*, ..., x_n^*)$ из последнего неравенства получим справедливость (4.2).

Остается показать, что функция $f_{BD}(x_1, x_2, ..., x_n)$ также является вогнутым продолжением булевой функции $f_B(x_1, x_2, ..., x_n)$. Для этого достаточно показать справедливость следующих свойств:

$$i) \quad f_{BD}(a_1, a_2, ..., a_n) = f_B(a_1, a_2, ..., a_n) \quad \forall (a_1, a_2, ..., a_n) \in \mathbb{B}^n.$$

$ii)$ Функция $f_{BD}(x_1, x_2, ..., x_n)$ на множестве $\mathbb{K}^n$ вогнутая.

$iii)$ Для любого $f_{CC}(x_1, x_2, ..., x_n)$ — вогнутого продолжения на $\mathbb{K}^n$ булевой функции $f_B(x_1, x_2, ..., x_n)$ — и любой $(x_1, x_2, ..., x_n) \in \mathbb{K}^n$ выполняется

$$f_{BD}(x_1, x_2, ..., x_n) \leq f_{CC}(x_1, x_2, ..., x_n).$$

$i)$ Действительно, $f_{BD}(a_1, a_2, ..., a_n) =$

$$\max_{\left(\lambda_{(0,0,...,0)},...,\lambda_{(1,1,...,1)}\right)\in\mathbf{\Lambda}(a_1,a_2,...,a_n)} \left[\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,...,b_n)} f_B(b_1,b_2,...,b_n)\right]$$

$$= \sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda_{(b_1,b_2,...,b_n)} \cdot f_B(b_1,b_2,...,b_n) = 1 \cdot f_B(a_1,a_2,...,a_n) +$$

$$\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n\setminus\{(a_1,a_2,...,a_n)\}} 0 \cdot f_B(b_1,b_2,...,b_n) = f_B(a_1,a_2,...,a_n),$$

так как в силу леммы 1 для любого набора $(a_1, a_2, ..., a_n) \in \mathbb{B}^n$ множество $\mathbf{\Lambda}(a_1, a_2, ..., a_n)$ состоит из одного элемента, в котором на месте $\lambda_{(a_1,a_2,...,a_n)}$ стоит единица, а на остальных местах нули.

$ii)$ Пусть $x^*, x^{**} \in \mathbb{K}^n$, $\alpha \in [0,1]$ и $\alpha \cdot x^* + (1-\alpha) \cdot x^{**} =$

$$(\alpha \cdot x_1^* + (1-\alpha) \cdot x_1^{**}, \alpha \cdot x_2^* + (1-\alpha) \cdot x_2^{**}, ..., \alpha \cdot x_n^* + (1-\alpha) \cdot x_n^{**}).$$

В силу теоремы Вейерштрасса существуют

$$(\lambda_{(0,0,...,0)}^*, \lambda_{(0,0,...,1)}^*, ..., \lambda_{(1,1,...,1)}^*) \in \mathbf{\Lambda}(x_1^*, x_2^*, ..., x_n^*)$$

и

$$(\lambda^{**}_{(0,0,...,0)}, \lambda^{**}_{(0,0,...,1)}, ..., \lambda^{**}_{(1,1,...,1)}) \in \mathbf{\Lambda}(x_1^{**}, x_2^{**}, ..., x_n^{**})$$

такие, что

$$f_{BD}(x_1^*, x_2^*, ..., x_n^*) = \sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda^*_{(b_1,b_2,...,b_n)} \cdot f_B(b_1, b_2, ..., b_n),$$

$$f_{BD}(x_1^{**}, x_2^{**}, ..., x_n^{**}) = \sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda^{**}_{(b_1,b_2,...,b_n)} \cdot f_B(b_1, b_2, ..., b_n).$$

Тогда $f_{BD}(\alpha x^* + (1-\alpha)x^{**}) =$

$$f_{BD}(\alpha x_1^* + (1-\alpha)x_1^{**}, \alpha x_2^* + (1-\alpha)x_2^{**}, ..., \alpha x_n^* + (1-\alpha)x_n^{**}) =$$

$$\max_{\left(\lambda_{(0,0,...,0)},...,\lambda_{(1,1,...,1)}\right)\in\mathbf{\Lambda}(\alpha x^*+(1-\alpha)x^{**})} \left[\sum_{(b_1,...,b_n)\in\mathbb{B}^n} \lambda_{(b_1,...,b_n)} \cdot f_B(b_1, ..., b_n) \right]$$

$$\geq \sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} (\alpha \cdot \lambda^*_{(b_1,b_2,...,b_n)} + (1-\alpha) \cdot \lambda^{**}_{(b_1,b_2,...,b_n)}) \cdot f_B(b_1, b_2, ..., b_n) =$$

$$\alpha \cdot \sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda^*_{(b_1,b_2,...,b_n)} \cdot f_B(b_1, b_2, ..., b_n) + (1-\alpha)\cdot$$

$$\sum_{(b_1,b_2,...,b_n)\in\mathbb{B}^n} \lambda^{**}_{(b_1,b_2,...,b_n)} \cdot f_B(b_1, b_2, ..., b_n) = \alpha \cdot f_{BD}(x_1^*, x_2^*, ..., x_n^*) +$$

$$(1-\alpha) \cdot f_{BD}(x_1^{**}, x_2^{**}, ..., x_n^{**}) = \alpha \cdot f_{BD}(x^*) + (1-\alpha) \cdot f_{BD}(x^{**}),$$

так как легко заметить, что

$$\left(\alpha\lambda^*_{(0,0,...,0)} + (1-\alpha)\lambda^{**}_{(0,0,...,0)}, \alpha\lambda^*_{(0,0,...,1)} + (1-\alpha)\lambda^{**}_{(0,0,...,1)}, ..., \alpha\lambda^*_{(1,1,...,1)} + \right.$$

$$\left.(1-\alpha)\lambda^{**}_{(1,1,...,1)}\right) \in \mathbf{\Lambda}(\alpha x_1^* + (1-\alpha)x_1^{**}, \alpha x_2^* + (1-\alpha)x_2^{**}, ..., \alpha x_n^* + (1-\alpha)x_n^{**}).$$

Из произвольности $(x_1^*, x_2^*, ..., x_n^*)$ и $(x_1^{**}, x_2^{**}, ..., x_n^{**})$ следует вогнутость функции $f_{BD}(x_1, x_2, ..., x_n)$ на $\mathbb{K}^n$.

iii) В силу *i*) и *ii*) справедливость данного пункта непосредственно следует из (4.2).

Единственность. В силу произвольности $g_{CC}(x_1, x_2, \ldots, x_n)$ единственность следует из неравенства (4.2). □

5. Явные формы вогнутых продолжений некоторых булевых функций

В качестве следствий теоремы 2 предъявим явные формы минимальных вогнутых продолжений булевых функций не более чем от двух переменных и базовых булевых функций $and_{(b_1,b_2,...,b_n)}(x_1,x_2,...,x_n) = x_1^{b_1} \wedge x_2^{b_2} \wedge ... \wedge x_n^{b_n}$ и $or_{(b_1,b_2,...,b_n)}(x_1,x_2,...,x_n) = x_1^{b_1} \vee x_2^{b_2} \vee ... \vee x_n^{b_n}$, которые непосредственно следуют из теоремы 2.

Следствие 1. *Для любой булевой функции $f_B(x)$, зависящей от одной переменной, функция вида*

$$f_{BD}(x) = (1-x)\cdot f_B(0) + x \cdot f_B(1)$$

является единственным минимумом среди всех её вогнутых продолжений на $\mathbb{K}^1$.

Следствие 2. *Для любой булевой функции $f_B(x,y)$, зависящей от двух переменных, функция вида*

$$f_{BD}(x,y) = (1-x-y)\cdot f_B(0,0) + x\cdot f_B(1,0) + y\cdot f_B(0,1) +$$

$$\frac{f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1)}{4} \cdot (2x+2y-1-|x-y|+|x+y-1|)$$

$$-\frac{|f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1)|}{4} \cdot (|x-y|+|x+y-1|-1)$$

является единственным минимумом среди всех её вогнутых продолжений на $\mathbb{K}^2$.

Следствие 3. *Для булевой функции вида $and_{(b_1,b_2,...,b_n)}(x_1,x_2,...,x_n) = x_1^{b_1} \wedge x_2^{b_2} \wedge ... \wedge x_n^{b_n}$ вещественная функция вида $f_{BD}(x_1,x_2,...,x_n) =$*

$$\min\left((2b_1-1)x_1 + 1 - b_1, (2b_2-1)x_2 + 1 - b_2, ..., (2b_n-1)x_n + 1 - b_n\right)$$

является единственным минимумом среди всех её вогнутых продолжений на $\mathbb{K}^n$.

Следствие 4. *Для булевой функции вида $or_{(b_1,b_2,...,b_n)}(x_1,x_2,...,x_n) = x_1^{b_1} \vee x_2^{b_2} \vee ... \vee x_n^{b_n}$ вещественная функция вида $f_{BD}(x_1,x_2,...,x_n) =$*

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

является единственным минимумом среди всех её вогнутых продолжений на $\mathbb{K}^n$.

6. Применение вогнутого продолжения булевой функции

Приведем одно из возможных приложений вогнутых продолжений булевых функций.

Рассмотрим систему булевых уравнений с единственным решением вида

$$p_k(x_1, x_2, ..., x_n) = 1, \quad k = 1, 2, ..., m, \tag{6.1}$$

где $p_k(x_1, x_2, ..., x_n)$ — произвольная булева функция от n переменных $x_1, x_2, ..., x_n$, $k \in \{1, 2, ..., m\}$. Система (6.1) может быть трансформирована к одному эквивалентному булеву уравнению вида

$$\widetilde{f_B}(x_1, x_2, ..., x_n) = \bigwedge_{1 \le k \le m} p_k(x_1, x_2, ..., x_n) = 1. \tag{6.2}$$

Для ясности дальнейшего рассуждения введем обозначения. Пусть $\widetilde{f_{BD}}(x_1, x_2, ..., x_n)$ – минимальное среди всех вогнутых продолжений на $\mathbb{K}^n$ булевой функции $\widetilde{f_B}(x_1, x_2, ..., x_n)$, а $(s_1, s_2, ..., s_n) \in \mathbb{B}^n$ – решение системы (6.1). Тогда справедливо следующее утверждение, устанавливающее связь между системой (6.1) и минимальным вогнутым продолжением $\widetilde{f_{BD}}(x_1, x_2, ..., x_n)$.

Утверждение 2. *Точка максимума вогнутой функции $\widetilde{f_{BD}}(x_1, ..., x_n)$ на множестве $\mathbb{K}^n$ единственна и равна $(s_1, s_2, ..., s_n)$.*

Доказательство. Во-первых, из теоремы 2 следует, что

$$0 \le \widetilde{f_{BD}}(x_1, x_2, ..., x_n) \le 1 \quad \forall (x_1, x_2, ..., x_n) \in \mathbb{K}^n. \tag{6.3}$$

Из (6.3) следует, что

$$\max_{(x_1, x_2, ..., x_n) \in \mathbb{K}^n} \widetilde{f_{BD}}(x_1, x_2, ..., x_n) \le 1. \tag{6.4}$$

Во-вторых, согласно предположению единственности решения системы (6.1) из следствия 3 следует, что

$$\widetilde{f_{BD}}(x_1, x_2, ..., x_n) = \min\left((2s_1 - 1)x_1 + 1 - s_1, ..., (2s_n - 1)x_n + 1 - s_n\right). \tag{6.5}$$

Заметим, что $\widetilde{f_{BD}}(s_1, s_2, ..., s_n) = 1$ и, следовательно, в силу включения $(s_1, s_2, ..., s_n) \in \mathbb{B}^n \subset \mathbb{K}^n$ и неравенства (6.4) имеем

$$\max_{(x_1, x_2, ..., x_n) \in \mathbb{K}^n} \widetilde{f_{BD}}(x_1, x_2, ..., x_n) = \widetilde{f_{BD}}(s_1, s_2, ..., s_n) = 1.$$

Для завершения доказательства остается показать, что если $(x_1, x_2, ..., x_n) \in \mathbb{K}^n \setminus \{(s_1, s_2, ..., s_n)\}$, то $\widetilde{f_{BD}}(x_1, x_2, ..., x_n) < 1$. Действительно,

если $(x_1, x_2, ..., x_n) \in \mathbb{K}^n \setminus \{(s_1, s_2, ..., s_n)\}$, то $\exists k \in \{1, 2, ..., n\} : x_k \neq s_k$. Отсюда в силу (6.5) получим

$$\widetilde{f_{BD}}(x_1, x_2, ..., x_n) \leq (2s_k - 1)x_k + 1 - s_k = \begin{cases} 1 - x_k, \text{ если } s_k = 0 \\ x_k, \text{ если } s_k = 1 \end{cases} < 1.$$

□

7. Заключение

В результате исследования конструктивно доказано, что для любой булевой функции $f_B : \mathbb{B}^n \to \mathbb{B}$ существует бесконечно много функций, каждая из которых является её вогнутым продолжением на $\mathbb{K}^n$. Для произвольной булевой функции $f_B : \mathbb{B}^n \to \mathbb{B}$ построена функция $f_{BD} : \mathbb{K}^n \to \mathbb{R}$, являющаяся минимумом среди всех её вогнутых продолжений на $\mathbb{K}^n$. Обосновано, что функция $f_{BD} : \mathbb{K}^n \to \mathbb{R}$ на $\mathbb{K}^n$ непрерывна и единственна. Также конструктивно аргументировано, что задача решения системы булевых уравнений может быть сведена к задаче непрерывной максимизации целевой функции, любой локальный максимум которой на $\mathbb{K}^n$ является глобальным максимумом. Полученные результаты позволяют в некоторых случаях заменять решение трудоемких, вообще говоря NP-трудных, задач с булевыми переменными на решение задач непрерывной вогнутой максимизации, для которых известны эффективные численные алгоритмы.

Автор выражает искреннюю благодарность рецензенту за полезные замечания и обнаружение ряда недостатков, использование и исправление которых помогло улучшить содержание статьи.

Список источников

1. Баротов Д. Н. Выпуклое продолжение булевой функции и его приложения // Дискретный анализ и исследование операций. 2024. Т. 31, № 1. С. 5–18. (Принята в печать)
2. Баротов Д. Н. О существовании и свойствах выпуклых продолжений булевых функций // Математические заметки. 2024. Т. 115, № 4. С. 533–551. (Принята в печать)
3. Баротов Д. Н., Баротов Р. Н. Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения // Вычислительные методы и программирование. 2023. Т. 24. С. 10–23. https://doi.org/10.26089/NumMet.v24r102
4. 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.

5. Файзуллин Р. Т., Дулькейт В. И., Огородников Ю. Ю. Гибридный метод поиска приближенного решения задачи 3-выполнимость, ассоциированной с задачей факторизации // Труды Института математики и механики УрО РАН. 2013. Т. 19, № 2. С. 285–294.
6. Abdel-Gawad A. H., Atiya A. F., Darwish N. M. Solution of systems of Boolean equations via the integer domain // Information Sciences. 2010. Vol. 180, N 2. P. 288–300. https://doi.org/10.1016/j.ins.2009.09.010
7. Armknecht F. Improving fast algebraic attacks // Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11. Springer Berlin Heidelberg, 2004. P. 65–82.
8. Bard G. V. Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis. University of Maryland, College Park, 2007.
9. Bardet M., Faugerebcd J. C., Salvye B., Spaenlehauer P. J. On the complexity of solving quadratic Boolean systems // Journal of Complexity. 2013. Vol. 29, N 1. P. 53–75. https://doi.org/10.1016/j.jco.2012.07.001
10. Transformation method for solving system of Boolean algebraic equations / D. Barotov, A. Osipov, S. Korchagin, E. Pleshakova, D. Muzafarov, R. Barotov, D. Serdechnyy // Mathematics. 2021. Vol. 9 (24), 3299. https://doi.org/10.3390/math9243299
11. Barotov D. N. Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution // Mathematics. 2022. Vol. 10 (12), 2097. https://doi.org/10.3390/math10122097
12. Barotov D. N., Barotov R. N. Polylinear Transformation Method for Solving Systems of Logical Equations // Mathematics. 2022. Vol. 10, 918. https://doi.org/10.3390/math10060918
13. The Development of Suitable Inequalities and Their Application to Systems of Logical Equations / D. N. Barotov, R. N. Barotov, V. Soloviev, V. Feklin, D. Muzafarov, T. Ergashboev, K. Egamov // Mathematics. 2022. Vol. 10, 1851. https://doi.org/10.3390/math10111851
14. Brown F. M. Boolean Reasoning: The logic of Boolean Equations. Boston : Kluwer Academic Publishers, 1990.
15. Courtois N. T. Fast algebraic attacks on stream ciphers with linear feedback // Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23. Heidelberg : Springer Berlin, 2003. P. 176–194.
16. Faugere J. C., Joux A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Grobner bases // Annual International Cryptology Conference. Heidelberg : Springer Berlin, 2003. P. 44–60.
17. Faugere J. C. A new efficient algorithm for computing Grobner bases (F4) // Journal of pure and applied algebra. 1999. Vol. 139, N. 1-3. P. 61–88. https://doi.org/10.1016/S0022-4049(99)00005-5
18. Faugere J. C. A new efficient algorithm for computing Grobner bases without reduction to zero (F5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation. 2002. P. 75–83.
19. Gu J. Global optimization for satisfiability (SAT) problem // IEEE Transactions on Knowledge and Data Engineering. 1994. Vol. 6, N. 3. P. 361–381. https://doi.org/10.1109/69.334864
20. Gu J. How to Solve Very Large-Scale Satisfiability (VLSS) Problems // Technical Report UCECETR-90-002. Calgary : University of Calgary, 1990.
21. Gu J. On optimizing a search problem // Artificial Intelligence Methods and Applications. 1992. P. 63–105. https://doi.org/10.1142/9789814354707_0002

22. Gu J., Gu Q., Du D. On optimizing the satisfiability (SAT) problem // Journal of Computer Science and Technology. 1999. Vol. 14, N 1. P. 1–17. https://doi.org/10.1007/BF02952482
23. Hammer P. L., Rudeanu S. Boolean Methods in Operations Research and Related Areas. Berlin : Springer Verlag, 1968.
24. Jensen J. L. W. V. Sur les fonctions convexes et les inegalites entre les valeurs moyennes // Acta mathematica. 1906. Vol. 30, N. 1. P. 175–193. https://doi.org/10.1007/BF02418571
25. Liu M., Lin D., Pei D. Fast algebraic attacks and decomposition of symmetric Boolean functions // IEEE Transactions on Information Theory. 2011. Vol. 57, N 7. P. 4817–4821. https://doi.org/10.1109/TIT.2011.2145690
26. Converting of Boolean Expression to Linear Equations, Inequalities and QUBO Penalties for Cryptanalysis / A. I. Pakhomchik, V. V. Voloshinov, V. M. Vinokur, G. B. Lesovik // Algorithms. 2022. Vol. 15, 33. https://doi.org/10.3390/a15020033

References

1. Barotov D.N. Convex continuation of a Boolean function and its applications. *Journal of Applied and Industrial Mathematics*, 2024, vol. 18, no. 1, pp. 1–9. (Accepted for publication)
2. Barotov D.N. On the existence and properties of convex continuations of Boolean functions. *Mathematical Notes*, 2024, vol. 115, no. 4, pp. 489–505. (Accepted for publication)
3. Barotov D.N., Barotov R.N. Polylinear Continuations of Some Discrete Functions and an Algorithm for Finding Them. *Numerical Methods and Programming (Vychislitel'nye Metody i Programmirovanie)*, 2023, vol. 24, pp. 10–23. https://doi.org/10.26089/NumMet.v24r102 (in Russian)
4. Barotov D.N., Muzafarov D.Z., Barotov R.N. On one method for solving systems of Boolean algebraic equations. *International Electronic Journal of Mathematics Education*, 2021, vol. 8, no. 1, pp. 17—23. (in Russian)
5. Faizullin R.T., Dul'keit V.I., Ogorodnikov Yu.Yu. Hybrid method for the approximate solution of the 3-satisfiability problem associated with the factorization problem. *Trudy Inst. Mat. i Mekh. UrO RAN.*, 2013, vol. 19, no. 2. pp. 285—294. (in Russian)
6. Abdel-Gawad A.H., Atiya A.F., Darwish N.M. Solution of systems of Boolean equations via the integer domain.*Information Sciences*, 2010, vol. 180, no. 2, pp. 288–300. https://doi.org/10.1016/j.ins.2009.09.010
7. Armknecht F. Improving fast algebraic attacks.*Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11*, Springer Berlin, Heidelberg, 2004, pp. 65–82.
8. Bard G.V. *Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis.* University of Maryland, College Park, 2007.
9. Bardet M., Faugerebcd J.C., Salvye B., Spaenlehauer P.J. On the complexity of solving quadratic Boolean systems. *Journal of Complexity*, 2013, vol. 29, no. 1, pp. 53–75. https://doi.org/10.1016/j.jco.2012.07.001
10. 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, 3299. https://doi.org/10.3390/math9243299

11. Barotov D.N. Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution. *Mathematics*, 2022, vol. 10, 2097. https://doi.org/10.3390/math10122097
12. Barotov D.N., Barotov R.N. Polylinear Transformation Method for Solving Systems of Logical Equations. *Mathematics*, 2022, vol. 10, 918. https://doi.org/10.3390/math10060918
13. 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, 1851. https://doi.org/10.3390/math10111851
14. Brown F.M. *Boolean Reasoning: The logic of Boolean Equations*. Kluwer Academic Publishers, Boston, 1990.
15. Courtois N.T. Fast algebraic attacks on stream ciphers with linear feedback. *Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23*, Springer Berlin, Heidelberg, 2003, pp. 176–194.
16. Faugere J.C., Joux A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Grobner bases. *Annual International Cryptology Conference*, Springer Berlin, Heidelberg, 2003, pp. 44–60.
17. Faugere J.C. A new efficient algorithm for computing Grobner bases (F4). *Journal of pure and applied algebra*, 1999, vol. 139, no. 1-3, pp. 61–88. https://doi.org/10.1016/S0022-4049(99)00005-5
18. Faugere J.C. A new efficient algorithm for computing Grobner bases without reduction to zero (F5). *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, 2002, pp. 75–83.
19. Gu J. Global optimization for satisfiability (SAT) problem. *IEEE Transactions on Knowledge and Data Engineering*, 1994, vol. 6, no. 3, pp. 361–381. https://doi.org/10.1109/69.334864
20. Gu J. How to Solve Very Large-Scale Satisfiability (VLSS) Problems. *Technical Report UCECETR-90-002*, University of Calgary, Calgary, 1990.
21. Gu J. On optimizing a search problem. *Artificial Intelligence Methods and Applications*, 1992, pp. 63–105. https://doi.org/10.1142/9789814354707_0002
22. Gu J., Gu Q., Du D. On optimizing the satisfiability (SAT) problem. *Journal of Computer Science and Technology*, 1999, vol. 14, no. 1, pp. 1–17. https://doi.org/10.1007/BF02952482
23. Hammer P. L., Rudeanu S. *Boolean Methods in Operations Research and Related Areas*. Springer Verlag, Berlin, 1968.
24. Jensen J.L.W.V. Sur les fonctions convexes et les inegalites entre les valeurs moyennes. *Acta mathematica*, 1906, vol. 30, no. 1, pp. 175–193. https://doi.org/10.1007/BF02418571
25. Liu M., Lin D., Pei D. Fast algebraic attacks and decomposition of symmetric Boolean functions. *IEEE Transactions on Information Theory*, 2011, vol. 57, no. 7, pp. 4817–4821. https://doi.org/10.1109/TIT.2011.2145690
26. Pakhomchik A.I., Voloshinov V.V., Vinokur V.M., Lesovik G.B. Converting of Boolean Expression to Linear Equations, Inequalities and QUBO Penalties for Cryptanalysis. *Algorithms*, 2022, vol. 15, 33. https://doi.org/10.3390/a15020033

Об авторах

Баротов Достонжон Нумонжонович, ст. преподаватель, Финансовый университет при Правительстве Российской Федерации, Москва, 109456, Российская Федерация, DNBarotov@fa.ru, https://orcid.org/0000-0001-5047-7710

About the authors

Dostonjon N. Barotov, Senior Lecturer, Financial University under the Government of the Russian Federation, Moscow, 109456, Russian Federation, DNBarotov@fa.ru, https://orcid.org/0000-0001-5047-7710

Поступила в редакцию / Received 13.01.2024
Поступила после рецензирования / Revised 02.03.2024
Принята к публикации / Accepted 12.03.2024