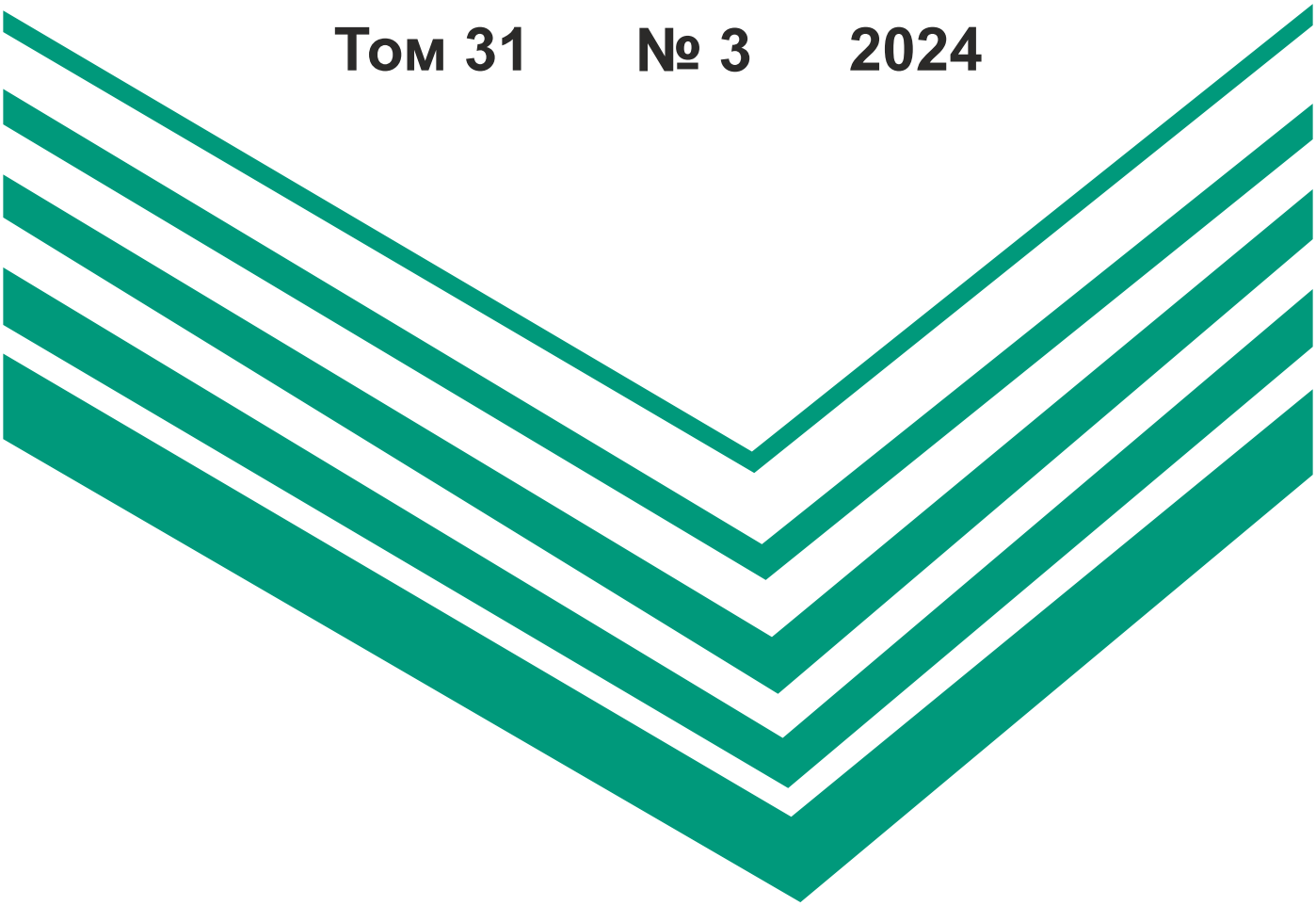
ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 31 № 3 2024



Новосибирск
Издательство Института математики

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2024. Т. 31, № 3. С. 5–23

УДК 519.8+518.25 DOI: 10.33048/daio.2024.31.789

ВЫПУКЛЫЕ ПРОДОЛЖЕНИЯ НЕКОТОРЫХ ДИСКРЕТНЫХ ФУНКЦИЙ

Д. Н. Баротов

Финансовый университет при Правительстве Российской Федерации,
4-й Вешняковский пр-д, 4, 109456 Москва, Россия

E-mail: dnbarotov@fa.ru

Аннотация. Построены выпуклые продолжения для дискретных функций, заданных на вершинах n-мерного единичного куба $[0,1]^n$, произвольного куба $[a,b]^n$ и параллелепипеда $[c_1,d_1]\times[c_2,d_2]\times\cdots\times[c_n,d_n]$. В каждом случае доказано, что, во-первых, для произвольной дискретной функции f, определённой на вершинах множества $\mathbb{G}\in\{[0,1]^n,[a,b]^n,[c_1,d_1]\times[c_2,d_2]\times\cdots\times[c_n,d_n]\}$, существует бесконечно много её выпуклых продолжений на $\mathbb{G}$ и, во-вторых, существует единственная функция вида $f_{DM}\colon\mathbb{G}\to\mathbb{R}$, которая является максимумом среди всех выпуклых продолжений f на $\mathbb{G}$, причём f_{DM} непрерывна на $\mathbb{G}$. Библиогр. 24.

Ключевые слова: дискретная функция, выпуклое продолжение дискретной функции, булева функция, псевдобулева функция.

Введение

В настоящее время теория булевых функций представляет собой замечательную область исследований в дискретной математике с обширными приложениями в криптографии и теории кодирования [1]. Встречается много основных задач, связанных с булевыми переменными, а некоторые задачи, несмотря на зрелость области, не имеют удовлетворительных методов решения. Среди них — проблема решения булевых уравнений и систем булевых уравнений [2]. Эта задача имеет множество приложений, таких как синтез, моделирование и тестирование цифровых сетей и систем СБИС, кодирование выходных данных и назначение состояний конечных автоматов, временной анализ и генерация тестов с задержкой-сбоем для комбинационных схем, автоматическая генерация тестовых

шаблонов, определение начального состояния в схемах, содержащих петли обратной связи [2–4]. В области криптографии она имеет приложения при анализе и взломе блочных шифров, поскольку их можно свести к проблеме решения крупномасштабной системы булевых уравнений [5–12]. В связи с этим развивается множество новых направлений и алгоритмов решения систем булевых уравнений. Одно из направлений заключается в том, что, во-первых, система булевых уравнений, заданная над кольцом булевых полиномов, преобразуется в систему уравнений над полем действительных чисел, а во-вторых, преобразованная система сводится либо к задаче численной минимизации соответствующей целевой функции [13–15], либо к задаче MILP или QUBO [16], либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [2], либо к эквивалентной системе полиномиальных уравнений, анализируемой и решаемой символьными методами [17].

Имеется много способов, позволяющих преобразовать систему булевых уравнений в задачу непрерывной минимизации, поскольку принципиальное отличие таких методов от «переборных» алгоритмов локального поиска в том, что на каждой итерации алгоритма сдвиг по антиградиенту производится по всем переменным одновременно [18–22]. Одна из основных проблем, возникающих при применении этих способов, заключается в том, что минимизируемая целевая функция в искомой области может иметь множество локальных минимумов, что значительно усложняет их практическое использование [13–15, 18, 19, 21, 22]. По теореме Д. Н. Баротова полилинейное продолжение булевой функции тоже играет важную роль для уменьшения числа локальных минимумов целевой функции [18, 22]. По данной тематике недавно в работе [18] были найдены явные формы полилинейных продолжений для произвольных функций, определённых на множестве вершин n-мерного единичного куба, произвольного куба и параллелепипеда, и в каждом конкретном случае была доказана единственность соответствующего полилинейного продолжения.

С учётом этой мотивации в настоящей работе совершенствуются (обобщаются) результаты, полученные недавно в [23]. В разд. 1 приводятся необходимые определения и обозначения. В разд. 2–4 для произвольной вещественнозначной дискретной функции f, определённой на вершинах множества $\mathbb{G} \in \{[0,1]^n, [a,b]^n, [c_1,d_1] \times [c_2,d_2] \times \cdots \times [c_n,d_n]\}$, в частности для любой булевой функции, конструктивно доказывается, что существуют, во-первых, бесконечно много её выпуклых продолжений на $\mathbb{G}$ и, во-вторых, функция $f_{DM} \colon \mathbb{G}^n \to \mathbb{R}$, которая является единственным максимумом среди всех её выпуклых продолжений $\mathbb{G}$.

1. Используемые обозначения и определения

Введём в рассмотрение следующие множества и обозначения:

- $\mathbb{B}^n = \{0,1\}^n$ — множество двоичных слов (булевых векторов) длины n;
- $\mathbb{K}^n = [0,1]^n$ — n-мерный куб, натянутый на множество булевых векторов длины n;
- $\operatorname{int}\mathbb{K}^n = (0,1)^n$ — множество внутренних точек куба $\mathbb{K}^n$;
- $\Lambda_{\mathbb{K}^n}(x) = \left\{\lambda = (\lambda_v)_{v\in\mathbb{B}^n} \in \mathbb{K}^{2^n} \mid \sum\limits_{v\in\mathbb{B}^n} \lambda_v \cdot (1,v) = (1,x)\right\}$ — множество весовых коэффициентов, используемых для представления точки $x \in \mathbb{K}^n$ как выпуклой комбинации вершин куба $\mathbb{K}^n$;
- $\mathbb{K}^n(a,b) = [a,b]^n$ — n-мерный куб со стороной $[a,b] \subset \mathbb{R}$, $a \neq b$;
- $\mathbb{B}^n(a,b) = \{a,b\}^n$ — множество вершин куба $\mathbb{K}^n(a,b)$;
- $\Lambda_{\mathbb{K}^n(a,b)}(x) = \left\{\lambda = (\lambda_v)_{v\in\mathbb{B}^n(a,b)} \in \mathbb{K}^{2^n} \mid \sum\limits_{v\in\mathbb{B}^n(a,b)} \lambda_v \cdot (1,v) = (1,x)\right\}$ — множество весовых коэффициентов, используемых для представления точки $x \in \mathbb{K}^n(a,b)$ как выпуклой комбинации вершин куба $\mathbb{K}^n(a,b)$;
- $\mathbb{P}^n = [c_1,d_1]\times[c_2,d_2]\times\cdots\times[c_n,d_n]$ — параллелепипед, определяемый парой различных точек $c = (c_1,c_2,\ldots,c_n)$, $d = (d_1,d_2,\ldots,d_n) \in \mathbb{R}^n$;
- $\mathbb{BP}^n = \{c_1,d_1\}\times\{c_2,d_2\}\times\cdots\times\{c_n,d_n\}$ — множество вершин параллелепипеда $\mathbb{P}^n$;
- $\Lambda_{\mathbb{P}^n}(x) = \left\{\lambda = (\lambda_v)_{v\in\mathbb{BP}^n} \in \mathbb{K}^{2^n} \mid \sum\limits_{v\in\mathbb{BP}^n} \lambda_v \cdot (1,v) = (1,x)\right\}$ — множество весовых коэффициентов, используемых для представления точки $x \in \mathbb{P}^n$ как выпуклой комбинации вершин параллелепипеда $\mathbb{P}^n$;
- $\rho(x,y) = \sum\limits_{k=1}^{n} I(x_k,y_k)$ — расстояние Хэмминга между векторами $x = (x_1,x_2,\ldots,x_n)$, $y = (y_1,y_2,\ldots,y_n) \in \mathbb{R}^n$, $I(x_k,y_k) = \begin{cases}0, & \text{если } x_k = y_k,\\ 1, & \text{если } x_k \neq y_k.\end{cases}$

Определение 1. Отображение вида $f\colon \mathbb{B}^n \to \mathbb{B}$ назовём *булевой функцией.*

Определение 2. Отображение вида $f\colon \mathbb{B}^n \to \mathbb{R}$ назовём *псевдобулевой функцией.*

Определение 3. Отображение вида $f\colon \mathbb{G} \to \mathbb{R}$, определённое на некотором выпуклом множестве $\mathbb{G}$, назовём *выпуклой функцией,* если для любых $x,y \in \mathbb{G}$ и любого $\alpha \in [0,1]$ выполняется

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

Определение 4. Отображение вида $f_D\colon \mathbb{K}^n \to \mathbb{R}$ назовём *выпуклым продолжением на* $\mathbb{K}^n$ (псевдо-) булевой функции $f\colon \mathbb{B}^n \to \mathbb{B}$ ($\mathbb{R}$), если выполнены следующие условия:

1) функция f_D выпукла на $\mathbb{K}^n$,
2) $f_D(v) = f_B(v)$ для любого $v \in \mathbb{B}^n$.

Определение 5. Отображение вида $f_{DM}\colon \mathbb{K}^n \to \mathbb{R}$ назовём *максимумом* среди всех выпуклых продолжений на $\mathbb{K}^n$ (псевдо-) булевой функции $f\colon \mathbb{B}^n \to \mathbb{B}$ ($\mathbb{R}$), если $f_D(x) \leqslant f_{DM}(x)$ для любого $x \in \mathbb{K}^n$ и любого выпуклого продолжения f_D на $\mathbb{K}^n$ функции f.

В начале работы обоснуем справедливость следующего вспомогательного утверждения.

Лемма 1. *Для любого $v \in \mathbb{BP}^n$ множество $\Lambda_{\mathbb{P}^n}(v)$ состоит из одного вектора, в котором $\lambda_v = 1$, а на остальных местах стоят нули.*

Доказательство. Рассмотрим три случая.

Случай 1. Пусть $v = c$. Тогда

$$\Lambda_{\mathbb{P}^n}(v) = \Lambda_{\mathbb{P}^n}(c) = \Big\{\lambda \in \mathbb{K}^{2^n} \mid \sum_{u\in\mathbb{BP}^n} \lambda_u = 1,\ \sum_{u\in\mathbb{BP}^n} \lambda_u u = c\Big\}.$$

Поскольку $c_k < d_k$, $k \in \{1, 2, \ldots, n\}$, и $\lambda_u \in [0, 1]$, $u \in \mathbb{BP}^n$, а $\sum\limits_{u\in\mathbb{BP}^n} \lambda_u = 1$, приравняв покоординатно, заметим, что

$$\lambda_u = \begin{cases} 1, & \text{если } u = c, \\ 0, & \text{если } u \in \mathbb{BP}^n \setminus \{c\}. \end{cases}$$

Действительно,

$$\sum_{u\in\mathbb{BP}^n} \lambda_u u - c = \sum_{u\in\mathbb{BP}^n} \lambda_u u - \sum_{u\in\mathbb{BP}^n} \lambda_u \cdot c = \\ = \sum_{u\in\mathbb{BP}^n} \lambda_u (u - c) = \sum_{u\in\mathbb{BP}^n\setminus\{c\}} \lambda_u (u - c) \geqslant 0,$$

и хотя бы одна координата этого вектора положительна, если существует $u^* \in \mathbb{BP}^n \setminus \{c\}$ такой, что $\lambda_{u^*} > 0$.

Случай 2. Пусть $v = d$. Тогда аналогичными рассуждениями приходим к выводу, что

$$\sum_{u\in\mathbb{BP}^n} \lambda_u u - d = \sum_{u\in\mathbb{BP}^n\setminus\{d\}} \lambda_u (u - d) \leqslant 0,$$

и хотя бы одна координата этого вектора отрицательна, если существует $u^* \in \mathbb{BP}^n \setminus \{d\}$ такой, что $\lambda_{u^*} > 0$, поэтому

$$\lambda_u = \begin{cases} 1, & \text{если } u = d, \\ 0, & \text{если } u \in \mathbb{BP}^n \setminus \{d\}. \end{cases}$$

Случай 3. Пусть $v \in \mathbb{BP}^n \setminus \{c, d\}$. Тогда

$$\sum_{u \in \mathbb{BP}^n} \lambda_u u - v = \sum_{u \in \mathbb{BP}^n \setminus \{v\}} \lambda_u (u - v). \tag{1}$$

Без ограничения общности предположим, что

$$v = (c_1, c_2, \ldots, c_p, d_{p+1}, d_{p+2}, \ldots, d_n)$$

для некоторого $p \in \{1, 2, \ldots, n-1\}$. В этом случае, если $1 \leqslant k \leqslant p$ и $\lambda_u > 0$ для некоторого вектора $u \in \mathbb{BP}^n \setminus \{v\}$ такого, что $u_k = d_k$, то k-я координата вектора (1) положительна. Аналогично если $p+1 \leqslant k \leqslant n$ и $\lambda_u > 0$ для некоторого вектора $u \in \mathbb{BP}^n \setminus \{v\}$ такого, что $u_k = c_k$, то k-я координата вектора (1) отрицательна. Отсюда

$$\lambda_u = \begin{cases} 1, & \text{если } u = v, \\ 0, & \text{если } u \in \mathbb{BP}^n \setminus \{v\}. \end{cases}$$

Лемма 1 доказана.

В качестве следствий приведём два факта, непосредственно вытекающих из леммы 1.

Следствие 1. *Для любого $v \in \mathbb{B}^n(a, b)$ множество $\Lambda_{\mathbb{K}^n(a,b)}(v)$ состоит из одного вектора, в котором $\lambda_v = 1$, а на остальных местах стоят нули.*

Следствие 2. *Для любого $v \in \mathbb{B}^n$ множество $\Lambda_{\mathbb{K}^n}(v)$ состоит из одного вектора, в котором $\lambda_v = 1$, а на остальных местах стоят нули.*

2. Выпуклые продолжения псевдобулевых функций

В этом разделе конструктивно докажем, что, во-первых, для любой псевдобулевой функции $f\colon \mathbb{B}^n \to \mathbb{R}$, в частности для любой булевой функции, существует бесконечно много функций, каждая из которых является её выпуклым продолжением на $\mathbb{K}^n$ и, во-вторых, для псевдобулевой функции $f\colon \mathbb{B}^n \to \mathbb{R}$, в частности для любой булевой функции, существует функция f_{DM}, которая является единственным максимумом среди всех её выпуклых продолжений $\mathbb{K}^n$.

Согласно следствию 1, приведённому в [18], произвольная псевдобулева функция $f\colon \mathbb{B}^n \to \mathbb{R}$ может быть задана как линейная комбинация базисных функций вида

$$f(x) = \sum_{b \in \mathbb{B}^n} f(b) I_b(x), \tag{2}$$

где базисная функция $I_b\colon \mathbb{B}^n \to \mathbb{B}$ с индексом $b = (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n$ может быть задана в виде

$$I_b(x) = \prod_{k=1}^{n}((2b_k - 1)x_k + 1 - b_k) = \begin{cases} 1, & \text{если } x = b, \\ 0, & \text{если } x \in \mathbb{B}^n \setminus \{b\}. \end{cases}$$

Согласно лемме 1, приведённой в [23], функция

$$f_{DM}^b(x) = \frac{1}{2}\left(1 + \sum_{k=1}^{n}((2b_k - 1)x_k - b_k) + \left|1 + \sum_{k=1}^{n}((2b_k - 1)x_k - b_k)\right|\right) \quad (3)$$

является единственным максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ булевой функции $I_b(x)$.

Теперь на основе (2) и (3) для произвольной псевдобулевой функции $f\colon \mathbb{B}^n \to \mathbb{R}$ конструируем соответствующее ей выпуклое продолжение на $\mathbb{K}^n$.

Лемма 2. *Пусть $f\colon \mathbb{B}^n \to \mathbb{R}$ — произвольная псевдобулева функция, $f_{\min} = \min\limits_{b\in\mathbb{B}^n} f(b)$. Тогда вещественная функция*

$$f_C(x) = f_{\min} + \sum_{b\in\mathbb{B}^n}(f(b) - f_{\min})f_{DM}^b(x) \quad (4)$$

является выпуклым продолжением на $\mathbb{K}^n$ функции f.

Доказательство. Действительно, сначала заметим, что функция $f_C(x)$ выпукла по построению как сумма некоторых выпуклых (непрерывных) на множестве $\mathbb{K}^n$ функций. Пусть $x, y \in \mathbb{K}^n$ и $\alpha \in [0, 1]$. Тогда в силу выпуклости функции $f_{DM}^b(x)$ и неравенства $f(b) - f_{\min} \geqslant 0$ для $b \in \mathbb{B}^n$, имеем

$$\begin{aligned} f_C(\alpha x + (1-\alpha)y) &= f_{\min} + \sum_{b\in\mathbb{B}^n}(f(b) - f_{\min})f_{DM}^b(\alpha x + (1-\alpha)y) \leqslant \\ &\leqslant f_{\min} + \sum_{b\in\mathbb{B}^n}(f(b) - f_{\min})\big(\alpha f_{DM}^b(x) + (1-\alpha)f_{DM}^b(y)\big) = \\ &= \alpha f_{\min} + (1-\alpha)f_{\min} + \alpha\sum_{b\in\mathbb{B}^n}(f(b) - f_{\min})f_{DM}^b(x) + \\ &\quad + (1-\alpha)\sum_{b\in\mathbb{B}^n}(f(b) - f_{\min})f_{DM}^b(y) = \alpha f_C(x) + (1-\alpha)f_C(y). \end{aligned}$$

Остаётся показать, что $f_C(a) = f(a)$ для любого $a \in \mathbb{B}^n$. В силу (2)–(4) получаем

$$f_C(a) = f_{\min} + \sum_{b\in\mathbb{B}^n}(f(b) - f_{\min}) \cdot f_{DM}^b(a) =$$

$$= f_{\min} + (f(a) - f_{\min}) f^a_{DM}(a) + \sum_{b \in \mathbb{B}^n \setminus \{a\}} (f(b) - f_{\min}) f^b_{DM}(a) =$$

$$= f_{\min} + (f(a) - f_{\min}) \cdot 1 + \sum_{b \in \mathbb{B}^n \setminus \{a\}} (f(b) - f_{\min}) \cdot 0 = f(a).$$

Лемма 2 доказана.

Замечание 1. Сконструированное выпуклое продолжение (4) в общем случае не является максимумом среди всех выпуклых продолжений на $\mathbb{K}^n$ псевдобулевой функции f. Наглядным примером является булева функция от трёх переменных $f(x_1, x_2, x_3) = x_1x_2x_3 \vee \overline{x}_1x_2x_3$.

Далее сформулируем и докажем теорему о том, что для любой псевдобулевой функции f существует бесконечно много функций, каждая из которых является её выпуклым продолжением на $\mathbb{K}^n$.

Теорема 1. *Для произвольной псевдобулевой функции* $f\colon \mathbb{B}^n \to \mathbb{R}$ *существует бесконечно много её выпуклых продолжений на* $\mathbb{K}^n$.

Доказательство. Существование выпуклого продолжения на $\mathbb{K}^n$ псевдобулевой функции f доказано в лемме 2. Бесконечность множества таких продолжений докажем от противного.

Пусть имеется конечное множество $S_C = \{g_1, g_2, \ldots, g_N\}$ выпуклых продолжений на $\mathbb{K}^n$ функции f. Тогда найдётся $N_0 \in \{1, 2, \ldots, N\}$ такое, что

$$g_{N_0}\left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right) \leqslant g_k\left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right), \quad k \in \{1, 2, \ldots, N\}.$$

Рассмотрим функцию

$$g_{\text{new}}(x) = g_{N_0}(x) - A \min\{x_1, 1 - x_1, x_2, 1 - x_2, \ldots, x_n, 1 - x_n\},$$

где $A > 0$ — произвольное число. Докажем, что функция g_{new} также является выпуклым продолжением на $\mathbb{K}^n$ функции f. Для этого достаточно показать, что

1) $g_{\text{new}}(a) = f(a)$ для любого $a \in \mathbb{B}^n$;
2) функция g_{new} выпукла на множестве $\mathbb{K}^n$.

1) Действительно, для любого $a \in \mathbb{B}^n$

$$g_{\text{new}}(a) = g_{N_0}(a) - A \min\{a_1, 1 - a_1, a_2, 1 - a_2, \ldots, a_n, 1 - a_n\} =$$
$$= g_{N_0}(a) - A \cdot 0 = g_{N_0}(a) = f(a).$$

2) Пусть $x^*, x^{**} \in \mathbb{K}^n$, $\alpha \in [0, 1]$. Тогда для любого $k \in \{1, 2, \ldots, n\}$ справедливы неравенства

$$\alpha x^*_k + (1 - \alpha) x^{**}_k \geqslant \alpha \min\{x^*_1, 1 - x^*_1, \ldots, x^*_n, 1 - x^*_n\} +$$
$$+ (1 - \alpha) \min\{x^{**}_1, 1 - x^{**}_1, \ldots, x^{**}_n, 1 - x^{**}_n\},$$

$$\alpha(1-x_k^*)+(1-\alpha)(1-x_k^{**}) \geqslant \alpha\min\{x_1^*,1-x_1^*,\ldots,x_n^*,1-x_n^*\}+ \\ +(1-\alpha)\min\{x_1^{**},1-x_1^{**},\ldots,x_n^{**},1-x_n^{**}\}.$$

Следовательно,

$$\min\{\alpha x_k^*+(1-\alpha)x_k^{**},\,\alpha(1-x_k^*)+(1-\alpha)(1-x_k^{**})\}_{k=1}^n \geqslant \\ \geqslant \alpha\min\{x_1^*,1-x_1^*,\ldots,x_n^*,1-x_n^*\}+ \\ +(1-\alpha)\min\{x_1^{**},1-x_1^{**},\ldots,x_n^{**},1-x_n^{**}\}.$$

Отсюда в силу того, что $A>0$, и выпуклости $g_{N_0}(x)$ получаем

$$g_{\text{new}}(\alpha x^*+(1-\alpha)x^{**}) = g_{N_0}(\alpha x^*+(1-\alpha)x^{**}) - \\ -A\min\{\alpha x_k^*+(1-\alpha)x_k^{**},1-\alpha x_k^*-(1-\alpha)x_k^{**}\}_{k=1}^n = \\ = g_{N_0}(\alpha x^*+(1-\alpha)x^{**}) - \\ -A\min\{\alpha x_k^*+(1-\alpha)x_k^{**},\alpha(1-x_k^*)+(1-\alpha)(1-x_k^{**})\}_{k=1}^n \leqslant \\ \leqslant \alpha g_{N_0}(x^*)+(1-\alpha)g_{N_0}(x^{**})-\alpha A\min\{x_1^*,1-x_1^*,\ldots,x_n^*,1-x_n^*\}- \\ -(1-\alpha)A\min\{x_1^{**},1-x_1^{**},\ldots,x_n^{**},1-x_n^{**}\} = \\ = \alpha g_{\text{new}}(x^*)+(1-\alpha)g_{\text{new}}(x^{**}).$$

Далее, заметим, что $g_{\text{new}}(x)<g_{N_0}(x)$ при $x\in\operatorname{int}\mathbb{K}^n$, поскольку $A>0$ и $\min\{x_1,1-x_1,x_2,1-x_2,\ldots,x_n,1-x_n\}>0$ при $x\in\operatorname{int}\mathbb{K}^n$. Отсюда непосредственно следует, что

$$g_{\text{new}}\left(\frac{1}{2},\frac{1}{2},\ldots,\frac{1}{2}\right)<g_{N_0}\left(\frac{1}{2},\frac{1}{2},\ldots,\frac{1}{2}\right)$$

и тем самым в силу выбора N_0 продолжение g_{new} на $\mathbb{K}^n$ функции f не принадлежит множеству S_C; противоречие. Теорема 1 доказана.

Замечание 2. Теорема 1 также доказывает, что не существует минимального выпуклого продолжения на $\mathbb{K}^n$ произвольной псевдобулевой функции f.

Далее докажем конструктивно, что для любой псевдобулевой функции f существует единственный максимум f_{DM} среди всех её выпуклых продолжений на $\mathbb{K}^n$.

Теорема 2. *Для произвольной псевдобулевой функции $f\colon\mathbb{B}^n\to\mathbb{R}$ функция*

$$f_{DM}(x)=\min_{\lambda\in\Lambda_{\mathbb{K}^n}(x)}\sum_{b\in\mathbb{B}^n}\lambda_b f(b)$$

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

Замечание 3. Функция f_{DM} корректно определена и непрерывна на $\mathbb{K}^n$ в силу компактности множества $\Lambda_{\mathbb{K}^n}(x)$ для любого $x \in \mathbb{K}^n$, непрерывности функции $\sum\limits_{b\in\mathbb{B}^n} \lambda_b f(b)$ и теоремы Вейерштрасса.

Доказательство теоремы 2. Сначала покажем, что для любого выпуклого продолжения g_C на $\mathbb{K}^n$ функции f имеет место неравенство

$$g_C(x) \leqslant f_{DM}(x), \quad x \in \mathbb{K}^n. \tag{5}$$

Действительно, если $x \in \mathbb{K}^n$, то $\Lambda_{\mathbb{K}^n}(x) \neq \varnothing$ в силу выпуклости множества $\mathbb{K}^n$. Ввиду выпуклости функции g_C и неравенства Йенсена [24] получаем

$$g_C(x) = g_C\Big(\sum_{b\in\mathbb{B}^n} \lambda_b b\Big) \leqslant \sum_{b\in\mathbb{B}^n} \lambda_b g_C(b) = \sum_{b\in\mathbb{B}^n} \lambda_b f(b)$$

для любого $\lambda \in \Lambda_{\mathbb{K}^n}(x)$. В частности,

$$g_C(x) \leqslant \min_{\lambda\in\Lambda_{\mathbb{K}^n}(x)} \sum_{b\in\mathbb{B}^n} \lambda_b f(b) = f_{DM}(x),$$

что доказывает справедливость (5).

Остаётся убедиться в том, что функция f_{DM} также является выпуклым продолжением f. Для этого достаточно показать, что

1) $f_{DM}(a) = f(a)$ для любого $a \in \mathbb{B}^n$;
2) функция f_{DM} выпукла на множестве $\mathbb{K}^n$.

1) Действительно, для любого $a \in \mathbb{B}^n$ имеем

$$f_{DM}(a) = \min_{\lambda\in\Lambda_{\mathbb{K}^n}(a)} \sum_{b\in\mathbb{B}^n} \lambda_b f(b) = f(a),$$

так как согласно следствию 2 множество $\Lambda_{\mathbb{K}^n}(a)$ состоит из одного вектора, в котором $\lambda_a = 1$, а на остальных местах нули.

2) Пусть $x^*, x^{**} \in \mathbb{K}^n$, $\alpha \in [0,1]$. По теореме Вейерштрасса существуют $\lambda^* \in \Lambda_{\mathbb{K}^n}(x^*)$ и $\lambda^{**} \in \Lambda_{\mathbb{K}^n}(x^{**})$ такие, что

$$f_{DM}(x^*) = \sum_{b\in\mathbb{B}^n} \lambda_b^* f(b), \quad f_{DM}(x^{**}) = \sum_{b\in\mathbb{B}^n} \lambda_b^{**} f(b).$$

Тогда

$$f_{DM}(\alpha x^* + (1-\alpha)x^{**}) = \min_{\lambda\in\Lambda_{\mathbb{K}^n}(\alpha x^*+(1-\alpha)x^{**})} \sum_{b\in\mathbb{B}^n} \lambda_b f(b) \leqslant$$

$$\leqslant \sum_{b\in\mathbb{B}^n} (\alpha\lambda_b^* + (1-\alpha)\lambda_b^{**}) f(b) = \alpha f_{DM}(x^*) + (1-\alpha) f_{DM}(x^{**}),$$

так как нетрудно заметить, что $\alpha\lambda^* + (1-\alpha)\lambda^{**} \in \Lambda_{\mathbb{K}^n}(\alpha x^* + (1-\alpha)x^{**})$. В силу произвольности x^*, x^{**} функция f_{DM} выпукла на $\mathbb{K}^n$.

Единственность максимума следует из (5) ввиду произвольности продолжения g_C на $\mathbb{K}^n$ функции f. Теорема 2 доказана.

3. Выпуклые продолжения дискретных функций вида $f\colon \mathbb{B}^n(a,b) \to \mathbb{R}$

В этом разделе конструктивно докажем, что для любой функции f, определённой на вершинах куба $\mathbb{K}^n(a,b)$, существует, во-первых, единственный максимум f_{DM} среди всех выпуклых продолжений на весь куб $\mathbb{K}^n(a,b)$ функции f, а во-вторых, бесконечно много таких продолжений.

Теорема 3. *Для произвольной дискретной функции $f\colon \mathbb{B}^n(a,b) \to \mathbb{R}$ функция*

$$f_{DM}(x) = \min_{\lambda \in \Lambda_{\mathbb{K}^n(a,b)}(x)} \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v f(v) \tag{6}$$

является единственным максимумом среди всех её выпуклых продолжений на $\mathbb{K}^n(a,b)$.

Замечание 4. Функция f_{DM} корректно определена и непрерывна на $\mathbb{K}^n(a,b)$. Обоснование этого аналогично обоснованию замечания 3.

Доказательство теоремы 3. Сначала покажем, что для любого выпуклого продолжения g_C на $\mathbb{K}^n(a,b)$ функции f имеет место неравенство

$$g_C(x) \leqslant f_{DM}(x), \quad x \in \mathbb{K}^n(a,b). \tag{7}$$

Действительно, если $x \in \mathbb{K}^n(a,b)$, то $\Lambda_{\mathbb{K}^n(a,b)}(x) \neq \varnothing$ ввиду выпуклости множества $\mathbb{K}^n(a,b)$. В силу выпуклости функции g_C и неравенства Йенсена [24] получаем

$$g_C(x) = g_C\Big(\sum_{v \in \mathbb{B}^n(a,b)} \lambda_v v\Big) \leqslant \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v g_C(v) = \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v f(v)$$

для любого $\lambda \in \Lambda_{\mathbb{K}^n(a,b)}(x)$. В частности,

$$g_C(x) \leqslant \min_{\lambda \in \Lambda_{\mathbb{K}^n(a,b)}(x)} \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v f(v) = f_{DM}(x),$$

что доказывает справедливость (7).

Остаётся убедиться в том, что функция f_{DM} также является выпуклым продолжением f. Для этого достаточно показать, что

1) $f_{DM}(u) = f(u)$ для любого $u \in \mathbb{B}^n(a,b)$;
2) функция f_{DM} выпукла на множестве $\mathbb{K}^n(a,b)$.

1) Действительно, для любого $u \in \mathbb{B}^n(a,b)$ имеем

$$f_{DM}(u) = \min_{\lambda \in \Lambda_{\mathbb{K}^n(a,b)}(u)} \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v f(v) = f(u),$$

так как согласно следствию 1 множество $\Lambda_{\mathbb{K}^n(a,b)}(u)$ состоит из одного вектора, в котором $\lambda_u = 1$, а на остальных местах нули.

2) Пусть $x^*, x^{**} \in \mathbb{K}^n(a,b)$, $\alpha \in [0,1]$. По теореме Вейерштрасса существуют $\lambda^* \in \Lambda_{\mathbb{K}^n(a,b)}(x^*)$ и $\lambda^{**} \in \Lambda_{\mathbb{K}^n(a,b)}(x^{**})$ такие, что

$$f_{DM}(x^*) = \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v^* f(v), \quad f_{DM}(x^{**}) = \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v^{**} f(v).$$

Тогда

$$f_{DM}(\alpha x^* + (1-\alpha)x^{**}) = \min_{\lambda \in \Lambda_{\mathbb{K}^n(a,b)}(\alpha x^* + (1-\alpha)x^{**})} \sum_{v \in \mathbb{B}^n(a,b)} \lambda_v f(v) \leqslant$$

$$\leqslant \sum_{v \in \mathbb{B}^n(a,b)} (\alpha\lambda_v^* + (1-\alpha)\lambda_v^{**}) f(v) = \alpha f_{DM}(x^*) + (1-\alpha) f_{DM}(x^{**}),$$

так как нетрудно заметить, что $\alpha\lambda^* + (1-\alpha)\lambda^{**} \in \Lambda_{\mathbb{K}^n(a,b)}(\alpha x^* + (1-\alpha)x^{**})$. В силу произвольности x^*, x^{**} функция f_{DM} выпукла на $\mathbb{K}^n(a,b)$.

Единственность максимума следует из (7) в силу произвольности продолжения g_C на $\mathbb{K}^n(a,b)$ функции f. Теорема 3 доказана.

Теорема 4. *Для произвольной дискретной функции $f\colon \mathbb{B}^n(a,b) \to \mathbb{R}$ существует бесконечно много её выпуклых продолжений на $\mathbb{K}^n(a,b)$.*

Доказательство. Существование для функции f выпуклого продолжения на $\mathbb{K}^n(a,b)$ доказано в теореме 3, согласно которой таковым является функция f_{DM}, определённая в (6). Бесконечность множества таких продолжений докажем от противного.

Пусть имеется конечное множество $S_C = \{g_1, g_2, \ldots, g_N\}$ выпуклых продолжений на $\mathbb{K}^n(a,b)$ функции f. Тогда найдётся $N_0 \in \{1, 2, \ldots, N\}$ такое, что для любого $k \in \{1, 2, \ldots, N\}$ имеем

$$g_{N_0}\Big(\frac{a+b}{2}, \frac{a+b}{2}, \ldots, \frac{a+b}{2}\Big) \leqslant g_k\Big(\frac{a+b}{2}, \frac{a+b}{2}, \ldots, \frac{a+b}{2}\Big).$$

Рассмотрим функцию

$$g_{\text{new}}(x) = g_{N_0}(x) - A \min\{x_k - a,\, b - x_k\}_{k=1}^n,$$

где $A > 0$ — произвольное число. Аналогично доказательству бесконечности в теореме 1 нетрудно показать, что, с одной стороны, функция g_{new} также является выпуклым продолжением на $\mathbb{K}^n(a,b)$ функции f, а с другой стороны, в силу выбора N_0 это выпуклое продолжение не принадлежит множеству S_C; противоречие. Теорема 4 доказана.

Замечание 5. Теорема 4 также доказывает, что не существует минимального выпуклого продолжения на $\mathbb{K}^n(a,b)$ произвольной дискретной функции $f\colon \mathbb{B}^n(a,b) \to \mathbb{R}$.

4. Выпуклые продолжения дискретных функций вида $f\colon \mathbb{BP}^n \to \mathbb{R}$

В этом разделе конструктивно докажем, что для любой функции f, определённой на вершинах параллелепипеда $\mathbb{P}^n$, существуют, во-первых, единственный максимум f_{DM} среди всех выпуклых продолжений на весь параллелепипед $\mathbb{P}^n$ функции f а во-вторых, бесконечно много таких продолжений. Напомним, что параллелепипед $\mathbb{P}^n$ определяется парой различных точек $c = (c_1, c_2, \ldots, c_n)$, $d = (d_1, d_2, \ldots, d_n) \in \mathbb{R}^n$ таких, что $c_k < d_k$, $k \in \{1, 2, \ldots, n\}$.

Теорема 5. *Для произвольной дискретной функции $f\colon \mathbb{BP}^n \to \mathbb{R}$ функция*

$$f_{DM}(x) = \min_{\lambda \in \Lambda_{\mathbb{P}^n}(x)} \sum_{v \in \mathbb{BP}^n} \lambda_v f(v) \tag{8}$$

является единственным максимумом среди всех её выпуклых продолжений на $\mathbb{P}^n$.

Замечание 6. Функция f_{DM} корректно определена и непрерывна на $\mathbb{P}^n$. Обоснование этого аналогично обоснованию замечания 3.

Доказательство теоремы 5. Сначала покажем, что для любого выпуклого продолжения g_C на $\mathbb{P}^n$ функции f имеет место неравенство

$$g_C(x) \leqslant f_{DM}(x), \quad x \in \mathbb{P}^n. \tag{9}$$

Действительно, если $x \in \mathbb{P}^n$, то $\Lambda_{\mathbb{P}^n}(x) \neq \varnothing$ в силу выпуклости множества $\mathbb{P}^n$. Ввиду выпуклости функции g_C и неравенства Йенсена [24] получаем

$$g_C(x) = g_C\Big(\sum_{v \in \mathbb{BP}^n} \lambda_v v\Big) \leqslant \sum_{v \in \mathbb{BP}^n} \lambda_v g_C(v) = \sum_{v \in \mathbb{BP}^n} \lambda_v f(v)$$

для любого $\lambda \in \Lambda_{\mathbb{P}^n}(x)$. В частности,

$$g_C(x) \leqslant \min_{\lambda \in \Lambda_{\mathbb{P}^n}(x)} \sum_{v \in \mathbb{BP}^n} \lambda_v f(v) = f_{DM}(x),$$

что доказывает справедливость (9).

Остаётся убедиться в том, что функция f_{DM} также является выпуклым продолжением f. Для этого достаточно доказать, что

1) $f_{DM}(u) = f(u)$ для любого $u \in \mathbb{BP}^n$;
2) функция f_{DM} выпукла на множестве $\mathbb{P}^n$.

1) Действительно, для любого $u \in \mathbb{BP}^n$ имеем

$$f_{DM}(u) = \min_{\lambda \in \Lambda_{\mathbb{P}^n}(u)} \sum_{v \in \mathbb{BP}^n} \lambda_v f(v) = f(u),$$

так как согласно лемме 1 множество $\Lambda_{\mathbb{P}^n}(u)$ состоит из одного вектора, в котором $\lambda_u = 1$, а на остальных местах нули.

2) Пусть $x^*, x^{**} \in \mathbb{P}^n$, $\alpha \in [0,1]$. По теореме Вейерштрасса существуют $\lambda^* \in \Lambda_{\mathbb{P}^n}(x^*)$ и $\lambda^{**} \in \Lambda_{\mathbb{P}^n}(x^{**})$ такие, что

$$f_{DM}(x^*) = \sum_{v \in \mathbb{BP}^n} \lambda_v^* f(v), \quad f_{DM}(x^{**}) = \sum_{v \in \mathbb{BP}^n} \lambda_v^{**} f(v).$$

Тогда

$$f_{DM}(\alpha x^* + (1-\alpha)x^{**}) = \min_{\lambda \in \Lambda_{\mathbb{P}^n}(\alpha x^* + (1-\alpha)x^{**})} \sum_{v \in \mathbb{BP}^n} \lambda_v f(v) \leqslant$$

$$\leqslant \sum_{v \in \mathbb{BP}^n} (\alpha\lambda_v^* + (1-\alpha)\lambda_v^{**}) f(v) = \alpha f_{DM}(x^*) + (1-\alpha) f_{DM}(x^{**}),$$

так как нетрудно заметить, что $\alpha\lambda^* + (1-\alpha)\lambda^{**} \in \Lambda_{\mathbb{P}^n}(\alpha x^* + (1-\alpha)x^{**})$. В силу произвольности x^*, x^{**} функция f_{DM} выпукла на $\mathbb{P}^n$.

Единственность максимума следует из (9) в силу произвольности продолжения g_C на $\mathbb{P}^n$ функции f. Теорема 5 доказана.

Теорема 6. *Для произвольной дискретной функции $f\colon \mathbb{BP}^n \to \mathbb{R}$ существует бесконечно много её выпуклых продолжений на $\mathbb{P}^n$.*

Доказательство. Существование для функции f выпуклого продолжения на $\mathbb{P}^n$ доказано в теореме 5, согласно которой таковым является функция f_{DM}, определённая в (8). Бесконечность множества таких продолжений докажем от противного.

Пусть имеется конечное множество $S_C = \{g_1, g_2, \ldots, g_N\}$ выпуклых продолжений на $\mathbb{P}^n$ функции f. Тогда найдётся $N_0 \in \{1, 2, \ldots, N\}$ такое, что для любого $k \in \{1, 2, \ldots, N\}$ имеем

$$g_{N_0}\left(\frac{c+d}{2}\right) \leqslant g_k\left(\frac{c+d}{2}\right).$$

Рассмотрим функцию

$$g_{\text{new}}(x) = g_{N_0}(x) - A \min\{x_k - c_k,\, d_k - x_k\}_{k=1}^n,$$

где $A > 0$ — произвольное число. Аналогично доказательству бесконечности в теореме 1 нетрудно показать, что, с одной стороны, функция g_{new} также является выпуклым продолжением на $\mathbb{P}^n$ функции f, а с другой стороны, в силу выбора N_0 это выпуклое продолжение не принадлежит множеству S_C; противоречие. Теорема 6 доказана.

Замечание 7. Теорема 6 также доказывает, что не существует минимального выпуклого продолжения на $\mathbb{P}^n$ произвольной дискретной функции $f\colon \mathbb{BP}^n \to \mathbb{R}$.

Заключение

В настоящей работе рассмотрены выпуклые продолжения дискретных функций, заданных на вершинах n-мерного единичного куба $\mathbb{K}^n$, произвольного куба $\mathbb{K}^n(a,b)$ и параллелепипеда $\mathbb{P}^n$. В каждом конкретном случае конструктивно доказано, что для произвольной дискретной функции f, определённой на вершинах $\mathbb{G}$, где $\mathbb{G} \in \{\mathbb{K}^n, \mathbb{K}^n(a,b), \mathbb{P}^n\}$, во-первых, существует бесконечно много её выпуклых продолжений на множество $\mathbb{G}$, а во-вторых, указана функция вида $f_{DM}\colon \mathbb{G} \to \mathbb{R}$, которая является единственным максимумом среди всех выпуклых продолжений f на $\mathbb{G}$. Обосновано также, что функция f_{DM} непрерывна на $\mathbb{G}$.

Финансирование работы

Исследование выполнено за счёт бюджета Финансового университета при Правительстве Российской Федерации. Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Автор заявляет, что у него нет конфликта интересов.

Литература

1. **Armario J. A.** Boolean functions and permanents of Sylvester Hadamard matrices // Mathematics. 2021. V. 9, No. 2. Paper ID 177. 8 p. DOI: 10.3390/math9020177.
2. **Abdel-Gawad A. H., Atiya A. F., Darwish N. M.** Solution of systems of Boolean equations via the integer domain // Inf. Sci. 2010. V. 180, No. 2. P. 288–300. DOI: 10.1016/j.ins.2009.09.010.
3. **Brown F. M.** Boolean reasoning: The logic of Boolean equations. Boston: Kluwer Acad. Publ., 1990. 304 p.
4. **Hammer P. L., Rudeanu S.** Boolean methods in operations research and related areas. Heidelberg: Springer, 1968. 330 p.
5. **Bard G. V.** Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis: PhD Thes. College Park, MD: Univ. Maryland, 2007. 178 p.
6. **Faugère J.-C., Joux A.** Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases // Advances in cryptology — CRYPTO 2003. Proc. 23rd Annu. Int. Cryptology Conf. (Santa Barbara, USA, Aug. 17–21, 2003). Heidelberg: Springer, 2003. P. 44–60. (Lect. Notes Comput. Sci.; V. 2729). DOI: 10.1007/978-3-540-45146-4_3.
7. **Armknecht F.** Improving fast algebraic attacks // Fast software encryption. Rev. Pap. 11th Int. Workshop (Delhi, India, Feb. 5–7, 2004). Heidelberg: Springer, 2004. P. 65–82. DOI: 10.1007/978-3-540-25937-4_5.

8. **Bardet M., Faugère J.-C., Salvye B., Spaenlehauer P. J.** On the complexity of solving quadratic boolean systems // J. Complex. 2013. V. 29. P. 53–75. DOI: 10.1016/j.jco.2012.07.001.
9. **Courtois N. T.** Fast algebraic attacks on stream ciphers with linear feedback // Advances in cryptology — CRYPTO 2003. Proc. 23rd Annu. Int. Cryptology Conf. (Santa Barbara, USA, Aug. 17–21, 2003). Heidelberg: Springer, 2003. P. 176–194. (Lect. Notes Comput. Sci.; V. 2729). DOI: 10.1007/978-3-540-45146-4_11.
10. **Faugère J.-C.** A new efficient algorithm for computing Gröbner bases (F4) // J. Pure Appl. Algebra. 1999. V. 139. P. 61–88. DOI: 10.1016/S0022-4049(99)00005-5.
11. **Faugère J.-C.** A new efficient algorithm for computing Gröbner bases without reduction to zero (F5) // Proc. 2002 Int. Symp. Symbolic and Algebraic Computation (Lille, France, July 7–10, 2002). New York: ACM, 2002. P. 75–83. DOI: 10.1145/780506.780516.
12. **Liu M., Lin D., Pei D.** Fast algebraic attacks and decomposition of symmetric Boolean functions // IEEE Trans. Inf. Theory. 2011. V. 57. P. 4817–4821. DOI: 10.1109/TIT.2011.2145690.
13. **Файзуллин Р. Т., Дулькейт В. И., Огородников Ю. Ю.** Гибридный метод поиска приближённого решения задачи 3-выполнимость, ассоциированной с задачей факторизации // Тр. Ин-та математики и механики. 2013. Т. 19, № 2. С. 285–294.
14. **Gu J.** Global optimization for satisfiability (SAT) problem // IEEE Trans. Knowl. Data Eng. 1994. V. 6, No. 3. 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. V. 14, No. 1. P. 1–17. DOI: 10.1007/BF02952482.
16. **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. V. 15, No. 2. Paper ID 33. 22 p. DOI: 10.3390/a15020033.
17. **Barotov D. N., Barotov R. N., Soloviev V., Feklin V., Muzafarov D., Ergashboev T., Egamov Kh.** The development of suitable inequalities and their application to systems of logical equations // Mathematics. 2022. V. 10, No. 11. Paper ID 1851. 9 p. DOI: 10.3390/math10111851.
18. **Баротов Д. Н., Баротов Р. Н.** Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения // Вычисл. методы и программирование. 2023. Т. 24, вып. 1. С. 10–23. DOI: 10.26089/NumMet.v24r102.
19. **Barotov D. N., Osipov A., Korchagin S., Pleshakova E., Muzafarov D., Barotov R. N., Serdechnyi D.** Transformation method for solving system of Boolean algebraic equations // Mathematics. 2021. V. 9, No. 24. Paper ID 3299. 12 p. DOI: 10.3390/math9243299.
20. **Owen G.** Multilinear extensions of games // Manage. Sci. 1972. V. 18, No. 5-2. P. 64–79. DOI: 10.1287/mnsc.18.5.64.

21. Barotov D. N., Barotov R. N. Polylinear transformation method for solving systems of logical equations // Mathematics. 2022. V. 10, No. 6. Paper ID 918. 10 p. DOI: 10.3390/math10060918.

22. Barotov D. N. Target function without local minimum for systems of logical equations with a unique solution // Mathematics. 2022. V. 10, No. 12. Paper ID 2097. 8 p. DOI: 10.3390/math10122097.

23. Баротов Д. Н. Выпуклое продолжение булевой функции и его приложения // Дискрет. анализ и исслед. операций. 2024. Т. 31, № 1. С. 5–18.

24. Jensen J. L. W. V. Sur les fonctions convexes et les inégalités entre les valeurs moyennes // Acta Math. 1906. V. 30. P. 175–193. [French]. DOI: 10.1007/BF02418571.

Баротов Достонжон Нумонжонович

Статья поступила
7 декабря 2023 г.
После доработки —
12 февраля 2024 г.
Принята к публикации
22 марта 2024 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2024. Vol. 31, No. 3. P. 5–23

UDC 519.8+518.25 DOI: 10.33048/daio.2024.31.789

CONVEX CONTINUATIONS OF SOME DISCRETE FUNCTIONS

D. N. Barotov

Financial University under the Government of the Russian Federation,
4 Chetvyortyi Veshnyakovskii Passage, 109456 Moscow, Russia

E-mail: dnbarotov@fa.ru

Abstract. We construct convex continuations of discrete functions defined on the vertices of the n-dimensional unit cube $[0,1]^n$, an arbitrary cube $[a,b]^n$, and a parallelepiped $[c_1,d_1]\times[c_2,d_2]\times\cdots\times[c_n,d_n]$. In each of these cases, we constructively prove that, for any discrete function f defined on the vertices of $\mathbb{G}\in\{[0,1]^n,[a,b]^n,[c_1,d_1]\times[c_2,d_2]\times\cdots\times[c_n,d_n]\}$, first, there exist infinitely many convex continuations to the set $\mathbb{G}$, and second, there exists a unique function $f_{DM}\colon\mathbb{G}\to\mathbb{R}$ that is the maximum of convex continuations of f to $\mathbb{G}$. We also show that the function f_{DM} is continuous on $\mathbb{G}$. Bibliogr. 24.

Keywords: discrete function, convex continuation of a discrete function, Boolean function, pseudo-Boolean function.

References

1. **J. A. Armario,** Boolean functions and permanents of Sylvester Hadamard matrices, *Mathematics* **9** (2), ID 177 (2021), DOI: 10.3390/math9020177.
2. **A. H. Abdel-Gawad, A. F. Atiya,** and **N. M. Darwish,** Solution of systems of Boolean equations via the integer domain, *Inf. Sci.* **180** (2), 288–300 (2010), DOI: 10.1016/j.ins.2009.09.010.
3. **F. M. Brown,** *Boolean Reasoning: The Logic of Boolean Equations* (Kluwer Acad. Publ., Boston, 1990).
4. **P. L. Hammer** and **S. Rudeanu,** *Boolean Methods in Operations Research and Related Areas* (Springer, Heidelberg, 1968).
5. **G. V. Bard,** Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis, *PhD Thesis* (Univ. Maryland, College Park, MD, 2007).

English transl.: *Journal of Applied and Industrial Mathematics* **18** (3), 412–423 (2024), DOI: 10.1134/S1990478924030049.

6. **J.-C. Faugère** and **A. Joux,** Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases, in *Advances in Cryptology — CRYPTO 2003* (Proc. 23rd Annu. Int. Cryptology Conf., Santa Barbara, USA, Aug. 17–21, 2003) (Springer, Heidelberg, 2003), pp. 44–60 (Lect. Notes Comput. Sci., Vol. 2729), DOI: 10.1007/978-3-540-45146-4_3.
7. **F. Armknecht,** Improving fast algebraic attacks, in *Fast Software Encryption* (Rev. Pap. 11th Int. Workshop, Delhi, India, Feb. 5–7, 2004) (Springer, Heidelberg, 2004), pp. 65–82, DOI: 10.1007/978-3-540-25937-4_5.
8. **M. Bardet, J.-C. Faugère, B. Salvye,** and **P. J. Spaenlehauer,** On the complexity of solving quadratic boolean systems, *J. Complex.* **29**, 53–75 (2013), DOI: 10.1016/j.jco.2012.07.001.
9. **N. T. Courtois,** Fast algebraic attacks on stream ciphers with linear feedback, in *Advances in Cryptology — CRYPTO 2003* (Proc. 23rd Annu. Int. Cryptology Conf., Santa Barbara, USA, Aug. 17–21, 2003) (Springer, Heidelberg, 2003), pp. 176–194 (Lect. Notes Comput. Sci., Vol. 2729), DOI: 10.1007/978-3-540-45146-4_11.
10. **J.-C. Faugère,** A new efficient algorithm for computing Gröbner bases (F4), *J. Pure Appl. Algebra* **139**, 61–88 (1999), DOI: 10.1016/S0022-4049(99)00005-5.
11. **J.-C. Faugère,** A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in *Proc. 2002 Int. Symp. Symbolic and Algebraic Computation, Lille, France, July 7–10, 2002* (ACM, New York, 2002), pp. 75–83, DOI: 10.1145/780506.780516.
12. **M. Liu, D. Lin,** and **D. Pei,** Fast algebraic attacks and decomposition of symmetric Boolean functions, *IEEE Trans. Inf. Theory* **57**, 4817–4821 (2011), DOI: 10.1109/TIT.2011.2145690.
13. **R. T. Faizullin, V. I. Dul'keit,** and **Yu. Yu. Ogorodnikov,** A hybrid method for the approximate solution of the 3-satisfiability problem associated with the factorization problem, *Tr. Inst. Mat. Mekh.* **19** (2), 285–294 (2013) [Russian].
14. **J. Gu,** Global optimization for satisfiability (SAT) problem, *IEEE Trans. Knowl. Data Eng.* **6** (3), 361–381 (1994), DOI: 10.1109/69.334864.
15. **J. Gu, Q. Gu,** and **D. Du,** On optimizing the satisfiability (SAT) problem, *J. Comput. Sci. Technol.* **14** (1), 1–17 (1999), DOI: 10.1007/BF02952482.
16. **A. I. Pakhomchik, V. V. Voloshinov, V. M. Vinokur,** and **G. B. Lesovik,** Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis, *Algorithms* **15** (2), ID 33 (2022), DOI: 10.3390/a15020033.
17. **D. N. Barotov, R. N. Barotov, V. Soloviev, V. Feklin, D. Muzafarov, T. Ergashboev,** and **Kh. Egamov,** The development of suitable inequalities and their application to systems of logical equations, *Mathematics* **10** (11), ID 1851 (2022), DOI: 10.3390/math10111851.
18. **D. N. Barotov** and **R. N. Barotov,** Polylinear continuations of some discrete functions and an algorithm for finding them, *Vychisl. Metody Program.* **24** (1), 10–23 (2023) [Russian], DOI: 10.26089/NumMet.v24r102.

19. D. N. Barotov, A. Osipov, S. Korchagin, E. Pleshakova, D. Muzafarov, R. N. Barotov, and **D. Serdechnyi,** Transformation method for solving system of Boolean algebraic equations, *Mathematics* **9** (24), ID 3299 (2021), DOI: 10.3390/math9243299.

20. G. Owen, Multilinear extensions of games, *Manage. Sci.* **18** (5-2), 64–79 (1972), DOI: 10.1287/mnsc.18.5.64.

21. D. N. Barotov and **R. N. Barotov,** Polylinear transformation method for solving systems of logical equations, *Mathematics* **10** (6), ID 918 (2022), DOI: 10.3390/math10060918.

22. D. N. Barotov, Target function without local minimum for systems of logical equations with a unique solution, *Mathematics* **10** (12), ID 2097 (2022), DOI: 10.3390/math10122097.

23. D. N. Barotov, Convex continuation of a Boolean function and its applications, *Diskretn. Anal. Issled. Oper.* **31** (1), 5–18 (2024) [Russian] [*J. Appl. Ind. Math.* **18** (1), 1–9 (2024)].

24. J. L. W. V. Jensen, Sur les fonctions convexes et les inégalités entre les valeurs moyennes, *Acta Math.* **30**, P. 175–193 (1906) [French], DOI: 10.1007/BF02418571.

Dostonjon N. Barotov

Received December 7, 2023
Revised February 12, 2024
Accepted March 22, 2024