2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

doi 10.26089/NumMet.v24r102 УДК 512.563

Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения

Д. Н. Баротов
Финансовый университет при Правительстве РФ,
департамент анализа данных и машинного обучения,
Москва, Российская Федерация
ORCID: 0000-0001-5047-7710, e-mail: DNBarotov@fa.ru

Р. Н. Баротов
Худжандский государственный университет имени академика Б. Гафурова,
кафедра математического анализа имени профессора А. Мухсинова,
Худжанд, Таджикистан
ORCID: 0000-0003-3729-6143, e-mail: ruzmet.tj@mail.ru

Аннотация: Исследована проблема существования и единственности полилинейных продолжений некоторых дискретных функций. Доказано, что для любой булевой функции существует соответствующее полилинейное продолжение и оно единственно. Предложен алгоритм нахождения полилинейного продолжения булевой функции и доказана его корректность. На основе предложенного алгоритма найдены явные формы полилинейных продолжений сначала для булевой функции, а затем для произвольной функции, определенной на множестве вершин n-мерного единичного куба, произвольного куба и параллелепипеда, и в каждом конкретном случае доказана единственность соответствующего полилинейного продолжения.

Ключевые слова: полилинейные функции, гармонические функции, системы булевых уравнений, псевдобулевы функции, алгоритмы.

Для цитирования: Баротов Д.Н., Баротов Р.Н. Полилинейные продолжения некоторых дискретных функций и алгоритм их нахождения // Вычислительные методы и программирование. 2023. **24**, № 1. 10–23. doi 10.26089/NumMet.v24r102.

Polylinear continuations of some discrete functions and an algorithm for finding them

Dostonjon N. Barotov
Financial University under the Government of the Russian Federation,
Department of Data Analysis and Machine Learning,
Moscow, Russia
ORCID: 0000-0001-5047-7710, e-mail: DNBarotov@fa.ru

Ruziboy N. Barotov
Khujand state university named after academician Bobojon Gafurov,
Department of Mathematical Analysis named after Professor A. Mukhsinov,
Khujand, Tajikistan
ORCID: 0000-0003-3729-6143, e-mail: ruzmet.tj@mail.ru

Abstract: In this paper, we study the existence and uniqueness of polylinear continuations of some discrete functions. It is proved that for any Boolean function, there exists a corresponding polylinear

© Д. Н. Баротов, Р. Н. Баротов

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

continuation and it is unique. An algorithm for finding a polylinear continuation of a Boolean function is proposed and its correctness is proved. Based on the result of the proposed algorithm, explicit forms of polylinear continuations are found first for a Boolean function and then for an arbitrary function defined only at the vertices of an n-dimensional unit cube, an arbitrary cube, and a parallelepiped, and in each particular case the uniqueness of the corresponding polylinear continuations is proved.

Keywords: polylinear functions, harmonic functions, systems of Boolean equations, pseudo-Boolean functions, algorithms.

For citation: D. N. Barotov, R. N. Barotov, "Polylinear continuations of some discrete functions and an algorithm for finding them," Numerical Methods and Programming. **24** (1), 10–23 (2023). doi 10.26089/NumMet.v24r102.

1. Введение. Система логических уравнений или задача выполнимости булевых формул (SAT) — одна из наиболее трудно решаемых задач математики и компьютерных наук, имеющая также значение для приложений [1–3]. В связи с этим развивается множество новых направлений и алгоритмов решения систем логических уравнений. Одно из направлений заключается в том, что, во-первых, система логических 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 [4], либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [2], либо к эквивалентной системе полиномиальных уравнений, решаемой символьными методами [5].

Имеется много способов, позволяющих преобразовать систему логических уравнений в задачу непрерывной минимизации [1, 6–11]. Но одна из основных проблем, возникающая 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 [1, 3, 7–10, 12]. По теореме Д. Н. Баротова [12], полилинейное продолжение булевой функции играет важную роль в том числе и для уменьшения числа локальных минимумов целевой функции. Поэтому с учетом этой мотивации в данной статье рассматривается полилинейное продолжение некоторых дискретных функций. В результате исследования найдены алгебраические явные формы полилинейных продолжений некоторых дискретных функций, заданных на множестве вершин n-мерного единичного куба, произвольного куба и параллелепипеда, т.е. явные формы не зависят от какого-либо условного оператора "если" или другого алгоритма.

Определение. Функцию $f(x_1, x_2, \ldots, x_n)$ будем называть полилинейной функцией, если она линейна по каждому из своих аргументов.

Пусть $\mathcal{B}^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in \{0, 1\}\}$ — множество всевозможных двоичных слов (булевых векторов) длины n, $\mathcal{K}^n = \{(x_1, x_2, \ldots, x_n) : 0 \leqslant x_1, x_2, \ldots, x_n \leqslant 1\}$ — n-мерный куб, натянутый на булевы векторы длины n.

Пусть $\mathcal{B}^n(a, b) = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in \{a, b\}\}$ и $\mathcal{K}^n(a, b) = \{(x_1, x_2, \ldots, x_n) : a \leqslant x_1, x_2, \ldots, x_n \leqslant b\}$.

Пусть $\mathcal{BP}^n = \{(x_1, x_2, \ldots, x_n) : x_1 \in \{a_1, b_1\}, x_2 \in \{a_2, b_2\}, \ldots, x_n \in \{a_n, b_n\}\}$ и $\mathcal{P}^n = \{(x_1, x_2, \ldots, x_n) : a_1 \leqslant x_1 \leqslant b_1, a_2 \leqslant x_2 \leqslant b_2, \ldots, a_n \leqslant x_n \leqslant b_n\}$.

2. Формы полилинейного продолжения логической функции $\mathrm{xor}(x_1, x_2, \ldots, x_n)$ **и его некоторые свойства.** В этом разделе конструируем полилинейное продолжение логической функции $\mathrm{xor}(x_1, x_2, \ldots, x_n)$. Для построения полилинейного продолжающего полинома исходим из того, что логическую двуместную функцию $\mathrm{xor}(x_1, x_2)$ (сложение по модулю 2) можно представить в виде полинома

$$\mathrm{xor}_D(x_1, x_2) = x_1 + x_2 - 2x_1x_2 \tag{1}$$

с обычными операциями сложения и умножения чисел. Данный полином внутри квадрата $\mathcal{K}^2$ является гармонической функцией и во внутренних точках квадрата принимает значения строго между 0 и 1. При этом в вершинах квадрата $\mathcal{K}^2$ полином принимает значение 0, если $(x_1, x_2) \in \{(0, 0), (1, 1)\}$, и значение 1,

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

если $(x_1, x_2) \in \{(0,1),(1,0)\}$, так как

$$0 \leqslant (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 \leqslant x_1 + x_2 - 2x_1x_2 = \operatorname{xor}_D(x_1, x_2) =$$
$$= x_1(1-x_2) + x_2(1-x_1) \leqslant \sqrt{x_1(1-x_2)} + \sqrt{x_2(1-x_1)} \leqslant$$
$$\leqslant \frac{1}{2}(x_1 + 1 - x_2) + \frac{1}{2}(x_2 + 1 - x_1) = 1, \quad \forall (x_1, x_2) \in \mathcal{K}^2.$$

Построим многомерный аналог полинома $\operatorname{xor}_D(x_1, x_2)$ рекуррентной формулой

$$\operatorname{xor}_D(x_1, x_2, \ldots, x_n) = \operatorname{xor}_D(\operatorname{xor}_D(x_1, \ldots, x_{n-1}), x_n). \tag{2}$$

Тогда справедлива следующая формула:

$$\operatorname{xor}_D(x_1, x_2, \ldots, x_n) = \frac{1}{2} - \frac{1}{2}(1-2x_1)(1-2x_2)\ldots(1-2x_n). \tag{3}$$

Действительно, при $n = 2$ формула справедлива в силу (1), а при $n > 2$, применив индукцию, получим:

$$\operatorname{xor}_D(x_1, x_2, \ldots, x_n) = \frac{1}{2} - \frac{1}{2}\left(1 - 2\operatorname{xor}_D(x_1, \ldots, x_{n-1})\right)(1-2x_n) =$$
$$= \frac{1}{2} - \frac{1}{2}\left(1 - 2\left(\frac{1}{2} - \frac{1}{2}(1-2x_1)(1-2x_2)\ldots(1-2x_{n-1})\right)\right)(1-2x_n) =$$
$$= \frac{1}{2} - \frac{1}{2}(1-2x_1)(1-2x_2)\ldots(1-2x_n).$$

Полином $\operatorname{xor}_D(x_1, x_2, \ldots, x_n)$, построенный и определяемый формулами (2) и (3), можно интерпретировать как многомерный алгебраический аналог логической двуместной функции $\operatorname{xor}(x, y)$ (сложение по модулю 2).

Теперь сформулируем и докажем основные свойства полинома $\operatorname{xor}_D(x_1, x_2, \ldots, x_n)$.

Утверждение 1. *Если* $(x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$ *и* $\operatorname{xor}_D(x_1, x_2, \ldots, x_n) = \frac{1}{2} - \frac{1}{2}(1-2x_1)(1-2x_2)\ldots(1-2x_n)$*, то справедливы следующие свойства:*

1°. *Полином* $\operatorname{xor}_D(x_1, x_2, \ldots, x_n)$ *в вершинах* n*-мерного куба* $\mathcal{K}^n$ *принимает одно из значений* 0 *или* 1.

2°. *Полином* $\operatorname{xor}_D(x_1, x_2, \ldots, x_n)$ *и его сужения на ребрах и гранях* n*-мерного куба* $\mathcal{K}^n$ *являются гармоническими функциями.*

3°. *Полином* $\operatorname{xor}_D(x_1, x_2, \ldots, x_n)$ *в* n*-мерном кубе* $\mathcal{K}^n$ *принимает значения* 0 *и* 1 *лишь в вершинах.*

4°. *Полином* $\operatorname{xor}_D(x_1, x_2, \ldots, x_n)$ *в вершине* n*-мерного куба* $\mathcal{K}^n$ *принимает значение* 0 (1) *тогда и только тогда, когда сумма координат вершины четна (нечетна).*

Доказательство.

1°. Действительно, для любого булевого вектора $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$ имеем: $(1-2x_1)(1-2x_2)\ldots(1-2x_n) \in \{-1, 1\}$, следовательно, согласно формуле (3), $\operatorname{xor}_D(x_1, x_2, \ldots, x_n) \in \{0, 1\}$.

2°. Данное свойство непосредственно вытекает из равенства

$$\frac{\partial^2}{\partial x_k^2}\left(\operatorname{xor}_D(x_1, x_2, \ldots, x_n)\right) = 0, \quad k = 1, \ldots, n.$$

Из свойств 1° и 2° следует, что $0 \leqslant \operatorname{xor}_D(x_1, x_2, \ldots, x_n) \leqslant 1$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$, так как общеизвестно, что любая функция, гармоническая внутри ограниченной области и непрерывная на замыкании области, принимает наибольшее и наименьшее значения на границе области.

3°. Действительно, если $(x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$, то включение $\operatorname{xor}_D(x_1, x_2, \ldots, x_n) \in \{0, 1\}$, согласно формуле (3), равносильно включению $(1-2x_1)(1-2x_2)\ldots(1-2x_n) \in \{-1, 1\}$. Последнее имеет место лишь в том случае, когда все множители по модулю равны 1. Следовательно, $\operatorname{xor}_D(x_1, x_2, \ldots, x_n) \in \{0, 1\}$, $(x_1, x_2, \ldots, x_n) \in \mathcal{K}^n \iff (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$.

4°. Проверяется по аналогии со свойством 3°: если $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, то $\operatorname{xor}_D(x_1, x_2, \ldots, x_n) = 0 \iff (1-2x_1)(1-2x_2)\ldots(1-2x_n) = 1 \iff (-1)^{x_1}(-1)^{x_2}\ldots(-1)^{x_n} = 1 \iff (x_1 + x_2 + \cdots + x_n)$ — четное число.

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

3. Формы полилинейного продолжения логической функции $\mathrm{and}(x_1, x_2, \ldots, x_n)$ **и его некоторые свойства.** В этом разделе конструируем полилинейное продолжение логической функции $\mathrm{and}(x_1, x_2, \ldots, x_n)$. Для построения полилинейного продолжающего полинома исходим из того, что логическую двуместную функцию $\mathrm{and}(x_1, x_2)$ можно представить в виде полинома

$$\mathrm{and}_D(x_1, x_2) = x_1 x_2$$

с обычными операциями сложения и умножения чисел. Данный полином внутри квадрата $\mathcal{K}^2$ является гармонической функцией и во внутренних точках квадрата принимает значения строго между 0 и 1. При этом в вершинах квадрата $\mathcal{K}^2$ полином принимает значение 0, если $x_1 = 0$ или $x_2 = 0$, и значение 1, если $(x_1, x_2) = (1, 1)$.

Построим многомерный аналог полинома $\mathrm{and}_D(x_1, x_2)$ рекуррентной формулой

$$\mathrm{and}_D(x_1, x_2, \ldots, x_n) = \mathrm{and}_D(\mathrm{and}_D(x_1, \ldots, x_{n-1}), x_n).$$

Тогда очевидно, что справедлива следующая формула:

$$\mathrm{and}_D(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n. \tag{4}$$

Теперь сформулируем и докажем основные свойства полинома $\mathrm{and}_D(x_1, x_2, \ldots, x_n)$.

Утверждение 2. *Если* $(x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$ *и* $\mathrm{and}_D(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$, *то справедливы следующие свойства:*

1°. *Полином* $\mathrm{and}_D(x_1, x_2, \ldots, x_n)$ *в вершинах* n*-мерного куба* $\mathcal{K}^n$ *принимает одно из значений* 0 *или* 1.

2°. *Полином* $\mathrm{and}_D(x_1, x_2, \ldots, x_n)$ *и его сужения на ребрах и гранях* n*-мерного куба* $\mathcal{K}^n$ *являются гармоническими функциями.*

3°. *Полином* $\mathrm{and}_D(x_1, x_2, \ldots, x_n)$ *в* n*-мерном кубе* $\mathcal{K}^n$ *принимает значение* 0, *если хотя бы одна из координат принимает значение* 0.

4°. *Полином* $\mathrm{and}_D(x_1, x_2, \ldots, x_n)$ *в вершине* n*-мерного куба* $\mathcal{K}^n$ *принимает значения* 1 *тогда и только тогда, когда* $(x_1, x_2, \ldots, x_n) = (1, 1, \ldots, 1)$.

Доказательство.

1°. Действительно, для любого булевого вектора $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$ имеем: $x_1 x_2 \ldots x_n \in \{0, 1\}$, следовательно, согласно формуле (4), $\mathrm{and}_D(x_1, x_2, \ldots, x_n) \in \{0, 1\}$.

2°. Данное свойство непосредственно вытекает из равенства

$$\frac{\partial^2}{\partial x_k^2} \left(\mathrm{and}_D(x_1, x_2, \ldots, x_n)\right) = 0, \quad k = 1, \ldots, n.$$

Из свойств 1° и 2° следует, что $0 \leqslant \mathrm{and}_D(x_1, x_2, \ldots, x_n) \leqslant 1$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$, так как общеизвестно, что любая функция, гармоническая внутри ограниченной области и непрерывная на замыкании области, принимает наибольшее и наименьшее значения на границе области.

3°. Действительно, $\mathrm{and}_D(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n = 0 \Longleftrightarrow x_1 = 0$, или $x_2 = 0$, …, или $x_n = 0$.

4°. Проверяется по аналогии со свойством 3°: если $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, то $\mathrm{and}_D(x_1, x_2, \ldots, x_n) = 1 \Longleftrightarrow x_1 x_2 \ldots x_n = 1 \Longleftrightarrow (x_1, x_2, \ldots, x_n) = (1, 1, \ldots, 1)$.

Теперь на основе утверждений 1, 2 докажем существование и единственность полилинейного продолжения для пар элементарных логических функций $\mathrm{xor}(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$, $\mathrm{and}(x_1, x_2, \ldots, x_n) = x_1 \otimes x_2 \otimes \ldots \otimes x_n$.

Лемма. *Для пар элементарных логических функций* $\mathrm{xor}(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$, $\mathrm{and}(x_1, x_2, \ldots, x_n) = x_1 \otimes x_2 \otimes \ldots \otimes x_n$ *существует пара* $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n)$ *полилинейных в* $\mathcal{K}^n$ *неотрицательных функций таких, что* $(\mathrm{xor}(x_1, x_2, \ldots, x_n), \mathrm{and}(x_1, x_2, \ldots, x_n)) = (f(x_1, x_2, \ldots, x_n), g(x_1, x_2, \ldots, x_n))$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, *и она единственна.*

Доказательство. Существование. Из утверждений 1, 2 следует, что в качестве пары $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n)$ можно взять $\mathrm{xor}_D(x_1, x_2, \ldots, x_n)$, $\mathrm{and}_D(x_1, x_2, \ldots, x_n)$, т.е.

$$(f(x_1, x_2, \ldots, x_n), g(x_1, x_2, \ldots, x_n)) = (\mathrm{xor}_D(x_1, x_2, \ldots, x_n), \mathrm{and}_D(x_1, x_2, \ldots, x_n)).$$

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

Единственность. Доказательство от противного: пусть существует другая пара $f_1(x_1, x_2, \ldots, x_n)$, $g_1(x_1, x_2, \ldots, x_n)$ полилинейных в $\mathcal{K}^n$ неотрицательных функций таких, что $(\mathrm{xor}(x_1, x_2, \ldots, x_n),\ \mathrm{and}(x_1, x_2, \ldots, x_n)) = (f_1(x_1, x_2, \ldots, x_n),\ g_1(x_1, x_2, \ldots, x_n))$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$. Тогда рассмотрим разность $(d_1(x_1, x_2 \ldots, x_n),\ d_2(x_1, x_2 \ldots, x_n)) = (\mathrm{xor}_D(x_1, x_2, \ldots, x_n) - f_1(x_1, x_2, \ldots, x_n),\ \mathrm{and}_D(x_1, x_2, \ldots, x_n) - g_1(x_1, x_2, \ldots, x_n))$. Заметим, что, во-первых, если $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, то $(d_1(x_1, x_2, \ldots, x_n),\ d_2(x_1, x_2, \ldots, x_n)) = (\mathrm{xor}(x_1, x_2, \ldots, x_n) - \mathrm{xor}(x_1, x_2, \ldots, x_n),\ \mathrm{and}(x_1, x_2, \ldots, x_n) - \mathrm{and}(x_1, x_2, \ldots, x_n)) = (0, 0)$. Во-вторых, функции $d_1(x_1, x_2, \ldots, x_n)$, $d_2(x_1, x_2, \ldots, x_n)$ полилинейны, так как

$$\left(\frac{\partial^2}{\partial x_k^2} \left(d_1(x_1, x_2, \ldots, x_n) \right), \frac{\partial^2}{\partial x_k^2} \left(d_2(x_1, x_2, \ldots, x_n) \right) \right) = (0 - 0, 0 - 0) = (0, 0), \quad k = 1, \ldots, n.$$

Из полилинейности функций $d_1(x_1, x_2, \ldots, x_n)$, $d_2(x_1, x_2, \ldots, x_n)$ и принципа максимума следуют неравенства [3, 4]

$$0 = \min_{(b_1, \ldots, b_n) \in \mathcal{B}^n} d_1(b_1, \ldots, b_n) \leqslant d_1(x_1, x_2, \ldots, x_n) \leqslant \max_{(b_1, \ldots, b_n) \in \mathcal{B}^n} d_1(b_1, \ldots, b_n) = 0,$$

$$0 = \min_{(b_1, \ldots, b_n) \in \mathcal{B}^n} d_2(b_1, \ldots, b_n) \leqslant d_2(x_1, x_2, \ldots, x_n) \leqslant \max_{(b_1, \ldots, b_n) \in \mathcal{B}^n} d_2(b_1, \ldots, b_n) = 0,$$

$$\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n.$$

Отсюда $(d_1(x_1, x_2, \ldots, x_n), d_2(x_1, x_2, \ldots, x_n)) \equiv (0, 0)$ или $(f_1(x_1, x_2, \ldots, x_n),\ g_1(x_1, x_2, \ldots, x_n)) \equiv (\mathrm{xor}_D(x_1, x_2, \ldots, x_n), \mathrm{and}_D(x_1, x_2, \ldots, x_n))$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$. Лемма доказана.

4. Полилинейное продолжение произвольного полинома Жегалкина $p(x_1, x_2, \ldots, x_n)$ и алгоритм его конструирования. В этом разделе алгоритмически конструируем полилинейное продолжение любого полинома Жегалкина $p(x_1, x_2, \ldots, x_n)$ и докажем корректность предлагаемого алгоритма.

Теорема 1. *Для произвольного полинома Жегалкина*

$$p(x_1, x_2, \ldots, x_n) = \bigoplus_{(b_1, \ldots, b_n) \in \mathcal{B}^n} c(b_1, b_2, \ldots, b_n) \otimes x_1^{b_1} \otimes x_2^{b_2} \otimes \cdots \otimes x_n^{b_n}$$

существует $p_D(x_1, x_2, \ldots, x_n)$ — полилинейная в $\mathcal{K}^n$ неотрицательная функция такая, что $p(x_1, x_2, \ldots, x_n) = p_D(x_1, x_2, \ldots, x_n)$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, и она единственна.

Доказательство. Сначала по заданному полиному Жегалкина $p(x_1, x_2, \ldots, x_n)$ конструируем соответствующую промежуточную функцию:

$$p_0(x_1, x_2, \ldots, x_n) = \frac{1}{2} - \frac{1}{2} \prod_{(b_1, \ldots, b_n) \in \mathcal{B}^n} \left(1 - 2c\left(b_1, \ldots, b_n\right) x_1^{b_1} \ldots x_n^{b_n} \right).$$

Из утверждений 1, 2 следует, что, во-первых, если $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, то $p(x_1, x_2, \ldots, x_n) = p_0(x_1, x_2, \ldots, x_n)$, во-вторых, если $(x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$, то $0 \leqslant p_0(x_1, x_2, \ldots, x_n) \leqslant 1$.

В общем случае полином $p_0(x_1, x_2, \ldots, x_n)$ неполилинейный, несложно привести контрпример. Модифицируя полином $p_0(x_1, x_2, \ldots, x_n)$, находим $p_D(x_1, x_2, \ldots, x_n)$.

Если в разложении полинома $p_0(x_1, x_2, \ldots, x_n)$ все степени x_i^k, где $k \in \{2, 3, 4, \ldots\}$, заменить на x_i, то после замены полученный полином будет полиномом $p_D(x_1, x_2, \ldots, x_n)$.

Если разложим полином $p_0(x_1, x_2, \ldots, x_n)$ и сгруппируем по степеням x_i, то он будет иметь следующий вид:

$$p_0(x_1, x_2, \ldots, x_n) = a_m x_i^m + a_{m-1} x_i^{m-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0,$$

где коэффициенты $a_j = a_j(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ — некоторые полиномы от $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$. Если все степени x_i^k, где $k \in \{2, 3, 4, \ldots\}$, заменить на x_i, то полученный полином примет вид $a_m x_i + a_{m-1} x_i + \ldots + a_2 x_i + a_1 x_i + a_0$, а это еще можно конструировать следующим образом:

$$\begin{aligned} a_m x_i + a_{m-1} x_i + \ldots + a_2 x_i + a_1 x_i + a_0 &= (a_m + a_{m-1} + \ldots + a_2 + a_1 + a_0) x_i - a_0 x_i + a_0 = \\ &= p_0(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) x_i - p_0(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)(x_i - 1) = \\ &= p_0(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) x_i + p_0(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)(1 - x_i). \end{aligned}$$

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

Алгоритм 1. Вычисление полилинейного продолжения

Algorithm 1. Calculating polylinear continuations

$\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$ — множество переменных, каждая из которых входит хотя бы в два монома полинома $p(x_1, x_2, \ldots, x_n)$

function *Transform*($\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$, $p_0(x_1, x_2, \ldots, x_n)$)
  for $s = 1 \ldots k$ **do**
    $p_s(x_1, x_2, \ldots, x_n) := p_{s-1}(x_1, x_2, \ldots, x_{i_s-1}, 1, x_{i_s+1}, \ldots, x_n)x_{i_s} + p_{s-1}(x_1, x_2, \ldots, x_{i_s-1}, 0, x_{i_s+1}, \ldots, x_n)(1 - x_{i_s})$
  end for
  $p_D(x_1, x_2, \ldots, x_n) := p_k(x_1, x_2, \ldots, x_n)$
  return $p_D(x_1, x_2, \ldots, x_n)$
end function

Обоснованием корректности алгоритма 1 являются следующие утверждения:

1°. $p_D(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n), \quad \forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$.

2°. Функция $p_D(x_1, x_2, \ldots, x_n)$ полилинейна.

3°. Если $(x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$, то $0 \leqslant p_D(x_1, x_2, \ldots, x_n) \leqslant 1$.

4°. $p_D(x_1, x_2, \ldots, x_n)$ — единственная полилинейная функция такая, что $p_D(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n), \ \forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$.

Докажем их справедливость. Обозначим $X_{\text{degree}} = \{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$.

1°. Действительно, так как $p_0(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n), \ \forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, и $0^k = 0$, $1^k = 1 \Longrightarrow p_D(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n), \forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$.

2°. Действительно, если $x_k \notin X_{\text{degree}}$, то $\dfrac{\partial^2}{\partial x_k^2}\left(p_D(x_1, x_2, \ldots, x_n)\right) = 0$, а если $x_k \in X_{\text{degree}}$, то $\dfrac{\partial^2}{\partial x_k^2}(p_D(x_1, x_2, \ldots, x_n)) = \dfrac{\partial^2}{\partial x_k^2}\left(a_m x_k + a_{m-1}x_k + \ldots + a_1 x_k + a_0\right) = 0$.

3°. Из свойств 1° и 2° следуют неравенства

$$0 \leqslant \min_{(b_1,\ldots,b_n)\in\mathcal{B}^n} p_D(b_1, \ldots, b_n) \leqslant p_D(x_1, x_2, \ldots, x_n) \leqslant \max_{(b_1,\ldots,b_n)\in\mathcal{B}^n} p_D(b_1, \ldots, b_n) \leqslant 1,$$

$$\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n.$$

4°. Доказательство от противного: пусть существует другая полилинейная функция $f_1(x_1, x_2, \ldots, x_n)$ такая, что $p(x_1, x_2, \ldots, x_n) = f_1(x_1, x_2, \ldots, x_n), \ \forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$. Тогда рассмотрим разность $d_1(x_1, x_2, \ldots, x_n) = p_D(x_1, x_2, \ldots, x_n) - f_1(x_1, x_2, \ldots, x_n)$. Заметим, что, во-первых, если $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, то $d_1(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n) - p(x_1, x_2, \ldots, x_n) = 0$. Во-вторых, функция $d_1(x_1, x_2, \ldots, x_n)$ полилинейна, так как $\dfrac{\partial^2}{\partial x_k^2}\left(d_1(x_1, x_2, \ldots, x_n)\right) = 0 - 0 = 0, \ k = 1, \ldots, n$. Из полилинейности функции $d_1(x_1, x_2, \ldots, x_n)$ и принципа максимума следуют неравенства [3, 4, 12]

$$0 = \min_{(b_1,\ldots,b_n)\in\mathcal{B}^n} d_1(b_1, \ldots, b_n) \leqslant d_1(x_1, x_2, \ldots, x_n) \leqslant \max_{(b_1,\ldots,b_n)\in\mathcal{B}^n} d_1(b_1, \ldots, b_n) = 0,$$

$$\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n.$$

Отсюда $d_1(x_1, x_2, \ldots, x_n) \equiv 0$ или $f_1(x_1, x_2, \ldots, x_n) \equiv p_D(x_1, x_2, \ldots, x_n), \ \forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$. Теорема доказана.

Теорема 2. *Результат предложенного алгоритма может быть представлен в следующем явном виде:*

$$p_D(x_1, x_2, \ldots, x_n) = \sum_{(b_1,b_2,\ldots,b_n)\in\mathcal{B}^n} p(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1)x_k + (1 - b_k)).$$

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

Доказательство. Применим индукцию по n.
1) Если $n = 1$, то

$$p_D(x_1) = (1 - x_1) \cdot p_D(0) + x_1 \cdot p_D(1) = \sum_{b_1 \in \mathcal{B}^1} p_D(b_1) \prod_{k=1}^{1} ((2b_k - 1)x_k + (1 - b_k)).$$

2) Если $n = m$, то предположим, что

$$p_D(x_1, x_2, \ldots, x_m) = \sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m} p_D(b_1, b_2, \ldots, b_m) \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k)).$$

3) Во-первых, из полилинейности $p_D(x_1, x_2, \ldots, x_m, x_{m+1})$ следует

$$p_D(x_1, x_2, \ldots, x_m, x_{m+1}) = p_D(x_1, x_2, \ldots, x_m, 0)(1 - x_{m+1}) + p_D(x_1, x_2, \ldots, x_m, 1)x_{m+1},$$

во-вторых, из 1)–2) следуют равенства

$$p_D(x_1, x_2, \ldots, x_m, 0) = \sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m} p_D(b_1, b_2, \ldots, b_m, 0) \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k)),$$

$$p_D(x_1, x_2, \ldots, x_m, 1) = \sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m} p_D(b_1, b_2, \ldots, b_m, 1) \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k)).$$

Отсюда

$$p_D(x_1, x_2, \ldots, x_m, x_{m+1}) = \left(\sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m} p_D(b_1, b_2, \ldots, b_m, 0) \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k)) \right) (1 - x_{m+1}) +$$

$$+ \left(\sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m} p_D(b_1, b_2, \ldots, b_m, 1) \cdot \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k)) \right) x_{m+1} =$$

$$= \sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m, b_{m+1}=0} p_D(b_1, b_2, \ldots, b_m, b_{m+1}) \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k))((2b_{m+1} - 1)x_{m+1} + (1 - b_{m+1})) +$$

$$+ \sum_{(b_1,b_2,\ldots,b_m) \in \mathcal{B}^m, b_{m+1}=1} p_D(b_1, b_2, \ldots, b_m, b_{m+1}) \prod_{k=1}^{m} ((2b_k - 1)x_k + (1 - b_k))((2b_{m+1} - 1)x_{m+1} + (1 - b_{m+1})) =$$

$$= \sum_{(b_1,b_2,\ldots,b_m,b_{m+1}) \in \mathcal{B}^{m+1}} p_D(b_1, b_2, \ldots, b_m, b_{m+1}) \prod_{k=1}^{m+1} ((2b_k - 1)x_k + (1 - b_k)).$$

Таким образом, во-первых, по индукции доказано, что

$$p_D(x_1, x_2, \ldots, x_n) = \sum_{(b_1,b_2,\ldots,b_n) \in \mathcal{B}^n} p_D(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1) \cdot x_k + (1 - b_k)), \quad \forall n \in \mathbb{N},$$

во-вторых, $p_D(b_1, b_2, \ldots, b_n) = p(b_1, b_2, \ldots, b_n), \ \forall (b_1, b_2, \ldots, b_n) \in \mathcal{B}^n$, и, следовательно,

$$p_D(x_1, x_2, \ldots, x_n) = \sum_{(b_1,b_2,\ldots,b_n) \in \mathcal{B}^n} p(b_1, b_2, \ldots, b_n) \cdot \prod_{k=1}^{n} ((2b_k - 1) \cdot x_k + (1 - b_k)).$$

Теорема доказана.

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

5. Полилинейное продолжение произвольной дискретной функции, определенной на множестве вершин параллелепипеда. В этом разделе на основе явного результата предложенного алгоритма конструируем единственное полилинейное продолжение произвольной дискретной функции, определенной на множестве вершин единичного куба, произвольного куба и параллелепипеда.

Следствие 1. *Пусть функция $f(x_1, x_2, \ldots, x_n)$ задана на множестве вершин единичного куба $\mathcal{K}^n$. Тогда полином*

$$f_D(x_1, x_2, \ldots, x_n) = \sum_{(b_1,b_2,\ldots,b_n)\in\mathcal{B}^n} f(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1)x_k + (1 - b_k))$$

является единственным полилинейным продолжением функции $f(x_1, x_2, \ldots, x_n)$ в $\mathcal{K}^n$.

Доказательство. *a*) Несложно заметить, что

$$f_D(b_1^*, b_2^*, \ldots, b_n^*) = f(b_1^*, b_2^*, \ldots, b_n^*), \quad \forall (b_1^*, b_2^*, \ldots, b_n^*) \in \mathcal{B}^n.$$

Действительно,

$$\begin{aligned}
f_D(b_1^*, b_2^*, \ldots, b_n^*) &= \sum_{(b_1,b_2,\ldots,b_n)\in\mathcal{B}^n} f(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1)b_k^* + (1 - b_k)) = \\
&= \sum_{(b_1,b_2,\ldots,b_n)=(b_1^*,b_2^*,\ldots,b_n^*)} f(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1)b_k^* + (1 - b_k)) + \\
&+ \sum_{(b_1,b_2,\ldots,b_n)\in\mathcal{B}^n\setminus(b_1^*,b_2^*,\ldots,b_n^*)} f(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1)b_k^* + (1 - b_k)) = \\
&= f(b_1^*, b_2^*, \ldots, b_n^*) \prod_{k=1}^{n} ((2b_k^* - 1)b_k^* + (1 - b_k^*)) + \sum_{(b_1,b_2,\ldots,b_n)\in\mathcal{B}^n\setminus(b_1^*,b_2^*,\ldots,b_n^*)} f(b_1, b_2, \ldots, b_n) \cdot 0 = \\
&= f(b_1^*, b_2^*, \ldots, b_n^*) \prod_{k=1}^{n} 1 + 0 = f(b_1^*, b_2^*, \ldots, b_n^*).
\end{aligned}$$

b) Единственность. Доказательство от противного: пусть существует другая полилинейная функция $f_{\text{different}}(x_1, x_2, \ldots, x_n)$ такая, что $f(x_1, x_2, \ldots, x_n) = f_{\text{different}}(x_1, x_2, \ldots, x_n)$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$. Тогда рассмотрим разность $d(x_1, x_2, \ldots, x_n) = f_D(x_1, x_2, \ldots, x_n) - f_{\text{different}}(x_1, x_2, \ldots, x_n)$. Заметим, что, во-первых, если $(x_1, x_2, \ldots, x_n) \in \mathcal{B}^n$, то $d(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) - f(x_1, x_2, \ldots, x_n) = 0$. Во-вторых, функция $d(x_1, x_2, \ldots, x_n)$ полилинейна как разность полилинейных функций. Из полилинейности функции $d(x_1, x_2, \ldots, x_n)$ и принципа максимума следуют неравенства [3, 4, 12]

$$0 = \min_{(b_1,\ldots,b_n)\in\mathcal{B}^n} d(b_1, \ldots, b_n) \leqslant d(x_1, x_2, \ldots, x_n) \leqslant \max_{(b_1,\ldots,b_n)\in\mathcal{B}^n} d(b_1, \ldots, b_n) = 0, \quad \forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n.$$

Отсюда $d(x_1, x_2, \ldots, x_n) \equiv 0$ или $f_{\text{different}}(x_1, x_2, \ldots, x_n) \equiv f_D(x_1, x_2, \ldots, x_n)$, $\forall (x_1, x_2, \ldots, x_n) \in \mathcal{K}^n$. Следствие доказано.

Теорема 3. *Пусть функция $f(x_1, x_2, \ldots, x_n)$ задана на множестве вершин куба $\mathcal{K}^n(a, b)$. Тогда полином*

$$\begin{aligned}
&f_D(x_1, x_2, \ldots, x_n) = \\
&= \sum_{(c_1,c_2,\ldots,c_n)\in\mathcal{B}^n} \left(f(a(1 - c_1) + bc_1, \ldots, a(1 - c_n) + bc_n) \prod_{k=1}^{n} \frac{(x_k - a)c_k + (b - x_k)(1 - c_k)}{b - a} \right)
\end{aligned}$$

является единственным полилинейным продолжением функции $f(x_1, x_2, \ldots, x_n)$ в $\mathcal{K}^n(a, b)$.

Доказательство. *a*) Несложно заметить, что

$$f_D(v_1^*, v_2^*, \ldots, v_n^*) = f(v_1^*, v_2^*, \ldots, v_n^*), \forall (v_1^*, v_2^*, \ldots, v_n^*) \in \mathcal{B}^n(a, b).$$

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

Действительно,

$$f_D(v_1^*, v_2^*, \ldots, v_n^*) =$$

$$= \sum_{(c_1,c_2,\ldots,c_n)\in\mathcal{B}^n} f(a(1-c_1)+bc_1, \ldots, a(1-c_n)+bc_n) \prod_{k=1}^{n} \frac{(v_k^*-a)c_k + (b-v_k^*)(1-c_k)}{b-a} =$$

$$= \left\{\exists!(c_1^*, c_2^*, \ldots, c_n^*) \in \mathcal{B}^n : (v_1^*, \ldots, v_n^*) = (a(1-c_1^*)+bc_1^*, \ldots, a(1-c_n^*)+bc_n^*)\right\} =$$

$$= \sum_{(c_1,\ldots,c_n)=(c_1^*,\ldots,c_n^*)} f(a(1-c_1)+bc_1, \ldots, a(1-c_n)+bc_n) \prod_{k=1}^{n} \frac{(v_k^*-a)c_k + (b-v_k^*)(1-c_k)}{b-a} +$$

$$+ \sum_{(c_1,\ldots,c_n)\in\mathcal{B}^n\setminus(c_1^*,\ldots,c_n^*)} f(a(1-c_1)+bc_1, \ldots, a(1-c_n)+bc_n) \prod_{k=1}^{n} \frac{(v_k^*-a)c_k + (b-v_k^*)(1-c_k)}{b-a} =$$

$$= f(v_1^*, v_2^*, \ldots, v_n^*) \prod_{k=1}^{n} \frac{b-a}{b-a} + \sum_{(c_1,\ldots,c_n)\in\mathcal{B}^n\setminus(c_1^*,\ldots,c_n^*)} f(a(1-c_1)+bc_1, \ldots, a(1-c_n)+bc_n) \cdot 0 =$$

$$= f(v_1^*, v_2^*, \ldots, v_n^*).$$

b) Единственность. Доказательство аналогично доказательству единственности в следствии 1. Теорема доказана.

Теорема 4. *Пусть функция $f(x_1, x_2, \ldots, x_n)$ задана на множестве вершин параллелепипеда $\mathcal{P}_n$. Тогда полином*

$$f_D(x_1, x_2, \ldots, x_n) =$$

$$= \sum_{(c_1,c_2,\ldots,c_n)\in\mathcal{B}^n} \left(f(a_1(1-c_1)+b_1c_1, \ldots, a_n(1-c_n)+b_nc_n) \prod_{k=1}^{n} \frac{(x_k-a_k)c_k + (b_k-x_k)(1-c_k)}{b_k-a_k} \right)$$

является единственным полилинейным продолжением функции $f(x_1, x_2, \ldots, x_n)$ в $\mathcal{P}^n$.

Доказательство. *a*) Несложно заметить, что

$$f_D(v_1^*, v_2^*, \ldots, v_n^*) = f(v_1^*, v_2^*, \ldots, v_n^*), \forall (v_1^*, v_2^*, \ldots, v_n^*) \in \mathcal{B}\mathcal{P}^n.$$

Действительно,

$$f_D(v_1^*, v_2^*, \ldots, v_n^*) =$$

$$= \sum_{(c_1,c_2,\ldots,c_n)\in\mathcal{B}^n} f(a_1(1-c_1)+b_1c_1, \ldots, a_n(1-c_n)+b_nc_n) \prod_{k=1}^{n} \frac{(v_k^*-a_k)c_k + (b_k-v_k^*)(1-c_k)}{b_k-a_k} =$$

$$= \left\{\exists!(c_1^*, c_2^*, \ldots, c_n^*) \in \mathcal{B}^n : (v_1^*, \ldots, v_n^*) = (a_1(1-c_1^*)+b_1c_1^*, \ldots, a_n(1-c_n^*)+b_nc_n^*)\right\} =$$

$$= \sum_{(c_1,\ldots,c_n)=(c_1^*,\ldots,c_n^*)} f(a_1(1-c_1)+b_1c_1, \ldots, a_n(1-c_n)+b_nc_n) \prod_{k=1}^{n} \frac{(v_k^*-a_k)c_k + (b_k-v_k^*)(1-c_k)}{b_k-a_k} +$$

$$+ \sum_{(c_1,\ldots,c_n)\in\mathcal{B}^n\setminus(c_1^*,\ldots,c_n^*)} f(a_1(1-c_1)+b_1c_1, \ldots, a_n(1-c_n)+b_nc_n) \prod_{k=1}^{n} \frac{(v_k^*-a_k)c_k + (b_k-v_k^*)(1-c_k)}{b_k-a_k} =$$

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

$$= f(v_1^*, v_2^*, \ldots, v_n^*) \prod_{k=1}^{n} \frac{b_k - a_k}{b_k - a_k} + \sum_{(c_1,\ldots,c_n)\in\mathcal{B}^n\setminus(c_1^*,\ldots,c_n^*)} f(a_1(1-c_1)+b_1c_1,\ldots,a_n(1-c_n)+b_nc_n)\cdot 0 =$$

$$= f(v_1^*, v_2^*, \ldots, v_n^*).$$

b) Единственность. Доказательство аналогично доказательству единственности в следствии 1. Теорема доказана.

6. Применение одной из полученных форм.

6.1. Конструирование системы полилинейных уравнений. В работах [3, 4] для приведения системы булевых уравнений к соответствующей системе полилинейных уравнений сначала система булевых уравнений

$$\begin{cases} p_1(x_1, x_2, \ldots, x_n) = \bigoplus\limits_{(b_1,\ldots,b_n)\in\mathcal{B}^n} c_1(b_1, b_2, \ldots, b_n) \otimes x_1^{b_1} \otimes x_2^{b_2} \otimes \cdots \otimes x_n^{b_n} = 0, \\ p_2(x_1, x_2, \ldots, x_n) = \bigoplus\limits_{(b_1,\ldots,b_n)\in\mathcal{B}^n} c_2(b_1, b_2, \ldots, b_n) \otimes x_1^{b_1} \otimes x_2^{b_2} \otimes \cdots \otimes x_n^{b_n} = 0, \\ \cdots \quad \cdots \quad \cdots, \\ p_m(x_1, x_2, \ldots, x_n) = \bigoplus\limits_{(b_1,\ldots,b_n)\in\mathcal{B}^n} c_m(b_1, b_2, \ldots, b_n) \otimes x_1^{b_1} \otimes x_2^{b_2} \otimes \cdots \otimes x_n^{b_n} = 0 \end{cases}$$

сводится к промежуточной системе

$$\begin{cases} f_1^*(x_1, x_2, \ldots, x_n) = \dfrac{1}{2} - \dfrac{1}{2} \prod\limits_{(b_1,\ldots,b_n)\in\mathcal{B}^n} (1 - 2c_1(b_1, \ldots, b_n) \cdot x_1^{b_1} \ldots x_n^{b_n}) = 0, \\ f_2^*(x_1, x_2, \ldots, x_n) = \dfrac{1}{2} - \dfrac{1}{2} \prod\limits_{(b_1,\ldots,b_n)\in\mathcal{B}^n} (1 - 2c_2(b_1, \ldots, b_n) \cdot x_1^{b_1} \ldots x_n^{b_n}) = 0, \\ \cdots \quad \cdots \quad \cdots, \\ f_m^*(x_1, x_2, \ldots, x_n) = \dfrac{1}{2} - \dfrac{1}{2} \prod\limits_{(b_1,\ldots,b_n)\in\mathcal{B}^n} (1 - 2c_m(b_1, \ldots, b_n) \cdot x_1^{b_1} \ldots x_n^{b_n}) = 0, \end{cases}$$

а затем каждое уравнение промежуточной системы модифицируется с помощью алгоритма и конструируется соответствующая система полилинейных уравнений

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0, \\ f_2(x_1, x_2, \ldots, x_n) = 0, \\ \cdots \quad \cdots \quad \cdots, \\ f_m(x_1, x_2, \ldots, x_n) = 0. \end{cases}$$

Собственно, применение одной из полученных форм заключается в том, что каждый полином последней системы $f_k(x_1, x_2, \ldots, x_n)$ можно конструировать сразу в явном виде

$$f_k(x_1, x_2, \ldots, x_n) =$$

$$= \sum_{(b_1,b_2,\ldots,b_n)\in\mathcal{B}^n} p_k(b_1, b_2, \ldots, b_n) \prod_{k=1}^{n} ((2b_k - 1)x_k + (1 - b_k)) =$$

$$= \sum_{p_k(b_1,b_2,\ldots,b_n)=1} \prod_{k=1}^{n} ((2b_k - 1)x_k + (1 - b_k)),$$

не используя промежуточную систему или алгоритм. Это значительно упрощает процесс конструирования соответствующей системы полилинейных уравнений.

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

6.2. Криптоанализ. Рассмотрим одну небольшую криптографическую задачу, а именно, рассмотрим систему булевых уравнений

$$\begin{cases}
x_1 \oplus x_3 \oplus y_1 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes x_2 \oplus x_1 \otimes x_3 \oplus x_0 \otimes y_1 \oplus y_2 \oplus 1 = 0,\\
x_0 \otimes x_1 \oplus x_0 \otimes x_3 \oplus x_0 \otimes y_1 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes x_2 \oplus x_0 \otimes y_1 \oplus x_1 \otimes y_1 \oplus x_1 \oplus y_2 \oplus 1 = 0,\\
x_0 \otimes x_3 \oplus x_0 \otimes y_1 \oplus x_0 \otimes y_2 \oplus x_1 \otimes y_2 \oplus x_0 \oplus x_1 \oplus y_2 \oplus 1 = 0,\\
x_0 \otimes y_3 \oplus x_1 \otimes y_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus y_2 \oplus y_3 = 0,\\
x_0 \otimes x_3 \oplus x_2 \otimes x_3 \oplus x_0 \oplus x_1 \oplus x_3 \oplus y_0 \oplus y_2 \oplus y_3 = 0,\\
x_1 \otimes x_2 \oplus x_1 \otimes y_0 \oplus x_2 \otimes y_0 \oplus x_0 \oplus x_2 \oplus x_3 \oplus y_0 \oplus y_3 \oplus 1 = 0,\\
x_1 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_2 \otimes y_1 \oplus x_0 \oplus x_1 \oplus x_3 \oplus y_0 \oplus y_2 \oplus y_3 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_0 \otimes y_0 \oplus x_1 \otimes y_0 \oplus x_0 \otimes y_1 \oplus x_0 \otimes y_2 \oplus x_2 \otimes y_2 \oplus x_1 \oplus x_3 \oplus y_2 \oplus y_3 = 0,\\
x_0 \otimes y_3 \oplus x_2 \otimes y_3 \oplus x_1 \oplus x_2 \oplus y_0 \oplus y_2 \oplus 1 = 0,\\
x_1 \otimes x_2 \oplus x_0 \otimes y_0 \oplus x_1 \otimes y_0 \oplus x_3 \otimes y_0 \oplus x_0 \otimes y_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus y_2 \oplus y_3 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes x_2 \oplus x_0 \otimes y_1 \oplus x_3 \otimes y_1 \oplus x_3 \oplus y_2 \oplus 1 = 0,\\
x_0 \otimes y_0 \oplus x_1 \otimes y_0 \oplus x_0 \otimes y_1 \oplus x_3 \otimes y_2 \oplus x_0 \oplus x_1 \oplus x_2 \oplus y_3 \oplus 1 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_0 \otimes y_3 \oplus x_3 \otimes y_3 \oplus x_0 \oplus x_1 \oplus x_3 \oplus y_0 \oplus y_2 \oplus y_3 = 0,\\
x_1 \otimes x_2 \oplus x_0 \otimes y_0 \oplus y_0 \otimes y_1 \oplus x_0 \otimes y_3 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus y_2 \oplus y_3 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes y_0 \oplus x_0 \otimes y_1 \oplus x_0 \otimes y_2 \oplus y_0 \otimes y_2 \oplus x_0 \otimes y_3 \oplus x_0 \oplus x_1 \oplus y_0 \oplus y_2 \oplus 1 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus y_0 \otimes y_3 \oplus x_1 \oplus y_2 \oplus 1 = 0,\\
x_0 \otimes x_3 \oplus x_0 \otimes y_0 \oplus x_1 \otimes y_0 \oplus x_0 \otimes y_2 \oplus y_1 \otimes y_2 \oplus x_2 \oplus y_2 \oplus y_3 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus y_1 \otimes y_3 \oplus x_2 \oplus y_0 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus y_2 \otimes y_3 \oplus x_0 \oplus x_2 \oplus x_3 \oplus 1 = 0,
\end{cases}$$

описывающую алгоритм (блок) шифрования S-KN2, где x_0, x_1, x_2, x_3 — входные биты S-KN2, а y_0, y_1, y_2, y_3 — выходные биты S-KN2, подробности приведены в статье [13]. Задача заключается в том, что по известным выходным битам $(y_0, y_1, y_2, y_3) = (y_0^*, y_1^*, y_2^*, y_3^*)$ нужно найти входные биты.

Пусть $(y_0, y_1, y_2, y_3) = (0, 0, 0, 0)$. Тогда соответствующая система примет следующий вид:

$$\begin{cases}
x_1 \oplus x_3 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes x_2 \oplus x_1 \otimes x_3 \oplus 1 = 0,\\
x_0 \otimes x_1 \oplus x_0 \otimes x_3 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes x_2 \oplus x_1 \oplus 1 = 0,\\
x_0 \otimes x_3 \oplus x_0 \oplus x_1 \oplus 1 = 0,\\
x_0 \oplus x_1 \oplus x_2 \oplus x_3 = 0,\\
x_0 \otimes x_3 \oplus x_2 \otimes x_3 \oplus x_0 \oplus x_1 \oplus x_3 = 0,\\
x_1 \otimes x_2 \oplus x_0 \oplus x_2 \oplus x_3 \oplus 1 = 0,\\
x_1 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_0 \oplus x_1 \oplus x_3 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_1 \oplus x_3 = 0,\\
x_1 \oplus x_2 \oplus 1 = 0,\\
x_1 \otimes x_2 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 = 0,\\
x_0 \otimes x_2 \oplus x_1 \otimes x_2 \oplus x_3 \oplus 1 = 0,\\
x_0 \oplus x_1 \oplus x_2 \oplus 1 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_0 \oplus x_1 \oplus x_3 = 0,\\
x_1 \otimes x_2 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 = 0,\\
x_0 \otimes x_2 \oplus x_0 \oplus x_1 \oplus 1 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_1 \oplus 1 = 0,\\
x_0 \otimes x_3 \oplus x_2 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_2 = 0,\\
x_0 \otimes x_2 \oplus x_0 \otimes x_3 \oplus x_0 \oplus x_2 \oplus x_3 \oplus 1 = 0.
\end{cases}$$

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

Для нахождения решения последней системы булевых уравнений используем полученные результаты, а именно по методике, указанной в [12], последнюю систему можно свести к задаче минимизации в $\mathcal{K}^4$ соответствующей полилинейной целевой функции $tf(x_0,x_1,x_2,x_3) = -x_0x_1x_2x_3+x_1x_2x_3+x_0x_1x_3-x_1x_3+1$. Минимизируемая функция $tf(x_0,x_1,x_2,x_3)$ полилинейна, т.е. она гармоническая по каждому аргументу и, следовательно, $\min\limits_{(x_0,x_1,x_2,x_3)\in\mathcal{K}^4} tf(x_0,x_1,x_2,x_3) = \min\limits_{(x_0,x_1,x_2,x_3)\in\mathcal{B}^4} tf(x_0,x_1,x_2,x_3)$. Теперь покажем, что в любой внутренней точке $\mathcal{K}^4$, только один раз вычислив градиент функции $tf(x_0,x_1,x_2,x_3)$, можно найти $\arg\min\limits_{(x_0,x_1,x_2,x_3)\in\mathcal{K}^4} tf(x_0,x_1,x_2,x_3)$ или решение последней системы. Для этого достаточно показать, что

$$tf'_{x_0}(x_0,x_1,x_2,x_3) > 0, \quad tf'_{x_1}(x_0,x_1,x_2,x_3) < 0,$$
$$tf'_{x_2}(x_0,x_1,x_2,x_3) > 0, \quad tf'_{x_3}(x_0,x_1,x_2,x_3) < 0, \quad \forall x_0,x_1,x_2,x_3 \in (0,1).$$

Действительно, если $x_0,x_1,x_2,x_3 \in (0,1)$, то

$$tf'_{x_0}(x_0,x_1,x_2,x_3) = -x_1x_2x_3 + x_1x_3 = x_1x_3(1-x_2) > 0,$$
$$tf'_{x_1}(x_0,x_1,x_2,x_3) = -x_0x_2x_3 + x_2x_3 + x_0x3 - x_3 = -x_3(x_0-1)(x_2-1) < 0,$$
$$tf'_{x_2}(x_0,x_1,x_2,x_3) = -x_0x_1x_3 + x_1x_3 = x_1x_3(1-x_0) > 0,$$
$$tf'_{x_3}(x_0,x_1,x_2,x_3) = -x_0x_1x_2 + x_1x_2 + x_0x_1 - x_1 = -x_1(x_0-1)(x_2-1) < 0.$$

Из этих неравенств следует, что $\min\limits_{(x_0,x_1,x_2,x_3)\in\mathcal{K}^4} tf(x_0,x_1,x_2,x_3) = tf(0,1,0,1) = 0$. Таким образом, с помощью полилинейного продолжения булевой функции найдены $(x_0,x_1,x_2,x_3) = (0,1,0,1)$ — входные биты S-KN2 для выходных битов $(y_0,y_1,y_2,y_3) = (0,0,0,0)$.

7. Заключение. В данной работе получен и теоретически обоснован важный результат, позволяющий в некоторых случаях заменять сложную логику анализа данных простыми аналитическими формами. Полученные результаты могут быть применены для развития основ дискретной математики, анализа и последующего улучшения текстов программ, решения задач распознавания образов, оптимизации и управления, искусственного интеллекта и алгебраического криптоанализа.

Список литературы

1. *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. **19**, № 2. 285–294.
2. *Abdel-Gawad A.H., Atiya A.F., Darwish N.M.* Solution of systems of Boolean equations via the integer domain // Information Sciences. 2010. **180**, N 2. 288–300. doi 10.1016/j.ins.2009.09.010.
3. *Barotov D.N., Barotov R.N.* Polylinear transformation method for solving systems of logical equations // Mathematics. 2022. **10**, N 6. Article Number 918. doi 10.3390/math10060918.
4. *Barotov D., Osipov A., Korchagin S., et al.* Transformation method for solving system of Boolean algebraic equations // Mathematics. 2021. **9**, N 24. Article Number 3299. doi 10.3390/math9243299.
5. *Barotov D.N., Barotov R.N., Soloviev V., et al.* The development of suitable inequalities and their application to systems of logical equations // Mathematics. 2022. **10**, N 11. Article Number 1851. doi 10.3390/math10111851.
6. *Faizullin R.T., Khnykin I.G., Dylkeyt V.I.* The SAT solving method as applied to cryptographic analysis of asymmetric ciphers // arXiv preprint: 0907.1755v1[cs.CR]. Ithaca: Cornell Univ. Library, 2009. https://arxiv.org/abs/0907.1755. Cited December 18, 2022.
7. *Gu J.* How to solve very large-scale satisfiability problems // Technical Report UUCS-Tr-88-032. Salt Lake City: University of Utah, 1988.
8. *Gu J.* On optimizing a search problem // Artificial intelligence: methods and applications. Singapore: World Scientific, 1992. 63–105. https://books.google.ru/books?id=0a_j0R0qh1EC&printsec=frontcover&hl=ru#v=onepage&q&f=false. Cited December 19, 2022.
9. *Gu J.* Global optimization for satisfiability (SAT) problem // IEEE Transactions on Knowledge and Data Engineering. 1994. **6**, N 3. 361–381. doi 10.1109/69.334864.

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

10. *Gu J., Gu Q., Du D.* On optimizing the satisfiability (SAT) problem // Journal of Computer Science and Technology. 1999. **14**, N 1. 1–17. doi 10.1007/BF02952482.
11. *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. **8**, № 1. 17–23.
12. *Barotov D.N.* Target function without local minimum for systems of logical equations with a unique solution // Mathematics. 2022. **10**, N 12. Article Number 2097. doi 10.3390/math10122097.
13. *Ishchukova E., Maro E., Pristalov P.* Algebraic analysis of a simplified encryption algorithm GOST R 34.12–2015 // Computation. 2020. **8**, N 2. Article Number 51. doi 10.3390/computation8020051.

Поступила в редакцию
07 ноября 2022 г.

Принята к публикации
05 декабря 2022 г.

Информация об авторах

Достонжон Нумонжонович Баротов — старший преподаватель; Финансовый университет при Правительстве РФ, департамент анализа данных и машинного обучения, 4-й Вешняковский проезд, д. 4, 109456, Москва, Российская Федерация.

Рузибой Нумонжонович Баротов — докторант; Худжандский государственный университет имени академика Б. Гафурова, кафедра математического анализа имени профессора А. Мухсинова, пр. Мавлонбекова , д. 1, 735700, Худжанд, Таджикистан.

References

1. R. T. Faizullin, V. I. Dul'keit, and Yu. Yu. Ogorodnikov, "Hybrid Method for the Approximate Solution of the 3-Satisfiability Problem Associated with the Factorization Problem," Trudy Inst. Mat. Mekh. UrO RAN. **19** (2), 285–294 (2013).
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. D. N. Barotov and R. N. Barotov, "Polylinear Transformation Method for Solving Systems of Logical Equations," Mathematics **10** (6), Article Number 918 (2022). doi 10.3390/math10060918.
4. D. Barotov, A. Osipov, S. Korchagin, et al., "Transformation Method for Solving System of Boolean Algebraic Equations," Mathematics **9** (24), Article Number 3299 (2021). doi 10.3390/math9243299.
5. D. N. Barotov, R. N. Barotov, V. Soloviev, et al., "The Development of Suitable Inequalities and Their Application to Systems of Logical Equations," Mathematics **10** (11), Article Number 1851 (2022). doi 10.3390/math10111851.
6. R. T. Faizullin, I. G. Khnykin, and V. I. Dylkeyt, *The SAT Solving Method as Applied to Cryptographic Analysis of Asymmetric Ciphers*, arXiv preprint: 0907.1755v1[cs.CR] (Cornell Univ. Library, Ithaca, 2009), https://arxiv.org/abs/0907.1755. Cited December 18, 2022.
7. J. Gu, *How to Solve Very Large-Scale Satisfiability Problems*, Technical Report UUCS-Tr-88-032, (University of Utah, Salt Lake City, 1988).
8. J. Gu, "On Optimizing a Search Problem," in *Artificial Intelligence: Methods and Applications* (World Scientific, Singapore, 1992), pp. 63–105. https://books.google.ru/books?id=0a_j0R0qh1EC&printsec=frontcover&hl=ru#v=onepage&q&f=false. Cited December 19, 2022.
9. J. Gu, "Global Optimization for Satisfiability (SAT) Problem," IEEE Trans. Knowl. Data Eng. **6** (3), 361–381 (1994). doi 10.1109/69.334864.
10. 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.
11. D. N. Barotov, D. Z. Muzafarov, and R. N. Barotov, "On One Method for Solving Systems of Boolean Algebraic Equations," Mod. Math. Concept Innov. Math. Educ. **8**, 17–23 (2021).
12. D. N. Barotov, "Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution," Mathematics **10** (12), Article Number 2097 (2022). doi 10.3390/math10122097.

2023, **24** (1), 10–23. doi 10.26089/NumMet.v24r102

13. E. Ishchukova, E. Maro, and P. Pristalov, "Algebraic Analysis of a Simplified Encryption Algorithm GOST R 34.12–2015," Computation **8** (2), Article Number 51 (2020). doi 10.3390/computation8020051.

Received
November 7, 2022

Accepted for publication
December 5, 2022

Information about the authors

Dostonjon N. Barotov — Senior Lecturer; Financial University under the Government of the Russian Federation, Department of Data Analysis and Machine Learning, 4-th Veshnyakovsky Passage, 4, 109456, Moscow, Russia.

Ruziboy N. Barotov — Doctoral Student; Khujand state university named after academician Bobojon Gafurov, Department of Mathematical Analysis named after Professor A. Mukhsinov, Mavlonbekov ave., 1, 735700, Khujand, Tajikistan.