ИПМ им.М.В.Келдыша РАН • Электронная библиотека

Препринты ИПМ • Препринт № 30 за 2024 г.

ISSN 2071-2898 (Print)
ISSN 2071-2901 (Online)

Д.Н. Баротов, В.А. Судаков

О неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций

Рекомендуемая форма библиографической ссылки: Баротов Д.Н., Судаков В.А. О неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций // Препринты ИПМ им. М.В.Келдыша. 2024. № 30. 13 с. **https://doi.org/10.20948/prepr-2024-30**
https://library.keldysh.ru/preprint.asp?id=2024-30

О р д е н а Л е н и н а
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
имени М.В.Келдыша
Р о с с и й с к о й а к а д е м и и н а у к

Д.Н. Баротов, В.А. Судаков

О неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций

Москва — 2024

Баротов Д.Н., Судаков В.А.

О неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций

Препринт посвящен исследованию неравенств между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций. В результате исследования доказано, что для заданной произвольной булевой функции от n переменных, во-первых, любое её выпуклое продолжение на n-мерный единичный куб не превосходит ее полилинейного продолжения на n-мерный единичный куб и, во-вторых, её полилинейное продолжение на n-мерный единичный куб не превосходит ни одного её вогнутого продолжения на n-мерный единичный куб. Доказано также, что равенство в этой последовательности неравенств может быть достигнуто тогда и только тогда, когда число существенных переменных заданной булевой функции не более одной. Полученный результат может быть использован при преобразовании систем булевых уравнений к задаче численной оптимизации и последующем поиске их решений.

Ключевые слова: выпуклое продолжение булевой функции, вогнутое продолжение булевой функции, полилинейное продолжение булевой функции, неравенство.

Dostonjon Numonjonovich Barotov, Vladimir Anatolievich Sudakov

On Inequalities Between Convex, Concave, and Multilinear Continuations of Boolean Functions

The preprint is devoted to the study of inequalities between convex, concave, and multilinear continuations of Boolean functions. As a result of the study, it was proved that for a given arbitrary Boolean function of n variables, firstly, any of its convex continuation does not exceed its multilinear continuation, and secondly, its multilinear continuation does not exceed any of its concave continuations. It is also proved that equality in this sequence of inequalities can be achieved if and only if the number of essential variables of a given Boolean function is no more than one. The obtained result in a number of cases can be used when transforming systems of Boolean equations into numerical optimization problems and subsequent searches for their solutions.

Key words: convex continuation of a Boolean function, concave continuation of a Boolean function, multilinear continuation of a Boolean function, inequality.

Введение

На протяжении многих десятилетий булевы переменные были основными переменными, используемыми в большинстве компьютерных операций. Встречается много задач, связанных с булевыми переменными, а некоторые задачи, несмотря на зрелость области, не имеют удовлетворительных методов решения. Среди них задача решения систем булевых уравнений [1]. Система булевых (логических) уравнений, или задача выполнимости булевых формул (SAT), – одна из трудно решаемых задач математики, имеющая также значение для приложений [1,2]. Решение логических уравнений проникает во многие области современной науки, такие как логическое проектирование, биология, грамматика, химия, юриспруденция, медицина, спектроскопия, криптография и теория графов [3]. Многие задачи исследования операций могут быть сведены к решению системы логических уравнений. Ярким примером является задача о коалиционной игре n агентов с отношением доминирования между различными стратегиями. Решения логических уравнений также служат важным инструментом при решении связанных с ними задач целочисленного линейного программирования [4]. Также 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 [1]. В области криптографии решение системы булевых уравнений применяется при анализе и атаках на блочные шифры, поскольку их можно свести к решению системы булевых уравнений [1,5,6]. В основном это связано с тем, что, во-первых, булевы функции с нелинейностью могут быть использованы в алгоритмах блочного шифрования [7], во-вторых, для конкретного шифра алгебраический криптоанализ основан на преобразовании шифра в систему полиномиальных уравнений (обычно над булевым кольцом) и решении полученной системы полиномиальных уравнений [5,6]. Одним из первых ярких приложений решения системы булевых уравнений в криптографии было решение сложной задачи – криптосистемы об отображениях скрытых полей (Hidden Fields Equations) в криптографии с открытым ключом [8]. Данная задача описывается системой квадратичных булевых многочленов от 80 переменных, и впервые ее решение было получено именно путем решения системы булевых уравнений с использованием алгоритма F5, который на сегодняшний день является одним из самых быстрых алгоритмов нахождения базиса Грёбнера [9]. Поэтому в настоящее время алгебраический криптоанализ является одним из перспективных методов в современном криптоанализе [1,5,8,10], а теория булевых функций представляет собой увлекательную область исследований в области дискретной математики, включая приложения к криптографии и теории кодирования [7].

Несмотря на то что большинство методов и алгоритмов, разработанных для решения систем булевых уравнений, до сих пор находят решения непосредственно на булевом множестве, в последнее время разрабатываются много новых направлений исследования и алгоритмов решения систем булевых уравнений [11,12]. Одно из направлений заключается в том, что система булевых уравнений, заданная над кольцом булевых многочленов, преобразуется в систему уравнений над полем действительных чисел и ищется решение на множестве действительных чисел, поскольку в этой области известно множество методов и алгоритмов решения систем. В свою очередь, в частности, преобразованная система может быть сведена либо к задаче численной оптимизации соответствующей целевой функции, что позволяет применять, анализировать и комбинировать такие методы вычислительной математики, как алгоритм наискорейшего спуска, метод Ньютона и алгоритм координатного спуска [2,11,12], либо к задаче MILP или QUBO, решаемой классическими алгоритмами дискретной оптимизации или квантовыми алгоритмами [13-15], либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [1], либо к эквивалентной системе полиномиальных уравнений, решаемой и анализируемой символьными методами [9].

Имеется много способов, позволяющих преобразовать систему булевых уравнений в задачу 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 по всем переменным одновременно [2,11,12,16]. В работе [12] доказано, что для SAT задачи с m переменными при достаточной близости начального решения к оптимальному метод наискорейшего спуска имеет скорость сходимости $\beta < 1$, метод Ньютона имеет скорость сходимости второго порядка, а скорость сходимости координатного метода спуска приблизительно равна $1 - \beta/m$. Также представлен алгоритм, основанный на методе координатного спуска для SAT. Но одна из основных проблем, возникающая при применении этих способов, заключается в том, что оптимизируемая целевая функция в искомой области может иметь множество локальных экстремумов, что значительно усложняет их практическое использование [2,11,12,16]. В [16] утверждается, что при решении системы булевых уравнений методом численной оптимизации полилинейное продолжение булевой функции также играет важную роль, в том числе в уменьшении числа локальных экстремумов соответствующей целевой функции. Были также найдены явные формы полилинейных продолжений для произвольных функций, определённых на множестве вершин n-мерного единичного куба $[0,1]^n$, произвольного куба и параллелепипеда, и в каждом конкретном случае была доказана единственность соответствующего полилинейного продолжения.

В работе [17] конструируется $f_C : [0,1]^n \to [0,1]$ – выпуклое продолжение произвольной булевой функции $f_B : \{0,1\}^n \to \{0,1\}$ на множество $[0,1]^n$. Более

того, доказывается, что для любой булевой функции f_B, не имеющей соседних точек на множестве $supp(f_B)$, построенная выпуклая функция f_C является не только выпуклым продолжением булевой функции f_B на $[0,1]^n$, но и её единственным суммарно максимально выпуклым продолжением на $[0,1]^n$. На базе этого, в частности, конструктивно утверждается, что задача решения произвольной системы булевых уравнений может быть сведена к задаче минимизации функции, любой локальный минимум которой в искомой области является глобальным минимумом, и тем самым для этой задачи проблема локальных минимумов полностью решается. В работе [18] доказано, что для любой булевой функции $f_B : \{0,1\}^n \to \{0,1\}$ существует бесконечно много функций, каждая из которых является её выпуклым продолжением на $[0,1]^n$. Конструктивно доказано, что для произвольной булевой функции $f_B: \{0,1\}^n \to \{0,1\}$ существует единственная функция вида $f_{DM} : [0,1]^n \to [0,1]$, являющаяся максимумом среди всех её выпуклых продолжений на множество $[0,1]^n$. Также аргументировано, что функция f_{DM} на $[0,1]^n$ непрерывна и является единственным суммарно максимально выпуклым продолжением на $[0,1]^n$ булевой функции f_B.

В данном препринте рассматривается задача о неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций. В ходе исследования подробно доказывается, что если $f_C(x_1, x_2, \dots, x_n)$, $f_{CC}(x_1, x_2, \dots, x_n)$ и $f_P(x_1, x_2, \dots, x_n)$ – любое выпуклое, вогнутое и полилинейное продолжение на множество $[0,1]^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$ соответственно, то $\forall(x_1, x_2, \dots, x_n) \in [0,1]^n$ и имеет место цепочка неравенств

$$f_C(x_1, x_2, \dots, x_n) \le f_P(x_1, x_2, \dots, x_n) \le f_{CC}(x_1, x_2, \dots, x_n).$$

Также доказывается, что равенство в цепочке достигается тогда и только тогда, когда число существенных переменных булевой функции f_B не более одной и f_C – максимум среди всех выпуклых продолжений на $[0,1]$ булевой функции f_B, а f_{CC} – минимум среди всех вогнутых продолжений на $[0,1]$ булевой функции f_B.

Используемые определения и обозначения

Определение 1. *Функцию $f_P(x_1, x_2, \dots, x_n)$ будем называть полилинейной функцией, если она линейна по каждому из своих аргументов, при фиксированных значениях остальных аргументов.*

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

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

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

Определение 2. *Отображение вида* $f_B: \mathbb{B}^n \to \mathbb{B}$ *назовём булевой функцией.*

Пусть $supp(f_B) = \{(b_1, b_2, \ldots, b_n) \in \mathbb{B}^n : f_B(b_1, b_2, \ldots, b_n) = 1\}$ – носитель булевой функции f_B, т. е. множество всех булевых векторов, на которых булева функция f_B принимает значение 1.

Пусть $f_B^{-1}(0) = \{(b_1, b_2, \ldots, b_n) \in \mathbb{B}^n : f_B(b_1, b_2, \ldots, b_n) = 0\}$ – множество нулей булевой функции f_B, т. е. множество всех булевых векторов, на которых булева функция f_B принимает значение 0.

Определение 3. *Переменную* x_k *булевой функции* $f_B(x_1, x_2, \ldots, x_n)$ *назовём существенной, если*

$$\exists (b_1^*, \ldots, b_{k-1}^*, 0, b_{k+1}^*, \ldots, b_n^*), (b_1^*, \ldots, b_{k-1}^*, 1, b_{k+1}^*, \ldots, b_n^*) \in \mathbb{B}^n :$$
$$f_B(b_1^*, \ldots, b_{k-1}^*, 0, b_{k+1}^*, \ldots, b_n^*) \neq f_B(b_1^*, \ldots, b_{k-1}^*, 0, b_{k+1}^*, \ldots, b_n^*).$$

Определение 4. *Отображение вида* $f_P: \mathbb{K}^n \to \mathbb{R}$ *назовём полилинейным продолжением на* $\mathbb{K}^n$ *булевой функции* $f_B: \mathbb{B}^n \to \mathbb{B}$, *если оно на* $\mathbb{K}^n$ *полилинейное и* $f_P(b_1, b_2, \ldots, b_n) = f_B(b_1, b_2, \ldots, b_n)\ \forall (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n$.

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

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

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

Определение 5. *Отображение вида* $f: \mathbb{K}^n \to \mathbb{R}$ *назовём выпуклой функцией на* $\mathbb{K}^n$, *если для любых* $x, y \in \mathbb{K}^n$ *и любого* $\alpha \in [0,1]$ *выполняется*

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

Определение 6. *Отображение вида* $f_C: \mathbb{K}^n \to \mathbb{R}$ *назовём выпуклым продолжением булевой функции* $f_B: \mathbb{B}^n \to \mathbb{B}$ *на* $\mathbb{K}^n$, *если выполняются следующие два условия:*

a) отображение f_C *на* $\mathbb{K}^n$ *является выпуклой функцией,*

b) имеет место $f_C(b_1, b_2, \ldots, b_n) = f_B(b_1, b_2, \ldots, b_n)\ \forall (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n$.

Определение 7. *Отображение 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 8. *Отображение вида* $f_{CC}: \mathbb{K}^n \to \mathbb{R}$ *назовём вогнутым продолжением булевой функции* $f_B: \mathbb{B}^n \to \mathbb{B}$ *на* $\mathbb{K}^n$, *если выполняются следующие два условия:*

a) отображение f_C *на* $\mathbb{K}^n$ *является вогнутой функцией,*

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

Основные результаты

В этом разделе сформулируем основные результаты о неравенствах между выпуклыми, вогнутыми и полилинейными продолжениями булевых функций в виде утверждений и докажем их.

Утверждение 1. *Пусть* $f_C(x_1, x_2, \dots, x_n)$, $f_{CC}(x_1, x_2, \dots, x_n)$ *и* $f_P(x_1, x_2, \dots, x_n)$ *– любое выпуклое, вогнутое и полилинейное продолжение на* $\mathbb{K}^n$ *произвольной булевой функции* $f_B(x_1, x_2, \dots, x_n)$ *соответственно. Тогда имеет место цепочка неравенств* $f_C(x_1, x_2, \dots, x_n) \le f_P(x_1, x_2, \dots, x_n) \le$

$$\le f_{CC}(x_1, x_2, \dots, x_n) \quad \forall (x_1, x_2, \dots, x_n) \in \mathbb{K}^n. \qquad (1)$$

Доказательство. Пусть $(x_1^*, x_2^*, \dots, x_n^*)$ - произвольная точка куба $\mathbb{K}^n$. Прежде всего, докажем, что имеет место следующее включение

$$\left(\lambda^*_{(0,0,\dots,0)}, \lambda^*_{(0,0,\dots,1)}, \dots, \lambda^*_{(1,1,\dots,1)}\right) \in \Lambda(x_1^*, x_2^*, \dots, x_n^*), \qquad (2)$$

где

$$\lambda^*_{(b_1,b_2,\dots,b_n)} = \prod_{k=1}^{n}\left((2b_k - 1)\cdot x_k^* + 1 - b_k\right), \qquad (b_1, b_2, \dots, b_n) \in \mathbb{B}^n.$$

Действительно, для этого достаточно показать справедливость следующих свойств:

1°. Для любого $(b_1, b_2, \dots, b_n) \in \mathbb{B}^n$ выполнено неравенство $\lambda^*_{(b_1,b_2,\dots,b_n)} \ge 0$.

2°. Имеет место равенство

$$\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n} \lambda^*_{(b_1,b_2,\dots,b_n)} = 1.$$

3°. Имеет место равенство

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

Докажем эти свойства:

1°. Действительно, в силу $(x_1^*, x_2^*, \dots, x_n^*) \in \mathbb{K}^n$ и $(b_1, b_2, \dots, b_n) \in \mathbb{B}^n$ имеем

$$0 \le 0 + 0 \le (1 - b_k)\cdot(1 - x_k^*) + x_k^* \cdot b_k = (2b_k - 1)\cdot x_k^* + 1 - b_k$$

и, следовательно,

$$\lambda^*_{(b_1,b_2,\dots,b_n)} = \prod_{k=1}^{n}\left((2b_k - 1)\cdot x_k^* + 1 - b_k\right) \ge 0.$$

2°. Действительно,

$$\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n} \lambda^*_{(b_1,b_2,\dots,b_n)} = \sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n} \prod_{k=1}^{n}\left((2b_k - 1)\cdot x_k^* + 1 - b_k\right) =$$

$$= \sum_{(b_1,b_2,\dots,b_{n-1})\in\mathbb{B}^{n-1}} \left((2\cdot 0 - 1)\cdot x_n^* + 1 - 0\right)\cdot \prod_{k=1}^{n-1}\left((2b_k - 1)\cdot x_k^* + 1 - b_k\right) +$$

$$+\sum_{(b_1,b_2,\dots,b_{n-1})\in\mathbb{B}^{n-1}}\big((2\cdot 1-1)\cdot x_n^*+1-1\big)\cdot\prod_{k=1}^{n-1}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=$$

$$(1-x_n^*)\cdot\sum_{(b_1,b_2,\dots,b_{n-1})\in\mathbb{B}^{n-1}}\prod_{k=1}^{n-1}\big((2b_k-1)\cdot x_k^*+1-b_k\big)+x_n^*\cdot$$

$$\cdot\sum_{(b_1,b_2,\dots,b_{n-1})\in\mathbb{B}^{n-1}}\prod_{k=1}^{n-1}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=(1-x_n^*+x_n^*)\cdot$$

$$\cdot\sum_{(b_1,b_2,\dots,b_{n-1})\in\mathbb{B}^{n-1}}\prod_{k=1}^{n-1}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=$$

$$=\sum_{(b_1,b_2,\dots,b_{n-1})\in\mathbb{B}^{n-1}}\prod_{k=1}^{n-1}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=\cdots=$$

$$=\sum_{b_1\in\mathbb{B}^1}\prod_{k=1}^{1}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=(1-x_1^*)+x_1^*=1.$$

3°. Для этого достаточно показать, что

$$\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot b_j=x_j^*,\qquad j\in\{1,2,\dots,n\}.$$

Действительно,

$$\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot b_j=\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\prod_{k=1}^{n}\big((2b_k-1)\cdot x_k^*+1-b_k\big)\cdot b_j=$$

$$=\sum_{(b_1,\dots,b_{j-1},0,b_{j+1},\dots,b_n)\in\mathbb{B}^n}0\cdot\prod_{\substack{k=1\\k\neq j}}^{n}\big((2b_k-1)\cdot x_k^*+1-b_k\big)+$$

$$+\sum_{(b_1,\dots,b_{j-1},1,b_{j+1},\dots,b_n)\in\mathbb{B}^n}x_j^*\cdot\prod_{\substack{k=1\\k\neq j}}^{n}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=$$

$$=x_j^*\cdot\sum_{(b_1,\dots,b_{j-1},1,b_{j+1},\dots,b_n)\in\mathbb{B}^n}\prod_{\substack{k=1\\k\neq j}}^{n}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=$$

$$=x_j^*\cdot\sum_{(b_1,\dots,b_{j-1},b_{j+1},\dots,b_n)\in\mathbb{B}^{n-1}}\prod_{\substack{k=1\\k\neq j}}^{n}\big((2b_k-1)\cdot x_k^*+1-b_k\big)=x_j^*,$$

так как из свойства 2° следует, что

$$\sum_{(b_1,\dots,b_{j-1},b_{j+1},\dots,b_n)\in\mathbb{B}^{n-1}}\prod_{\substack{k=1\\k\neq j}}^{n}\left((2b_k-1)\cdot x_k^*+1-b_k\right)=1.$$

Включение (2) доказано. Теперь если $f_C(x_1,x_2,\dots,x_n)$ – любое выпуклое продолжение на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1,x_2,\dots,x_n)$, тогда в силу (2), выпуклости функции $f_C(x_1,x_2,\dots,x_n)$ и неравенства Йенсена [19] имеем

$$f_C(x_1^*,x_2^*,\dots,x_n^*)=f_C\left(\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot(b_1,b_2,\dots,b_n)\right)\leq$$

$$\leq\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot f_C(b_1,b_2,\dots,b_n)=$$

$$=\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot f_B(b_1,b_2,\dots,b_n)=$$

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

Если же $f_{CC}(x_1,x_2,\dots,x_n)$ – любое вогнутое продолжение на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1,x_2,\dots,x_n)$, тогда в силу (2), вогнутости функции $f_{CC}(x_1,x_2,\dots,x_n)$ и неравенства Йенсена [19] имеем

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

$$\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}f_{CC}(b_1,b_2,\dots,b_n)\cdot\prod_{k=1}^{n}\left((2b_k-1)\cdot x_k^*+1-b_k\right)=$$

$$=\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot f_{CC}(b_1,b_2,\dots,b_n)\leq$$

$$\leq f_{CC}\left(\sum_{(b_1,b_2,\dots,b_n)\in\mathbb{B}^n}\lambda^*_{(b_1,b_2,\dots,b_n)}\cdot(b_1,b_2,\dots,b_n)\right)=f_{CC}(x_1^*,x_2^*,\dots,x_n^*).$$

В силу теоремы 2, приведённой в работе [16], величина

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

Равна значению $f_P(x_1,x_2,\dots,x_n)$ – единственного полилинейного продолжения на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1,x_2,\dots,x_n)$ в точке $(x_1^*,x_2^*,\dots,x_n^*)$, и, следовательно, имеет место цепочка неравенств

$$f_C(x_1^*,x_2^*,\dots,x_n^*)\leq f_P(x_1^*,x_2^*,\dots,x_n^*)\leq f_{CC}(x_1^*,x_2^*,\dots,x_n^*).\qquad(3)$$

В силу произвольности точки $(x_1^*, x_2^*, \dots, x_n^*) \in \mathbb{K}^n$ из (3) следует (1). Утверждение доказано.

Далее докажем, что равенство в цепочке (1) достигается тогда и только тогда, когда число существенных переменных булевой функции f_B не более одной и f_C – максимум среди всех выпуклых продолжений на $\mathbb{K}$ булевой функции f_B, а f_{CC} – минимум среди всех вогнутых продолжений на $\mathbb{K}$ булевой функции f_B.

Утверждение 2. *Пусть $f_C(x_1, x_2, \dots, x_n)$, $f_{CC}(x_1, x_2, \dots, x_n)$ и $f_P(x_1, x_2, \dots, x_n)$ – выпуклое, вогнутое и полилинейное продолжение на $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$ соответственно. Если выполнено*

$$f_C(x_1, x_2, \dots, x_n) = f_P(x_1, x_2, \dots, x_n) \quad \forall (x_1, x_2, \dots, x_n) \in \mathbb{K}^n \tag{4}$$

или

$$f_P(x_1, x_2, \dots, x_n) = f_{CC}(x_1, x_2, \dots, x_n) \quad \forall (x_1, x_2, \dots, x_n) \in \mathbb{K}^n, \tag{5}$$

тогда число существенных переменных булевой функции f_B не более одной, причём если выполнено (4), то f_C – максимум среди всех выпуклых продолжений на $\mathbb{K}$ булевой функции f_B, а если выполнено (5), то f_{CC} – минимум среди всех вогнутых продолжений на $\mathbb{K}$ булевой функции f_B.

Доказательство. Прежде всего докажем, что если количество существенных переменных произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$ больше единицы, то функция $f_P(x_1, x_2, \dots, x_n)$ не является ни выпуклой, ни вогнутой. Не теряя общности, можно считать, что все переменные $x_1, x_2, \dots, x_n$ булевой функции $f_B(x_1, x_2, \dots, x_n)$ являются существенными. Рассмотрим два случая.

Случай 1. Пусть $n = 2$. Нетрудно заметить, что из существенности переменных x_1, x_2 булевой функции $f_B(x_1, x_2)$ следует

$$f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1) \neq 0. \tag{6}$$

В силу теоремы 2, приведённой в работе [16], имеем

$$f_P(x_1, x_2) = f_B(0,0) + \big(f_B(1,0) - f_B(0,0)\big) \cdot x_1 + \big(f_B(0,1) - f_B(0,0)\big) \cdot x_2 + \\ + \big(f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1)\big) \cdot x_1 x_2. \tag{7}$$

Заметим, что первое слагаемое в (7), имеющее вид

$$f_B(0,0) + \big(f_B(1,0) - f_B(0,0)\big) \cdot x_1 + \big(f_B(0,1) - f_B(0,0)\big) \cdot x_2,$$

является линейной и, следовательно, одновременно выпуклой и вогнутой функцией на $\mathbb{K}^2$, а второе слагаемое в (7), имеющее вид

$$\big(f_B(0,0) - f_B(0,1) - f_B(1,0) + f_B(1,1)\big) \cdot x_1 x_2,$$

в силу (6) на $\mathbb{K}^2$ не является ни выпуклой, ни вогнутой функцией. Отсюда получим, что $f_P(x_1, x_2)$ на $\mathbb{K}^2$ не является ни выпуклой, ни вогнутой функцией.

Случай 2. Пусть $n \geq 3$. Нетрудно заметить, что из существенности переменных $x_1, x_2, \dots, x_n$ булевой функции $f_B(x_1, x_2, \dots, x_n)$ следует существование набора

$(b_1^*, b_2^*, \dots, b_n^*) \in \mathbb{B}^n$, такого, что переменные x_1, x_2 суженной булевой функции $f_B(x_1, x_2, b_3^*, \dots, b_n^*)$ будут существенными. Проводя рассуждения, аналогичные рассуждениям в случае 1, получаем, что суженная полилинейная функция $f_P(x_1, x_2, b_3^*, \dots, b_n^*)$ на суженном множестве

$$\mathbb{K}^n_{restriction} = \left\{ (x_1, x_2, b_3^*, \dots, b_n^*) \colon (x_1, x_2) \in \mathbb{K}^2 \right\}$$

не является ни выпуклой, ни вогнутой функцией. Следовательно, в силу $\mathbb{K}^n_{restriction} \subset \mathbb{K}^n$ функция $f_P(x_1, x_2, \dots, x_n)$ на $\mathbb{K}^n$ не является ни выпуклой, ни вогнутой.

Теперь докажем, что если $f_P(x_1)$ – полилинейное продолжение на $\mathbb{K}$ булевой функции $f_B(x_1)$, существенно зависящей не более чем от одной переменной, то, во-первых, f_P – максимум среди всех выпуклых продолжений на $\mathbb{K}$ булевой функции f_B, а во-вторых, f_P – минимум среди всех вогнутых продолжений на $\mathbb{K}$ булевой функции f_B. Действительно, в силу теоремы 2, приведённой в работе [16], имеем

$$f_P(x_1) = (1 - x_1) \cdot f_B(0) + x_1 \cdot f_B(1).$$

В таком случае нетрудно заметить, что, во-первых, имеет место равенство $f_P(x_1) = f_B(x_1), \ \forall x_1 \in \mathbb{B}$, а во-вторых, функция $f_P(x_1)$ является линейной и, следовательно, на $\mathbb{K}$ одновременно выпуклой и вогнутой функцией.

Теперь если $f_C(x_1)$ – любое выпуклое продолжение на $\mathbb{K}$ булевой функции $f_B(x_1)$, тогда в силу выпуклости функции $f_C(x_1)$ и неравенства Йенсена [19] получим, что $\forall x_1 \in \mathbb{K}$ справедливо

$$f_C(x_1) = f_C\big((1 - x_1) \cdot 0 + x_1 \cdot 1\big) \le (1 - x_1) \cdot f_C(0) + x_1 \cdot f_C(1) = \\ = (1 - x_1) \cdot f_B(0) + x_1 \cdot f_B(1) = f_P(x_1).$$

Если же $f_{CC}(x_1)$ – любое вогнутое продолжение на $\mathbb{K}$ булевой функции $f_B(x_1)$, тогда в силу вогнутости функции $f_{CC}(x_1)$ и неравенства Йенсена [19] получим, что $\forall x_1 \in \mathbb{K}$ справедливо

$$f_P(x_1) = (1 - x_1) \cdot f_B(0) + x_1 \cdot f_B(1) = (1 - x_1) \cdot f_{CC}(0) + x_1 \cdot f_{CC}(1) \le \\ \le f_{CC}\big((1 - x_1) \cdot 0 + x_1 \cdot 1\big) = f_{CC}(x_1).$$

Утверждение доказано.

Заключение

В результате исследования доказано, что если

- $f_C(x_1, x_2, \dots, x_n)$ – любое выпуклое продолжение на множество $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$,
- $f_{CC}(x_1, x_2, \dots, x_n)$ – любое вогнутое продолжение на множество $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$,
- $f_P(x_1, x_2, \dots, x_n)$ – любое полилинейное продолжение на множество $\mathbb{K}^n$ произвольной булевой функции $f_B(x_1, x_2, \dots, x_n)$,

тогда полилинейное продолжение $f_P(x_1, x_2, \dots, x_n)$ остается между выпуклым $f_C(x_1, x_2, \dots, x_n)$ и вогнутым $f_{CC}(x_1, x_2, \dots, x_n)$ продолжением, т. е. имеет место цепочка неравенств

$$f_C(x_1, x_2, \dots, x_n) \le f_P(x_1, x_2, \dots, x_n) \le f_{CC}(x_1, x_2, \dots, x_n) \quad \forall (x_1, x_2, \dots, x_n) \in \mathbb{K}^n.$$

Также доказано, что равенство в цепочке достигается в том и только в том случае, если количество существенных переменных булевой функции f_B не более одной и f_C – максимум среди всех выпуклых продолжений на $\mathbb{K}$ булевой функции f_B, а f_{CC} – минимум среди всех вогнутых продолжений на $\mathbb{K}$ булевой функции f_B. Полученный результат в некоторых случаях может быть использован при преобразовании систем булевых уравнений к задаче численной непрерывной оптимизации на множестве $\mathbb{K}^n$ и последующем поиске их решений, поскольку полилинейные, выпуклые и вогнутые продолжения булевых функций на $\mathbb{K}^n$ – продолжения с минимальными количествами или отсутствующими локальными экстремумами на $\mathbb{K}^n$.

Библиографический список

1. 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. — P. 288–300. — DOI: 10.1016/j.ins.2009.09.010.

2. 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.

3. Brown F. M. Boolean reasoning: the logic of Boolean equations. — Courier Corporation, 2003.

4. Hammer P. L., Rudeanu S. Boolean methods in operations research and related areas. Vol. 7. — Springer Science & Business Media, 2012.

5. 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.

6. Ishchukova E., Maro E., Pristalov P. Algebraic analysis of a simplified encryption algorithm GOST R 34.12-2015 // Computation. — 2020. — Vol. 8, no. 2. — P. 51. — DOI: 10.3390/computation8020051.

7. Armario Sampalo J. A. Boolean Functions and Permanents of Sylvester Hadamard Matrices // Mathematics. — 2021. — Vol. 9, no. 2. — P. 177. — DOI: 10.3390/math9020177.

8. Faug`ere J.-C., Joux A. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gr¨obner Bases // Advances in Cryptology - CRYPTO 2003 / ed. by D. Boneh. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2003. — P. 44–60. — ISBN 978-3-540-45146-4.

9. Faugere J. C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F 5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation. — 2002. — P. 75–83.
10. 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. 2003. — P. 176–194.
11. Gu J. Global optimization for satisfiability (SAT) problem // IEEE Transactions on Knowledge and Data Engineering. — 1994. — Vol. 6, no. 3. — P. 361–381. — DOI: 10.1109/69.334864.
12. Gu J., Gu Q., Du D. On optimizing the satisfiability (SAT) problem // Journal of Computer Science and Technology. — 1999. — Vol. 14, no. 1. — P. 1–17. — DOI: 10.1007/BF02952482.
13. Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis / A. I. Pakhomchik [et al.] // Algorithms. — 2022. — Vol. 15, no. 2. — P. 33. — DOI: 10.3390/a15020033.
14. Algebraic attacks on block ciphers using quantum annealing / E. Burek [и др.] // IEEE Transactions on Emerging Topics in Computing. – 2022. – т. 10, № 2. – С. 678–689. – DOI: 10.1109/TETC.2022.3143152.
15. Сивакова Т.В., Судаков В.А., Шимко В.С. Исследование методов решения задач смешанного целочисленного линейного программирования // Препринты ИПМ им. М.В.Келдыша. – 2024. – № 24. – С. 1–18. – DOI: 10.20948/prepr-2024-24.
16. 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. – DOI: 10.26089/NumMet.v24r102.
17. Баротов Д. Н. Выпуклое продолжение булевой функции и его приложения // Дискретный анализ и исследование операций. – 2024. – Т. 31, № 1. – С. 5–18. – DOI: 10.33048/daio.2024.31.779.
18. Баротов Д. Н. О существовании и свойствах выпуклых продолжений булевых функций // Математические заметки. – 2024. – Т. 115, № 4. – С. 533–551.
19. Jensen J. L. W. V. Sur les fonctions convexes et les inégalités entre les valeurs moyennes // Acta mathematica. — 1906. — Vol. 30, no. 1. — C. 175—193. — DOI: 10.1007/BF02418571.

Оглавление