MODELING AND ANALYSIS OF INFORMATION SYSTEMS, VOL. 30, NO. 2, 2023
journal homepage: www.mais-journal.ru

DISCRETE MATHEMATICS IN RELATION TO COMPUTER SCIENCE

The Zhegalkin Polynomial of Multiseat Sole Sufficient Operator

L. Y. Bystrov[1], E. V. Kuzmin[1]

DOI: 10.18255/1818-1015-2023-2-106-127

[1]P. G. Demidov Yaroslavl State University, 14 Sovetskaya, Yaroslavl 150003, Russia.

MSC2020: 06E30
Research article
Full text in Russian

Received February 27, 2023
After revision May 15, 2023
Accepted May 17, 2023

Among functionally complete sets of Boolean functions, sole sufficient operators are of particular interest. They have a wide range of applicability and are not limited to the two-seat case. In this paper, the conditions, imposed on the Zhegalkin polynomial coefficients, are formulated. The conditions are necessary and sufficient for the polynomial to correspond to a sole sufficient operator. The polynomial representation of constant-preserving Boolean functions is considered. It is shown that the properties of monotone and linearity do not require special consideration in describing a sole sufficient operator. The concept of a dual remainder polynomial is introduced. The value of it allows one to determine the self-duality of a Boolean function. It is proved that the preserving 0 and 1 or preserving neither 0 nor 1 Boolean function is self-dual if and only if the dual remainder of its corresponding Zhegalkin polynomial is equal to 0 for any sets of function variable values. Based on this fact, a system of leading coefficients is obtained. The solution of the system made it possible to formulate the criterion for the self-duality of the Boolean function represented by the Zhegalkin polynomial. It imposes necessary and sufficient conditions on the polynomial coefficients. Thus, it is shown that Zhegalkin polynomials are a rather convenient tool for studying precomplete classes of Boolean functions.

Keywords: Zhegalkin polynomial; sole sufficient operator; Sheffer function; precomplete classes; constant-preserving Boolean functions; self-dual Boolean functions; dual remainder polynomial; leading coefficient

INFORMATION ABOUT THE AUTHORS

Leonid Y. Bystrov	orcid.org/0000-0002-0610-5466. E-mail: bystrovl0306@mail.ru Undergraduate Student, Chair of Theoretical Informatics.
Egor V. Kuzmin corresponding author	orcid.org/0000-0003-0500-306X. E-mail: kuzmin@uniyar.ac.ru Head of the Chair of Theoretical Informatics, Doctor of Science.

Funding: Yaroslavl State University (project VIP-016).

For citation: L. Y. Bystrov and E. V. Kuzmin, “The Zhegalkin Polynomial of Multiseat Sole Sufficient Operator”, *Modeling and analysis of information systems*, vol. 30, no. 2, pp. 106-127, 2023.

МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ, ТОМ 30, № 2, 2023
сайт журнала: www.mais-journal.ru

DISCRETE MATHEMATICS IN RELATION TO COMPUTER SCIENCE

Полином Жегалкина многоместного самодостаточного оператора

Л. Ю. Быстров[1], Е. В. Кузьмин[1]

DOI: 10.18255/1818-1015-2023-2-106-127

[1]Ярославский государственный университет им. П. Г. Демидова, ул. Советская, 14, Ярославль, 150000, Россия.

УДК 510.6
Научная статья
Полный текст на русском языке

Получена 27 февраля 2023 г.
После доработки 15 мая 2023 г.
Принята к публикации 17 мая 2023 г.

Среди полных систем булевых функций особый интерес представляют самодостаточные операторы. Они обладают широкой областью применимости и не ограничиваются двухместным случаем. В данной работе формулируются условия, накладываемые на коэффициенты полинома Жегалкина, необходимые и достаточные для того, чтобы полином соответствовал самодостаточному оператору. Рассмотрено полиномиальное представление булевых функций, сохраняющих константу. Показано, что свойства монотонности и линейности не требуют специального рассмотрения при описании самодостаточного оператора. Вводится понятие полинома двойственного остатка, значение которого позволяет определить самодвойственность булевой функции. Доказано, что сохраняющая 0 и 1 или не сохраняющая ни 0, ни 1 булева функция является самодвойственной тогда и только тогда, когда двойственный остаток соответствующего ей полинома Жегалкина равен 0 для любых наборов значений переменных функции. На основании этого факта получена система ведущих коэффициентов. Решение данной системы позволило сформулировать критерий самодвойственности булевой функции, представленной полиномом Жегалкина, накладывающий необходимые и достаточные условия на коэффициенты полинома. Таким образом, показано, что полиномы Жегалкина являются достаточно удобным инструментом при исследовании предполных классов булевых функций.

Ключевые слова: полином Жегалкина; самодостаточный оператор; функция Шеффера; предполные классы; булевы функции; сохраняющие константу; самодвойственные булевы функции; полином двойственного остатка; ведущий коэффициент

ИНФОРМАЦИЯ ОБ АВТОРАХ

Леонид Юрьевич Быстров
orcid.org/0000-0002-0610-5466. E-mail: bystrovl0306@mail.ru
студент, кафедра теоретической информатики.

Егор Владимирович Кузьмин
автор для корреспонденции
orcid.org/0000-0003-0500-306X. E-mail: kuzmin@uniyar.ac.ru
заведующий кафедрой теоретической информатики, доктор физ.-мат. наук.

Финансирование: ЯрГУ (проект № VIP-016).

Для цитирования: L. Y. Bystrov and E. V. Kuzmin, “The Zhegalkin Polynomial of Multiseat Sole Sufficient Operator”, *Modeling and analysis of information systems*, vol. 30, no. 2, pp. 106-127, 2023.

Введение

Набор булевых функций, через суперпозицию которых можно записать любую булеву функцию, называется полной системой булевых функций [1]. Для определения полноты системы булевых функций используется Теорема Поста о полноте, опирающаяся на понятие предполных классов.

Булева функция, сама по себе образующая полную систему булевых функций, называется самодостаточным оператором (sole sufficient operator), или функцией Шеффера [2]. Наиболее известными из самодостаточных операторов являются двухместные функции: штрих Шеффера и стрелка Пирса. Функции Шеффера обладают широкой областью применимости [3].

Использование самодостаточных операторов не ограничено только лишь двухместным случаем. Например, самодостаточным является трехместный (тернарный) оператор А. А. Маркова [4].

Любая булева функция может быть представлена в виде полинома Жегалкина. В статье [5] С. Н. Селезневой было показано, что для систем булевых функций, заданных полиномами Жегалкина, существует алгоритм определения полноты системы с полиномиальной сложностью.

В данной работе исследуется общий вид полинома Жегалкина, реализующего собой самодостаточный многоместный оператор. Сформулирован и доказан ряд утверждений о свойствах булевых функций, представленных в виде полинома Жегалкина, относительно их принадлежности к предполным классам. Особое внимание уделено свойству самодвойственности. Сформулирован критерий самодвойственности булевой функции, заданной полиномом Жегалкина. Наконец, получен общий вид полинома Жегалкина многоместного самодостаточного оператора.

1. Основные понятия

Замыканием $[A]$ называется множество всех булевых функций, представимых в виде суперпозиции функций множества A. Множество A является *функционально замкнутым классом*, если $[A] = A$. Множество называется *полной системой булевых функций*, если любая булева функция может быть записана в виде суперпозиции через функции этой системы [1].

Класс R булевых функций называется *предполным*, если он не полон, но для любой булевой функции f, не принадлежащей этому классу, множество $R \cup \{f\}$ является полным [6]. Эмиль Пост показал, что этому условию удовлетворяют следующие классы [7]: класс S самодвойственных функций, класс M монотонных функций, класс L линейных функций, класс T_0 функций, сохраняющих 0, и класс T_1 функций, сохраняющих 1.

Булева функция $f(x_1, \dots, x_n)$ *сохраняет константу* 0, если $f(0, \dots, 0) = 0$.

Булева функция $f(x_1, \dots, x_n)$ *сохраняет константу* 1, если $f(1, \dots, 1) = 1$.

Функция $f(x_1, \dots, x_n)$ называется *линейной*, если она представима полиномом Жегалкина не выше первой степени [8], т. е. если существуют такие константы $a_i \in \{0, 1\}$, $i \in \overline{0, n}$, что

$$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n.$$

Для двух наборов значений переменных $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \dots, \beta_n)$ выполнено *отношение предшествования* $\tilde{\alpha} \preceq \tilde{\beta}$, если

$$\alpha_1 \leqslant \beta_1, \dots, \alpha_n \leqslant \beta_n.$$

Функция $f(x_1, \dots, x_n)$ называется *монотонной*, если для любых двух наборов $\tilde{\alpha}$ и $\tilde{\beta}$, таких что $\tilde{\alpha} \preceq \tilde{\beta}$, имеет место неравенство

$$f(\tilde{\alpha}) \leqslant f(\tilde{\beta}).$$

Булева функция f^*, $f^*(x_1, \dots, x_n) = \overline{f}(\overline{x_1}, \dots, \overline{x_n})$, называется *двойственной* функцией к функции $f(x_1, \dots, x_n)$. Функция f является *самодвойственной*, если $f = f^*$. Для самодвойственной функции имеет место тождество [1]

$$\overline{f}(\overline{x_1}, \dots, \overline{x_n}) = f(x_1, \dots, x_n).$$

Булева функция называется *антисамодвойственной*, или *самосопряженной*, если выполняется условие [9]

$$f(x_1, \dots, x_n) = f(\overline{x_1}, \dots, \overline{x_n}).$$

Теорема 1. (**Теорема Поста о полноте [1]**) *Для того чтобы система булевых функций была полной, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из классов T_0, T_1, S, M и L.*

Любая булева функция может быть записана в виде формулы, представляющей собой сумму по модулю 2 слагаемых вида $x_{i_1} x_{i_2} \cdots x_{i_s}$ и, быть может, константы 1. Эта формула носит название *полинома Жегалкина* [10]. Полином Жегалкина P булевой функции f от n переменных в общем виде выглядит следующим образом:

$$P(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{1,2} x_1 x_2 \oplus a_{1,3} x_1 x_3 \oplus \dots \oplus a_{1,\dots,n} x_1 \cdots x_n, \text{ где } a_0, \dots, a_{1,\dots,n} \in \{0, 1\}.$$

2. Свойства сохранения 0 и 1 в полиномах Жегалкина

Чтобы получить самодостаточный оператор, то есть полную систему булевых функций, состоящую только из одной функции, мы будем поэтапно преобразовывать полином общего вида $P(x_1, \dots, x_n)$, соответствующий булевой функции $f(x_1, \dots, x_n)$, так, чтобы исключить функцию f из каждого из предполных классов.

Лемма 1. *Булева функция f сохраняет 0 тогда и только тогда, когда соответствующий ей полином Жегалкина P имеет нулевой свободный коэффициент:*

$$f \in T_0 \iff a_0 = 0.$$

Доказательство. Функция f, представленная полиномом P, будет сохранять 0, если на нулевом наборе переменных она принимает значение 0. Следовательно, имеют место равенства

$$P(0, \dots, 0) = a_0 = 0.$$

Обратно. Если в полиноме P свободный коэффициент a_0 равен 0, то на нулевом наборе значений переменных полином P будет равен 0. Следовательно, $f(0, \dots, 0) = 0$. □

Лемма 2. *Булева функция f сохраняет 1 тогда и только тогда, когда в соответствующем ей полиноме Жегалкина P число единичных коэффициентов нечётно:*

$$f \in T_1 \iff a_0 \oplus \bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1.$$

Доказательство. Для выполнения условия $f \in T_1$ необходимо, чтобы на единичном входном наборе булева функция f принимала значение 1. Рассмотрим для f полином P на этом наборе:

$$P(1, \dots, 1) = a_0 \oplus a_1 \oplus a_2 \oplus \dots \oplus a_n \oplus a_{1,2} \oplus a_{1,3} \oplus \dots \oplus a_{1,\dots,n} = 1; \quad \Longrightarrow \quad P(1, \dots, 1) = \underbrace{1 \oplus \dots \oplus 1}_{\text{нечёт. кол-во}};$$

$$a_0 \oplus \bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1.$$

Обратно. Соответствующий функции f полином P с нечётным количеством ненулевых коэффициентов на единичном наборе значений переменных будет равен 1. Действительно,

$$f(1, \dots, 1) = P(1, \dots, 1) = a_0 \oplus a_1 \oplus a_2 \oplus \dots \oplus a_n \oplus a_{1,2} \oplus a_{1,3} \oplus \dots \oplus a_{1,\dots,n} = \underbrace{1 \oplus \dots \oplus 1}_{\text{нечёт. кол-во}} = 1.$$

□

Леммы 1 и 2 показывают, как свойства сохранения 0 и 1 булевой функции f переносятся на соответствующий ей полином P. Самодостаточный оператор не обладает ни одним из этих свойств.

Полином Жегалкина, соответствующий самодостаточному n-местному оператору обозначим через $\hat{P}(x_1, \dots, x_n)$.

Лемма 3. *Для полинома $\hat{P}(x_1, \dots, x_n)$ выполняется:*

1) $a_0 = 1$,
2) $\bigoplus\limits_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1.$

Доказательство. Самодостаточный оператор не сохраняет 0. Следовательно, по Лемме 1 в полиноме $\hat{P}$ свободный коэффициент равен 1, т. е. $a_0 = 1$.

Самодостаточный оператор не сохраняет 1. Следовательно, по Лемме 2 число единичных коэффициентов полинома $\hat{P}$ чётно:

$$a_0 \oplus \bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 0.$$

Из того факта, что $a_0 = 1$, получаем

$$\bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1.$$

□

3. О свойствах монотонности и линейности

Лемма 4. *Булева функция $f(x_1, \dots, x_n)$, не сохраняющая ни 0, ни 1, не является монотонной.*

Доказательство. Предположим противное. Пусть булева функция f, не сохраняющая ни 0, ни 1, является монотонной. Тогда для нулевого и единичного наборов значений переменных $x_1, \dots, x_n$ должно быть справедливо неравенство $f(0, \dots, 0) \preceq f(1, \dots, 1)$. Но поскольку функция f не сохраняет ни 0, ни 1, имеем $f(0, \dots, 0) = 1$ и $f(1, \dots, 1) = 0$. Получили, что $1 \preceq 0$. Пришли к противоречию. Следовательно, рассматриваемая функция f не является монотонной. □

Булева функция, соответствующая полиному $\hat{P}$, не сохраняет ни 0, ни 1. Из Леммы 4 следует, что эта функция не обладает свойством монотонности.

На данном этапе нерассмотренными предполными классами остались класс S самодвойственных функций и класс L линейных функций.

Существует теорема, которая утверждает, что *любая булева функция, не принадлежащая одновременно классам T_0, T_1 и S, не является линейной* (не принадлежит классу L) [11]. Поэтому нет необходимости рассматривать класс L отдельно от класса S. Если исключить функцию f, соответствующую полиному $\hat{P}$, из класса S, то это будет означать и исключение её из класса L.

4. Самодвойственность в полиномах Жегалкина

Перейдём к рассмотрению свойства самодвойственности в полиномах Жегалкина.

4.1. Самодвойственность и полином двойственного остатка

Самодвойственная функция по определению должна либо одновременно сохранять 0 и 1, либо не сохранять ни 0, ни 1.

Определение 1. Пусть P — полином Жегалкина булевой функции f,

$$P(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{1,2} x_1 x_2 \oplus a_{1,3} x_1 x_3 \oplus \dots \oplus a_{1,\dots,n} x_1 \cdots x_n, \text{ где } a_0, \dots, a_{1,\dots,n} \in \{0, 1\}.$$

Полином N вида

$$N(x_1, \dots, x_n) = a_{1,2}(x_1 \oplus x_2) \oplus a_{1,3}(x_1 \oplus x_3) \oplus \dots \oplus a_{(n-1),n}(x_{n-1} \oplus x_n) \oplus a_{1,2,3}(x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_1 \oplus x_2 \oplus x_3) \oplus$$

$$\oplus \dots \oplus a_{1,\dots,n}(x_1 x_2 \cdots x_{n-1} \oplus x_1 x_2 \cdots x_{n-2} x_n \oplus \dots \oplus x_2 x_3 \cdots x_n \oplus \dots \oplus x_1 \oplus x_2 \oplus \dots \oplus x_n).$$

назовём *полиномом двойственного остатка полинома P*, или *двойственным остатком P*.

Теорема 2. *Пусть булева функция f сохраняет 0 и 1 или не сохраняет ни 0, ни 1. Функция f является самодвойственной тогда и только тогда, когда двойственный остаток N соответствующего ей полинома Жегалкина P равен 0 для любых наборов значений переменных $x_1, x_2, \dots, x_n$.*

Доказательство. Доказательство теоремы разбивается на 2 случая: 1) функция f сохраняет 0 и 1, 2) функция f не сохраняет ни 0, ни 1.

1. Функция f сохраняет и 0, и 1. По Лемме 1 в полиноме P свободный коэффициент a_0 равен 0, а по Лемме 2 сумма коэффициентов полинома нечётна:

$$\bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1. \tag{1}$$

Полином P имеет вид

$$P(x_1, \dots, x_n) = a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{1,2} x_1 x_2 \oplus a_{1,3} x_1 x_3 \oplus \dots \oplus a_{1,\dots,n} x_1 \cdots x_n.$$

Условие самодвойственности функции f может быть переписано в виде

$$\overline{f}(x_1, \dots, x_n) = f(\overline{x_1}, \dots, \overline{x_n}) \iff \overline{P}(x_1, \dots, x_n) = P(\overline{x_1}, \dots, \overline{x_n}). \tag{2}$$

Функции отрицания $\overline{x}$ соответствует полином Жегалкина $x \oplus 1$, поэтому $P(\overline{x_1}, \dots, \overline{x_n})$ можно записать следующим образом:

$$P(\overline{x_1}, \dots, \overline{x_n}) = a_1(x_1 \oplus 1) \oplus a_2(x_2 \oplus 1) \oplus \dots \oplus a_n(x_n \oplus 1) \oplus a_{1,2}(x_1 \oplus 1)(x_2 \oplus 1) \oplus$$

$$\oplus a_{1,3}(x_1 \oplus 1)(x_3 \oplus 1) \oplus \dots \oplus a_{1,\dots,n}(x_1 \oplus 1)(x_2 \oplus 1) \cdots (x_n \oplus 1).$$

Раскроем скобки и сгруппируем полученные слагаемые:

$$P(\overline{x_1}, \dots, \overline{x_n}) = a_1 \oplus a_2 \oplus \dots \oplus a_n \oplus a_{1,2} \oplus a_{1,3} \oplus \dots \oplus a_{1,\dots,n} \oplus$$

$$\oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{1,2} x_1 x_2 \oplus a_{1,3} x_1 x_3 \oplus \dots \oplus a_{1,\dots,n} x_1 \cdots x_n \oplus$$

$$\oplus a_{1,2}(x_1 \oplus x_2) \oplus a_{1,3}(x_1 \oplus x_3) \oplus \dots \oplus a_{1,\dots,n}(x_1 x_2 \cdots x_{n-1} \oplus x_1 x_2 \cdots x_{n-2} x_n \oplus \dots \oplus x_2 x_3 \cdots x_n \oplus \dots \oplus x_1 \oplus x_2 \oplus \dots \oplus x_n).$$

Мы разделили полином $P(\overline{x_1}, \dots, \overline{x_n})$ на 3 части: сумма коэффициентов полинома, сам полином $P(x_1, \dots, x_n)$ и его двойственный остаток $N(x_1, \dots, x_n)$. Воспользуемся свойством (1) полинома P, чтобы заменить сумму коэффициентов полинома на 1:

$$P(\overline{x_1}, \dots, \overline{x_n}) = \underbrace{a_1 \oplus a_2 \dots \oplus a_n \oplus a_{1,2} \oplus a_{1,3} \oplus \dots \oplus a_{1,\dots,n}}_{1} \oplus$$

$$\oplus \underbrace{a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus \ldots \oplus a_{1,\ldots,n}x_1 \cdots x_n}_{P(x_1,\ldots,x_n)} \oplus$$

$$\oplus \underbrace{a_{1,2}(x_1 \oplus x_2) \oplus a_{1,3}(x_1 \oplus x_3) \oplus \ldots \oplus a_{1,\ldots,n}(x_1x_2 \cdots x_{n-1} \oplus x_1x_2 \cdots x_{n-2}x_n \oplus \ldots \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_n)}_{N(x_1,\ldots,x_n)}.$$

В результате полином $P(\overline{x_1}, \ldots, \overline{x_n})$ приобретёт вид

$$P(\overline{x_1}, \ldots, \overline{x_n}) = 1 \oplus P(x_1, \ldots, x_n) \oplus N(x_1, \ldots, x_n) = \overline{P}(x_1, \ldots, x_n) \oplus N(x_1, \ldots, x_n).$$

При $N = 0$ выполнено условие самодвойственности (2):

$$P(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) = \overline{P}(x_1, \ldots, x_n).$$

Таким образом, если функция f является самодвойственной, то двойственный остаток N соответствующего ей полинома P должен быть равен 0 для любых наборов переменных $x_1, x_2, \ldots, x_n$, и наоборот: если двойственный остаток N равен 0 для любых наборов переменных $x_1, x_2, \ldots, x_n$, то выполнено условие самодвойственности.

2. Функция f не сохраняет ни 0, ни 1. По Лемме 1 в полиноме P свободный коэффициент a_0 равен 1, а по Лемме 2 сумма коэффициентов полинома чётна. Следовательно, сумма всех коэффициентов полинома без a_0 нечётна:

$$\bigoplus_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\ldots,i_k} = 1. \tag{3}$$

Полином P имеет вид

$$P(x_1, \ldots, x_n) = 1 \oplus a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus \ldots \oplus a_{1,\ldots,n}x_1 \cdots x_n.$$

$P(\overline{x_1}, \ldots, \overline{x_n})$ можно записать как

$$P(\overline{x_1}, \ldots, \overline{x_n}) = 1 \oplus a_1(x_1 \oplus 1) \oplus a_2(x_2 \oplus 1) \oplus \ldots \oplus a_n(x_n \oplus 1) \oplus a_{1,2}(x_1 \oplus 1)(x_2 \oplus 1) \oplus$$

$$\oplus a_{1,3}(x_1 \oplus 1)(x_3 \oplus 1) \oplus \ldots \oplus a_{1,\ldots,n}(x_1 \oplus 1)(x_2 \oplus 1) \cdots (x_n \oplus 1).$$

Раскроем скобки и сгруппируем полученные слагаемые:

$$P(\overline{x_1}, \ldots, \overline{x_n}) = a_1 \oplus a_2 \oplus \ldots \oplus a_n \oplus a_{1,2} \oplus a_{1,3} \oplus \ldots \oplus a_{1,\ldots,n} \oplus$$

$$\oplus 1 \oplus a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus \ldots \oplus a_{1,\ldots,n}x_1 \cdots x_n \oplus$$

$$\oplus a_{1,2}(x_1 \oplus x_2) \oplus a_{1,3}(x_1 \oplus x_3) \oplus \ldots \oplus a_{1,\ldots,n}(x_1x_2 \cdots x_{n-1} \oplus x_1x_2 \cdots x_{n-2}x_n \oplus \ldots \oplus x_2x_3 \cdots x_n \oplus \ldots \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_n).$$

Аналогично случаю 1 мы разделили полином на 3 части. Используя свойство (3), получим

$$P(\overline{x_1}, \ldots, \overline{x_n}) = \underbrace{a_1 \oplus a_2 \oplus \ldots \oplus a_n \oplus a_{1,2} \oplus a_{1,3} \oplus \ldots \oplus a_{1,\ldots,n}}_{1} \oplus$$

$$\oplus \underbrace{1 \oplus a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus \ldots \oplus a_{1,\ldots,n}x_1 \cdots x_n}_{P(x_1,\ldots,x_n)} \oplus$$

$$\oplus \underbrace{a_{1,2}(x_1 \oplus x_2) \oplus a_{1,3}(x_1 \oplus x_3) \oplus \ldots \oplus a_{1,\ldots,n}(x_1x_2 \cdots x_{n-1} \oplus x_1x_2 \cdots x_{n-2}x_n \oplus \ldots \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_n)}_{N(x_1,\ldots,x_n)}.$$

В результате $P(\overline{x_1}, \dots, \overline{x_n})$ приобретёт вид

$$P(\overline{x_1}, \dots, \overline{x_n}) = 1 \oplus P(x_1, \dots, x_n) \oplus N(x_1, \dots, x_n) = \overline{P}(x_1, \dots, x_n) \oplus N(x_1, \dots, x_n).$$

При $N = 0$ выполнено условие самодвойственности (2):

$$P(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}) = \overline{P}(x_1, \dots, x_n).$$

□

Из Теоремы 2 следует, что самодвойственность в полиномах Жегалкина определяется двойственным остатком. Если двойственный остаток равен 0 для любых наборов значений переменных $x_1, x_2, \dots, x_n$, то можно говорить о самодвойственности функции. Проверка данного условия путём последовательного рассмотрения двойственного остатка на каждом из наборов выглядит трудоёмкой задачей. Поэтому результат Теоремы 2 скорее теоретический, чем практический. Решению этой проблемы посвящён следующий раздел.

4.2. Система ведущих коэффициентов

Обозначим через $P_{i_1,\dots,i_k}$ полином Жегалкина $P'(x_{i_1}, \dots, x_{i_k})$, в котором все коэффициенты, кроме старшего и свободного, единичные:

$$P_{i_1} = P'(x_{i_1}) = 0,$$

$$P_{i_1,\dots,i_k} = P'(x_{i_1}, \dots, x_{i_k}) = x_{i_1} \oplus x_{i_2} \oplus \dots \oplus x_{i_k} \oplus x_{i_1}x_{i_2} \oplus x_{i_1}x_{i_3} \oplus \dots \oplus x_{i_1}x_{i_2} \cdots x_{i_{k-1}} \oplus x_{i_1}x_{i_2} \cdots x_{i_{k-2}}x_{i_k} \oplus \dots \oplus x_{i_2}x_{i_3} \cdots x_{i_k}.$$

Пример 1. Построим полином $P_{1,2,3}$.

Полином Жегалкина $P(x_1, x_2, x_3)$ в общем виде имеет следующее представление:

$$P(x_1, x_2, x_3) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_{1,2}x_1x_2 \oplus a_{1,3}x_1x_3 \oplus a_{2,3}x_2x_3 \oplus a_{1,2,3}x_1x_2x_3.$$

В полиноме $P_{1,2,3}$ по определению старший и свободный коэффициенты равны 0: $a_0 = a_{1,2,3} = 0$. Все остальные коэффициенты равны 1. Полином $P_{1,2,3} = P'(x_1, x_2, x_3)$ записывается следующим образом:

$$P_{1,2,3} = x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3.$$

Двойственный остаток N полинома P можно переписать через полиномы $P_{i_1,\dots,i_k}$:

$$N(x_1, \dots, x_n) = a_{1,2}(x_1 \oplus x_2) \oplus a_{1,3}(x_1 \oplus x_3) \oplus \dots \oplus a_{1,\dots,n}(x_1x_2 \cdots x_{n-1} \oplus x_1x_2 \cdots x_{n-2}x_n \oplus \dots \oplus x_1 \oplus x_2 \oplus \dots \oplus x_n) \iff$$

$$\iff N(x_1, \dots, x_n) = a_{1,2}P_{1,2} \oplus a_{1,3}P_{1,3} \oplus \dots \oplus a_{1,\dots,n}P_{1,\dots,n}.$$

Лемма 5. *Число слагаемых полинома $P_{i_1,\dots,i_k}$ чётно.*

Доказательство. Число слагаемых полинома $P_{i_1,\dots,i_k}$ можно найти через сумму числа сочетаний, где каждому сочетанию C_k^i соответствует число способов сформировать конъюнкцию i-ой степени из k переменных:

$$C_k^1 + C_k^2 + \dots + C_k^{k-1} = 2^k - 2.$$

□

Теорема 3. *Функция, соответствующая полиному Жегалкина $P_{i_1,\dots,i_k}$, на любом наборе значений переменных, кроме нулевого и единичного, равна 1.*

Доказательство. На нулевом наборе все слагаемые полинома $P_{i_1,\dots,i_k}$ равны 0. Значит, $P'(0,\dots,0) = 0$. На единичном наборе все слагаемые полинома $P_{i_1,\dots,i_k}$ равны 1. По Лемме 5 число всех слагаемых полинома $P_{i_1,\dots,i_k}$ чётно. Следовательно, $P'(1,\dots,1) = 0$.

Теперь рассмотрим произвольный набор значений переменных $\tilde{\alpha} = (\alpha_{i_1},\dots,\alpha_{i_k})$, для которого выполняется условие, что $\exists t, p \in \overline{1,k},\ t \neq p\colon\ \alpha_{i_t} = 1,\ \alpha_{i_p} = 0$.

В полиноме $P_{i_1,\dots,i_k}$ конъюнкции, содержащие переменную x_{i_p}, равны 0 для всех найденных p. Рассмотрим полином $P_{i_1,\dots,i_k}$ без этих конъюнкций (считаем их равными 0). Полином содержит только конъюнкции с переменными x_{i_t} для найденных t. Будем считать, что таких t было найдено m штук, где $m < k$:

$$P_{i_1,\dots,i_k}(\tilde{\alpha}) = P'(\alpha_{i_{t_1}},\dots,\alpha_{i_{t_m}}) \oplus \alpha_{i_{t_1}} \cdots \alpha_{i_{t_m}} = P_{i_{t_1},\dots,i_{t_m}} \oplus \alpha_{i_{t_1}} \cdots \alpha_{i_{t_m}}.$$

По Лемме 5 число слагаемых $P_{i_{t_1},\dots,i_{t_m}}$ чётно. Все слагаемые $P_{i_{t_1},\dots,i_{t_m}}$ на наборе $\tilde{\alpha}$ равны 1. Следовательно, $P_{i_{t_1},\dots,i_{t_m}} = 0$.

Все члены конъюнкции $\alpha_{i_{t_1}} \cdots \alpha_{i_{t_m}}$ равны 1. Следовательно, сама конъюнкция равна 1. Таким образом, полином $P_{i_1,\dots,i_k}$ на наборе $\tilde{\alpha}$ равен 1.

□

Определение 2. Коэффициент $a_{i_1,\dots,i_k}$ полинома двойственного остатка $N(x_1,\dots,x_n)$ назовём *ведущим на наборе* $\tilde{\alpha} = (\alpha_1,\dots,\alpha_n)$, $k \leqslant n$, если соответствующий этому коэффициенту полином $P_{i_1,\dots,i_k}$ на наборе $\tilde{\alpha}$ принимает значение 1.

Теорема 2 утверждает, что самодвойственность функции f определяется двойственным остатком N соответствующего функции f полинома P. Если для всех наборов переменных $x_1, x_2, \dots, x_n$ двойственный остаток N равен 0, то сохраняющая 0 и 1 или не сохраняющая ни 0, ни 1 функция f является самодвойственной. Значение полинома N на некотором наборе переменных $(\alpha_1,\dots,\alpha_n)$ определяется ведущими на этом наборе коэффициентами.

Равенство нулю двойственного остатка N для любого набора переменных $x_1, x_2, \dots, x_n$ означает, что вектор значений коэффициентов $a_{1,2}, a_{1,3}, \dots, a_{1,\dots,n}$ является решением системы:

$$\begin{cases} N(0,0,0,\dots,0,0) = 0, \\ N(1,0,0,\dots,0,0) = 0, \\ N(0,1,0,\dots,0,0) = 0, \\ N(1,1,0,\dots,0,0) = 0, \\ \dots \\ N(1,0,1,\dots,1,1) = 0, \\ N(0,1,1,\dots,1,1) = 0, \\ N(1,1,1,\dots,1,1) = 0. \end{cases} \tag{4}$$

Для того чтобы определить, является ли коэффициент $a_{i_1,\dots,i_k}$ ведущим на наборе $\tilde{\alpha}$, необходимо вычислить значение полинома $P_{i_1,\dots,i_k}$ на этом наборе $\tilde{\alpha}$. Следующая теорема позволяет находить ведущие коэффициенты без использования полиномов $P_{i_1,\dots,i_k}$.

Теорема 4. *Коэффициент $a_{i_1,\dots,i_k}$ полинома двойственного остатка $N(x_1,\dots,x_n)$ является ведущим на наборе $\tilde{\alpha} = (\alpha_1,\dots,\alpha_n)$, если $\exists\ t, p \in \overline{1,k},\ t \neq p\ :\ \alpha_{i_t} = 1$ и $\alpha_{i_p} = 0$.*

Коэффициент $a_{i_1,\dots,i_k}$ не является ведущим на наборе $\tilde{\alpha}$, если для $\forall t \in \overline{1,k}$ выполнено $\alpha_{i_t} = 1$ или если для $\forall p \in \overline{1,k}$ выполнено $\alpha_{i_p} = 0$.

Доказательство. Если $\forall t \in \overline{1,k}$ имеем $\alpha_{i_t} = 1$, то для полинома $P_{i_1,\dots,i_k}$ набор $\tilde{\alpha}$ является единичным. Из Теоремы 3 следует, что $P_{i_1,\dots,i_k} = 0$. По определению $a_{i_1,\dots,i_k}$ не является ведущим коэффициентом.

Если $\forall p \in \overline{1,k}$ имеем $\alpha_{i_p} = 0$, то для полинома $P_{i_1,\dots,i_k}$ набор $\tilde{\alpha}$ является нулевым. Из Теоремы 3 следует, что $P_{i_1,\dots,i_k} = 0$. Таким образом, $a_{i_1,\dots,i_k}$ — не ведущий коэффициент.

Теперь пусть $\exists\ t, p \in \overline{1,k},\ t \neq p : \alpha_{i_t} = 1$ и $\alpha_{i_p} = 0$. Для полинома $P_{i_1,\dots,i_k}$ набор $\tilde{\alpha}$ не является ни единичным, ни нулевым. Следовательно, по Теореме 3 полином $P_{i_1,\dots,i_k}$ на наборе $\tilde{\alpha}$ равен 1. Получили, что $a_{i_1,\dots,i_k}$ — ведущий коэффициент.

□

Теорема 4 позволяет переписать систему (4) через ведущие коэффициенты. Перед тем как это сделать, систему (4) можно упростить, используя следующую теорему:

Теорема 5. *Полином двойственного остатка N любого полинома Жегалкина P обладает свойством антисамодвойственности. Причём если коэффициент $a_{i_1,\dots,i_k}$ был ведущим на наборе значений переменных $(\alpha_1,\dots,\alpha_n)$, то он является ведущим и на противоположном наборе $(\overline{\alpha_1},\dots,\overline{\alpha_n})$.*

Доказательство. Рассмотрим $N(\overline{x_1},\dots,\overline{x_n})$:

$$N(\overline{x_1},\dots,\overline{x_n}) = a_{1,2}P'(\overline{x_1},\overline{x_2}) \oplus a_{1,3}P'(\overline{x_1},\overline{x_3}) \oplus \dots \oplus a_{1,\dots,n}P'(\overline{x_1},\dots,\overline{x_n}).$$

Из Теоремы 3 следует, что полином $P_{i_1,\dots,i_k}$, где $k \leqslant n$, равен 0 на нулевом и единичном, то есть противоположном к нулевому, наборах переменных. По той же Теореме значение полинома $P_{i_1,\dots,i_k}$ на любом другом наборе и противоположном к нему равно 1. Следовательно, $P_{i_1,\dots,i_k}$ обладает свойством антисамодвойственности:

$$P'(\overline{x_{i_1}},\dots,\overline{x_{i_k}}) = P'(x_{i_1},\dots,x_{i_k}) = P_{i_1,\dots,i_k}.$$

Полином двойственного остатка N также обладает свойством антисамодвойственности. Причём все ведущие коэффициенты на некотором наборе переменных $\tilde{\alpha}$ остаются ведущими и на противоположном к $\tilde{\alpha}$ наборе:

$$N(\overline{x_1},\dots,\overline{x_n}) = a_{1,2}P_{1,2} \oplus a_{1,3}P_{1,3} \oplus \dots \oplus a_{1,\dots,n}P_{1,\dots,n} = N(x_1,\dots,x_n).$$

□

Из Теоремы 5 следует, что система (4) содержит одинаковые уравнения. Так как N на любом наборе значений переменных $\tilde{\alpha}$ имеет такой же вид как на противоположном к $\tilde{\alpha}$ наборе, в системе (4) достаточно рассмотреть только половину всех входных наборов. Следующая теорема показывает, что выбор таковой половины можно проводить относительно любой переменной $x_1, x_2, \dots, x_n$.

Лемма 6.

$$\forall i,j \in \overline{1,n} : \forall(\alpha_1,\alpha_2,\dots,\alpha_{i-1},\alpha_{i+1},\dots,\alpha_n)\ \exists\ (\beta_1,\beta_2,\dots,\beta_{j-1},\beta_{j+1},\dots,\beta_n):$$

$$N(\alpha_1,\alpha_2,\dots,\alpha_{i-1},0,\alpha_{i+1},\dots,\alpha_n) = N(\beta_1,\beta_2,\dots,\beta_{j-1},0,\beta_{j+1},\dots,\beta_n).$$

Доказательство. Если $i = j$, то равенство выполняется при $\beta_1 = \alpha_1, \dots, \beta_{i-1} = \alpha_{i-1}, \beta_{i+1} = \alpha_{i+1}, \dots, \beta_n = \alpha_n$:

$$N(\alpha_1,\alpha_2,\dots,\alpha_{i-1},0,\alpha_{i+1},\dots,\alpha_n) = N(\alpha_1,\alpha_2,\dots,\alpha_{i-1},0,\alpha_{i+1},\dots,\alpha_n).$$

Пусть $i \neq j$. Не ограничивая общности рассуждений, положим, что $i < j$. Если $\alpha_j = 0$, то равенство выполняется при $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_{i-1} = \alpha_{i-1}, \beta_i = 0, \beta_{i+1} = \alpha_{i+1}, \dots, \beta_n = \alpha_n$:

$$N(\alpha_1,\alpha_2,\dots,\alpha_{i-1},0,\alpha_{i+1},\dots,\alpha_{j-1},0,\alpha_{j+1},\dots,\alpha_n) = N(\alpha_1,\alpha_2,\dots,\alpha_{i-1},0,\alpha_{i+1},\dots,\alpha_{j-1},0,\alpha_{j+1},\dots,\alpha_n).$$

Если $\alpha_j = 1$, то $\overline{\alpha_j} = 0$. Из Теоремы 5 получаем

$$N(\alpha_1, \alpha_2, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_{j-1}, 1, \alpha_{j+1}, \dots, \alpha_n) = N(\overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_{i-1}}, 1, \overline{\alpha_{i+1}}, \dots, \overline{\alpha_{j-1}}, 0, \overline{\alpha_{j+1}}, \dots, \overline{\alpha_n}).$$

Утверждение Леммы выполняется, если в качестве β выбрать следующие числа: $\beta_1 = \overline{\alpha_1}, \beta_2 = \overline{\alpha_2}, \dots, \beta_{i-1} = \overline{\alpha_{i-1}}, \beta_i = 1, \beta_{i+1} = \overline{\alpha_{i+1}}, \dots, \beta_n = \overline{\alpha_n}$. □

Благодаря Лемме 6 для исключения повторяющихся уравнений в системе (4) достаточно рассмотреть наборы, где одна переменная равна 0. Пусть этой переменной будет x_n. Сделаем ещё одно упрощение: так как на нулевом наборе значений переменных никакой коэффициент не является ведущим, исключим этот набор из системы (4). Получим систему вида:

$$\begin{cases} N(1, 0, 0, \dots, 0, 0) = 0, \\ N(0, 1, 0, \dots, 0, 0) = 0, \\ N(1, 1, 0, \dots, 0, 0) = 0, \\ \dots \\ N(0, 1, 1, \dots, 1, 0) = 0, \\ N(1, 1, 1, \dots, 1, 0) = 0. \end{cases} \tag{5}$$

Теперь, используя Теорему 4, каждое уравнение системы (5) можно переписать через сумму ведущих коэффициентов:

$$\begin{cases} a_{1,2} \oplus a_{1,3} \oplus \dots \oplus a_{1,n} \oplus \dots \oplus a_{1,3,4,\dots,n} \oplus a_{1,2,3,\dots,n} = 0, \\ a_{1,2} \oplus a_{2,3} \oplus \dots \oplus a_{2,n} \oplus \dots \oplus a_{2,3,4,\dots,n} \oplus a_{1,2,3,\dots,n} = 0, \\ a_{1,3} \oplus a_{1,4} \oplus \dots \oplus a_{1,n} \oplus a_{2,3} \oplus a_{2,4} \oplus \dots \oplus a_{2,n} \oplus \dots \oplus a_{2,3,4,\dots,n} \oplus a_{1,2,3,\dots,n} = 0, \\ \dots\dots\dots \\ a_{1,2} \oplus a_{1,3} \oplus \dots \oplus a_{1,(n-1)} \oplus a_{2,n} \oplus a_{3,n} \oplus a_{(n-1),n} \oplus \dots \oplus a_{2,3,4,\dots,n} \oplus a_{1,2,3,\dots,n} = 0, \\ a_{1,n} \oplus a_{2,n} \oplus \dots \oplus a_{(n-1),n} \oplus \dots \oplus a_{2,3,4,\dots,n} \oplus a_{1,2,3,\dots,n} = 0. \end{cases} \tag{6}$$

4.3. Критерий самодвойственности

Система (6) представляет собой систему линейных булевых уравнений. Чтобы решить полученную систему, приведём её к ступенчатому виду, используя метод, близкий к классическому методу Гаусса для решения систем линейных алгебраических уравнений [12]. Сначала для каждого уравнения системы (6) построим прямые суммы $S_d^{i_1,i_2,\dots,i_k}$, а затем обратные суммы $S_r^{i_1,i_2,\dots,i_k}$, $k \in \overline{1, n-1}$.

Замечание. С этого момента в индексах коэффициентов, наборов переменных и сумм могут использоваться операции над множествами, чтобы показать, что расширение индекса может происходить добавлением не только последовательно идущих чисел, но любых чисел, отсутствующих в исходном индексе.

Обозначим через $\alpha^{i_1,i_2,\dots,i_k}$ набор значений переменных $x_1, x_2, \dots, x_n$, в котором $x_{i_1} = 1$, $x_{i_2} = 1, \dots, x_{i_k} = 1$, а все остальные переменные в наборе равны 0.

Через $S_d^{i_1,i_2,\dots,i_k}$ обозначим сумму

$$N(\alpha^{i_1}) \oplus N(\alpha^{i_2}) \oplus \dots \oplus N(\alpha^{i_k}) \oplus N(\alpha^{i_1,i_2}) \oplus N(\alpha^{i_1,i_3}) \oplus \dots \oplus N(\alpha^{i_{k-1},i_k}) \oplus \dots \oplus N(\alpha^{i_1,i_2,\dots,i_{k-1}}) \oplus$$

$$\oplus N(\alpha^{i_1,i_2,\dots,i_{k-2},i_k}) \oplus \dots \oplus N(\alpha^{i_2,i_3,\dots,i_k}) \oplus N(\alpha^{i_1,i_2,\dots,i_k}),$$

где N — полином двойственного остатка, $k \in \overline{1, n-1}$.

Через $S_r^{i_1,i_2,\ldots,i_k}$, $k \in \overline{1,n-1}$, обозначим сумму

$$S_r^{1,2,\ldots,(n-1)} = S_d^{1,2,\ldots,(n-1)},$$

$$S_r^{i_1,i_2,\ldots,i_k} = S_d^{i_1,i_2,\ldots,i_k} \oplus \bigoplus_{\substack{1\leqslant i_{k+1}<i_{k+2}<\ldots<i_{k+l}\leqslant n-1 \\ \{i_{k+1},i_{k+2},\ldots,i_{k+l}\}\cap\{i_1,i_2,\ldots,i_k\}=\varnothing \\ l\in\overline{1,n-1-k}}} S_r^{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},\ldots,i_{k+l}\}},\ k \in \overline{1,n-2}.$$

Последняя запись означает, что при формировании суммы $S_r^{i_1,i_2,\ldots,i_k}$ учитываются суммы S_r большего порядка, степень которых образуется из чисел i_1, i_2, …, i_k и чисел 1, 2, …, n, не вошедших в множество $\{i_1, i_2, \ldots, i_k\}$

Пример 2. Решим систему (6) для n, равного 4, используя прямые и обратные суммы S_d и S_r.

$$\begin{cases} N(1,0,0,0) = 0, \\ N(0,1,0,0) = 0, \\ N(1,1,0,0) = 0, \\ N(0,0,1,0) = 0, \\ N(1,0,1,0) = 0, \\ N(0,1,1,0) = 0, \\ N(1,1,1,0) = 0. \end{cases} \Leftrightarrow \begin{cases} a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,3} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,3} \oplus a_{2,3} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2} \oplus a_{1,4} \oplus a_{2,3} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2} \oplus a_{2,4} \oplus a_{1,3} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,4} \oplus a_{2,4} \oplus a_{3,4} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0. \end{cases}$$

Образуем прямые суммы S_d:

$$S_d^1 = N(\alpha^1),$$
$$S_d^2 = N(\alpha^2),$$
$$S_d^{1,2} = N(\alpha^1) \oplus N(\alpha^2) \oplus N(\alpha^{1,2}),$$
$$S_d^3 = N(\alpha^3),$$
$$S^{1,3} = N(\alpha^1) \oplus N(\alpha^3) \oplus N(\alpha^{1,3}),$$
$$S_d^{2,3} = N(\alpha^2) \oplus N(\alpha^3) \oplus N(\alpha^{2,3}),$$
$$S_d^{1,2,3} = N(\alpha^1) \oplus N(\alpha^2) \oplus N(\alpha^3) \oplus N(\alpha^{1,2}) \oplus N(\alpha^{1,3}) \oplus N(\alpha^{2,3}) \oplus N(\alpha^{1,2,3}).$$

Преобразуем систему через суммирование строк системы по правилам прямых сумм S_d, описанным выше:

$$\begin{cases} S_d^1 = 0, \\ S_d^2 = 0, \\ S_d^{1,2} = 0, \\ S_d^3 = 0, \\ S_d^{1,3} = 0, \\ S_d^{2,3} = 0, \\ S_d^{1,2,3} = 0. \end{cases} \Leftrightarrow \begin{cases} a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,3} \oplus a_{2,3} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2,3} \oplus a_{1,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2,3} \oplus a_{2,3,4} \oplus a_{1,2,3,4} = 0, \\ a_{1,2,3,4} = 0. \end{cases}$$

Теперь образуем обратные суммы S_r:

$$S_r^{1,2,3} = S_d^{1,2,3} = a_{1,2,3,4},$$

$$S_r^{2,3} = S_d^{2,3} \oplus S_r^{1,2,3} = a_{1,2,3} \oplus a_{2,3,4} \oplus a_{1,2,3,4} \oplus a_{1,2,3,4} = a_{1,2,3} \oplus a_{2,3,4},$$

$$S_r^{1,3} = S_d^{1,3} \oplus S_d^{1,2,3} = a_{1,2,3} \oplus a_{1,3,4} \oplus a_{1,2,3,4} \oplus a_{1,2,3,4} = a_{1,2,3} \oplus a_{1,3,4},$$

$$S_r^3 = S_d^3 \oplus S_r^{1,3} \oplus S_r^{2,3} \oplus S_r^{1,2,3} = a_{1,3} \oplus a_{2,3} \oplus a_{3,4} \oplus a_{1,2,3} \oplus a_{1,3,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} \oplus a_{1,2,3} \oplus a_{1,3,4} \oplus a_{1,2,3} \oplus a_{2,3,4} \oplus a_{1,2,3,4} =$$

$$= a_{1,3} \oplus a_{2,3} \oplus a_{3,4} \oplus a_{1,2,3},$$

$$S_r^{1,2} = S_d^{1,2} \oplus S_r^{1,2,3} = a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,2,3,4} \oplus a_{1,2,3,4} = a_{1,2,3} \oplus a_{1,2,4},$$

$$S_r^2 = S_d^2 \oplus S_r^{1,2} \oplus S_r^{2,3} \oplus S_r^{1,2,3} = a_{1,2} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{2,3,4} \oplus a_{1,2,3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,2,3} \oplus a_{2,3,4} \oplus a_{1,2,3,4} =$$

$$= a_{1,2} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{1,2,3},$$

$$S_r^1 = S_d^1 \oplus S_r^{1,2} \oplus S_r^{1,3} \oplus S_r^{1,2,3} = a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,3,4} \oplus a_{1,2,3,4} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus a_{1,2,3} \oplus a_{1,3,4} \oplus a_{1,2,3,4} =$$

$$= a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{1,2,3}.$$

На месте каждой прямой суммы S_d в системе сформируем сумму S_r по правилам, указанным выше:

$$\begin{cases} S_d^{1,2,3} = 0, \\ S_d^{2,3} = 0, \\ S_d^{1,3} = 0, \\ S_d^3 = 0, \\ S_d^{1,2} = 0, \\ S_d^2 = 0, \\ S_d^1 = 0. \end{cases} \Leftrightarrow \begin{cases} S_r^{1,2,3} = 0, \\ S_r^{2,3} = 0, \\ S_r^{1,3} = 0, \\ S_r^3 = 0, \\ S_r^{1,2} = 0, \\ S_r^2 = 0, \\ S_r^1 = 0. \end{cases} \Leftrightarrow \begin{cases} a_{1,2,3,4} = 0, \\ a_{1,2,3} \oplus a_{2,3,4} = 0, \\ a_{1,2,3} \oplus a_{1,3,4} = 0, \\ a_{1,3} \oplus a_{2,3} \oplus a_{3,4} \oplus a_{1,2,3} = 0, \\ a_{1,2,3} \oplus a_{1,2,4} = 0, \\ a_{1,2} \oplus a_{2,3} \oplus a_{2,4} \oplus a_{1,2,3} = 0, \\ a_{1,2} \oplus a_{1,3} \oplus a_{1,4} \oplus a_{1,2,3} = 0. \end{cases}$$

В качестве свободных переменных в векторе решения возьмём $a_{1,2}$, $a_{1,3}$, $a_{2,3}$, $a_{1,2,3}$. Тогда решение системы можно выписать следующим образом:

$$a_{1,2,3,4} = 0,$$

$$a_{2,3,4} = a_{1,3,4} = a_{1,2,4} = a_{1,2,3},$$

$$a_{3,4} = a_{1,3} \oplus a_{2,3} \oplus a_{1,2,3},$$

$$a_{2,4} = a_{1,2} \oplus a_{2,3} \oplus a_{1,2,3},$$

$$a_{1,4} = a_{1,2} \oplus a_{1,3} \oplus a_{1,2,3}.$$

Определение 3. Коэффициент $a_{j_1,j_2,\ldots,j_m}$, $m \leqslant n$, полинома двойственного остатка $N(x_1, \ldots, x_n)$ назовём *ведущим на сумме* $S_d^{i_1,i_2,\ldots,i_k}$ ($S_r^{i_1,i_2,\ldots,i_k}$), $k \in \overline{1, n-1}$, если он является ведущим коэффициентом на нечётном числе наборов соответствующих слагаемых суммы $S_d^{i_1,i_2,\ldots,i_k}$ (на нечётном числе слагаемых суммы $S_r^{i_1,i_2,\ldots,i_k}$).

Использование чётности в определении ведущего на сумме коэффициента естественно возникает из того факта, что чётное количество равных слагаемых в сумме по модулю 2 даёт 0. Соответственно, чтобы коэффициент присутствовал в сумме, необходимо, чтобы он входил в нечётное число слагаемых.

Число слагаемых суммы $S_d^{i_1,i_2,\ldots,i_k}$ может быть довольно большим. При определении ведущего на сумме коэффициента перебор всех слагаемых суммы выглядит трудоёмкой задачей. Сократим этот перебор. Для этого сумму $S_d^{i_1,i_2,\ldots,i_k}$ разобьём на 2 части. Первая часть S_1 будет содержать слагаемые, соответствующие наборам, где переменная x_{i_1} равна 0, а вторая S_2 — слагаемые, соответствующие наборам, где переменная x_{i_1} равна 1. Подобное разбиение можно проводить относительно любой переменной $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$, но для определённости была выбрана переменная x_{i_1}.

Определение 4. Набор $\tilde{\beta} = (\beta_1, \beta_2, \dots, \beta_n)$ назовём *парным* к набору $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ *относительно переменной* x_k, $k \in \overline{1,n}$, если $\tilde{\beta}$ отличается от $\tilde{\alpha}$ только значением переменной x_k

$$\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_{k-1} = \alpha_{k-1}, \beta_k = \overline{\alpha_k}, \beta_{k+1} = \alpha_{k+1}, \dots, \beta_n = \alpha_n.$$

Далее, будем рассматривать парные наборы относительно только переменной x_{i_1} ввиду того, что разбиение суммы $S_d^{i_1,i_2,\dots,i_k}$ на S_1 и S_2 было проведено относительно этой переменной.

Лемма 7. *Для выбранного числа $i_1 \in \{j_1, j_2, \dots, j_m\}$ коэффициент $a_{j_1,j_2,\dots,j_m}$, $m \leqslant n$, является ведущим на сумме $S_d^{i_1,i_2,\dots,i_k}$ тогда и только тогда, когда он является ведущим на нечётном числе наборов, для которых*

$$x_{j_1} = 1, x_{j_2} = 1, \dots, x_{i_1} = 0, \dots, x_{j_m} = 1 \tag{7}$$

или

$$x_{j_1} = 0, x_{j_2} = 0, \dots, x_{i_1} = 1, \dots, x_{j_m} = 0 \tag{8}$$

и значения прочих переменных подобраны таким образом, чтобы полученные наборы соответствовали слагаемым суммы $S_d^{i_1,i_2,\dots,i_k}$.

Доказательство. Покажем, что из нечётности числа наборов вида (7) и (8), соответствующих слагаемым суммы $S_d^{i_1,i_2,\dots,i_k}$, следует, что коэффициент $a_{j_1,j_2,\dots,j_m}$ является ведущим на сумме $S_d^{i_1,i_2,\dots,i_k}$.

Если некоторый коэффициент $a_{j_1,j_2,\dots,j_m}$ являлся ведущим на каком-то наборе слагаемого суммы S_1 и на парном к нему наборе слагаемого суммы S_2, то он является ведущим на двух наборах суммы $S_d^{i_1,i_2,\dots,i_k}$. Соответственно, число всех парных наборов слагаемых сумм S_1 и S_2, на которых коэффициент $a_{j_1,j_2,\dots,j_m}$ будет ведущим, является чётным. Поэтому для проверки чётности числа вообще всех наборов в сумме $S_d^{i_1,i_2,\dots,i_k}$, на которых рассматриваемый коэффициент является ведущим, будет достаточно рассмотреть только наборы специального вида, то есть такие наборы, на которых некоторый коэффициент является ведущим только в одной из сумм S_1 или S_2 и не является ведущим на парных к ним наборах в другой сумме. Так как число парных наборов всегда чётное, необходимо определить чётность числа наборов специального вида. Если их количество будет нечётным, то сумма нечётного и чётного чисел даст нечётное число и коэффициент $a_{j_1,j_2,\dots,j_m}$ будет ведущим на сумме $S_d^{i_1,i_2,\dots,i_k}$. И наоборот: если количество специальных наборов будет чётным, то вместе с чётным числом парных наборов они дадут в сумме чётное число, и коэффициент $a_{j_1,j_2,\dots,j_m}$ не будет ведущим на сумме.

По Теореме 4 коэффициент $a_{j_1,j_2,\dots,j_m}$, $m \leqslant n$, является ведущим на наборе $\tilde{\alpha}$, если $\exists t, p \in \overline{1,n}, t \neq p$: $\alpha_{j_t} = 1$ и $\alpha_{j_p} = 0$. То есть он является ведущим на наборе $\tilde{\alpha}$, если среди значений переменных $x_{j_1}, x_{j_2}, \dots, x_{j_m}$ в наборе есть хотя бы один ноль и хотя бы одна единица. Соответственно, коэффициент $a_{j_1,j_2,\dots,j_m}$ не является ведущим на наборе $\tilde{\alpha}$, когда все значения переменных $x_{j_1}, x_{j_2}, \dots, x_{j_m}$ в этом наборе равны 1 или равны 0. Такие наборы будут парными относительно переменной x_{i_1} для наборов соответствующих слагаемых S_1 вида $x_{j_1} = 1, x_{j_2} = 1, \dots, x_{i_1} = 0, \dots, x_{j_m} = 1$ и наборов соответствующих слагаемых S_2 вида $x_{j_1} = 0, x_{j_2} = 0, \dots, x_{i_1} = 1, \dots, x_{j_m} = 0$. Как можно видеть, коэффициент $a_{j_1,j_2,\dots,j_m}$ по Теореме 4 является ведущим на наборах вида (7) и (8). Если таких наборов нечётное число, то коэффициент $a_{j_1,j_2,\dots,j_m}$ является ведущим на сумме $S_d^{i_1,i_2,\dots,i_k}$, в противном случае — не является ведущим.

Докажем утверждение Леммы в обратную сторону. Пусть коэффициент $a_{j_1,j_2,\dots,j_m}$ является ведущим на сумме $S_d^{i_1,i_2,\dots,i_k}$. По определению это означает, что коэффициент $a_{j_1,j_2,\dots,j_m}$ является ведущим на нечётном числе наборов соответствующих слагаемых суммы $S_d^{i_1,i_2,\dots,i_k}$. Среди этих наборов присутствуют парные наборы слагаемых сумм S_1 и S_2, на которых коэффициент $a_{j_1,j_2,\dots,j_m}$ является ведущим. Таких наборов всегда чётное число. Поэтому, исключив их из общего нечётного числа наборов, для которых коэффициент $a_{j_1,j_2,\dots,j_m}$ ведущий, получим нечётное число оставшихся наборов.

Такими наборами будут наборы, на которых коэффициент $a_{j_1,j_2,\ldots,j_m}$ является ведущим только в одной из сумм S_1 и S_2 и не является ведущим на наборах, парных к данным. Как было показано ранее (в первой части доказательства), такие наборы имеют специальный вид (7) и (8). Следовательно, число наборов вида (7) и (8) в сумме нечётно. □

Используя Лемму 7, докажем следующую теорему.

Теорема 6. *На сумме $S_d^{i_1,i_2,\ldots,i_k}$ только коэффициенты вида $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{1,n-k}$, являются ведущими.*

Доказательство. Запись $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}$ означает, что в индексации коэффициента $a_{\{i_1,i_2,\ldots,i_k\}}$ мы добавляем числа $1, 2, \ldots, n$, отличные от $i_1, i_2, \ldots, i_k$, в количестве от 1 до l.

Рассмотрим случай при $k = 1$: $S_d^{i_1} = N(\alpha^{i_1})$. Сумма $S_d^{i_1}$ состоит только из одного слагаемого. На наборе, соответствующем этому слагаемому, $x_{i_1} = 1$ и $\forall j \in \overline{2,n} : x_{i_j} = 0$. По Теореме 4 ведущими на наборе α^{i_1} будут только те коэффициенты, которые содержат i_1, т. е. $a_{\{i_1\}\cup\{i_2,\ldots,i_{1+l}\}}, \forall l \in \overline{1,n-1}$.

При $k > 1$ требуется рассмотреть 4 случая:

1) Коэффициент $a_{i_1,i_2,\ldots,i_k}$ не является ведущим на сумме $S_d^{i_1,i_2,\ldots,i_k}$.
2) Коэффициенты вида $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{1,n-k}$, являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_k}$.
3) Коэффициенты, полученные из $a_{i_1,i_2,\ldots,i_k}$ исключением из индекса коэффициента одного или более чисел $i_1, i_2, \ldots, i_k$, не являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_k}$.
4) Коэффициенты, полученные из $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{1,n-k}$, исключением из индекса коэффициента одного или более чисел $i_1, i_2, \ldots, i_k$, не являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_k}$.

В каждом конкретном случае необходимо посчитать количество наборов вида (7) и (8) Леммы 7. Если полученное число будет нечётным, то коэффициент является ведущим на сумме, иначе коэффициент не будет являться ведущим.

1. Рассмотрим коэффициент $a_{i_1,i_2,\ldots,i_k}$. Такой коэффициент является ведущим на единственном наборе вида (8) — наборе α^{i_1}. Этот набор соответствует слагаемому $N(\alpha^{i_1})$ суммы $S_d^{i_1,i_2,\ldots,i_k}$:

$$S_d^{i_1,i_2,\ldots,i_k} = N(\alpha^{i_1}) \oplus N(\alpha^{i_2}) \oplus \ldots \oplus N(\alpha^{i_k}) \oplus N(\alpha^{i_1,i_2}) \oplus N(\alpha^{i_1,i_3}) \oplus \ldots \oplus N(\alpha^{i_{k-1},i_k}) \oplus \ldots \oplus N(\alpha^{i_1,i_2,\ldots,i_{k-1}}) \oplus$$

$$\oplus N(\alpha^{i_1,i_2,\ldots,i_{k-2},i_k}) \oplus \ldots \oplus N(\alpha^{i_2,i_3,\ldots,i_k}) \oplus N(\alpha^{i_1,i_2,\ldots,i_k}).$$

Набором специального вида (7) в этом случае является единственный набор $\alpha^{i_2,i_3,\ldots,i_k}$. Он соответствует слагаемому $N(\alpha^{i_2,i_3,\ldots,i_k})$.

Таким образом, коэффициент $a_{i_1,i_2,\ldots,i_k}$ является ведущим на двух наборах специального вида. Следовательно, по Лемме 7 коэффициент $a_{i_1,i_2,\ldots,i_k}$ не является ведущим на сумме $S_d^{i_1,i_2,\ldots,i_k}$.

2. Теперь рассмотрим коэффициенты вида $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{1,n-k}$. Слагаемым суммы $S_d^{i_1,i_2,\ldots,i_k}$ соответствуют наборы, в которых только переменные $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ могут принимать единичные значения. Следовательно, значения переменных $x_{i_{k+1}}, x_{i_{k+2}}, \ldots, x_{i_{k+l}}$ на любых наборах в сумме $S_d^{i_1,i_2,\ldots,i_k}$ равны 0. Так как $l > 0$, то в любом наборе слагаемых суммы $S_d^{i_1,i_2,\ldots,i_k}$ всегда найдётся хотя бы один ноль среди значений переменных $x_{i_{k+1}}, x_{i_{k+2}}, \ldots, x_{i_{k+l}}$. Но в наборах специального вида (7) среди переменных $x_{i_1}, x_{i_2}, \ldots, x_{i_{k+l}}$ только переменная x_{i_1} должна быть равна 0. Следовательно, наборов вида (7) для рассматриваемых коэффициентов не будет.

К наборам вида (8) будет относиться только один набор α^{i_1}. Следовательно, поскольку набор специального вида всего один, то коэффициенты, имеющие вид $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{1,n-k}$, по Лемме 7 являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_k}$.

3. В коэффициенте $a_{i_1,i_2,\ldots,i_k}$ исключим из индекса некоторое количество чисел i_1, i_2, ..., i_k. Будем считать, что число i_1 не было исключено. В противном случае разбиение на S_1 и S_2 проведём относительно любой другой переменной x_{i_j}, где i_j — одно из оставшихся в индексе чисел i_2, i_3, ..., i_k.

Из индекса может быть исключено не более $(k-2)$ чисел. Только одно число остаться в индексе не может, так как коэффициенты вида a_{i_1} не являются коэффициентами полинома двойственного остатка N.

Пусть в индексе коэффициента среди чисел i_1, i_2, ..., i_k осталось m-ое количество чисел, включая i_1. К наборам специального вида (7) будут относиться такие наборы, где значение переменной x_{i_1} равно 0 и значения всех прочих $(m-1)$ переменных равны 1, а к наборам вида (8) — наборы, где значение переменной x_{i_1} равно 1 и значения всех прочих $(m-1)$ переменных равны 0. Число наборов каждого из видов (7) и (8) равно количеству способов выбрать значения $(k-m)$ переменных, номера которых были исключены из индекса коэффициента, то есть равно чётному числу

$$2^{k-m}.$$

По Лемме 7 коэффициенты для случая 3 не являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_k}$.

4. В коэффициентах вида $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{1,n-k}$, исключим из индекса некоторое количество чисел i_1, i_2, ..., i_k. Как и в случае 3, будем считать, что число i_1 не было исключено. Если были исключены все числа i_1, i_2, ..., i_k, то полученный коэффициент не будет являться ведущим ни на одном наборе слагаемых суммы $S_d^{i_1,i_2,\ldots,i_k}$. Следовательно, он не будет ведущим и на самой сумме.

Пусть в индексе коэффициента среди чисел i_1, i_2, ..., i_k осталось m-ое количество чисел, включая i_1. В данном случае к наборам специального вида типа (8) будут относиться такие наборы, в которых значение переменной x_{i_1} равно 1 и значения всех прочих $(m-1)$ переменных равны 0. Их число равно количеству способов выбрать значения $(k-m)$ переменных, номера которых были исключены из индекса коэффициента, то есть равно чётному числу

$$2^{k-m}.$$

Наборов специального вида (7) в данном случае не будет, так как значения $x_{i_{k+1}}$, $x_{i_{k+2}}$, $x_{i_{k+l}}$ на любом наборе суммы $S_d^{i_1,i_2,\ldots,i_k}$ равны 0, а на наборах вида (7) они должны быть равны 1.

Таким образом, коэффициенты, полученные из $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},i_{k+2},\ldots,i_{k+l}\}}, \forall l \in \overline{0,n-k}$, исключением одного или более чисел i_1, i_2, ..., i_k по Лемме 7 не являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_k}$. □

Используя Теорему 6, преобразуем систему ведущих коэффициентов (6) следующим образом: к каждому элементу системы $N(\alpha^{i_1,i_2,\ldots,i_k})$ мы прибавим (сложением по модулю 2) элементы, входящие в сумму $S_d^{i_1,i_2,\ldots,i_k}$, исключая тот элемент, к которому осуществляется прибавление, так как он уже принадлежит сумме $S_d^{i_1,i_2,\ldots,i_k}$. Таким образом, получим систему вида

$$\begin{cases} S_d^1 = 0, \\ S_d^2 = 0, \\ S_d^{1,2} = 0, \\ \ldots \\ S_d^{2,3,\ldots,(n-1)} = 0, \\ S_d^{1,2,\ldots,(n-1)} = 0. \end{cases} \Leftrightarrow \begin{cases} a_{1,2} \oplus a_{1,3} \oplus \ldots \oplus a_{1,n} \oplus a_{1,2,3} \oplus \ldots \oplus a_{1,3,4,\ldots,n} \oplus a_{1,2,\ldots,n} = 0, \\ a_{1,2} \oplus a_{2,3} \oplus \ldots \oplus a_{2,n} \oplus a_{1,2,3} \oplus \ldots \oplus a_{2,3,\ldots,n} \oplus a_{1,2,\ldots,n} = 0, \\ a_{1,2,3} \oplus a_{1,2,4} \oplus \ldots \oplus a_{1,2,n} \oplus a_{1,2,3,4} \oplus \ldots \oplus a_{1,2,4,5,\ldots,n} \oplus a_{1,2,\ldots,n} = 0, \\ \ldots \\ a_{1,2,\ldots,(n-1)} \oplus a_{2,3,\ldots,n} \oplus a_{1,2,\ldots,n} = 0, \\ a_{1,2,\ldots,n} = 0. \end{cases} \tag{9}$$

Теорема 7. *На сумме $S_r^{i_1,i_2,\ldots,i_k}$ ведущими являются только коэффициенты вида $a_{\{i_1,i_2,\ldots,i_k\}\cup\{i_{k+1},\ldots,i_{k+l}\}}$, $l \in \overline{1,n-k}$, где при $l>1$ для $\forall j \in \overline{k+1,k+l}$ выполнено $i_j \neq n$.*

Доказательство. Запись «$l>1$ для $\forall j \in \overline{k+1,k+l}$ выполнено $i_j \neq n$» означает, что число n может содержаться в индексе коэффициента только при $l=1$.

Доказательство проведём индукцией по k. В качестве базы индукции рассмотрим $k = n - 1$. Сумма $S_r^{i_1,i_2,\ldots,i_{n-1}}$ в этом случае имеет вид

$$S_r^{i_1,i_2,\ldots,i_{n-1}} = S_r^{1,2,\ldots,n-1} = S_d^{1,2,\ldots,n-1}.$$

Коэффициент вида $a_{\{i_1,i_2,\ldots,i_{n-1}\}\cup\{i_n,\ldots,i_{n-1+l}\}}$ всего один: $a_{1,2,\ldots,n}$, при $l = 1$. По Теореме 6 на сумме $S_d^{1,2,\ldots,n-1}$ только этот коэффициент является ведущим.

Пусть для $m \geqslant k$ на сумме $S_r^{i_1,i_2,\ldots,i_m}$ только коэффициенты вида $a_{\{i_1,i_2,\ldots,i_m\}\cup\{i_{m+1},\ldots,i_{m+l}\}}$ являются ведущими, $l \in \overline{1, n-m}$, где при $l > 1$ для $\forall j \in \overline{m+1, m+l}$ выполнено $i_j \neq n$.

Рассмотрим сумму $S_r^{i_1,i_2,\ldots,i_{m-1}}$:

$$S_r^{i_1,i_2,\ldots,i_{m-1}} = S_d^{i_1,i_2,\ldots,i_{m-1}} \oplus \bigoplus_{\substack{1\leqslant i_m<i_{m+1}<\ldots<i_{m-1+l}\leqslant n-1 \\ \{i_m,i_{m+1},\ldots,i_{m-1+l}\}\cap\{i_1,i_2,\ldots,i_{m-1}\}=\varnothing \\ l\in\overline{1,n-m}}} S_r^{\{i_1,i_2,\ldots,i_{m-1}\}\cup\{i_m,\ldots,i_{m-1+l}\}}. \tag{10}$$

По Теореме 6 на сумме $S_d^{i_1,i_2,\ldots,i_{m-1}}$ только коэффициенты вида $a_{\{i_1,i_2,\ldots,i_{m-1}\}\cup\{i_m,i_{m+1},\ldots,i_{m-1+l}\}}$ являются ведущими, для $\forall l \in \overline{1, n-m+1}$. На суммах S_d большего порядка ведущие коэффициенты также должны удовлетворять такому виду, поэтому нет необходимости отдельно рассматривать коэффициенты, не соответствующие описанному в Теореме 6 виду.

Коэффициенты, содержащие число n в своём индексе, $a_{\{i_1,i_2,\ldots,i_{m-1},\ldots,i_{m-1+l}\}\cup\{n\}}$, $l \in \overline{1, n-m}$, по предположению индукции являются ведущими только на суммах вида $S_r^{\{i_1,i_2,\ldots,i_{m-1+l}\}}$ при фиксированном l, причём каждому такому коэффициенту соответствует только одна S_r сумма. Также по Теореме 6 коэффициенты такого вида являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_{m-1}}$. Итак, среди сумм формулы (10) рассматриваемые коэффициенты будут ведущими только на двух суммах $S_d^{i_1,i_2,\ldots,i_{m-1}}$ и $S_r^{\{i_1,i_2,\ldots,i_{m-1+l}\}}$ (чётное число), то есть не будут ведущими на сумме $S_r^{i_1,i_2,\ldots,i_{m-1}}$.

Коэффициенты, не содержащие число n в своём индексе, $a_{\{i_1,i_2,\ldots,i_{m-1},\ldots,i_{m-1+l}\}}$, $l \in \overline{1, n-m}$, при $l > 1$: $i_j \neq n, j \in \overline{m, m-1+l}$, по Теореме 6 являются ведущими на сумме $S_d^{i_1,i_2,\ldots,i_{m-1}}$. По предположению индукции данные коэффициенты при фиксированном l также являются ведущими на суммах вида $S_r^{\{i_1,i_2,\ldots,i_{m-1+l-p}\}}$ при значениях p от 1 до $(m-2+l)$, то есть на суммах, полученных из $S^{\{i_1,i_2,\ldots,i_{m-1+l}\}}$ исключением p чисел из степени суммы. Число таких сумм S_r равно числу способов исключить p чисел из степени суммы $S^{\{i_1,i_2,\ldots,i_{m-1+l}\}}$. Найдём это число, используя формулу числа сочетаний:

$$C_{m-1+l}^1 + C_{m-1+l}^2 + \ldots + C_{m-1+l}^{m-2+l} = 2^{m-1+l} - 2.$$

Таким образом, общее число коэффициентов вида $a_{\{i_1,i_2,\ldots,i_{m-1},\ldots,i_{m-1+l}\}}$, $l \in \overline{1, n-m}$, где при $l > 1$ для $j \in \overline{m, m-1+l}$ выполнено $i_j \neq n$, равно нечётному числу $2^{m-1+l} - 1$. Следовательно, только такие коэффициенты будут ведущими на сумме $S_r^{i_1,i_2,\ldots,i_{m-1}}$. Шаг индукции доказан. □

С помощью Теоремы 7 преобразуем систему (9), заменив каждую сумму $S_d^{i_1,i_2,\ldots,i_k}$, $k \in \overline{1, n-1}$, соответствующей суммой $S_r^{i_1,i_2,\ldots,i_k}$:

$$\begin{cases} S_r^1 = 0, \\ S_r^2 = 0, \\ S_r^{1,2} = 0, \\ \ldots \\ S_r^{2,3,\ldots,(n-1)} = 0, \\ S_r^{1,2,\ldots,(n-1)} = 0. \end{cases} \Leftrightarrow \begin{cases} a_{1,n} \oplus a_{1,2} \oplus a_{1,3} \oplus \ldots \oplus a_{1,(n-1)} \oplus a_{1,2,3} \oplus \ldots \oplus a_{1,3,4,\ldots,(n-1)} \oplus a_{1,2,\ldots,(n-1)} = 0, \\ a_{2,n} \oplus a_{1,2} \oplus a_{2,3} \oplus \ldots \oplus a_{2,(n-1)} \oplus a_{1,2,3} \oplus \ldots \oplus a_{2,3,\ldots,(n-1)} \oplus a_{1,2,\ldots,(n-1)} = 0, \\ a_{1,2,n} \oplus a_{1,2,3} \oplus a_{1,2,4} \oplus \ldots \oplus a_{1,2,(n-1)} \oplus a_{1,2,3,4} \oplus \ldots \oplus a_{1,2,4,5,\ldots,(n-1)} \oplus \\ \oplus a_{1,2,\ldots,(n-1)} = 0, \\ \ldots \\ a_{2,3,\ldots,n} \oplus a_{1,2,\ldots,(n-1)} = 0, \\ a_{1,2,\ldots,n} = 0. \end{cases} \tag{11}$$

Число всех ведущих коэффициентов равно числу способов формирования конъюнкций из переменных $x_1, x_2, \dots, x_n$:

$$C_n^2 + C_n^3 + \dots + C_n^n = 2^n - C_n^1 - C_n^0 = 2^n - n - 1.$$

Число уравнений системы (11) равно половине всех возможных наборов значений переменных x_1, x_2, ..., x_n без нулевого набора:

$$\frac{2^n}{2} - 1 = 2^{n-1} - 1. \tag{12}$$

Таким образом, решение системы (11) должно иметь $2^{n-1} - 1$ зависимых переменных. Число свободных переменных равно

$$2^n - n - 1 - 2^{n-1} + 1 = 2^{n-1} - n. \tag{13}$$

При преобразовании системы (4) в (5) мы выбрали половину наборов переменных $x_1, x_2, \dots, x_n$, положив переменную x_n равной нулю. Это было сделано для того, чтобы в решении системы (11) зависимыми ведущими коэффициентами, выраженными через свободные коэффициенты, были те, которые в своём индексе содержат число n. Посчитаем количество таких коэффициентов в системе (11). Оно равно количеству способов выбрать числа, содержащиеся в индексе ведущего коэффициента помимо n:

$$C_{n-1}^1 + C_{n-1}^2 + \dots + C_{n-1}^{n-1} = 2^{n-1} - 1.$$

Получили число, равное количеству зависимых переменных (12). Следовательно, система (11) уже приведена к виду, где в каждой её строке записано выражение зависимых ведущих коэффициентов через свободные. Полученные условия на ведущие коэффициенты являются необходимыми и достаточными для того, чтобы полином двойственного остатка N был равен 0 на любых наборах значений переменных $x_1, x_2, \dots, x_n$.

Теорема 8. (*Критерий самодвойственности*) *Булева функция $f(x_1, x_2, \dots, x_n)$ является самодвойственной тогда и только тогда, когда коэффициенты соответствующего ей полинома Жегалкина P удовлетворяют условиям:*

$$\bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1,$$

$$a_{1,2,\dots,n} = 0,$$

$$a_{i_1,i_2,\dots,i_k,n} = \bigoplus_{\substack{1 \leqslant i_{k+1} < i_{k+2} < \dots < i_{k+l} \leqslant n-1 \\ \{i_{k+1},i_{k+2},\dots,i_{k+l}\} \cap \{i_1,i_2,\dots,i_k\} = \varnothing \\ l \in \overline{1,n-1-k}}} a_{\{i_1,i_2,\dots,i_k\} \cup \{i_{k+1},\dots,i_{k+l}\}},\ k \in \overline{1,n-2}.$$

Доказательство. По Теореме 2 сохраняющая 0 и 1 или не сохраняющая ни 0, ни 1 функция f является самодвойственной тогда и только тогда, когда двойственный остаток N соответствующего ей полинома P равен 0 для любых наборов переменных x_1, x_2, ..., x_n. Это условие выполняется тогда и только тогда, когда коэффициенты полинома P удовлетворяют системе (11). Выражая из системы (11) коэффициенты, содержащие число n в своём индексе, получаем все условия Теоремы, кроме первого.

Первое условие Теоремы фактически означает нечётность суммы единичных коэффициентов в полиноме Жегалкина P. При этом свободный коэффициент a_0 можно не учитывать. Докажем это.

Самодвойственная функция сохранят 0 и 1 или не сохраняет ни 0, ни 1. По Лемме 2, чтобы функция f сохраняла 1, сумма коэффициентов полинома P должна быть нечётной:

$$a_0 \oplus \bigoplus_{\substack{1 \leqslant i_1 < \dots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\dots,i_k} = 1.$$

Если $a_0 = 0$, то

$$\bigoplus_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\ldots,i_k} = 1.$$

Если $a_0 = 1$, то функция f не сохраняет 0 по Лемме 1. Следовательно, сумма коэффициентов полинома P должна быть чётной:

$$a_0 \oplus \bigoplus_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\ldots,i_k} = 0.$$

Из того что $a_0 = 1$, получаем

$$\bigoplus_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\ldots,i_k} = 1.$$

□

Пример 3. Пусть булева функция $f(x_1, x_2, x_3, x_4)$ представлена в виде полинома Жегалкина P:

$$P(x_1, x_2, x_3, x_4) = 1 \oplus x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4.$$

Определим, является ли функция f самодвойственной.

Свободный коэффициент a_0 равен 1. Количество единичных коэффициентов в P, за исключением свободного коэффициента, равно 5 (нечётное число). Первое условие Теоремы 8 выполнено:

$$\bigoplus_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\ldots,i_k} = 1.$$

По Теореме 8 коэффициенты полинома P также должны удовлетворять следующим условиям

$$a_{1,2,3,4} = 0,$$

$$a_{2,3,4} = a_{1,3,4} = a_{1,2,4} = a_{1,2,3},$$

$$a_{3,4} = a_{1,3} \oplus a_{2,3} \oplus a_{1,2,3},$$

$$a_{2,4} = a_{1,2} \oplus a_{2,3} \oplus a_{1,2,3},$$

$$a_{1,4} = a_{1,2} \oplus a_{1,3} \oplus a_{1,2,3}.$$

В полиноме P коэффициенты равны

$$a_{1,2,3,4} = a_{2,3,4} = a_{1,3,4} = a_{1,2,4} = a_{1,2,3} = a_{1,2} = a_{3,4} = 0,$$

$$a_{1,3} = a_{1,4} = a_{2,3} = a_{2,4} = 1.$$

Как можно видеть, условия Теоремы 8 выполняются. Следовательно, булева функция f является самодвойственной.

Пример 4. Определим, является ли самодвойственной следующая функция $f(x_1, x_2, x_3, x_4, x_5)$, представленная в виде полинома Жегалкина P:

$$P(x_1, x_2, \ldots, x_5) = 1 \oplus x_1 \oplus x_2 \oplus x_5 \oplus x_2x_5 \oplus x_1x_2x_5 \oplus x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_4x_5.$$

Старший коэффициент $a_{1,2,3,4,5}$ в полиноме P равен 1. Следовательно, по Теореме 8 функция f не является самодвойственной.

Пример 5. Используя Теорему 8, вычислим количество всех самодвойственных булевых функций от n переменных.

В Теореме 8 число свободных коэффициентов, через которые выражаются зависимые коэффициенты в системе (9), равно $2^{n-1} - n$ (см. формулу (13)). Количество способов выбора различных наборов значений этих коэффициентов равняется

$$2^{2^{n-1}-n}.$$

Кроме определения свободных коэффициентов для формирования самодвойственной функции в виде полинома Жегалкина, необходимо определить значения коэффициентов a_0, a_1, a_2, ..., a_n. По Теореме 8 эти коэффициенты должны иметь такие значения, чтобы общее количество единичных коэффициентов, за исключением свободного коэффициента, было нечётным.

Пусть количество единиц среди нелинейных коэффициентов (индекс содержит более одного числа) нечётно. Тогда число единиц среди линейных коэффициентов (индекс содержит одно число) должно быть чётным. Число способов выбрать единицы среди линейных коэффициентов равно

$$C_n^0 + C_n^2 + C_n^4 + \ldots + C_n^{2\left[\frac{n}{2}\right]} = 2^{n-1}.$$

Если количество единиц среди нелинейных коэффициентов чётно, то количество единиц среди линейных коэффициентов должно быть нечётным. Число способов выбрать единицы среди линейных коэффициентов в этом случае равно

$$C_n^1 + C_n^3 + C_n^5 + \ldots + C_n^{2\left[\frac{n-1}{2}\right]+1} = 2^{n-1}.$$

В обоих случаях число способов выбрать единицы среди линейных коэффициентов получилось одним и тем же.

Свободный коэффициент a_0 можно выбрать двумя способами: 0 или 1.

По правилу умножения общее число способов выбрать коэффициенты полинома Жегалкина таким образом, чтобы соответствующая полиному функция f была самодвойственной, равно

$$2^{2^{n-1}-n} \cdot 2 \cdot 2^{n-1} = 2^{2^{n-1}-n+n} = 2^{2^{n-1}}.$$

5. Общий вид самодостаточного оператора

После обширного раздела, посвящённого самодвойственности в полиномах Жегалкина, мы можем наконец описать общий вид полинома Жегалкина многоместного самодостаточного оператора.

Теорема 9. *Полином Жегалкина $\hat{P}$ является самодостаточным n-местным оператором тогда и только тогда, когда*

1) $a_0 = 1$;
2) $\bigoplus\limits_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ k \in \overline{1,n}}} a_{i_1,\ldots,i_k} = 1$;

и когда хотя бы одно из следующих условий не выполняется (*условие несамодвойственности*)

$$a_{1,2,\ldots,n} = 0,$$

$$a_{i_1,i_2,\ldots,i_k,n} = \bigoplus_{\substack{1 \leqslant i_{k+1} < i_{k+2} < \ldots < i_{k+l} \leqslant n-1 \\ \{i_{k+1},i_{k+2},\ldots,i_{k+l}\} \cap \{i_1,i_2,\ldots,i_k\} = \varnothing \\ l \in \overline{1,n-1-k}}} a_{\{i_1,i_2,\ldots,i_k\} \cup \{i_{k+1},\ldots,i_{k+l}\}}, \; k \in \overline{1,n-2}.$$

Доказательство. Условия 1 и 2 следуют из Леммы 3. Чтобы самодостаточный оператор не обладал свойством самодвойственности, не должны выполняться условия Теоремы 8. □

Пример 6. Проверим, является ли данный полином Жегалкина самодостаточным оператором:

$$P(x_1, x_2, \dots, x_5) = 1 \oplus x_1 \oplus x_2 \oplus x_5 \oplus x_2x_5 \oplus x_1x_2x_5 \oplus x_3x_4x_5 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_4x_5.$$

Свободный коэффициент a_0 равен 1. Условие 1 Теоремы 9 выполнено.

Количество всех единичных коэффициентов полинома, за исключением a_0, равно 9 — нечётное число. Условие 2 Теоремы 9 выполнено.

Старший коэффициент $a_{1,2,3,4,5}$ равен 1. Следовательно, выполнено условие несамодвойственности Теоремы 9.

По Теореме 9 полином P соответствует самодостаточному 5-местному оператору.

Пример 7. Выясним, будет ли следующий полином Жегалкина самодостаточным оператором:

$$P(x_1, x_2, x_3, x_4) = 1 \oplus x_1 \oplus x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4.$$

Свободный коэффициент a_0 равен 1. Условие 1 Теоремы 9 выполнено.

Сумма единичных коэффициентов полинома без a_0 равна 5 — нечётное число. Следовательно, условие 2 Теоремы 9 выполнено.

Проверим выполнение условия несамодвойственности. Чтобы полином P не обладал самодвойственностью, хотя бы одно из следующих равенств не должно выполняться:

$$a_{1,2,3,4} = 0,$$

$$a_{2,3,4} = a_{1,3,4} = a_{1,2,4} = a_{1,2,3},$$

$$a_{3,4} = a_{1,3} \oplus a_{2,3} \oplus a_{1,2,3},$$

$$a_{2,4} = a_{1,2} \oplus a_{2,3} \oplus a_{1,2,3},$$

$$a_{1,4} = a_{1,2} \oplus a_{1,3} \oplus a_{1,2,3}.$$

В полиноме P старший коэффициент $a_{1,2,3,4}$ равен 0 (в отличие от полинома из Примера 6). Для проверки несамодвойственности полинома придётся рассмотреть остальные равенства.

В полиноме P не рассмотренные ранее коэффициенты равны

$$a_{2,3,4} = a_{1,3,4} = a_{1,2,4} = a_{1,2,3} = a_{1,2} = a_{1,3} = a_{3,4} = 0,$$

$$a_{1,4} = a_{2,3} = a_{2,4} = 1.$$

Равенство, содержащее коэффициент $a_{3,4}$, не выполнено:

$$a_{3,4} \neq a_{1,3} \oplus a_{2,3} \oplus a_{1,2,3}; \quad 0 \neq 0 \oplus 1 \oplus 0; \quad 0 \neq 1.$$

Условие несамодвойственности выполнено. Следовательно, полином P является самодостаточным 4-местным оператором.

Заключение

С помощью коэффициентов полинома Жегалкина могут быть описаны различные свойства булевой функции, которую он задаёт. Например, может быть рассмотрен ряд свойств, касающихся принадлежности функции к предполным классам. В частности, интерес представляет свойство самодвойственности функции применительно к последующему описанию общего вида n-местного самодостаточного оператора.

В данной статье для определения, обладает ли свойством самодвойственности некоторая булева функция, заданная в виде полинома Жегалкина, вводится понятие полинома двойственного остатка. Показано, что сохраняющая 0 и 1 или не сохраняющая ни 0, ни 1 функция f является самодвойственной тогда и только тогда, когда двойственный остаток N соответствующего ей полинома Жегалкина P равен 0 для любых наборов значений переменных x_1, x_2, ..., x_n (Теорема 2). На основании этого условия была получена система ведущих коэффициентов (6).

Система (6) решается вариацией метода Гаусса с использованием прямых S_d и обратных S_r сумм, определение которых было дано в разделе 4.3. Полученное решение этой системы позволило сформулировать критерий самодвойственности булевой функции (Теорема 8). Критерий самодвойственности опирается на значения коэффициентов полинома Жегалкина рассматриваемой функции, описывая для них соответствующие ограничения.

Основным результатом статьи является Теорема 9, формулировка которой содержит условия (накладываемые на коэффициенты), которым должен удовлетворять полином Жегалкина, реализующий n-местный самодостаточный оператор. Доказательство Теоремы 9 базируется на критерии самодвойственности (Теорема 8) и Лемме 3, полученной на основе свойств сохранения полиномом Жегалкина констант 0 и 1.

Отметим, что представление булевой функции в виде полинома Жегалкина является достаточно удобным для описания критериев принадлежности функции к предполным классам. Кроме очевидного определения линейности функций, по виду полинома Жегалкина можно сделать вывод о наличии у функций свойств самодвойственности, а также свойств сохранения констант. Как было показано, полином Жегалкина позволяет определить необходимые и достаточные условия многоместного самодостаточного оператора.

Исходя из этого, можно заключить, что полиномиальное представление булевой функции является полезным при исследовании предполных классов, чем подчёркивается особое значение полиномов Жегалкина.

References

[1] S. V. Yablonskiy, *Introduction into discrete mathematics*, 5th ed. HSE, 2008, 384 pp.

[2] N. M. Martin, *Systems of Logic*. Cambridge University Press, 1989, 318 pp.

[3] R. L. Graham, “On n-valued functionally complete truth functions”, *The Journal of Symbolic Logic*, vol. 32, no. 2, pp. 190–195, 1967.

[4] T. C. Wesselkamper, “A sole sufficient operator”, *NDJFAM*, vol. 16, no. 1, pp. 86–88, 1975.

[5] S. N. Selezneva, “O slozhnosti raspoznavaniya polnoty mnozhestv bulevyh funkcij, realizovannyh polinomami Zhegalkina”, *DMA*, vol. 9, no. 4, pp. 24–31, 1997, in Russian.

[6] S. S. Marchenkov, *Zamknutye klassy bulevyh funkcij*. Fizmatlit, 2000, 128 pp., in Russian.

[7] V. P. Barashev and S. A. Unuchek, *Diskretnaya matematika*. RTU MIREA, 2012, 268 pp., in Russian.

[8] G. P. Gavrilov and A. A. Sapozhenko, *Zadachi i uprazhneniya po diskretnoj matematike*. Fizmatlit, 2005, 416 pp., in Russian.

[9] N. V. Nikonov, “O svyazyah i otlichiyah poluzapretov I, II-go roda i zapretov K-znachnyh funkcij”, *Forestry bulletin*, no. 1, pp. 124–133, 2006, in Russian.

[10] S. S. Marchenkov, *Osnovy teorii bulevyh funkcij*. Fizmatlit, 2014, 136 pp., in Russian.

[11] L. Y. Bystrov and V. S. Rublev, “Bulevy funkcii, ne prinadlezhashchie predpolnym klassam”, in vol. 13, in Russian, Yaroslavl: P.G. Demidov Yaroslavl State University, 2021, pp. 22–26.

[12] A. I. Kostrikin, *Vvedenie v algebpu. Chast’ 1. Osnovy algebpy*. Fizmatlit, 2000, 367 pp., in Russian.