

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/20/1

УДК 519.7

О НЕКОТОРЫХ СВОЙСТВАХ СЛАБО ПОЛОЖИТЕЛЬНЫХ И СЛАБО ОТРИЦАТЕЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ

С. П. Горшков

*Институт криптографии, связи и информатики, г. Москва, Россия***E-mail:** spg54@bk.ru

Исследуются некоторые свойства слабо положительных (антихорновских) и слабо отрицательных (хорновских) булевых функций. В частности, оценивается сложность задачи построения приведённых представлений этих функций, показывается, что нет ограничений на вес таких функций, оценивается возможная длина записи рассматриваемых функций.

Ключевые слова: *слабо положительная (антихорновская) булева функция, слабо отрицательная (хорновская) булева функция, вычислительная сложность.*

1. Некоторые известные свойства исследуемых функций

Определение 1. Булева функция $f(x_1, \dots, x_n)$, $n \geq 1$, называется:

1) *слабо положительной (антихорновской)*, если $f \equiv 1$ или существует представление f в виде следующей КНФ:

$$f \equiv \bigwedge_{i=1}^t (x_{s_{i1}}^{\alpha_i} \vee x_{s_{i2}} \vee \dots \vee x_{s_{ik_i}}),$$

где $\alpha_i \in \{0, 1\}$, $i = 1, \dots, t$;

2) *слабо отрицательной (хорновской)*, если $f \equiv 1$ или существует представление f в виде следующей КНФ:

$$f \equiv \bigwedge_{i=1}^t (x_{s_{i1}}^{\alpha_i} \vee \bar{x}_{s_{i2}} \vee \dots \vee \bar{x}_{s_{ik_i}}),$$

где $\alpha_i \in \{0, 1\}$, $i = 1, \dots, t$.

Множество всех слабо положительных (слабо отрицательных) функций обозначим WP (WN). Указанные записи соответственно функций классов WP , WN называются *приведёнными представлениями*. Функции из классов WP , WN , зависящие от k переменных, обозначим WP_k , WN_k .

Актуальность задачи изучения указанных функций отмечена в работе [1].

Обозначим:

V_k — множество двоичных k -мерных векторов;

$V_k^{(i)} = \{\alpha \in V_k : \|\alpha\| = i\}$, где $i \in \{0, \dots, k\}$ (слой векторов веса i);

$[c]$ — целая часть действительного числа c .

Пусть $q_1(n), q_2(n)$ — действительные функции от натурального аргумента n ; тогда если существует такое n_0 , что для всех $n \geq n_0$ выполняется неравенство $q_1(n) > q_2(n)$, то будем записывать $q_1(n) \succ q_2(n)$.

Вектор $(\alpha_1, \dots, \alpha_k) \in V_k$ назовём *выполняющим вектором* функции $f(x_1, \dots, x_k)$, если $f(\alpha_1, \dots, \alpha_k) = 1$. Множество всех выполняющих векторов функции f обозначим E_f .

Если $\alpha = (\alpha_1, \dots, \alpha_k), \beta = (\beta_1, \dots, \beta_k)$ — двоичные векторы, $f(x_1, \dots, x_k)$ — булева функция, то полагаем $f(\alpha) = f(\alpha_1, \dots, \alpha_k)$, $\alpha \vee \beta = (\alpha_1 \vee \beta_1, \dots, \alpha_k \vee \beta_k)$, $\alpha \wedge \beta = (\alpha_1 \wedge \beta_1, \dots, \alpha_k \wedge \beta_k)$.

Замечание 1. Слабо положительные и слабо отрицательные функции близки между собой, поскольку $f(x_1, \dots, x_k) \in WP$, если и только если $f(\bar{x}_1, \dots, \bar{x}_k) \in WN$. Ввиду этой симметрии некоторые свойства будем формулировать только для слабо положительных функций.

Свойство 1 (критерий слабой положительности) [2]. Функция $f(x_1, \dots, x_k) \neq 0$ является слабо положительной, если и только если для любых двух выполняющих векторов $\{\alpha, \beta\} \subseteq E_f$ этой функции справедливо свойство

$$(\alpha \vee \beta) \in E_f.$$

Свойство 2 (критерий слабой отрицательности) [2]. Функция $f(x_1, \dots, x_k) \neq 0$ является слабо отрицательной, если и только если для любых двух выполняющих векторов $\{\alpha, \beta\} \subseteq E_f$ этой функции справедливо свойство

$$(\alpha \wedge \beta) \in E_f.$$

Замечание 2. В случае $|E_f| = 1$, $E_f = \{\alpha\}$, $\alpha = (\alpha_1, \dots, \alpha_k) \in V_k$ для пары $\{\alpha, \alpha\} \subseteq E_f$ получим $(\alpha \vee \alpha) = \alpha \in E_f$ ($(\alpha \wedge \alpha) = \alpha \in E_f$) и, согласно критериям, $f \in WP$ и $f \in WN$, что справедливо, поскольку $f = x_1^{\alpha_1} \cdot \dots \cdot x_k^{\alpha_k}$.

Замечание 3. Если $E_f = \emptyset$, то $f \in WP$ и $f \in WN$, поскольку $f = x_1 \cdot \bar{x}_1$.

Пусть $f(x_1, \dots, x_k) \in WP$. На множестве E_f зададим отношение частичного порядка $\leq_f$ по правилу: если $\beta = (\beta_1, \dots, \beta_k) \in E_f, \gamma = (\gamma_1, \dots, \gamma_k) \in E_f$, то $\beta \leq_f \gamma$ тогда и только тогда, когда $\beta_i \leq \gamma_i, i = 1, \dots, k$.

Свойство 3. Множество E_f слабо положительной функции f с отношением частичного порядка $\leq_f$ является верхней полурешёткой (определение верхней полурешётки см. в [3]).

Свойство 4 [4]. Для числа слабо положительных функций (а значит, и слабо отрицательных функций) справедлива оценка

$$\log_2 |WP_k| = \binom{k}{\lfloor k/2 \rfloor} (1 + O(k^{-1/4} \log_2 k)). \quad (1)$$

Заметим, что для числа $m(k)$ монотонных функций от k переменных, которые составляют подкласс слабо положительных функций, верна оценка [5]

$$\log_2 m(k) = \binom{k}{\lfloor k/2 \rfloor} (1 + O(2^{-k/2})).$$

Для задач распознавания свойств булевых функций

$$f \stackrel{?}{\in} WP, \quad f \stackrel{?}{\in} WN \quad (2)$$

справедливы следующие оценки сложности.

Свойство 5 [6]. Задачи (2) при задании булевых функций в виде КНФ или ДНФ являются NP -трудными. Эти задачи при задании булевых функций в виде СКНФ, СДНФ или многочлена Жегалкина являются полиномиальными.

Определение 2. Булева функция $f(x_1, \dots, x_n)$, $n \geq 1$, называется *бионктивной*, если $f \equiv 1$ или существует представление f в виде 2-КНФ

$$f \equiv \left(\bigwedge_{i=1}^{t_1} x_{s_i}^{\alpha_i} \right) \wedge \left(\bigwedge_{i=1}^{t_2} (x_{r_{i1}}^{\beta_{i1}} \vee x_{r_{i2}}^{\beta_{i2}}) \right),$$

где $t_1 \geq 0$, $t_2 \geq 0$ (в случае $t_1 = 0$ или $t_2 = 0$ считаем, что соответствующий сомножитель отсутствует); $\alpha_i \in \{0, 1\}$, $i = 1, \dots, t_1$; $\beta_{i1}, \beta_{i2} \in \{0, 1\}$, $i = 1, \dots, t_2$.

Свойство 6 [7]. Справедливо соотношение

$$WP \cap WN = Bi \cap WP \cap WN,$$

где Bi — множество бионктивных функций.

Свойство 7 [8]. Для любого целого $k \geq 2$ максимальной группой преобразований области определения функций от k переменных, относительно которых множество слабо положительных (слабо отрицательных) функций инвариантно, является группа всех перестановок переменных функций.

Свойство 8 [1]. Задача построения по СКНФ слабо положительной (слабо отрицательной) функции её сокращённой КНФ имеет полиномиальную сложность.

Свойство 9 [1]. Задача построения по многочлену Жегалкина монотонной (слабо положительной) функции её сокращённой КНФ не является полиномиальной.

2. Некоторые результаты о сложности нахождения приведённых представлений монотонных и антимонотонных булевых функций

В работе [1] приведены некоторые результаты о сложности нахождения приведённых представлений слабо положительных и слабо отрицательных булевых функций. В данной работе приведены результаты о сложности нахождения приведённого представления для подклассов слабо положительных и слабо отрицательных функций (а именно, монотонных и антимонотонных).

Определение 3. Булева функция f называется *антимонотонной*, если и только если $\bar{f}$ — монотонная функция.

В [1] не рассматриваются случаи исходного задания функций в виде КНФ или ДНФ. Нетрудно показать, что задачи распознавания « f — монотонная (антимонотонная) функция?» являются NP -трудными, однако представляет интерес задача нахождения приведённого представления указанных функций, когда заведомо известно, что данная КНФ или ДНФ есть монотонная (или антимонотонная) функция.

Функция $h(x_1, \dots, x_k)$ называется *имплицентай* функции $f(x_1, \dots, x_k)$, если

$$f(x_1, \dots, x_k) \wedge h(x_1, \dots, x_k) \equiv f(x_1, \dots, x_k).$$

Имплиценты вида

$$x_{s_1}^{\alpha_1} \vee x_{s_2}^{\alpha_2} \vee \dots \vee x_{s_r}^{\alpha_r},$$

где $s_i \neq s_j$ при $i \neq j$, называются *элементарными имплицентами*. Элементарная имплицента функции f называется *простой*, если никакая её собственная часть не является имплицентай функции f .

Любая функция $f(x_1, \dots, x_k)$, $E_f \neq V_k$, представляется конъюнкцией всех своих простых имплицентов. Конъюнктивная нормальная форма функции f , в которую входят все простые имплиценты функции f и только они, называется *сокращённой* КНФ функции f . Любая функция $f(x_1, \dots, x_k)$ имеет единственную, с точностью до перестановки сомножителей, сокращённую КНФ.

Функция $g(x_1, \dots, x_k)$ называется *импликантой* функции $f(x_1, \dots, x_k)$, если

$$f(x_1, \dots, x_k) \vee g(x_1, \dots, x_k) \equiv f(x_1, \dots, x_k).$$

Приведённым представлением монотонной функции называется представление f в виде следующей КНФ:

$$f \equiv \bigwedge_{i=1}^t (x_{s_{i1}} \vee \dots \vee x_{s_{ik_i}}).$$

Приведённым представлением антимонотонной функции называется представление f в виде следующей КНФ:

$$f \equiv \bigwedge_{i=1}^t (\bar{x}_{s_{i1}} \vee \dots \vee \bar{x}_{s_{ik_i}}).$$

Утверждение 1. Задача построения по КНФ монотонной функции минимальной (приведённой) КНФ имеет полиномиальную сложность.

Доказательство. Пусть монотонная функция $f(x_1, \dots, x_k)$, не равная тождественно единице, записана в КНФ, которую можем представить в виде

$$f \equiv \bigwedge_{i \in I} (x_{s_{i1}} \vee \dots \vee x_{s_{it_i}} \vee \bar{x}_{s_{it_i+1}} \vee \dots \vee \bar{x}_{s_{ik_i}}). \quad (3)$$

Заметим, что если $t_i = 0$ для некоторого $i \in I$, то $f(1, \dots, 1) = 0$ и $f \equiv 0$. Случай $t_i < k_i$ для всех $i \in I$ невозможен, так как при этом $f(0, \dots, 0) = 1$, $f \equiv 1$, и функция f не может быть записана в виде (3). Далее предполагаем, что $t_i \geq 1$ для всех $i \in I$. По функции f построим функцию g :

$$g \equiv \bigwedge_{i \in I} (x_{s_{i1}} \vee \dots \vee x_{s_{it_i}}). \quad (4)$$

Покажем, что

$$f \equiv g. \quad (5)$$

Пусть некоторый вектор $\alpha = (\alpha_1, \dots, \alpha_k) \in V_k$ не является выполняющим вектором для функции f : $f(\alpha) = 0$. Тогда найдётся элементарная имплицента функции f (для простоты записи эту имплиценту обозначим $x_1 \vee \dots \vee x_t \vee \bar{x}_{t+1} \vee \dots \vee \bar{x}_q$), такая, что $\alpha_1 \vee \dots \vee \alpha_t \vee \bar{\alpha}_{t+1} \vee \dots \vee \bar{\alpha}_q = 0$. То есть $\alpha_1 = \dots = \alpha_t = 0$, и вектор α не удовлетворяет имплиценте $x_1 \vee \dots \vee x_t$ функции g и $g(\alpha) = 0$. Поэтому

$$f \geq g. \quad (6)$$

Предположим теперь, что $g(\beta) = 0$ для некоторого $\beta \in V_k$ и вектор β не удовлетворяет имплиценте $x_1 \vee \dots \vee x_t$ функции g . Следовательно, $\beta_1 = \dots = \beta_t = 0$. Рассмотрим вектор $\gamma = (\underbrace{0, \dots, 0}_t, 1, \dots, 1) \in V_k$. Ясно, что $g(\gamma) = f(\gamma) = 0$. Ввиду монотонности функции f получим $f(\beta) = 0$. Поэтому

$$f \leq g. \quad (7)$$

Из соотношений (6) и (7) следует справедливость (5).

Нетрудно показать, что для монотонных функций сокращённая КНФ совпадает с минимальной КНФ. Поэтому достаточно привести требуемый алгоритм построения сокращённой КНФ. Итак, пусть монотонная функция f задана конъюнктивной нормальной формой (4).

Докажем следующее свойство: если

$$x_1 \vee \dots \vee x_t \quad (8)$$

— простая имплицента функции f , то эта имплицента содержится среди элементарных имплицентов КНФ (4). Предположим противное: $x_1 \vee \dots \vee x_t$ — имплицента функции f , но эта имплицента не содержится среди элементарных имплицентов (4). Тогда, с одной стороны, поскольку $x_1 \vee \dots \vee x_t$ — имплицента функции f , то

$$f(0, \dots, 0, x_{t+1}, \dots, x_k) \equiv 0. \quad (9)$$

С другой стороны, так как (8) — простая имплицента, то никакая её собственная часть не является имплицентой функции f и любая имплицента записи (4) содержит хотя бы одну переменную, отличную от $x_1, \dots, x_t$. Следовательно, $f(0, \dots, 0, 1, \dots, 1) \equiv 1$, что противоречит условию (9). Из приведённого свойства вытекает, что все простые имплиценты содержатся в записи (4), достаточно их лишь выделить. Напомним, что необходимым и достаточным условием простоты имплиценты $x_1 \vee \dots \vee x_t$ является выполнение условия (9) и условий

$$f(\underbrace{0, \dots, 0}_{i-1}, 1, 0, \dots, 0, x_{t+1}, \dots, x_k) \neq 0, i = 1, \dots, t. \quad (10)$$

Всё это проверяется с полиномиальной сложностью. ■

Аналогично утверждению 1 можно доказать следующие результаты.

Утверждение 2. Задача построения по КНФ антимонотонной функции минимальной (приведённой) КНФ имеет полиномиальную сложность.

Утверждение 3. Задача построения по ДНФ монотонной (антимонотонной) функции минимальной ДНФ этой функции имеет полиномиальную сложность.

Утверждение 4. Задача построения по ДНФ монотонной функции её минимальной (приведённой) КНФ имеет экспоненциальную сложность.

Доказательство. Пусть $k \geq 2$. Рассмотрим монотонную функцию

$$f \equiv x_1 x_2 \vee x_3 x_4 \vee \dots \vee x_{2\lfloor k/2 \rfloor - 1} x_{2\lfloor k/2 \rfloor}.$$

Легко показать, что сокращённая КНФ функции f имеет вид

$$f \equiv \bigwedge_{\substack{i_1 \in \{1,2\} \\ i_2 \in \{3,4\} \\ i_{\lfloor k/2 \rfloor} \in \{2\lfloor k/2 \rfloor - 1, 2\lfloor k/2 \rfloor\}}} (x_{i_1} \vee x_{i_2} \vee \dots \vee x_{i_{\lfloor k/2 \rfloor}}). \quad (11)$$

Длина сокращённой КНФ (11) имеет порядок $2^{k/2}$, то есть в общем случае задача построения по ДНФ монотонной функции её сокращённой КНФ имеет экспоненциальную сложность. ■

Аналогично утверждению 4 может быть доказано

Утверждение 5. Задача построения по ДНФ антимонотонной функции её сокращённой КНФ имеет экспоненциальную сложность.

3. Некоторые другие свойства слабо положительных и слабо отрицательных булевых функций

Приведём некоторые другие ранее не известные свойства слабо положительных и слабо отрицательных функций. Эти свойства из разных областей исследования рассматриваемых булевых функций.

Теорема 1. Для любого $k \geq 1$ и любого $t \in \{1, \dots, 2^k - 1\}$ найдётся слабо положительная функция веса t , существенно зависящая от всех k переменных.

Доказательство. Пусть $k \geq 1$ и $t \in \{1, \dots, 2^k - 1\}$. Построим слабо положительную функцию $f(x_1, \dots, x_k)$ с требуемыми свойствами. Полагаем $f(0, \dots, 0) = 1$. Выберем наибольшее r , такое, что $\sum_{i=k-r}^k \binom{k}{i} \leq t - 1$. Обозначим $q = \sum_{i=k-r}^k \binom{k}{i}$. Для всех $i \geq k - r$ и $(\alpha_1, \dots, \alpha_k) \in V_k^{(i)}$ полагаем $f(\alpha_1, \dots, \alpha_k) = 1$.

Если $q = t - 1$, то на слоях с весом $1, \dots, k - r - 1$ полагаем $f(\alpha_1, \dots, \alpha_k) = 0$. В случае $q < t - 1$ на слое с весом $k - r - 1$ для $t - q - 1$ произвольно выбранных векторов полагаем $f(\alpha_1, \dots, \alpha_k) = 1$. На остальных векторах этого слоя и на всех векторах слоёв с весом $1, \dots, k - r - 2$ значение функции полагаем равным нулю.

В соответствии с приведённым выше критерием слабой положительности находим, что построенная функция является слабо положительной (но не монотонной, так как $f(0, \dots, 0) = 1$, $\|f\| \neq 2^k$).

Если $t \leq 2^k - k$, то $f(\alpha) = 0$ для всех $\alpha \in V_k$, $\|\alpha\| = 1$, и поэтому функция f (помним, что $f(0, \dots, 0) = 1$) существенно зависит от всех переменных. При $2^k - k < t \leq 2^k - 1$ найдётся вектор $\beta \in V_k^{(1)}$, такой, что $f(\beta) = 0$. Поскольку $f(\beta) = 1$ для всех $\beta \in V_k^{(2)}$ и $f(0, \dots, 0) = 1$, то функция f существенно зависит от всех переменных. Теорема доказана. ■

Замечание 4. Утверждение теоремы не может быть распространено на значения $t = 0$ или $t = 2^k$, поскольку в этих случаях функция f от всех переменных зависит несущественно.

Замечание 5. Может быть построена монотонная функция с приведёнными в теореме 1 свойствами. Для доказательства этого факта необходимо несколько изменить функцию f , построенную выше, а именно положить $f(0, \dots, 0) = 0$, а в самом верхнем слое, содержащем невыполняющие векторы функции f (пусть одним из таких векторов будет β), положить $f(\beta) = 1$.

Замечание 6. Поскольку функции-константы $f \equiv 0$ и $f \equiv 1$ являются и слабо положительными, и слабо отрицательными, то можно утверждать, что нет ограничений на вес слабо положительных и слабо отрицательных функций.

Замечание 7. Известно [7, 9], что любая мультиаффинная функция $f(x_1, \dots, x_k)$ имеет вес 2^m , $m \in \{0, \dots, k\}$, а равновероятных биюнктивных функций, существенно зависящих от $k \geq 5$ переменных, не существует [10]. Результат теоремы 1 показывает, что относительно веса функции классы слабо положительных и слабо отрицательных функций значительно богаче.

Аналогично теореме 1 может быть доказана

Теорема 2. Для любого $k \geq 1$ и любого $t \in \{1, \dots, 2^k - 1\}$ найдётся слабо отрицательная функция веса t , существенно зависящая от всех k переменных.

Теорема 3. При любом виде записи слабо положительных (слабо отрицательных) функций в любом конечном алфавите A для любого полинома $p(k)$ можно ука-

зять k_0 (которое зависит от алфавита A и полинома $p(k)$), такое, что при $k \geq k_0$ найдутся функции из WP_k (WN_k), длина записи которых превышает $p(k)$.

Доказательство. Из формулы (1), представления биномиальных коэффициентов, оценок Стирлинга

$$\sqrt{2\pi k} \left(\frac{k}{e}\right)^k < k! < \sqrt{2\pi k} \left(\frac{k}{e}\right)^k e^{1/12k} \quad (12)$$

следует асимптотическое неравенство

$$|WP_k| \lesssim 2^{2^{k-1}/\sqrt{k}}. \quad (13)$$

Для полинома $p(k)$ найдутся $c_1 \in N$, $c_2 \in N$, такие, что $p(k) \leq c_1 \cdot k^{c_2}$. Количество T слов в алфавите A длины не больше, чем $p(k)$, не более

$$T \leq |A|^{c_1 k^{c_2}}. \quad (14)$$

Поскольку $|A|$ — это некоторое натуральное число, то из соотношений (13) и (14) следует справедливость теоремы. ■

Замечание 8. Для любой мультиаффинной или бионктивной функции $f(x_1, \dots, x_k)$ существует короткая запись (не длиннее $p(k)$, где p — некоторый полином), такой короткой записью для этих функций является приведённое представление [7]. Из теоремы 3 следует, что для всех слабо положительных (и слабо отрицательных) функций короткой записи не существует.

В свете результата теоремы 3 представляет интерес рассмотрение слабо положительных или слабо отрицательных функций, которые коротко записываются в некотором базисе.

В работе [11] исследованы классы функций $Q_k = Bi_k \cap WP_k$, то есть функций, являющихся одновременно слабо положительными и бионктивными. Поскольку длина записи приведённого представления любой бионктивной функции не больше n^3 , слабо положительные функции из класса Q_k имеют короткую запись. Аналогичным свойством обладают слабо отрицательные функции из класса $Bi_k \cap WN_k$. Отметим, что для числа функций класса Q_k справедливы оценки $2^{(k^2 - k \log_2 k)/4} < |Q_k| < 2^{(k^2/2) + 2k \log_2 k + 3k}$ [11]. В следующей теореме оценивается снизу число слабо отрицательных функций, для которых существует короткое представление многочленом Жегалкина.

Теорема 4. Существует не менее $\lfloor 2^{rk \log_2 k/2} \rfloor$ слабо отрицательных функций от k переменных, длина записи которых многочленом Жегалкина не больше чем n^r , где $r \geq 5$.

Доказательство. Будем рассматривать только антимонотонные функции вида

$$f(x_1, \dots, x_k) = \bigwedge_{1 \leq i_1 < \dots < i_t \leq k} (\lambda_{i_1, \dots, i_t} \vee \bar{x}_{i_1} \vee \dots \vee \bar{x}_{i_t}), \quad (15)$$

где $t \in \{1, \dots, k\}$; $\vec{\lambda} = (\lambda_{12\dots t}, \dots, \lambda_{(k-t+1), \dots, (k-1)k}) \in V_{\binom{k}{t}}$ — набор коэффициентов; $\|\vec{\lambda}\| = q$; q — некоторое число из интервала $\{1, \dots, 2^{\binom{k}{t}}\}$, $2^{\binom{k}{t}} = |V_{\binom{k}{t}}|$ — мощность множества $V_{\binom{k}{t}}$. При каждом наборе $\vec{\lambda}$ имеем антимонотонную функцию, записанную в виде КНФ (считаем, что сомножители вида $(1 \vee \bar{x}_{i_1} \vee \dots \vee \bar{x}_{i_t})$ удаляются).

Покажем (от противного), что функции вида (15) имеют единственное представление в виде (15). Пусть функция $f(x_1, \dots, x_k)$, кроме (15), представима в виде

$$f(x_1, \dots, x_k) = \bigwedge_{1 \leq i_1 < \dots < i_t \leq k} (\mu_{i_1 \dots i_t} \vee \bar{x}_{i_1} \vee \dots \vee \bar{x}_{i_t}), \quad (16)$$

где $\vec{\mu} = (\mu_{12\dots t}, \dots, \mu_{(k-t+1)\dots(k-1)k}) \in V_{\binom{k}{t}}$, $\vec{\mu} \neq \vec{\lambda}$. Без ограничения общности можем считать, что $\lambda_{12\dots t} = 1$, $\mu_{12\dots t} = 0$. Тогда из (15) следует, что $f(\underbrace{1, \dots, 1}_t, 0, \dots, 0) = 0$, а из записи (16) вытекает $f(\underbrace{1, \dots, 1}_t, 0, \dots, 0) = 1$. Получили противоречие.

Число функций (15) равно

$$N = \binom{\binom{k}{t}}{q}.$$

Поскольку $\bar{x}_{i_1} \vee \dots \vee \bar{x}_{i_t} = x_{i_1} \cdot \dots \cdot x_{i_t} \oplus 1$, то длина записи функций (15) многочленом Жегалкина не больше

$$T \leq 2^q \cdot k^2,$$

так как число мономов в этом многочлене не больше 2^q , а каждый моном $x_{i_1} \cdot \dots \cdot x_{i_u}$, $1 \leq i_1 < \dots < i_u \leq k$, можно записать словом в алфавите $\{x, 0, 1, ;\}$ длины не больше k^2 (при этом индексы при неизвестных записываем двоичными словами).

Далее положим $t = \lfloor k/2 \rfloor$, $q = \lfloor (r-2) \log_2 k \rfloor$. При этом длина многочлена Жегалкина функции не более чем $T \leq k^r$, число функций (15) равно

$$N = \binom{\binom{k}{\lfloor k/2 \rfloor}}{\lfloor (r-2) \log_2 k \rfloor}.$$

Учитывая соотношение (12), находим

$$N \gtrsim \binom{\left\lfloor \frac{2^k}{2\sqrt{k}} \right\rfloor + 1}{\lfloor (r-2) \log_2 k \rfloor} \gtrsim \binom{\left\lfloor \frac{2^k}{2\sqrt{k}} \right\rfloor + 1}{\lfloor (r-2) \log_2 k \rfloor}^{\lfloor (r-2) \log_2 k \rfloor} \gtrsim 2^{rk \log_2 k/2}.$$

Теорема доказана. ■

Замечание 9. При $k \geq 6$ функции (15) не являются биюнктивными, поскольку в этих условиях элементарные имплиценты, входящие в (15), простые и зависят более чем от трёх переменных.

ЛИТЕРАТУРА

1. Горшков С. П. О сложности нахождения приведённых представлений слабо положительных и слабо отрицательных булевых функций // Прикладная дискретная математика. 2008. Т. 1. Вып. 1. С. 7–9.
2. Гизунов С. А., Носов В. А. О классификации всех булевых функций четырёх переменных по классам Шеффера // Обзорение прикладной промышленной математики. Сер. дискретной математики. 1995. Т. 2. Вып. 3. С. 440–467.
3. Гретцер Г. Общая теория решёток. М.: Мир, 1982. 456 с.
4. Алексеев В. Б. О числе семейств подмножеств, замкнутых относительно пересечения // Дискретная математика. 1989. Т. 1. Вып. 2. С. 129–136.
5. Коршунов А. Д. О числе монотонных булевых функций. Проблемы кибернетики. Вып. 38. М.: Наука, 1981. С. 5–108.

6. Горшков С. П. О сложности распознавания мультиаффинности, бионктивности, слабой положительности и слабой отрицательности булевых функций // Обзорение прикладной промышленной математики. Сер. дискретной математики. 1997. Т. 4. Вып. 2. С. 440–467.
7. Горшков С. П. Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений // Обзорение прикладной промышленной математики. Сер. дискретной математики. 1995. Т. 2. Вып. 3. С. 325–398.
8. Горшков С. П., Тарасов А. В. О максимальных группах инвариантных преобразований мультиаффинных, бионктивных, слабо положительных и слабо отрицательных булевых функций // Дискретная математика. 2009. Т. 21. Вып. 2. С. 94–101.
9. Schaefer T. Complexity of satisfiability problems // Proc. 10 Annual ACM Symposium on Theory of Computing Machinery. New York, NY, USA: ACM, 1978. P. 216–226.
10. Тарасов А. В. О свойствах функций, представимых в виде 2-КНФ // Дискретная математика. 2001. Т. 13. Вып. 4. С. 99–115.
11. Горшков С. П. О пересечении классов мультиаффинных, бионктивных, слабо положительных и слабо отрицательных булевых функций // Обзорение прикладной промышленной математики. Сер. дискретной математики. 1997. Т. 4. Вып. 2. С. 238–259.