Общероссийский математический портал

С. П. Горшков, Функции из классов Шефера, переходящие при отрицании в другие классы Шефера, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 4, 23–48

DOI: <https://doi.org/10.4213/mvk166>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.147.182.235

26 апреля 2023 г., 16:16:37

УДК: 519.571

Функции из классов Шефера, переходящие при отрицании в другие классы Шефера

С. П. Горшков

Академия криптографии Российской Федерации, Москва

Получено 20.IV.2015

Мультиаффинные, биективные (2-КРФ), слабо положительные и слабо отрицательные (хорновские) булевы функции порождают полиномиально решаемые классы систем уравнений. Эти множества булевых функций называются классами Шефера. В работе описаны множества булевых функций f из классов Шефера, для которых $\bar{f}$ принадлежит другому классу Шефера. Полученные результаты могут иметь приложения при решении систем булевых уравнений.

Ключевые слова: мультиаффинные булевы функции, 2-КНФ, хорновские булевы функции, системы булевых уравнений

**Functions from Schaefer classes having negations belonging
to other Schaefer classes**

S. P. Gorshkov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Multiaffine, bijective (2-CNF), weakly positive and weakly negative (Horn's) Boolean functions generates polynomially solvable systems of equations. These sets of Boolean functions are called the Schaefer classes. We describe sets of Boolean functions f from any Schaefer class such that $\bar{f}$ belongs to another Schaefer class. The results obtained may be applied to the solution of systems of Boolean equations.

Key words: multiaffine Boolean functions, 2-CNF, Horn's Boolean functions, systems of Boolean equations

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 4, pp. 23–48 (Russian).

© 2015 С. П. Горшков

Основные обозначения и определения

N — множество натуральных чисел;

$N_0 = N \cup \{0\}$;

V_n — n -мерное пространство булевых векторов, $n \in N$;

F_n — множество булевых функций от $n \in N_0$ переменных (слово «булевых» иногда будем опускать);

F'_n — множество функций из F_n , существенно зависящих от всех n переменных;

$F'_{\leq n}$ — множество функций, существенно зависящих не более чем от n переменных;

$F'_{\geq n}$ — множество функций, существенно зависящих не менее чем от n переменных;

M_1 — множество монотонных функций;

M_2 — множество антимонотонных функций;

$\text{Sym}(n)$ — симметрическая группа степени n ;

S_n — симметрическая группа перестановок координат векторов из V_n , подгруппа $\text{Sym}(2^n)$, изоморфна $\text{Sym}(n)$;

Σ_n — группа сдвигов, является подгруппой S_{2^n} , состоит из преобразований $\tau_\beta(x) = x \oplus \beta$, где $x, \beta \in V_n$;

Q_n — группа Джевонса, являющаяся полупрямым произведением групп S_n и Σ_n , состоит из преобразований вида

$$s_{\pi, \beta}(x) = \tau_\beta(\pi(x)), \text{ где } \tau_\beta \in \Sigma_n, \pi \in S_n;$$

$[f(x_1, \dots, x_n)]_{\langle S_n \rangle}$ — класс эквивалентности булевых функций с представителем $f(x_1, \dots, x_n)$ относительно группы S_n ;

$[f(x_1, \dots, x_n)]_{\langle Q_n \rangle}$ — класс эквивалентности булевых функций с представителем f относительно группы Джевонса;

$$\{f(x_1, \dots, x_n)\}_C = \{f(y_1, \dots, y_n) \mid y_{j_i} \in \{0, 1, x_i\}, i = 1, \dots, n\}$$

(при этом для всякого $i \in \{1, \dots, n\}$ символ y_i есть или одна из констант $\{0, 1\}$, или символ переменной x_i ; $\{f\}_C$ есть набор всех функций с указанным свойством).

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

1) *мультиаффинной*, если существует представление функции f в виде конъюнкции аффинных функций:

$$f \equiv \bigwedge_{i=1}^t (a_{i1}x_1 \oplus \dots \oplus a_{in}x_n \oplus a_{i0}), \quad (1)$$

где $a_{ij} \in \{0, 1\}$, $i = 1, \dots, t$, $j = 0, \dots, n$;

2) *биунктивной*, если $f \equiv 1$ или существует представление функции f в виде следующей конъюнктивной нормальной формы (КНФ):

$$f \equiv \left(\bigwedge_{i=1}^t x_{s_i}^{\alpha_i} \right) \wedge \left(\bigwedge_{j=1}^q \left(x_{s_{j1}}^{\beta_{j1}} \vee x_{s_{j2}}^{\beta_{j2}} \right) \right), \quad (2)$$

где $\alpha_i, \beta_{j1}, \beta_{j2} \in \{0, 1\}$, $s_i, s_{j1}, s_{j2} \in \{1, \dots, k\}$, $i = 1, \dots, t$, $j = 1, \dots, q$;

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

$$f \equiv \bigwedge_{i=1}^t (x_{s_{i1}}^{\alpha_i} \vee x_{s_{i2}} \vee \dots \vee x_{s_{in_i}}), \quad (3)$$

где $\alpha_i \in \{0, 1\}$, $n_i \leq n$, $s_{ij} \in \{1, \dots, n\}$, $i = 1, \dots, t$, $j = 1, \dots, n_i$;

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

$$f \equiv \bigwedge_{i=1}^t (x_{s_{i1}}^{\alpha_i} \vee \bar{x}_{s_{i2}} \vee \dots \vee \bar{x}_{s_{in_i}}), \quad (4)$$

где $\alpha_i \in \{0, 1\}$, $n_i \leq n$, $s_{ij} \in \{1, \dots, n\}$, $i = 1, \dots, t$, $j = 1, \dots, n_i$.

Множество всех функций соответственно классов 1–4 обозначим A, Bi, WP, WN . Для функций классов A, Bi, WP, WN представления (1), (2), (3), (4) будем называть *приведенными*.

Классы функций A, Bi, WP, WN будем также называть *классами Шефера*.

Обозначим $S = \{A \cup Bi \cup WP \cup WN\}$.

Вектор $(\alpha_1, \dots, \alpha_n) \in V_n$ назовем *выполняющим вектором* функции $f(x_1, \dots, x_n)$, если $f(\alpha_1, \dots, \alpha_n) = 1$. Множество всех выполняющих векторов функции f обозначим E_f . Вектор $(\alpha_1, \dots, \alpha_n) \in V_n$ назовем *невыполняющим вектором* функции $f(x_1, \dots, x_n)$, если $f(\alpha_1, \dots, \alpha_n) = 0$, $\bar{E}_f = V_n \setminus E_f$.

Символом $\|f(x_1, \dots, x_n)\|$ обозначим вес булевой функции f , $\|f\| = |E_f|$, $\|\alpha\|$ — вес вектора $\alpha \in V_n$.

Запись вида $f(x_i = a, x_j = b) = c$ будет обозначать, что $f(x_1, \dots, x_n) = c$, если $x_i = a, x_j = b$.

Условие отличия функции f от тождественной константы будем записывать в виде $f \not\equiv c$.

Если $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n)$ — двоичные векторы, $f(x_1, \dots, x_n)$ — булева функция, то полагаем

$$f(\alpha) = f(\alpha_1, \dots, \alpha_n),$$

$$\begin{aligned}\alpha \vee \beta &= (\alpha_1 \vee \beta_1, \dots, \alpha_n \vee \beta_n), \alpha \wedge \beta = \alpha \cdot \beta = (\alpha_1 \wedge \beta_1, \dots, \alpha_n \wedge \beta_n), \\ \alpha \oplus \beta &= (\alpha_1 \oplus \beta_1, \dots, \alpha_n \oplus \beta_n), \\ 0_n &= (\underbrace{0, \dots, 0}_n), 1_n = (\underbrace{1, \dots, 1}_n).\end{aligned}$$

Критерий мультиаффинности [1]. Функция $f(x_1, \dots, x_n) \not\equiv 0$ является мультиаффинной, если и только если для любых трех выполняющих векторов $\{\alpha, \beta, \gamma\} \subseteq E_f$ этой функции

$$(\alpha \oplus \beta \oplus \gamma) \in E_f. \quad (5)$$

Критерий биунктивности [1]. Функция $f(x_1, \dots, x_n) \not\equiv 0$ является биунктивной, если и только если для любых трех выполняющих векторов $\{\alpha, \beta, \gamma\} \subseteq E_f$ этой функции

$$((\alpha \wedge \beta) \oplus (\alpha \wedge \gamma) \oplus (\beta \wedge \gamma)) \in E_f. \quad (6)$$

Критерий слабой положительности [2]. Функция $f(x_1, \dots, x_n) \not\equiv 0$ является слабо положительной, если и только если для любых двух выполняющих векторов $\{\alpha, \beta\} \subseteq E_f$ этой функции

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

Критерий слабой отрицательности [2]. Функция $f(x_1, \dots, x_n) \not\equiv 0$ является слабо отрицательной, если и только если для любых двух выполняющих векторов $\{\alpha, \beta\} \subseteq E_f$ этой функции

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

Функция $h(x_1, \dots, x_n)$ называется имплицентой функции $f(x_1, \dots, x_n)$, если

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

Имплиценты вида

$$x_{s_1}^{\alpha_1} \vee \dots \vee x_{s_t}^{\alpha_t},$$

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

Любая функция $f(x_1, \dots, x_n)$, $f \not\equiv 1$, представляется конъюнкцией всех своих простых имплицентов. Конъюнктивная нормальная форма функции f ,

в которую входят все простые имплиценты функции f и только они, называется *сокращенной* КНФ функции f . Любая функция $f(x_1, \dots, x_n)$ имеет единственную, с точностью до перестановки сомножителей, сокращенную КНФ.

Перейдем к исследованию таких функций f , что f принадлежит одному классу Шефера, а $\bar{f}$ — другому классу Шефера.

Такая особенность может быть использована при решении систем булевых уравнений. Пусть требуется решить систему уравнений вида

$$\begin{cases} f(x_{s_{11}}, \dots, x_{s_{1n}}) = \alpha_1, \\ \dots \\ f(x_{s_{m1}}, \dots, x_{s_{mn}}) = \alpha_m. \end{cases} \quad (7)$$

Обозначим $I_1 = \{i \in \{1, \dots, m\} \mid \alpha_i = 1\}$, $I_0 = \{1, \dots, m\} \setminus I_1$. Систему (7) разобьем на две подсистемы:

$$\{f(x_{s_{i1}}, \dots, x_{s_{in}}) = 1, \quad i \in I_1, \quad (8)$$

$$\{f(x_{s_{i1}}, \dots, x_{s_{in}}) = 0, \quad i \in I_0. \quad (9)$$

Систему (9) перепишем в виде

$$\{\bar{f}(x_{s_{i1}}, \dots, x_{s_{in}}) = 1, \quad i \in I_0. \quad (10)$$

Если функция f принадлежит одному из классов Шефера, то система (8) является полиномиально решаемой, при этом система (9) используется только как проверочная. Если $f \in S$ и $\bar{f} \in S$, то полиномиально решаемыми являются и система (8), и система (10), что может ускорить решение исходной системы (7).

В [3, с. 373–386] исследованы такие функции, что f и $\bar{f}$ принадлежат одному и тому же классу Шефера (дважды мультиаффинные функции и др.). В данной работе изучаются такие функции f , что f и $\bar{f}$ принадлежат разным классам Шефера.

При исследовании этой задачи достаточно рассмотреть следующие классы функций:

$$T_1 = \{f \in F \mid f \in A, \bar{f} \in Bi\},$$

$$T_2 = \{f \in F \mid f \in A, \bar{f} \in WP\},$$

$$T_3 = \{f \in F \mid f \in Bi, \bar{f} \in WP\},$$

$$T_4 = \{f \in F \mid f \in WP, \bar{f} \in WN\}.$$

Остальные классы таких функций просто получаются из этих классов с помощью двух свойств. Например:

- 1) $\{f \in Bi, \bar{f} \in A\} \leftrightarrow \{g \in A, \bar{g} \in Bi\}$, где $g \equiv \bar{f}$;
- 2) $\{f(x_1, \dots, x_n) \in A, \bar{f} \in WN\} \leftrightarrow \{f(\bar{x}_1, \dots, \bar{x}_n) \in A, \bar{f}(\bar{x}_1, \dots, \bar{x}_n) \in WP\}$.

1. Функции $f : f \in A, \bar{f} \in Bi$

Заметим, что если $f(x_1, \dots, x_n) \in T_1$, то $[f(x_1, \dots, x_n)]_{\langle Q_n \rangle} \subset T_1$.

Теорема 1. *Класс функций T_1 имеет следующую структуру:*

$$T_1 = F'_{\leq 1} \cup (F'_2 \setminus [x_1 \vee x_2]_{\langle Q_2 \rangle}). \quad (11)$$

Доказательство. Очевидно, что $T_1 \cap F'_{\leq 2} = F'_{\leq 1} \cup (F'_2 \setminus [x_1 \vee x_2]_{\langle Q_2 \rangle})$.

Докажем (от противного), что $T_1 \cap F'_{\geq 3} = \emptyset$. Пусть $f(x_1, \dots, x_n) \in T_1 \cap F'_{\geq 3}$ и f существенно зависит от всех своих переменных. При этом $\|f\| = 2^r$, $r \in \{0, \dots, n-1\}$, функция $\bar{f}$ существенно зависит от всех переменных, $\|\bar{f}\| = 2^n - 2^r$.

Без ограничения общности считаем, что $x_1 \vee x_2$ — имплицента функции $\bar{f}$, тогда все векторы вида $(0, 0, \alpha_3, \dots, \alpha_n)$ являются невыполняющими для $\bar{f}$ и $\|\bar{f}\| \leq \frac{3}{4} \cdot 2^n$. Также без ограничения общности можем считать, что функция $\bar{f}$ имеет имплиценту вида $x_3 \vee x_4$ или имплиценту $x_1^\alpha \vee x_3$. В первом случае любой вектор вида $(1, 1, 0, 0, \dots) \in V_n$ является невыполняющим и $\|\bar{f}\| < \frac{3}{4} \cdot 2^n$. Во втором случае любой вектор вида $(\bar{\alpha}, 1, 0, \dots) \in V_n$ является невыполняющим и $\|\bar{f}\| < \frac{3}{4} \cdot 2^n$. То есть в любом случае $\|f\| > \frac{1}{4} \cdot 2^n$ и $\|f\| = 2^{n-1}$.

Поэтому f — аффинная функция, зависящая от трех или более переменных. Пусть $f \equiv x_1 \oplus \dots \oplus x_n$, тогда $\bar{f} \equiv x_1 \oplus \dots \oplus x_n \oplus 1$ и $\bar{f} \notin Bi$, так как не выполняется критерий бионктивности для векторов

$$(1, 1, 0, 0, \dots, 0), \quad (1, 0, 1, 0, \dots, 0), \quad (0, 1, 1, 0, \dots, 0).$$

Если $f \equiv x_1 \oplus \dots \oplus x_n \oplus 1$, то $\bar{f} \equiv x_1 \oplus \dots \oplus x_n$ и $\bar{f} \notin Bi$, так как не выполняется критерий бионктивности для векторов

$$(1, 0, 0, 0, \dots, 0), \quad (0, 1, 0, 0, \dots, 0), \quad (0, 0, 1, 0, \dots, 0).$$

Теорема доказана.

2. Функции $f : f \in A, \bar{f} \in WP$

Обозначим

$$T'_{n2} = F'_n \cap T_2.$$

Ясно, что все булевы функции $f(x_1, \dots, x_n)$, существенно зависящие не более чем от одного переменного, таковы, что $f \in A, \bar{f} \in WP$.

Далее будем рассматривать функции от двух и более переменных.

Теорема 2. При $n \geq 2$ справедливо соотношение

$$T'_{n2} = (\bar{x}_1 \cdot \dots \cdot \bar{x}_n) \cup [(x_1 \cdot \bar{x}_2 \cdot \dots \cdot \bar{x}_n)]_{\langle S_n \rangle} \cup [(x_1 \oplus x_2) \cdot \bar{x}_3 \cdot \dots \cdot \bar{x}_n]_{\langle S_n \rangle}.$$

Доказательство теоремы 2 разобьем на несколько лемм.

Лемма 1. Пусть $\|f(x_1, \dots, x_n)\| = 1$ (в случае $\|f\| = 1$ всегда $f \in A$ и f существенно зависит от всех n переменных). Тогда $\bar{f} \in WP$, если и только если $f \equiv \bar{x}_1 \cdot \dots \cdot \bar{x}_{i-1} \cdot x_i^\alpha \cdot \bar{x}_{i+1} \cdot \dots \cdot \bar{x}_n$, где $i \in \{1, \dots, n\}$, $\alpha \in \{0, 1\}$.

Доказательство очевидно, поскольку

$$\bar{f} \equiv x_1 \vee \dots \vee x_{i-1} \vee x_i^{\bar{\alpha}} \vee x_{i+1} \vee \dots \vee x_n \in WP.$$

Лемма 2. Пусть $\|f(x_1, \dots, x_n)\| = 2$ и f существенно зависит от всех n переменных (в случае $\|f\| = 2$ всегда $f(x_1, \dots, x_n) \in A$). Тогда $\bar{f} \in WP$, если и только если

$$f \in [(x_1 \oplus x_2) \cdot \bar{x}_3 \cdot \dots \cdot \bar{x}_n]_{\langle S_n \rangle} \quad (12)$$

$$(\bar{f} \in [(\bar{x}_1 \vee x_2 \vee \dots \vee x_n) \cdot (x_1 \vee \bar{x}_2 \vee x_3 \vee \dots \vee x_n)]_{\langle S_n \rangle}).$$

Доказательство. Так как $\|f\| = 2$, то $\bar{f} \equiv (x_1^{\beta_1} \vee \dots \vee x_n^{\beta_n}) \cdot (x_1^{\delta_1} \vee \dots \vee x_n^{\delta_n})$. Обозначим $\beta = (\beta_1, \dots, \beta_n)$, $\delta = (\delta_1, \dots, \delta_n)$, при этом $\beta \neq \delta$. Легко видеть, что если $\|\beta\| \leq n - 3$ или $\|\delta\| \leq n - 3$, то $f \notin WP$. Далее считаем, что $\|\beta\| \geq n - 2$, $\|\delta\| \geq n - 2$. Если $\|\beta\| = n - 2$ или $\|\delta\| = n - 2$, то $\bar{f}$ — слабо положительная только при условии

$$\begin{aligned} \bar{f} &\in \{(\bar{x}_1 \vee \bar{x}_2 \vee x_3 \vee \dots \vee x_n) \cdot (x_1 \vee \bar{x}_2 \vee x_3 \vee \dots \vee x_n)\}_{\langle S_n \rangle} = \\ &= \{(\bar{x}_2 \vee x_3 \vee \dots \vee x_n)\}_{\langle S_n \rangle}. \end{aligned}$$

В этом случае функция f существенно зависит от $n - 1$ переменных.

Далее считаем, что $\|\beta\| \geq n - 1$, $\|\delta\| \geq n - 1$. Случай $\|\beta\| = n$, $\|\delta\| = n$ невозможен, так как тогда $\beta = \delta$. Невозможны также случаи $\|\beta\| = n - 1$, $\|\delta\| = n$ или $\|\beta\| = n$, $\|\delta\| = n - 1$, так как тогда функция f существенно

зависит от $n - 1$ переменных. Остается только случай $\|\beta\| = n - 1$, $\|\delta\| = n - 1$, который соответствует функции (12).

При $D \subseteq V_n$, $\alpha \in V_n$ обозначим $D \oplus \alpha = \{\beta \oplus \alpha \mid \beta \in D\}$. Если D — линейное пространство, то $D \oplus \alpha$ будем называть линейным многообразием.

Приведем без доказательств некоторые простые свойства.

Свойство 1. Если $f \in A$ ($f \in Bi$, $f \in WP$ или $f \in WN$), то $\{f\}_C \subset A$ ($\{f\}_C \subset Bi$, $\{f\}_C \subset WP$ или $\{f\}_C \subset WN$).

Следствие 1. Если $f \in T_i$, $i \in \{1, 2, 3, 4\}$, то и любые подфункции f , получаемые фиксацией переменных, тоже принадлежат множеству T_i .

Следствие 2. Если для функции $f(x_1, \dots, x_n)$ какая-либо подфункция, получаемая фиксацией переменных, не принадлежит T_i , то $f \notin T_i$.

Свойство 2. Если E , $E \subseteq V_n$, — линейное многообразие, $\alpha \in E$, то $E \oplus \alpha$ — линейное пространство.

Свойство 3. Множество $E \subseteq V_n$ является линейным многообразием тогда и только тогда, когда E есть множество выполняющих векторов некоторой мультиаффинной функции от n переменных.

Пусть $\alpha = (\alpha_1, \dots, \alpha_n) \in V_n$, $1 < k < n$, $1 \leq i_1 < i_2 < \dots < i_k \leq n$. Введем обозначения:

$$\alpha|_{i_1, \dots, i_k} = (\alpha_{i_1}, \dots, \alpha_{i_k}), \quad \alpha|_{(k)} = (\alpha_1, \dots, \alpha_k).$$

Считаем, что

$$f(x_1, \dots, x_n) \in A, \quad \|f\| = 2^k, \quad k \geq 1. \quad (13)$$

Свойство 4. При выполнении (13) существуют такие номера координат $1 \leq i_1 < i_2 < \dots < i_k \leq n$, что

$$\bigcup_{\alpha \in E_f} \alpha|_{i_1, \dots, i_k} = V_k.$$

Далее для простоты обозначений полагаем

$$i_1 = 1, \quad i_2 = 2, \dots, \quad i_k = k. \quad (14)$$

Пусть выполняется (14) и, кроме того,

$$\beta^{(0)} = (\underbrace{0, \dots, 0}_k, 1, 0, \dots, 0) \in E_f. \quad (15)$$

Пусть такие векторы $\{\varepsilon^{(1)}, \dots, \varepsilon^{(k+1)}\} \subset E_f$, что

$$\begin{aligned}\varepsilon^{(1)} &= (1, 1, \dots, 1, 1, 0, \varepsilon_{k+1}^{(1)}, \varepsilon_{k+2}^{(1)}, \dots, \varepsilon_n^{(1)}), \\ \varepsilon^{(2)} &= (1, 1, \dots, 1, 0, 1, \varepsilon_{k+1}^{(2)}, \varepsilon_{k+2}^{(2)}, \dots, \varepsilon_n^{(2)}), \\ &\dots \\ \varepsilon^{(k)} &= (0, 1, \dots, 1, 1, 1, \varepsilon_{k+1}^{(k)}, \varepsilon_{k+2}^{(k)}, \dots, \varepsilon_n^{(k)}), \\ \varepsilon^{(k+1)} &= (\underbrace{1, 1, \dots, 1, 1, 1}_k, \varepsilon_{k+1}^{(k+1)}, \varepsilon_{k+2}^{(k+1)}, \dots, \varepsilon_n^{(k+1)}).\end{aligned}\tag{16}$$

Обозначим

$$\begin{aligned}\varepsilon'^{(1)} &= (1, 1, \dots, 1, 1, 0, \varepsilon_{k+1}^{(1)} \oplus 1, \varepsilon_{k+2}^{(1)}, \dots, \varepsilon_n^{(1)}), \\ \varepsilon'^{(2)} &= (1, 1, \dots, 1, 0, 1, \varepsilon_{k+1}^{(2)} + 1, \varepsilon_{k+2}^{(2)}, \dots, \varepsilon_n^{(2)}), \\ &\dots \\ \varepsilon'^{(k)} &= (0, 1, \dots, 1, 1, 1, \varepsilon_{k+1}^{(k)} \oplus 1, \varepsilon_{k+2}^{(k)}, \dots, \varepsilon_n^{(k)}), \\ \varepsilon'^{(k+1)} &= (\underbrace{1, 1, \dots, 1, 1, 1}_k, \varepsilon_{k+1}^{(k+1)} \oplus 1, \varepsilon_{k+2}^{(k+1)}, \dots, \varepsilon_n^{(k+1)}).\end{aligned}\tag{17}$$

Свойство 5. Если k — четное, то векторы $\{\varepsilon'^{(1)}, \dots, \varepsilon'^{(k)}\}$ образуют базис пространства $E_f \oplus \beta^{(0)}$. Если k — нечетное, то векторы $\{\varepsilon'^{(1)}, \dots, \varepsilon'^{(k-1)}, \varepsilon'^{(k+1)}\}$ образуют базис пространства $E_f \oplus \beta^{(0)}$.

Пусть $f(x_1, \dots, x_n)$ — булева функция. Обозначим

$$m_f = \min_{\alpha \in E_f} \|\alpha\|, \quad m'_f = \max_{\alpha \in E_f} \|\alpha\|.$$

Лемма 3. Пусть $f(x_1, \dots, x_n)$ — булева функция, $\alpha \in E_f$, $\|\alpha\| \geq 2$, и $\beta \notin E_f$ для всех $\beta < \alpha$, $\|\beta\| = 1$. Тогда $\bar{f} \notin WP$.

Доказательство. Для функции $\bar{f}$ имеем $\alpha \notin E_{\bar{f}}$, $\|\alpha\| \geq 2$, и $\beta \in E_{\bar{f}}$ для всех $\beta < \alpha$, $\|\beta\| = 1$. Ясно, что $\alpha = \bigvee_{\beta < \alpha, \|\beta\|=1} \beta$, и если бы выполнялось условие $\bar{f} \in WP$, то мы имели бы $\alpha \in E_{\bar{f}}$. Но это не так, поэтому $\bar{f} \notin WP$.

Следствие. Пусть $f(x_1, \dots, x_n)$ — булева функция, $m_f \geq 2$. Тогда $\bar{f} \notin WP$.

Пусть $f(x_1, \dots, x_n)$ — булева функция, $\alpha \in V_n$. Символом $T_{f,\alpha}$ обозначим множество

$$T_{f,\alpha} = \{\beta \in V_n \mid \beta < \alpha, f(\beta) = 0\}.$$

Пример 1. Если $f(x_1, \dots, x_n)$ — монотонная функция, $\alpha \notin E_f$, то $T_{f,\alpha}$ — множество всех векторов, меньших α , при этом

$$|T_{f,\alpha}| = 2^{\|\alpha\|} - 1.$$

Лемма 4. Пусть $f(x_1, \dots, x_n) \in WP$, $\alpha \notin E_f$. Тогда

$$2^{\|\alpha\|-1} - 1 \leq |T_{f,\alpha}| \leq 2^{\|\alpha\|} - 1. \quad (18)$$

Доказательство. Соотношение (18) верно при $\alpha = 0_n$. Далее считаем $\alpha \neq 0_n$. Верхняя оценка (18) справедлива, поскольку число всех векторов, меньших α , равно $2^{\|\alpha\|} - 1$.

Обозначим $\bar{T}_{f,\alpha} = \{\beta \in V_n \mid \beta < \alpha, f(\beta) = 1\}$. Если бы выполнялось равенство $(\bigvee_{\beta \in \bar{T}_{f,\alpha}} \beta) = \alpha$, то ввиду условия $f \in WP$ мы имели бы $f(\alpha) = 1$. Но это не так, поэтому $(\bigvee_{\beta \in \bar{T}_{f,\alpha}} \beta) < \alpha$ и существует такое i , что в векторе α i -я координата равна 1, а во всех векторах $\beta \in \bar{T}_{f,\alpha}$ эта координата равна 0. Поэтому $|\bar{T}_{f,\alpha}| \leq 2^{\|\alpha\|-1}$. Так как $|T_{f,\alpha}| + |\bar{T}_{f,\alpha}| = 2^{\|\alpha\|} - 1$, то верна нижняя оценка в (18). Лемма доказана.

Замечание. Верхняя и нижняя оценки в (18) достижимы. Пример 1 показывает, что верхняя оценка достижима. Нижняя оценка достижима для функции $f(x_1, \dots, x_n) \equiv \bar{x}_i$ и вектора $\alpha = 1_n$.

Лемма 5. Пусть $f(x_1, \dots, x_n) \in WP$, $\bar{E}_f \neq \emptyset$, $\alpha \in \bar{E}_f$. Тогда

$$|\bar{E}_f| \geq 2^{\|\alpha\|-1}. \quad (19)$$

Доказательство. Легко видеть, что $|\bar{E}_f| \geq |T_{f,\alpha}| + 1$ (единицу добавили в силу того, что учли вектор α). Осталось воспользоваться формулой (18).

Лемма 6. Пусть $f(x_1, \dots, x_n)$ — булева функция, $\|f\| = 2^k$, существует такой вектор $\alpha \in E_f$, что $\|\alpha\| \geq k + 2$. Тогда $\bar{f} \notin WP$.

Доказательство (от противного). Предположим, что $\bar{f} \in WP$. При этом $\alpha \in \bar{E}_{\bar{f}}$. В силу леммы 5 имеем $|\bar{E}_{\bar{f}}| \geq 2^{\|\alpha\|-1} \geq 2^{k+2-1} = 2^{k+1}$, то есть не выполняется соотношение $|\bar{E}_{\bar{f}}| = \|f\|$.

Следствие. Если $f(x_1, \dots, x_n) \in A$, $\bar{f} \in WP$, $\|f\| = 2^k$, $k \geq 1$, то

$$m'_f \leq k + 1. \quad (20)$$

Лемма 7. Пусть $f(x_1, \dots, x_n) \in A$, $\bar{f} \in WP$, $\|f\| = 2^k$, $k \geq 1$, существует такой вектор $\alpha \in E_{\bar{f}}$, что $\|\alpha\| = k + 1$. Тогда

$$f(x_1, \dots, x_n) \in [x_1 \cdot \bar{x}_2 \cdot \dots \cdot \bar{x}_{n-k}]_{\langle S_n \rangle}. \quad (21)$$

Доказательство. Пусть $j_1, \dots, j_{k+1}$ — номера всех единичных координат вектора α . Согласно доказательству леммы 4 найдется такая координата $j \in \{j_1, \dots, j_{k+1}\}$, что векторы $\beta = (\beta_1, \dots, \beta_n)$, $\beta \leq \alpha$, с $\beta_j = 1$ принадлежат $\bar{E}_{\bar{f}}$ (то есть принадлежат $E_{\bar{f}}$). Таких векторов 2^k , то есть это все выполняющие векторы функции f . Поэтому

$$f \equiv x_j \cdot \bigwedge_{i \in \{1, \dots, n\} \setminus \{j_1, \dots, j_{k+1}\}} \bar{x}_i,$$

откуда следует (21).

Следствие. В условиях леммы 7 функция $f(x_1, \dots, x_n)$ существенно зависит не от всех переменных.

Лемма 8. Пусть $f(x_1, \dots, x_n) \in A$, $\bar{f} \in WP$, $\|f\| = 2^k$, $k \geq 1$, f существенно зависит от всех переменных. Тогда $m'_f = k$.

Доказательство. Согласно свойству 4 и следствию из леммы 6 имеем $k \leq m'_f \leq k + 1$. Если $m'_f = k + 1$, то функция $f(x_1, \dots, x_n)$ существенно зависит не от всех переменных (следствие из леммы 7). Поэтому $m'_f = k$.

Теорема 3. Пусть $f(x_1, \dots, x_n) \in A$, $\|f\| = 2^k$, $2 \leq k < n$, f существенно зависит от всех переменных. Тогда $\bar{f} \notin WP$.

Доказательство проведем от противного. Предположим, что существует такая функция $f(x_1, \dots, x_n) \in A$, что $\|f\| = 2^k$, $2 \leq k < n$, f существенно зависит от всех переменных, $\bar{f} \in WP$.

Считаем, что выполняется (14). Упорядочим множество E_f в лексикографическом порядке по первым k координатам (подвекторы, состоящие из этих координат, образуют V_k):

$$E_f = \begin{cases} (0, 0, \dots, 0, 0, 0, \dots), \\ (0, 0, \dots, 0, 0, 1, \dots), \\ (0, 0, \dots, 0, 1, 0, \dots), \\ (0, 0, \dots, 0, 1, 1, \dots), \\ \dots \\ (1, 1, \dots, 1, 1, 1, \dots). \end{cases} \quad (22)$$

Вес любого вектора из (22) не более k , поэтому последний вектор в (22) имеет вид

$$\varepsilon^{(k+1)} = (\underbrace{1, \dots, 1}_k, 0, \dots, 0). \quad (23)$$

Рассмотрим первый вектор из E_f , $\beta^{(0)} \in E_f$, $\beta^{(0)}|_{(k)} = 0_k$. Тогда $\|\beta^{(0)}\| \leq 1$, так как в противном случае $\bar{f} \notin WP$ по лемме 3.

1. Пусть $\beta^{(0)} = 0_n$. Тогда E_f — линейное пространство. Рассмотрим такой вектор $\phi = (\phi_1, \dots, \phi_n) \in E_f$, что $\|(\phi_1, \dots, \phi_k)\| = 1$. Если $\|(\phi_{k+1}, \dots, \phi_n)\| \geq 1$, то $\bar{f} \notin WP$ по лемме 3. Далее можем считать, что $\|(\phi_{k+1}, \dots, \phi_n)\| = 0$ для всех векторов $\phi = (\phi_1, \dots, \phi_n) \in E_f$, $\|(\phi_1, \dots, \phi_k)\| = 1$. Поскольку E_f — линейное пространство, то во всех векторах из E_f координаты с номерами, большими k , равны 0. Следовательно, $f \equiv \bar{x}_{k+1} \cdot \dots \cdot \bar{x}_n$ и функция f существенно зависит не от всех переменных.

2. Пусть первый вектор в (22) равен $(\underbrace{0, \dots, 0}_k, 1, 0, \dots, 0)$. Рассмотрим следующие выполняющие векторы функции $\bar{f}$:

$$\begin{aligned} \beta^{(0)} &= (0, 0, \dots, 0, 0, 0, 1, 0, \dots, 0), \\ \beta^{(1)} &= (0, 0, \dots, 0, 0, 1, \beta_{k+1}^{(1)}, \beta_{k+2}^{(1)}, \dots, \beta_n^{(1)}), \\ \beta^{(2)} &= (0, 0, \dots, 0, 1, 0, \beta_{k+1}^{(2)}, \beta_{k+2}^{(2)}, \dots, \beta_n^{(2)}), \\ &\dots \\ \beta^{(k)} &= (\underbrace{1, 0, \dots, 0}_k, 0, 0, \beta_{k+1}^{(k)}, \beta_{k+2}^{(k)}, \dots, \beta_n^{(k)}). \end{aligned} \quad (24)$$

Обозначим $\gamma = (\beta_{k+1}^{(1)}, \beta_{k+1}^{(2)}, \dots, \beta_{k+1}^{(k)})$.

Случай 2.1. Пусть $\|\gamma\| \leq k - 2$. Без ограничения общности можем считать, что $\beta_{k+1}^{(1)} = \beta_{k+1}^{(2)} = 0$. Для справедливости включения $\bar{f} \in WP$ необходимо (в силу леммы 3), чтобы $(\beta_{k+2}^{(1)}, \dots, \beta_n^{(1)}) = (\beta_{k+2}^{(2)}, \dots, \beta_n^{(2)}) = 0_{n-k-1}$. Рассмотрим выполняющий вектор $\bar{f}$ вида

$$\lambda = (\underbrace{0, \dots, 0}_{k-2}, 1, 1, \lambda_{k+1}, \lambda_{k+2}, \dots, \lambda_n).$$

Используя векторы $\beta^{(0)}, \beta^{(1)}, \beta^{(2)}$ и соотношение (5), находим $\lambda_{k+1} = 1$, $(\lambda_{k+2}, \dots, \lambda_n) = 0_{n-k-1}$. Для указанной ниже подфункции

$$\begin{aligned} f'(x_{k-1}, x_k, x_{k+1}) &\equiv f(x_1 = 0, \dots, x_{k-2} = 0, x_{k+2} = 0, \dots, x_n = 0) \equiv \\ &\equiv x_{k-1} \oplus x_k \oplus x_{k+1}. \end{aligned}$$

Значит, $\bar{f}' \notin WP$ и $\bar{f} \notin WP$.

Случай 2.2. Предположим, что $\|\gamma\| = k$. Возможны два подслучая: k — четное и k — нечетное.

2.2.1. $\|\gamma\| = k$, k — четное. Поскольку E_f — линейное многообразие, то

$$\delta^{(1)} = \beta^{(0)} \oplus \beta^{(1)} \oplus \beta^{(2)} \in E_f,$$

$$\delta^{(2)} = \delta^{(1)} \oplus \beta^{(3)} \oplus \beta^{(4)} \in E_f,$$

...

$$\delta^{(\frac{k}{2})} = \delta^{(\frac{k}{2}-1)} \oplus \beta^{(k-1)} \oplus \beta^{(k)} \in E_f.$$

Вектор $\delta^{(\frac{k}{2})}$ имеет вид $\delta^{(\frac{k}{2})} = (\underbrace{1, \dots, 1}_{k+1}, \delta_{k+2}^{(\frac{k}{2})}, \dots, \delta_n^{(\frac{k}{2})})$, что невозможно (см.

лемму 8).

2.2.2. $\|\gamma\| = k$, k — нечетное. Данный подслучай рассматривается как и предыдущий, при этом используются выполняющие векторы

$$\eta^{(1)} = \beta^{(1)} \oplus \beta^{(2)} \oplus \beta^{(3)} \in E_f,$$

$$\eta^{(2)} = \eta^{(1)} \oplus \beta^{(4)} \oplus \beta^{(5)} \in E_f,$$

...

$$\eta^{(\frac{k-1}{2})} = \eta^{(\frac{k-1}{2}-1)} \oplus \beta^{(k-1)} \oplus \beta^{(k)} \in E_f.$$

Вектор $\eta^{(\frac{k-1}{2})}$ имеет вид $\eta^{(\frac{k-1}{2})} = (\underbrace{1, \dots, 1}_{k+1}, \eta_{k+2}^{(\frac{k-1}{2})}, \dots, \eta_n^{(\frac{k-1}{2})})$, что невозможно.

Случай 2.3. Пусть $\|\gamma\| = k - 1$. Без ограничения общности можем считать, что $\beta_{k+1}^{(1)} = 0, \beta_{k+1}^{(2)} = \dots = \beta_{k+1}^{(k)} = 1$. Кроме того, нетрудно видеть, что

$$\beta^{(1)} = (\underbrace{0, \dots, 0}_k, 1, 0, \dots, 0).$$

Покажем, что во всех векторах множества E_f $(k + 1)$ -я координата равна отрицанию k -й координаты. Для векторов (24) это верно. Пусть $\chi = (\chi_1, \dots, \chi_n) \in E_f$, $\|(\chi_1, \dots, \chi_k)\| \geq 2$. Рассмотрим четыре подслучая.

а) Число $\|(\chi_1, \dots, \chi_k)\|$ является четным, и $\chi_k = 0$. Без ограничения общности считаем $(\chi_1, \dots, \chi_k) = (\underbrace{1, \dots, 1}_v, 0, \dots, 0)$, где $2 \leq v < k$ — четное.

Тогда

$$\chi = (\beta^{(0)} \oplus \beta^{(k)} \oplus \beta^{(k-1)}) \oplus (\beta^{(k-2)} \oplus \beta^{(k-1)}) \oplus \dots \oplus (\beta^{(k-v+2)} \oplus \beta^{(k-v+1)}),$$

откуда следует, что $\eta_k = 0, \eta_{k+1} = 1$.

б) Число $\|(\chi_1, \dots, \chi_k)\|$ является нечетным, и $\chi_k = 0$. Без ограничения общности считаем, что $(\chi_1, \dots, \chi_k) = (\underbrace{1, \dots, 1}_v, 0, \dots, 0)$, где $2 \leq v < k$ — нечетное. Тогда

$$\chi = (\beta^{(k)} \oplus \beta^{(k-1)} \oplus \beta^{(k-2)}) \oplus (\beta^{(k-3)} \oplus \beta^{(k-4)}) \oplus \dots \oplus (\beta^{(k-v+2)} \oplus \beta^{(k-v+1)}),$$

откуда следует, что $\eta_k = 1, \eta_{k+1} = 0$.

в) Число $\|(\chi_1, \dots, \chi_k)\|$ является четным, и $\chi_k = 1$. В этом случае аналогичным образом (см. пп. а и б) можно показать, что $\eta_k = 1, \eta_{k+1} = 0$.

г) Число $\|(\chi_1, \dots, \chi_k)\|$ является нечетным, и $\chi_k = 1$. В этом случае аналогичным образом (см. пп. а и б) можно показать, что $\eta_k = 0, \eta_{k+1} = 1$.

Для векторов $\varepsilon^{(i)}, i = 1, \dots, k$ (см. (10)), справедливы равенства

$$\varepsilon_{k+1}^{(1)} = 1, \quad \varepsilon_{k+1}^{(2)} = \dots = \varepsilon_{k+1}^{(k)} = 0, \quad (25)$$

$$\varepsilon_j^{(i)} = 0, \quad i \in \{1, \dots, k\}, \quad j \in \{k+2, \dots, n\}. \quad (26)$$

Равенства (25) следуют из того, что элементы $(k+1)$ -го столбца есть инвертированные элементы k -го столбца. Соотношения (26) вытекают из леммы 8.

Используя свойства 6, равенства (23), (26) и соотношение между элементами k -го и $(k+1)$ -го столбцов в (22), находим, что

$$\bar{f}(x_1, \dots, x_n) \equiv (x_k \oplus x_{k+1}) \cdot \bar{x}_{k+2} \cdot \dots \cdot \bar{x}_n$$

и $\bar{f}$ существенно зависит не от всех переменных. Полученное противоречие заканчивает доказательство теоремы.

Доказательство теоремы 2 непосредственно следует из лемм 1, 2 и теоремы 3.

Лемма 9. Число t_n функций $\bar{f}(x_1, \dots, x_n)$, $\bar{f} \in A, \bar{f} \in WP$, существенно зависящих от всех переменных, равно

$$t_n = \frac{n^2 + n + 2}{2}.$$

Доказательство следует из лемм 1, 2 и теоремы 2.

3. Функции $f : f \in \mathbf{Bi}, \bar{f} \in \mathbf{WP}$

Если функция $f(x_1, \dots, x_n)$ не имеет имплицент вида x_i^α , то будем говорить, что функция f не имеет однолитеральных имплицент.

Свойство 6. Функция f является слабо положительной, если и только если ее сокращенная КНФ имеет вид (2).

Следствие. Если сокращенная КНФ функции f не имеет вид (2), то $f \notin \mathbf{WP}$.

Свойство 7. Пусть $(x_i^\alpha \vee x_j^\beta)$ — имплицента функции $f(x_1, \dots, x_n)$, $f \not\equiv 0$. Тогда $f(x_i = \bar{\alpha}, x_j = \bar{\beta}) \equiv 0$, $\bar{f}(x_i = \bar{\alpha}, x_j = \bar{\beta}) \equiv 1$ и в каждую элементарную имплиценту функции $\bar{f}$ входит по крайней мере один из литералов $x_i^{\bar{\alpha}}$ или $x_j^{\bar{\beta}}$.

Следствие. Если функция f имеет имплиценту x_i^α , то в каждую элементарную имплиценту функции $\bar{f}$ входит литерал $x_i^{\bar{\alpha}}$.

Свойство 8. Функции $f(x_1, \dots, x_n)$ и $\bar{f}(x_1, \dots, x_n)$ существенно зависят от одинакового множества переменных.

Для доказательства достаточно заметить, что многочлены Жегалкина функций f и $\bar{f}$ различаются только свободным членом.

Свойство 9. Если литерал x_i^α входит в сокращенную КНФ функции $f(x_1, \dots, x_n)$, то функция f от переменного x_i зависит существенно.

Доказательство. Пусть $(x_i^\alpha \vee x_{j_1}^{\beta_1} \vee \dots \vee x_{j_r}^{\beta_r})$ есть простая имплицента функции f . Тогда $f(x_i = \bar{\alpha}, x_{j_1} = \bar{\beta}_1, \dots, x_{j_r} = \bar{\beta}_r) \equiv 0$, $f(x_{j_1} = \bar{\beta}_1, \dots, x_{j_r} = \bar{\beta}_r) \equiv 0$, следовательно, $f(x_i = \alpha, x_{j_1} = \bar{\beta}_1, \dots, x_{j_r} = \bar{\beta}_r) \not\equiv 0$. Отсюда вытекает, что найдутся два соседних вектора из V_n , отличающихся только i -й координатой, на которых функция f принимает различные значения. Свойство доказано.

Следствие. Если литерал x_i^α входит в сокращенную КНФ функции $f(x_1, \dots, x_n)$, то литерал вида x_i^β входит в любую КНФ функции $\bar{f}$.

Свойство 10. Пусть $f(x_1, \dots, x_n)$ — булева функция, $f(x_{i_1} = \alpha_{i_1}, \dots, x_{i_r} = \alpha_{i_r})$ — подфункция функции $f(x_1, \dots, x_n)$, полученная фиксацией соответствующих переменных. Если литерал x_i^α входит в сокращенную КНФ функции $f(x_{i_1} = \alpha_{i_1}, \dots, x_{i_r} = \alpha_{i_r})$, то литерал x_i^α входит в любую КНФ функции $f(x_1, \dots, x_n)$.

Доказательство (от противного). Без ограничения общности можем считать, что $\alpha = 0$, $i = 1$, $i_1 = n - r + 1, \dots, i_r = n$. Итак: 1) пусть $\bar{x}_1$ входит в сокращенную КНФ функции $f(x_{n-r+1} = \alpha_{n-r+1}, \dots, x_n = \alpha_n)$; 2) в КНФ

(некоторую КНФ) функции $f(x_1, \dots, x_n)$ входит x_1 , но не входит $\bar{x}_1$. Из п. 2 следует, что если $(0, \delta_2, \dots, \delta_n) \in E_f$, то всегда $(1, \delta_2, \dots, \delta_n) \in E_f$.

Рассмотрим теперь функцию $f'(x_1, \dots, x_{n-r}) \equiv \bar{f}(x_{n-r+1} = \alpha_{n-r+1}, \dots, x_n = \alpha_n)$. Покажем, что найдется вектор вида $(0, \eta_2, \dots, \eta_{n-r}) \in E_{f'}$, для которого $(1, \eta_2, \dots, \eta_{n-r}) \notin E_{f'}$. Это следует из простоты элементарной имплиценты, в которую входит $\bar{x}_1$. Из полученного противоречия следует справедливость утверждения.

Свойство 11. Если литерал x_i^α входит в сокращенную КНФ функции $f(x_1, \dots, x_n)$, то литерал вида $x_i^{\bar{\alpha}}$ входит в любую КНФ функции $\bar{f}$.

Доказательство. Пусть $i = 1$, $\alpha = 1$. Найдется такая фиксация $x_2 = \beta_2, \dots, x_n = \beta_n$, что $f(x_2 = \beta_2, \dots, x_n = \beta_n) \equiv x_1$. Тогда $\bar{f}(x_2 = \beta_2, \dots, x_n = \beta_n) \equiv \bar{x}_1$. Осталось воспользоваться свойством 10.

Свойство 12. Если $f(x_1, \dots, x_n) \in Bi$, f не имеет однолитеральных имплицентов, то все элементарные имплиценты функции f , содержащие два литерала, являются простыми.

Доказательство. очевидно, следует из того, что f не имеет однолитеральных имплицентов.

Свойство 13. Пусть некоторая подфункция f' функции $f(x_1, \dots, x_n)$, получаемая фиксацией переменных, не равна тождественно нулю и имеет имплиценту $x_i \cdot x_j$, $i \neq j$. Тогда $\bar{f} \notin WP$.

Доказательство. Ясно, что в каждую простую имплиценту функции $\bar{f}'$, $\bar{f}' \neq 1$, должны входить литерал $\bar{x}_i$ и литерал $\bar{x}_j$. Поэтому $\bar{f}' \notin WP$ и $\bar{f} \notin WP$.

Лемма 10. Если $f(x_1, \dots, x_n) \in T_3$, $f'(x_1, \dots, x_n) \in Bi \cap M_2$, то

$$f(x_1, \dots, x_n) \cdot f'(x_1, \dots, x_n) \in T_3. \quad (27)$$

Доказательство. Ясно, что $f \cdot f' \in Bi$. Имеем

$$\overline{f \cdot f'} \equiv \bar{f} \vee \bar{f}', \quad (28)$$

где $\bar{f} \in WP$, $\bar{f}' \in M_1$. Обозначим $h \equiv \bar{f} \vee \bar{f}'$. Пусть $\alpha \in E_h$, $\beta \in E_h$. Если $\alpha \in E_{\bar{f}'}$ или $\beta \in E_{\bar{f}'}$, то $\alpha \vee \beta \in E_{\bar{f}'}$ и $\alpha \vee \beta \in E_h$. Если $\alpha \notin E_{\bar{f}'}$ и $\beta \notin E_{\bar{f}'}$, то $\alpha \in E_{\bar{f}}$ и $\beta \in E_{\bar{f}}$. Значит, $\alpha \vee \beta \in E_{\bar{f}}$ и $\alpha \vee \beta \in E_h$. Лемма доказана.

Следствие. Если $f'(x_1, \dots, x_n) \in Bi \cap M_2$, то $f' \in T_3$.

Для доказательства достаточно в (27) положить $f \equiv 1$.

Лемма 11. Пусть $f(x_1, \dots, x_n) \in Bi$, $f \neq 0$, функция f имеет имплиценту вида x_j ,

$$f(x_1, \dots, x_n) \equiv x_j \cdot f'(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n). \quad (29)$$

Тогда $f \in T_3$, если и только если $f' \in Bi \cap M_2$.

Доказательство. Пусть выполняется (29), где $f' \in Bi \cap M_2$. Тогда $f \in T_3$ по лемме 10.

Предположим теперь, что $f \in T_3$. При этом функция f имеет вид (29), где $\bar{f}' \in WP$ (поскольку $f' \equiv f(x_1 = 1)$). Докажем (от противного), что $f' \in M_2$. Пусть $f' \in Bi$, $f' \notin M_2$ (тогда $\bar{f}' \notin M_1$). Можем считать, что запись (2) — это сокращенная КНФ функции $\bar{f}'$, при этом в (2) присутствует литерал в нулевой степени. Тогда

$$\begin{aligned} \overline{x_j \cdot f'(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)} &\equiv \bar{x}_j \vee \bar{f}'(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \equiv \\ &\equiv \bigwedge_{i=1}^t (\bar{x}_j \vee x_{s_{i1}}^{\alpha_i} \vee x_{s_{i2}} \vee \dots \vee x_{s_{in_i}}). \end{aligned} \quad (30)$$

Запись (30) — это сокращенная КНФ функции $\bar{f}$, один из сомножителей содержит два литерала в нулевой степени, и $\bar{f} \notin WP$. Лемма доказана.

Лемма 12. Пусть $f(x_1, \dots, x_n) \in Bi$, $f \neq 0$, функция f имеет имплиценту вида $\bar{x}_j$, при этом

$$f(x_1, \dots, x_n) \equiv \bar{x}_j \cdot f'(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n).$$

Тогда $f \in T_3$, если и только если $f' \in T_3$.

Доказательство. Если $f' \in T_3$, то $f \in T_3$ по лемме 10.

В случае $f \in T_3$ имеем $f' \equiv f(x_i = 0) \in T_3$. Лемма доказана.

Заметим, что если функция $f(x_1, \dots, x_n)$ не имеет однолитераловых имплицент, то $f(x_r = \alpha) \neq 0$ для любого $r \in \{1, \dots, n\}$ и любого $\alpha \in \{0, 1\}$.

Лемма 13. Пусть функция $f(x_1, \dots, x_n) \in T_3$ не имеет однолитераловых имплицент. Тогда f не имеет имплицент вида

$$(x_i \vee \bar{x}_r)(x_j \vee \bar{x}_r), \quad r \neq i, \quad r \neq j.$$

Доказательство (от противного). Пусть функция f имеет имплиценту $(x_i \vee \bar{x}_r)(x_j \vee \bar{x}_r)$, $r \neq i$, $r \neq j$. При этом функция $f(x_r = 1)$ имеет имплиценту $x_i \cdot x_j$, $f(x_r = 1) \neq 0$. Тогда $\bar{f} \notin WP$ по свойству 13, что противоречит условию.

Лемма 14. Пусть функция $f(x_1, \dots, x_n) \in T_3$ имеет вид

$$f(x_1, \dots, x_n) \equiv (x_i \vee x_j) \cdot f'(x_1, \dots, x_n),$$

у функции f нет однолитераловых имплицент. Тогда в записи функции f' в первой степени могут быть только переменные x_i или x_j .

Доказательство. Предположим, что в записи функции f' имеется литерал вида x_t , $t \neq i$, $t \neq j$. Согласно свойству 11 в сокращенной КНФ функции $\bar{f}$ должен содержаться литерал $\bar{x}_t$. С учетом свойства 7 и того, что функция f имеет простую имплиценту $(x_i \vee x_j)$, находим $\bar{f} \notin WP$, т. е. $f \notin T_3$.

Положим

$$f_1(x_1, \dots, x_{t+r+2}) \equiv (x_1 \vee x_2)(\bar{x}_1 \vee \bar{x}_2) \wedge \bigwedge_{i=1}^t (x_1 \vee \bar{x}_{i+2}) \wedge \bigwedge_{j=1}^r (x_2 \vee \bar{x}_{t+j+2}),$$

$$f_2(x_1, \dots, x_{t+r+2}) \equiv (x_1 \vee \bar{x}_2 \vee x_3 \vee \dots \vee x_{t+2})(\bar{x}_1 \vee x_2 \vee x_{t+3} \vee \dots \vee x_{t+r+2}).$$

Лемма 15. *Справедливо соотношение*

$$\bar{f}_1(x_1, \dots, x_{t+r+2}) \equiv f_2(x_1, \dots, x_{t+r+2}).$$

Доказательство. Для доказательства леммы достаточно показать, что $V_{t+r+2} \setminus E_{f_1} = E_{f_2}$.

1. Покажем, что $(V_{t+r+2} \setminus E_{f_1}) \subseteq E_{f_2}$. Пусть $\alpha = (\alpha_1, \dots, \alpha_{t+r+2}) \in V_{t+r+2} \setminus E_{f_1}$. Вектор α не удовлетворяет хотя бы одной простой имплиценте функции f_1 . Рассмотрим возможные варианты. Пусть α не удовлетворяет первой или второй имплиценте f_1 . Тогда $\alpha_1 = \alpha_2$ и $\alpha \in E_{f_2}$.

Если α не выполняет имплиценту вида $(x_1 \vee \bar{x}_{i+2})$, $i \in \{1, \dots, t\}$, имеем $\alpha_1 = 0$, $\alpha_{i+2} = 1$ и $\alpha \in E_{f_2}$. Аналогично рассматривается случай, когда α не выполняет имплиценту вида $(x_2 \vee \bar{x}_{t+j+2})$, $j \in \{1, \dots, r\}$.

2. Несложно показать, что $(V_{t+r+2} \setminus E_{f_1}) \supseteq E_{f_2}$. Лемма доказана.

Следствие. *Класс T_3 содержит функции вида*

$$\left[(x_1 \vee x_2)(\bar{x}_1 \vee \bar{x}_2) \wedge \bigwedge_{i=1}^t (x_1 \vee \bar{x}_{i+2}) \wedge \bigwedge_{j=1}^r (x_2 \vee \bar{x}_{t+j+2}) \right]_{\langle S_{t+r+2} \rangle}, \quad (31)$$

$$r = 0, 1, \dots, \quad t \geq r.$$

Теорема 4. *Пусть $f(x_1, \dots, x_n) \in T_3$, функция f не имеет однолитеральных имплицент, функция f имеет имплиценту вида $(x_i \vee x_j)(\bar{x}_i \vee \bar{x}_j)$. Тогда*

$$f(x_1, \dots, x_n) \equiv f'(x_1, \dots, x_n) \cdot f''(x_1, \dots, x_n),$$

где функция f' принадлежит классу (31), $f'' \in Bi \cap M_2$.

Справедливость теоремы вытекает из лемм 10, 13, 14 и 15.

Лемма 16. *Множество T_3 содержит подкласс функций*

$$[(x_1 \vee x_2)(x_1 \vee \bar{x}_3) \dots (x_1 \vee \bar{x}_n)]_{\langle S_n \rangle}, \quad n = 2, 3, \dots$$

Доказательство. Достаточно заметить, что

$$\overline{(x_1 \vee x_2)(x_1 \vee \bar{x}_3) \dots (x_1 \vee \bar{x}_n)} \equiv \bar{x}_1(\bar{x}_2 \vee x_3 \vee \dots \vee x_n).$$

Следствие. Если $f(x_1, \dots, x_n) \in Bi$, функция f имеет вид

$$f(x_1, \dots, x_n) \equiv (x_i \vee x_j) \cdot f'(x_1, \dots, x_n),$$

функция f не имеет однолитеральных имплицентов, в первой степени в КНФ функции f' входит только литерал x_i или только литерал x_j , то $\bar{f} \in WP$.

Пусть функция $f(x_1, \dots, x_n) \in T_3$ имеет имплиценту $(x_1 \vee x_2)$, функция f не имеет однолитеральных имплицентов, f не имеет имплиценты $(\bar{x}_1 \vee \bar{x}_2)$. При этом с учетом лемм 13, 14, следствия из леммы 16 и теоремы 4 осталось рассмотреть случай, когда f имеет имплиценту

$$(x_1 \vee x_2) \wedge \bigwedge_{i=1}^t (x_1 \vee \bar{x}_{i+2}) \wedge \bigwedge_{j=1}^r (x_2 \vee \bar{x}_{t+j+2}), \quad (32)$$

где $t \geq 1, r \geq 1$; в (32) включены все простые имплиценты функции f с литералами в первой степени.

Функцию (32) обозначим $f_3(x_1, \dots, x_{t+r+2})$. Тогда

$$f(x_1, \dots, x_n) \equiv f_3(x_1, \dots, x_{t+r+2}) \cdot f'(x_1, \dots, x_n), \quad (33)$$

где $f'(x_1, \dots, x_n) \in Bi \cap M_2$.

Лемма 17.

1. Пусть $f \in WP$ и выполняется (33). Тогда

$$f(x_{i+2} = 1, x_{t+j+2} = 1) \equiv 0 \quad (34)$$

для любых $i \in \{1, \dots, t\}, j \in \{1, \dots, r\}$.

2. Для $i \in \{1, \dots, t\}, j \in \{1, \dots, r\}$ выполняется (34), если и только если функция f имеет хотя бы одну из имплицентов

$$(\bar{x}_1 \vee \bar{x}_{2+t+j}), \quad (\bar{x}_2 \vee \bar{x}_{2+i}), \quad (\bar{x}_{2+i} \vee \bar{x}_{2+t+j}). \quad (35)$$

Доказательство.

1. Если найдутся такие $i \in \{1, \dots, t\}, j \in \{1, \dots, r\}$, что $f(x_{2+i} = 1, x_{2+t+j} = 1) \not\equiv 0$, то функция $f(x_{2+i} = 1, x_{2+t+j} = 1)$ имеет имплиценту $x_1 \cdot x_2$ и $\bar{f} \notin WP$.

2. При выполнении (33) фиксации $x_{2+i} = 1, x_{2+t+j} = 1$ влекут соотношения $x_1 = 1, x_2 = 1$. Поэтому если функция f имеет хотя бы одну из имплицентов (35), то $f(x_{2+i} = 1, x_{2+t+j} = 1) \equiv 0$.

Докажем (от противного), что если $f(x_{2+i} = 1, x_{2+t+j} = 1) \equiv 0$, то функция f имеет хотя бы одну из имплицентов (35). Предположим, что $f(x_{2+i} = 1, x_{2+t+j} = 1) \equiv 0$, но функция f не имеет хотя бы одну из имплицентов (35). Функция f не имеет имплиценты $(\bar{x}_1 \vee \bar{x}_2)$. Поскольку функция не имеет однолитеральных имплицентов, то функции $(\bar{x}_1 \vee \bar{x}_{2+i})$ и $(\bar{x}_2 \vee \bar{x}_{2+t+j})$ не являются имплицентами f . Нетрудно видеть, что при этом двоичный вектор размерности n , у которого 1-я, 2-я, i -я и j -я координаты равны 1, а остальные координаты равны 0, является выполняющим для функции f . Тогда $f(x_{2+i} = 1, x_{2+t+j} = 1) \not\equiv 0$. Пришли к противоречию.

Лемма 18. *Следующие функции принадлежат множеству T_3 :*

$$(x_1 \vee x_2)(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_3 \vee \bar{x}_4), \quad (36)$$

$$(x_1 \vee x_2)(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_1 \vee \bar{x}_4), \quad (37)$$

$$(x_1 \vee x_2)(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_2 \vee \bar{x}_3). \quad (38)$$

Доказывается непосредственной проверкой.

Теорема 5. *При выполнении (33) верно соотношение $\bar{f} \in WP$, если и только если $f(x_{2+i} = 1, x_{2+t+j} = 1) \equiv 0$ для любых $i \in \{1, \dots, t\}$, $j \in \{1, \dots, r\}$.*

Доказательство. Легко видеть, что если $\bar{f} \in WP$, то для любых $i \in \{1, \dots, t\}$, $j \in \{1, \dots, r\}$: $f(x_{2+i} = 1, x_{2+t+j} = 1) \equiv 0$.

Пусть для любых $i \in \{1, \dots, t\}$, $j \in \{1, \dots, r\}$: $f(x_{2+i} = 1, x_{2+t+j} = 1) \equiv 0$. Покажем, что тогда $\bar{f} \in WP$. Для этого докажем, что если $\alpha \notin E_f$, $\beta \notin E_f$, то $\alpha \vee \beta \notin E_f$ (отсюда будет следовать, что $\bar{f} \in WP$). Вектор α не удовлетворяет некоторой простой имплиценте функции f , вектор β не удовлетворяет некоторой простой имплиценте функции f . Если α или β не выполняют имплиценту вида $(\bar{x}_r \vee \bar{x}_t)$, то $\alpha \vee \beta$ также не выполняет эту имплиценту. Далее считаем, что α и β не выполняют простую имплиценту, содержащую литерал в первой степени. Используя лемму 17, находим, что векторы α и β одновременно не удовлетворяют одной из имплицентов вида

$$f'' \equiv (x_1 \vee x_2)(x_1 \vee \bar{x}_i)(x_2 \vee \bar{x}_j)(\bar{x}_i \vee \bar{x}_j), \quad (39)$$

$$(x_1 \vee x_2)(x_1 \vee \bar{x}_i)(x_2 \vee \bar{x}_j)(\bar{x}_1 \vee \bar{x}_j), \quad (40)$$

$$(x_1 \vee x_2)(x_1 \vee \bar{x}_i)(x_2 \vee \bar{x}_j)(\bar{x}_2 \vee \bar{x}_i). \quad (41)$$

Пусть векторы α и β одновременно не удовлетворяют имплиценте (39). Так как $\bar{f}'' \in WP$ (см. лемму 18), то вектор $\alpha \vee \beta$ не удовлетворяет f'' . Дальнейшее доказательство очевидно.

Следствие. При выполнении (33) соотношение $\bar{f} \in WP$ верно тогда и только тогда, когда для любых $i \in \{1, \dots, t\}$, $j \in \{1, \dots, r\}$ функция f имеет хотя бы одну из имплицентов (35).

Далее будем рассматривать такие функции $f(x_1, \dots, x_n) \in T_3$, что f не имеет однолитераловых имплицентов и имплицентов вида $(x_i \vee x_j)$.

Заметим, что множество T_3 содержит подкласс функций

$$[(x_1 \vee \bar{x}_2) \dots (x_1 \vee \bar{x}_n)]_{\langle S_n \rangle}, \quad n = 2, 3, \dots$$

Для доказательства этого факта достаточно в лемме 16 положить $x_2 = 1$.

Лемма 19. Пусть $f(x_1, \dots, x_n) \in T_3$, f не имеет однолитераловых имплицентов, f не имеет имплицентов вида $(x_i \vee x_j)$. Тогда функция f не имеет имплицентов вида $(x_i \vee \bar{x}_j)(\bar{x}_i \vee x_j)$.

Доказательство (от противного). Пусть функция f имеет имплиценту $(x_i \vee \bar{x}_j)(\bar{x}_i \vee x_j)$. Предположим, кроме того, что функция f имеет имплиценту вида

$$(x_i \vee \bar{x}_j)(\bar{x}_i \vee x_j)(\bar{x}_i \vee x_r). \quad (42)$$

Функция $f(x_i = 1)$ имеет имплиценту $x_j \cdot x_r$, следовательно, $\bar{f}(x_i = 1) \notin WP$, $\bar{f} \notin WP$. Значит, функция f не имеет имплицентов вида (42). Отсюда следует, что

$$f'(x_i, x_j) \equiv f(x_1 = \dots = x_{i-1} = x_{i+1} = \dots = x_{j-1} = x_{j+1} = \dots = x_n = 0) \equiv (x_i \vee \bar{x}_j)(\bar{x}_i \vee x_j).$$

При этом $\bar{f}' \notin WP$, $\bar{f} \notin WP$. Из полученного противоречия следует справедливость леммы.

Лемма 20. Пусть функция $f(x_1, \dots, x_n) \in T_3$ не имеет однолитераловых имплицентов, не имеет имплицентов вида $(x_i \vee x_j)$, не имеет имплицентов вида $(x_i \vee \bar{x}_j)(\bar{x}_i \vee x_j)$, не имеет имплицентов вида $(x_i \vee \bar{x}_r)(x_j \vee \bar{x}_r)$. Кроме того, пусть функция f имеет имплиценту

$$(x_1 \vee \bar{x}_{i_1})(x_2 \vee \bar{x}_{i_2}) \dots (x_k \vee \bar{x}_{i_k}),$$

где $k \geq 2$, все $i_1, \dots, i_k$ различны. Тогда

$$\{1, \dots, k\} \cap \{i_1, \dots, i_k\} = \emptyset.$$

Доказательство. Предположим, что $\{1, \dots, k\} \cap \{i_1, \dots, i_k\} \neq \emptyset$.

1. Пусть $i_1 = 2$. Тогда $i_2 \neq 1$. Функция $f(x_{i_2} = 1)$ имеет имплиценту $x_1 \cdot x_2$. Поэтому $\bar{f}(x_{i_2} = 1) \notin WP$ и $\bar{f} \notin WP$.

2. Далее можем считать, что f имеет имплиценту

$$(x_1 \vee \bar{x}_{r+1})(x_2 \vee \bar{x}_{r+2}) \dots (x_{r-1} \vee \bar{x}_{2r-1})(x_r \vee \bar{x}_1),$$

где $r \geq 2$.

Отсюда следует, что функция $f(x_{r+1} = 1)$ имеет имплиценту $x_1 \cdot x_r$, то есть $\bar{f} \notin WP$. Лемма доказана.

Далее будем считать, что функция $f(x_1, \dots, x_n) \in T_3$ не имеет однолитеральных имплицент, не имеет имплицент вида $(x_i \vee x_j)$, не имеет имплицент вида $(x_i \vee \bar{x}_j)(\bar{x}_i \vee x_j)$, не имеет имплицент вида $(x_i \vee \bar{x}_r)(x_j \vee \bar{x}_r)$. То есть произведение всех простых имплицент функции f с литералами в положительных степенях имеет вид

$$\bigwedge_{i=1}^{t_1} (x_1 \vee \bar{x}_{s_i}) \wedge \bigwedge_{j=1}^{t_2} (x_2 \vee \bar{x}_{r_j}) \wedge \dots \wedge \bigwedge_{l=1}^{t_k} (x_k \vee \bar{x}_{w_l}), \quad (43)$$

где $k \geq 2$, переменные $\{x_{s_i} \mid i = 1, \dots, t_1\}$, $\{x_{r_j} \mid j = 1, \dots, t_2\}$, $\dots$, $\{x_{w_l} \mid l = 1, \dots, t_k\}$ встречаются по одному разу, кроме того,

$$\{x_1, \dots, x_k\} \cap (\{x_{s_i} \mid i = 1, \dots, t_1\} \cup \{x_{r_j} \mid j = 1, \dots, t_2\} \cup \dots \cup \{x_{w_l} \mid l = 1, \dots, t_k\}) = \emptyset.$$

Пусть функция (43) зависит от переменных $x_1, \dots, x_{k+t_1+\dots+t_k}$. Обозначим $u = k + t_1 + \dots + t_k$. Функция (43) принадлежит классу эквивалентности $[f_4(x_1, \dots, x_u)]_{\langle S_u \rangle}$, где

$$f_4(x_1, \dots, x_u) \equiv \bigwedge_{i=1}^{t_1} (x_1 \vee \bar{x}_{k+i}) \wedge \bigwedge_{j=1}^{t_2} (x_2 \vee \bar{x}_{k+t_1+j}) \wedge \dots \wedge \bigwedge_{l=1}^{t_k} (x_k \vee \bar{x}_{k+t_1+\dots+t_{k-1}+l}), \quad (44)$$

$k \geq 2$, $t_i \geq 1$, $i = 1, \dots, k$. В (44) включены все простые имплиценты функции f с литералами в первой степени.

При этом

$$f(x_1, \dots, x_n) \equiv f_4(x_1, \dots, x_u) \cdot f'(x_1, \dots, x_n), \quad (45)$$

где $f'(x_1, \dots, x_n) \in Bi \cap M_2$.

Лемма 21.

1. Пусть $f \in T_3$ и выполняются (44), (45). Тогда

$$f(x_{k+t_1+\dots+t_i+r} = 1, x_{k+t_1+\dots+t_j+w} = 1) \equiv 0 \quad (46)$$

для любых $i \in \{0, \dots, k-1\}$, $j \in \{0, \dots, k-1\}$, $i \neq j$, $r \in \{1, \dots, t_i\}$, $w \in \{1, \dots, t_j\}$.

2. Условие (46) выполняется для всех $i \in \{0, \dots, k-1\}$, $j \in \{0, \dots, k-1\}$, $i \neq j$, $r \in \{1, \dots, t_i\}$, $w \in \{1, \dots, t_j\}$, если и только если функция $\bar{f}$ имеет хотя бы одну из имплицентов

$$(\bar{x}_1 \vee \bar{x}_2), (\bar{x}_1 \vee \bar{x}_{k+t_1+\dots+t_i+w}), (\bar{x}_2 \vee \bar{x}_{k+t_1+\dots+t_i+r}), (\bar{x}_{k+t_1+\dots+t_i+r} \vee \bar{x}_{r+t_1+\dots+t_j+w}). \quad (47)$$

Доказательство аналогично доказательству леммы 17.

Лемма 22. Следующие функции принадлежат множеству T_3 :

$$(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_1 \vee \bar{x}_2), \quad (48)$$

$$(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_1 \vee \bar{x}_4), \quad (49)$$

$$(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_2 \vee \bar{x}_3), \quad (50)$$

$$(x_1 \vee \bar{x}_3)(x_2 \vee \bar{x}_4)(\bar{x}_3 \vee \bar{x}_4). \quad (51)$$

Доказывается непосредственной проверкой.

Теорема 6. При выполнении (44), (45) соотношение $\bar{f} \in WP$ верно, если и только если

$$\bar{f}(x_{k+t_1+\dots+t_i+r} = 1, x_{k+t_1+\dots+t_j+w} = 1) \equiv 0 \quad (52)$$

для любых $i \in \{0, \dots, k-1\}$, $j \in \{0, \dots, k-1\}$, $i \neq j$, $r \in \{1, \dots, t_i\}$, $w \in \{1, \dots, t_j\}$.

Доказательство. Легко видеть, что если $\bar{f} \in WP$, то верно (52).

Пусть

$$\bar{f}(x_{k+t_1+\dots+t_i+r} = 1, x_{k+t_1+\dots+t_j+w} = 1) \equiv 0$$

для любых $i \in \{0, \dots, k-1\}$, $j \in \{0, \dots, k-1\}$, $i \neq j$, $r \in \{1, \dots, t_i\}$, $w \in \{1, \dots, t_j\}$.

Покажем, что тогда $\bar{f} \in WP$. Для этого докажем, что если $\alpha \notin E_{\bar{f}}$, $\beta \notin E_{\bar{f}}$, то $\alpha \vee \beta \notin E_{\bar{f}}$ (отсюда будет следовать, что $\bar{f} \in WP$). Вектор α не удовлетворяет некоторой простой имплиценте функции $\bar{f}$, вектор β не удовлетворяет некоторой простой имплиценте функции $\bar{f}$. Если α или β не выполняют имплиценту вида $(\bar{x}_r \vee \bar{x}_t)$, то $\alpha \vee \beta$ также не выполняет эту имплиценту. Далее считаем, что α и β не выполняют простую имплиценту, содержащую литерал в первой степени. Используя лемму 21, находим, что векторы α и β одновременно не удовлетворяют одной из имплицентов вида

$$(\bar{x}_1 \vee \bar{x}_{k+t_1+\dots+t_i+r})(\bar{x}_2 \vee \bar{x}_{r+t_1+\dots+t_j+w})(\bar{x}_1 \vee \bar{x}_2), \quad (53)$$

$$(\bar{x}_1 \vee \bar{x}_{k+t_1+\dots+t_i+r})(\bar{x}_2 \vee \bar{x}_{r+t_1+\dots+t_j+w})(\bar{x}_1 \vee \bar{x}_{k+t_1+\dots+t_j+w}), \quad (54)$$

$$(\bar{x}_1 \vee \bar{x}_{k+t_1+\dots+t_i+r})(\bar{x}_2 \vee \bar{x}_{r+t_1+\dots+t_j+w})(\bar{x}_2 \vee \bar{x}_{k+t_1+\dots+t_i+r}), \quad (55)$$

$$(\bar{x}_1 \vee \bar{x}_{k+t_1+\dots+t_i+r})(\bar{x}_2 \vee \bar{x}_{r+t_1+\dots+t_j+w})(\bar{x}_{k+t_1+\dots+t_i+r} \vee \bar{x}_{r+t_1+\dots+t_j+w}). \quad (56)$$

Пусть векторы α и β одновременно не удовлетворяют имплиценте (53). Так как $\bar{f}_3 \in WP$ (см. лемму 22), то вектор $\alpha \vee \beta$ не удовлетворяет $\bar{f}_3$. Дальнейшее доказательство очевидно.

Следствие. При выполнении (45) соотношение $\bar{f} \in WP$ верно, если и только если для любых $i \in \{0, \dots, k-1\}$, $j \in \{0, \dots, k-1\}$, $i \neq j$, $r \in \{1, \dots, t_i\}$, $w \in \{1, \dots, t_j\}$ функция f имеет хотя бы одну из имплицент (47).

4. Функции $f : f \in WP, \bar{f} \in WN$

Теорема 7. Функция $f(x_1, \dots, x_n) \in WP$ принадлежит множеству T_4 , если и только если $f(x_1, \dots, x_n) \in M_1$ или в сокращенной КНФ функции $\bar{f}$ только одно переменное x_i , $i \in \{1, \dots, n\}$, встречается в нулевой степени.

Доказательство теоремы 7 разобьем на несколько лемм.

Лемма 23. Справедливо включение

$$T_4 \supset M_1.$$

Доказательство. Если $f \in M_1$, то $f \in WP$, $\bar{f} \in M_2$, $\bar{f} \in WN$.

Пример 2. Примеры функций $f \in WP$, $f \notin M_1$, $\bar{f} \in WN$:

$$f \equiv x_1 \vee \dots \vee x_{i-1} \vee \bar{x}_i \vee x_{i+1} \vee \dots \vee x_n \in WP,$$

$$\bar{f} \equiv \bar{x}_1 \cdot \dots \cdot \bar{x}_{i-1} \cdot x_i \cdot \bar{x}_{i+1} \cdot \dots \cdot \bar{x}_n \in WN,$$

$$f \equiv x_1 \cdot \dots \cdot x_{i-1} \cdot \bar{x}_i \cdot x_{i+1} \cdot \dots \cdot x_n \in WP,$$

$$\bar{f} \equiv \bar{x}_1 \vee \dots \vee \bar{x}_{i-1} \vee x_i \vee \bar{x}_{i+1} \vee \dots \vee \bar{x}_n \in WN.$$

Лемма 24. Пусть $f(x_1, \dots, x_k) \in WP$, в сокращенной КНФ функции $\bar{f}$ только x_i , $i \in \{1, \dots, n\}$, встречается в нулевой степени. Тогда $\bar{f} \in WN$.

Доказательство. Покажем, что в сокращенную КНФ функции $\bar{f}$ только x_i может входить в первой степени. В самом деле, если в сокращенную КНФ функции $\bar{f}$ входит x_j , $j \neq i$, в первой степени, то в сокращенную КНФ функции f должен входить литерал x_j в нулевой степени, а это не так. Дальнейшее доказательство очевидно.

Лемма 25. Пусть $f(x_1, \dots, x_n) \in T_4$, тогда $\bar{f}(\bar{x}_1, \dots, \bar{x}_n) \in T_4$.

Доказательство. Имеем $f \in WP$, $\bar{f} \in WN$. Из условия $f(x_1, \dots, x_n) \in WP$ следует $f(\bar{x}_1, \dots, \bar{x}_n) \in WN$ (достаточно воспользоваться приведенной записью функции f). Из условия $\bar{f}(x_1, \dots, x_n) \in WN$ следует, что $\bar{f}(\bar{x}_1, \dots, \bar{x}_n) \in WP$. Лемма доказана.

Замечание 1. Лемму 25 можно сформулировать следующим образом: функция $f(x_1, \dots, x_n) \in T_4$, если и только если $\bar{f}(\bar{x}_1, \dots, \bar{x}_n) \in T_4$.

Замечание 2. Поскольку $\|\bar{f}(\bar{x}_1, \dots, \bar{x}_n)\| = 2^n - r$ при $\|f(x_1, \dots, x_n)\| = r$, лемма 25 позволяет по множеству всех функций $f(x_1, \dots, x_n) \in T_4$, $\|f\| = r$ просто получить множество всех функций $g(x_1, \dots, x_n) \in T_4$, $\|g\| = 2^n - r$.

Лемма 26. В сокращенную КНФ функции $f(x_1, \dots, x_n) \in WP$ литерал $\bar{x}_1$ входит, если и только если найдутся два таких соседних вектора $\alpha, \beta \in V_n$, $\|\beta\| = \|\alpha\| + 1$, что $\alpha \in E_f$, $\beta \notin E_f$.

Доказательство. Пусть $\alpha, \beta \in V_n$, $\|\beta\| = \|\alpha\| + 1$, векторы α и β различаются в 1-й координате, причем $\alpha \in E_f$, $\beta \notin E_f$, но литерал $\bar{x}_1$ не входит в сокращенную КНФ функции f . Тогда из условия $\alpha \in E_f$ следует $\beta \in E_f$, но это не так. Поэтому литерал $\bar{x}_1$ входит в сокращенную КНФ функции f .

Предположим теперь, что литерал $\bar{x}_1$ входит в сокращенную КНФ функции f . Без ограничения общности можем считать, что функция f имеет простую имплиценту

$$(\bar{x}_1 \vee x_2 \vee \dots \vee x_k). \quad (57)$$

Тогда

$$f(x_1 = 1, x_2 = 0, \dots, x_k = 0) \equiv 0, \quad (58)$$

$$f(x_1 = 0, x_2 = 0, \dots, x_k = 0) \neq 0. \quad (59)$$

Поэтому найдется выполняющий вектор вида $(\underbrace{0, \dots, 0}_k, \alpha_{k+1}, \dots, \alpha_n)$.

В силу (58)

$$(\underbrace{1, 0, \dots, 0}_k, \alpha_{k+1}, \dots, \alpha_n) \notin E_f.$$

Лемма доказана.

Замечание. Доказанную лемму можно естественным образом переформулировать для $\bar{x}_i$.

Доказательство теоремы 7. Функции, указанные в формулировке теоремы, принадлежат множеству T_4 (леммы 23, 24).

Покажем (по индукции), что в классе T_4 других функций нет. Непосредственной проверкой устанавливается, что это верно при $n = 2$. Предположим, что теорема верна при $n - 1$, докажем (от противного), что она верна для n . Пусть в сокращенную КНФ функции $f(x_1, \dots, x_n) \in WP$ входят литералы $\bar{x}_1, \bar{x}_n$. Для x_1 соответствующие векторы из леммы 26 обозначим $\alpha^{(1)}$,

$\beta^{(1)}$, для x_n соответствующие векторы из леммы 26 обозначим $\alpha^{(2)}$, $\beta^{(2)}$. Без ограничения общности можем считать, что

$$\begin{aligned}\alpha^{(1)} &= (0, 0, \dots, 0, 0, \dots, 0, 1, \dots, 1, 1, \dots, 1, \eta), \\ \beta^{(1)} &= (1, 0, \dots, 0, 0, \dots, 0, 1, \dots, 1, 1, \dots, 1, \eta), \\ \alpha^{(2)} &= (\lambda, 0, \dots, 0, 1, \dots, 1, 0, \dots, 0, 1, \dots, 1, 0), \\ \beta^{(2)} &= (\lambda, \underbrace{0, \dots, 0}_{r_1}, \underbrace{1, \dots, 1}_{r_2}, \underbrace{0, \dots, 0}_{r_3}, \underbrace{1, \dots, 1}_{r_4}).\end{aligned}$$

В случае $r_1 \geq 1$ рассмотрим функцию $f(x_2 = 0)$. Сокращенная КНФ этой функции содержит литералы $\bar{x}_1, \bar{x}_n$, функция $f(x_2 = 0)$ зависит от $n - 1$ переменных. По предположению индукции $f(x_2 = 0) \notin T_4$ и $f \notin T_4$. Аналогично рассматривается случай $r_4 \geq 1$. Далее считаем, что $r_1 = 0$, $r_4 = 0$.

Пусть $r_2 \geq 2$. Рассмотрим функцию, получаемую из f отождествлением переменных x_2 и x_3 : $f(x_2 = x_3)$. По предположению индукции имеем $f(x_2 = x_3) \notin T_4$, $f \notin T_4$. Далее считаем, что $r_2 \leq 1$, $r_3 \leq 1$.

Таким образом, осталось рассмотреть функции от четырех переменных $f(x_1, x_2, x_3, x_4) \in WP$, удовлетворяющие условиям

$$\begin{aligned}f(0, 0, 1, \eta) &= 1, \\ f(1, 0, 1, \eta) &= 0, \\ f(\lambda, 1, 0, 0) &= 1, \\ f(\lambda, 1, 0, 1) &= 0,\end{aligned}\tag{60}$$

для различных $(\eta, \lambda) \in V_2$. Такая работа была проделана с помощью компьютера и было установлено, что все эти функции не являются слабо отрицательными. Теорема 7 доказана.

Автор выражает признательность А. М. Зубкову за ценные замечания.

Список литературы

- [1] Schaefer T. "Complexity of satisfiability problems", *Proc. 10 Annual ACM Symp. on Theory of Computing Machinery*, 1978, 216–226.
- [2] Гизунов С. А., Носов В. А., "О классификации всех булевых функций четырех переменных по классам Шефера", *Обозр. прикл. и промышл. матем.*, 2:3 (1995), 440–467.
- [3] Горшков С. П., "Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений", *Обозр. прикл. и промышл. матем.*, 2:3 (1995), 325–398.