Math-Net.Ru

Общероссийский математический портал

С. П. Горшков, А. В. Тарасов, О весах булевых функций, представимых в виде 2-КНФ или 3-КНФ, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 1, 5–26

DOI: <https://doi.org/10.4213/mvk242>

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: 52.205.19.152

26 апреля 2023 г., 18:34:12

**О весах булевых функций,
представимых в виде 2-КНФ или 3-КНФ**

С. П. Горшков¹, А. В. Тарасов²

¹ Академия криптографии Российской Федерации, Москва

² Московский государственный университет информационных технологий,
радиотехники и электроники, Москва

Получено 11.V.2017

Аннотация. Найдены множества возможных значений весов бижунктивных булевых функций (2-КНФ). Для булевых функций, существенно зависящих от всех переменных, описаны: множества бижунктивных функций веса, близкого к максимальному, и множества функций максимального веса, представимых 3-КНФ. Сформулирована гипотеза о максимальном весе функций, представимых k -КНФ ($k \geq 4$) и существенно зависящих от всех переменных. Описаны некоторые множества равновероятных булевых функций, представимых k -КНФ.

Ключевые слова: вес булевой функции, бижунктивные булевы функции, k -КНФ

On the weights of Boolean functions representable by 2-CNF or 3-CNF

S. P. Gorshkov¹, A. V. Tarasov²

¹ Academy of Cryptography of the Russian Federation, Moscow

² Moscow State University of Information Technologies, Radioengineering and Electronics,
Moscow

Abstract. Sets of possible values of weights of bijunctive Boolean functions (2-CNF) are found. For Boolean functions having all variables as essential ones we describe: sets of bijunctive functions with weight close (but not equal) to the maximal value and sets of functions of maximal weight represented as 3-CNF. A hypothesis on the maximal weight of functions representable as k -CNF ($k \geq 4$) and having all variables as essential ones is formulated. Some sets of balanced Boolean functions representable as k -CNF are described.

Key words: weight of Boolean function, bijunctive Boolean functions, k -CNF

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 1, pp. 5–26 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Основные обозначения и определения

$\mathbb{N}$ — множество натуральных чисел,

V_n — n -мерное пространство булевых векторов, $n \in \mathbb{N}$,

$V_n^{(i)}$ — множество всех векторов из V_n веса i , $i \in \{0, 1, \dots, n\}$,

F_n — множество булевых функций от $n \in \mathbb{N}$ переменных,

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

$\|f(x_1, \dots, x_n)\|$ — вес булевой функции $f(x_1, \dots, x_n)$ (далее слово «булевой» иногда будем опускать).

Если для функций $f(x_1, \dots, x_n), h(x_1, \dots, x_n)$ выполняется соотношение $f \cdot h = f$, то h называется *имплицентай* функции f .

Имплиценты вида $x_{i_1} \vee \dots \vee x_{i_q}$, $1 \leq i_1 < \dots < i_q \leq n$, называются *элементарными имплицентами*. Элементарная имплицента называется *простой*, если никакая ее собственная часть не является имплицентай функции f . Конъюнкция всех простых имплицентай функции f называется *сокращенной КНФ* функции f .

Переменная x_i или ее отрицание $\bar{x}_i$ называется *литералом*.

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

Пусть $f(x_1, \dots, x_n) \in F_n$, $r \in \{1, \dots, n\}$, $1 \leq i_1 < \dots < i_r \leq n$, $(\alpha_1, \dots, \alpha_r) \in V_r$. Символом $f(x_1 = \alpha_1, \dots, x_r = \alpha_r)$ обозначим подфункцию функции f , получаемую фиксацией переменных $x_1 = \alpha_1, \dots, x_r = \alpha_r$.

Функция $f(x_1, \dots, x_n)$ называется *1-выполнимой*, если $f(1, \dots, 1) = 1$. Множество 1-выполнимых функций обозначим $1-S$.

Функция $f(x_1, \dots, x_n)$ называется *биюнктивной*, если $f \equiv 1$ или существует представление функции f в виде следующей конъюнктивной нормальной формы (КНФ):

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

Введем обозначения:

Bi — множество биюнктивных функций,

$Bi_n = Bi \cap F_n$ — множество биюнктивных функций от n переменных,

$Bi'_n = Bi_n \cap F'_n$ — множество биюнктивных функций от n переменных, существенно зависящих от всех переменных,

Bi''_n — множество биюнктивных функций от n переменных, существенно зависящих от всех переменных и не имеющих однолитеральных имплицентай,

M — множество монотонных булевых функций,

$Bi_n''' = Bi_n'' \cap M$ — множество монотонных биюнктивных функций, существенно зависящих от всех переменных и не имеющих однолитеральных имплицентов,

$Sym(n)$ — симметрическая группа степени n ,

S_n — симметрическая группа перестановок координат векторов из V_n , подгруппа $Sym(2^n)$, изоморфна $Sym(n)$,

Σ_n — группа сдвигов на пространстве V_n ,

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

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

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

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

$$R_n = \left[\bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \right]_{\langle Q_n \rangle}, \quad \text{где } n \geq 2,$$

$$W_n = \left[\bigwedge_{i=1}^{n-3} (x_1 \vee x_{i+1}) \cdot (x_{n-1} \vee x_n) \right]_{\langle Q_n \rangle}, \quad \text{где } n \geq 4,$$

$$w_n = 3 \cdot 2^{n-3} + 3,$$

$[a]$ — целая часть числа a ,

$\lceil a \rceil$ — наименьшее целое, большее или равное a .

Вершинным покрытием неориентированного графа без петель $G = (V, E)$ называется такое множество вершин $V' \subseteq V$, что каждое ребро из E инцидентно хотя бы одной вершине из V' . Вершинное покрытие V' называется *минимальным*, если все другие покрытия имеют мощность, не меньшую $|V'|$. Мощность минимального вершинного покрытия графа G обозначим $v(G)$.

Паросочетанием неориентированного графа без петель $G = (V, E)$ называется такое множество ребер $E' \subseteq E$, что никакие два ребра из E' не имеют общей вершины. Паросочетание называется *максимальным*, если все другие паросочетания имеют мощность, не большую $|E'|$. Мощность максимального паросочетания графа G обозначим через $m(G)$.

Пусть $k \in N$. Конъюнктивная нормальная форма $f(x_1, \dots, x_n)$ называется k -КНФ, если она имеет вид

$$f(x_1, \dots, x_n) \equiv \bigwedge_{i=1}^l (x_{s_{i1}}^{\alpha_{i1}} \vee \dots \vee x_{s_{in_i}}^{\alpha_{in_i}}), \quad \text{где } n_i \leq k, i = 1, \dots, l.$$

Представимые в виде k -КНФ функции называют *k -юнктивными*, по аналогии с названием биюнктивных для функций, представимых в виде 2-КНФ [1, 2].

Множество всех k -юнктивных булевых функций обозначим (k) -КНФ.

Задача решения системы булевых уравнений, каждое уравнение которых зависит не более чем от фиксированного числа k неизвестных, сводится к задаче нахождения выполняющих векторов соответствующей формулы, записанной в виде k -КНФ. Сложность «в худшем случае» задачи распознавания выполнимости k -КНФ ниже полного перебора (см., например, [3, 4]), а при $k = 2$ является полиномиальной [1]. Поэтому представляет интерес исследование функций из класса (k) -КНФ.

1. О весе биюнктивных булевых функций

Важной характеристикой любого класса булевых функций от n переменных является спектр весов функций этого класса. В работе [5] показано, что если $n \geq 5$ и f — биюнктивная функция, существенно зависящая от всех n переменных, то либо $\|f\| = 2^{n-1} + 1$, либо $\|f\| < 2^{n-1}$, причем $\|f\| = 2^{n-1} + 1$ тогда и только тогда, когда

$$f(x_1, \dots, x_n) \in R_n.$$

Нижеследующие теорема 1 и теорема 2 уточняют это утверждение.

Теорема 1. Для любого натурального n и любого $t \in \{1, 2, \dots, 2^{\lfloor \frac{n}{2} \rfloor}\}$ существует такая функция $f \in Bi'_n \cap (1-S)$, что $\|f\| = t$.

Доказательство. Докажем теорему индукцией по n . При $n = 1$ единственное допустимое значение — это $t = 1$. Условию теоремы удовлетворяет функция x_1 . При $n = 2$ выполняется условие $t \in \{1, 2\}$ и соответствующие функции — это x_1x_2 и $x_1 \oplus x_2 \oplus 1$. Предположим, что утверждение верно для $n \geq 2$. Докажем его справедливость для $n+2$.

Пусть $t \in \{1, \dots, 2^{\lfloor \frac{n+2}{2} \rfloor}\}$. Если $t \leq 2^{\lfloor \frac{n}{2} \rfloor}$, то по предположению индукции найдется функция $f_t^{(n)} \in Bi'_n \cap (1-S)$ с $\|f_t^{(n)}\| = t$.

Положив $f_t^{(n+2)} = f_t^{(n)} \cdot x_{n+1} \cdot x_{n+2}$, получим функцию такого же веса, существенно зависящую от всех $n+2$ переменных.

При $2^{\lfloor \frac{n}{2} \rfloor} < t \leq 2^{\lfloor \frac{n+2}{2} \rfloor}$ рассмотрим два случая.

Если t четно, то $t = 2 \cdot t'$, $t' \leq 2^{\lfloor \frac{n}{2} \rfloor}$. По предположению индукции найдется функция $f_{t'}^{(n)} \in Bi'_n \cap (1-S)$ с $\|f_{t'}^{(n)}\| = t'$.

Положим $f_t^{(n+2)} = f_{t'}^{(n)} \cdot (x_{n+1} \oplus x_{n+2} \oplus 1)$. Тогда $f_t^{(n+2)} \in Bi'_{n+2} \cap (1-S)$ и $\|f_t^{(n+2)}\| = 2 \cdot t' = t$.

Пусть теперь t нечетно, т. е. $t = 2 \cdot t' + 1$, $t' \leq 2^{\lfloor \frac{n}{2} \rfloor}$ и $f_{t'}^{(n)} \in Bi'_n \cap (1-S)$, $\|f_{t'}^{(n)}\| = t'$. Рассмотрим функцию

$$f_t^{(n+2)}(x_1, \dots, x_{n+2}) = f_{t'}^{(n)}(x_1, \dots, x_n) \wedge \bigwedge_{i=1}^{n+1} (x_i \vee x_{n+2}).$$

Ясно, что это 1-выполнимая биюнктивная функция. При этом

$$f_t^{(n+2)}(x_{n+2}=1) = f_{t'}^{(n)}(x_1, \dots, x_n).$$

Поэтому функция $f_t^{(n+2)}$ существенно зависит от переменных $x_1, \dots, x_n$. Так как

$$(1, \dots, 1, 0, 0) \notin E_{f_t^{(n+2)}}, (1, \dots, 1, 0, 1) \in E_{f_t^{(n+2)}}, (1, \dots, 1, 1, 0) \in E_{f_t^{(n+2)}},$$

то функция $f_t^{(n+2)}$ существенно зависит от x_{n+1} и x_{n+2} .

Вес функции $f_t^{(n+2)}$ равен

$$\begin{aligned} \|f_t^{(n+2)}\| &= \|f_t^{(n+2)}(x_{n+2}=0)\| + \|f_t^{(n+2)}(x_{n+2}=1)\| = \\ &= 1 + 2\|f_{t'}^{(n)}\| = 2t' + 1 = t. \end{aligned}$$

В силу справедливости базы индукции для $n = 1$ и для $n = 2$ утверждение теоремы верно для всех натуральных n . $\square$

Замечание 1. Всякая биюнктивная 1-выполнимая булева функция является слабо положительной булевой функцией (определение слабо положительной функции см. [1, 2]).

Далее исследуем биюнктивные функции вида

$$f(x_1, \dots, x_n) \in Bi'_n, \quad f \notin R_n,$$

имеющие максимальный вес. Сформулируем некоторые простые свойства, доказательство которых авторам представляется очевидным.

Свойство 1. Пусть $f(x_1, \dots, x_n)$ имеет имплиценту $h(x_1, \dots, x_k) \in F_k$, $\|h\| = r$. Тогда $\|f\| \leq r \cdot 2^{n-k}$.

Свойство 2. Для любой булевой функции $f(x_1, \dots, x_n)$ и для любых $r \in \{1, \dots, n\}$, $1 \leq i_1 < \dots < i_r \leq n$, справедливо соотношение

$$\|f(x_1, \dots, x_n)\| = \sum_{(\alpha_1, \dots, \alpha_r) \in V_r} \|f(x_{i_1}=\alpha_1, \dots, x_{i_r}=\alpha_r)\|.$$

Свойство 3. Если $f(x_1, \dots, x_n) \in W_n$, то

$$\begin{aligned} \|f\| &= \left\| \bigwedge_{i=1}^{n-3} (x_1 \vee x_{i+1}) \right\| \cdot \|(x_{n-1} \vee x_n)\| = \\ &= (2^{n-3} + 1) \cdot 3 = 3 \cdot 2^{n-3} + 3 = w_n, \end{aligned}$$

где считаем, что функция $\bigwedge_{i=1}^{n-3} (x_1 \vee x_{i+1})$ зависит от $n-2$ переменных, а функция $x_{n-1} \vee x_n$ — от 2 переменных.

Свойство 4. Пусть $f(x_1, \dots, x_n), h(x_1, \dots, x_n) \in Bi_n'''$, $h = f \cdot (x_i \vee x_j)$ и функция $x_i \vee x_j$ не является имплицентов функции f . Тогда

$$\|h\| < \|f\|.$$

Свойство 5. Для функций $f \in Bi_n'''$ формула

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^q (x_{s_{i1}} \vee x_{s_{i2}}), \quad (2)$$

где $s_{i1} \neq s_{i2}$, $i = 1, \dots, q$, является минимальной и сокращенной КНФ, причем в (2) встречаются все переменные $x_1, \dots, x_n$.

Символом U_n обозначим множество неориентированных графов $G = (V, E)$ без петель и изолированных вершин, $V = \{x_1, \dots, x_n\}$. Определим отображение $T_n : Bi_n''' \rightarrow U_n$ по принципу: для функции $f \in Bi_n'''$ вида (2) граф $T_n(f)$ есть неориентированный граф $G_f = (V_f, E_f) \in U_n$, в котором вершины x_i и x_j соединены ребром тогда и только тогда, когда имплицента $x_i \vee x_j$ входит в 2-КНФ (2). Данное отображение, очевидно, является взаимно однозначным.

Свойство 6 ([6, с. 170]). Для графов G_f выполняется соотношение

$$m(G_f) \geq \left\lceil \frac{v(G_f)}{2} \right\rceil. \quad (3)$$

Свойство 7. Для рассматриваемых графов G_f равенство $v(G_f) = 1$ имеет место, если и только если

$$f(x_1, \dots, x_n) \in \left[\bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \right]_{\langle S_n \rangle}.$$

Теорема 2. Пусть $f(x_1, \dots, x_n) \in Bi'_n$, $f \notin R_n$, $n \geq 7$. Тогда $\|f\| \leq w_n$, причем $f \in W_n$, если $\|f\| = w_n$.

Доказательство теоремы разобьем на несколько лемм.

Лемма 1. Если $n \geq 3$ и функция $f(x_1, \dots, x_n) \in Bi'_n$ имеет однолитеральную имплиценту, то $\|f\| < w_n$.

Доказательство. Предположим, что функция f имеет однолитеральную имплиценту x_1 . Поскольку $n \geq 3$, без ограничения общности можем считать, что функция имеет имплиценту $x_1 \cdot (x_2 \vee x_3)$. При этом в силу свойства 1

$$\|f\| \leq \|x_1(x_2 \vee x_3)\| \cdot 2^{n-3} = 3 \cdot 2^{n-3} < w_n. \quad \square$$

Далее считаем, что функция не имеет однолитеральных имплицент.

Лемма 2. Пусть функция $f(x_1, \dots, x_n) \in Bi''_n$, $n \geq 5$, имеет сокращенную 2-КНФ вида

$$f \equiv \bigwedge_{j=1}^q \left(x_{s_{j1}}^{\beta_{j1}} \vee x_{s_{j2}}^{\beta_{j2}} \right), \quad (4)$$

и в запись (7) функции f некоторое переменное входит в разных степенях. Тогда

$$\|f(x_1, \dots, x_n)\| < w_n.$$

Доказательство. Все функции из класса $[f(x_1, \dots, x_n)]_{\langle Q_n \rangle}$ имеют одинаковый вес, поэтому в ходе доказательства при рассмотрении функции $f(x_1, \dots, x_n)$ будем выбирать наиболее удобного представителя из класса $[f(x_1, \dots, x_n)]_{\langle Q_n \rangle}$.

Пусть переменное x_1 в запись (7) входит в разных степенях. Представим функцию $f(x_1, \dots, x_n)$ в виде

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^r (x_1 \vee x_{i+1}) \wedge \bigwedge_{j=1}^t (\bar{x}_1 \vee x_{s_j}^{\alpha_j}) \wedge g(x_2, \dots, x_n),$$

где $r \geq 1, t \geq 1$. Без ограничения общности будем считать, что x_1 — переменная, входящая в разных степенях, и для нее значение $r + t$ максимально. Если $r \geq 1, t \geq 2$, то

$$\|f\| = \|f(x_1=0)\| + \|f(x_1=1)\| \leq 2^{n-r-1} + 2^{n-t-1} \leq 2^{n-2} + 2^{n-3} < w_n.$$

Аналогично рассматривается случай $r \geq 2, t \geq 1$.

Далее считаем $r = 1, t = 1$ (ясно, что при этом $g \neq 1$). Пусть $s_1 = 2$. Если $\alpha_1 = 1$, то функция f имеет однолитеральную имплиценту x_2 , что невозможно. Поэтому считаем, что $\alpha_1 = 0$. Тогда функция f имеет имплиценту $x_1 \oplus x_2$. Воспользуемся тем, что $g \neq 1$. Возможны следующие варианты:

либо функция f имеет имплиценту $(x_1 \oplus x_2)(x_3 \vee x_4)$, в этом случае

$$\|f\| \leq 2 \cdot 3 \cdot 2^{n-4} < w_n,$$

либо функция f имеет имплиценту $(x_1 \oplus x_2)(x_2^\beta \vee x_3)$, в этом случае

$$\|f\| \leq 3 \cdot 2^{n-3} < w_n.$$

Тем самым случай, когда $s_1 = 2$, полностью рассмотрен. Далее без ограничения общности считаем, что $x_{s_1}^{\alpha_1} = x_3$. В этом случае f имеет имплиценту $(x_1 \vee x_2)(\bar{x}_1 \vee x_3)$.

Нетрудно показать, что если у функции f есть имплицента вида

$$(x_1 \vee x_2)(\bar{x}_1 \vee x_3)(x_2^\alpha \vee x_3^\beta),$$

где $\alpha \cdot \beta = 0$, то $\|f\| < w_n$.

Вместе с тем, если $\alpha \cdot \beta = 1$, т. е. $\alpha = \beta = 1$, то

$$\begin{aligned} (x_1 \vee x_2)(\bar{x}_1 \vee x_3)(x_2^\alpha \vee x_3^\beta) &= \\ &= (x_1 \vee x_2)(\bar{x}_1 \vee x_3)(x_2 \vee x_3) = (x_1 \vee x_2)(\bar{x}_1 \vee x_3). \end{aligned}$$

Поскольку функция f существенно зависит также от переменных x_4 и x_5 , рассмотрим случай, когда f имеет имплиценту

$$(x_1 \vee x_2)(\bar{x}_1 \vee x_3)(x_4 \vee x_5). \quad (5)$$

Тогда

$$\|f\| \leq 4 \cdot 3 \cdot 2^{n-5} = 3 \cdot 2^{n-3} < w_n.$$

Осталось рассмотреть случай, когда функция f не имеет имплицент вида (8). В этом случае переменные $x_4, \dots, x_n$ входят в имплиценты либо только с переменной x_2 , либо только с переменной x_3 .

Пусть переменная x_2 входит в разных степенях. Тогда функция f имеет имплиценту вида

$$(x_1 \vee x_2)(\bar{x}_1 \vee x_3)(\bar{x}_2 \vee x_4).$$

При этом

$$\|f\| \leq 5 \cdot 2^{n-4} < w_n,$$

т.е. x_2 может входить только в первой степени. Аналогично показывается, что x_3 может входить только в первой степени. В рассматриваемых условиях функция f имеет имплиценту

$$(x_1 \vee x_2)(\bar{x}_1 \vee x_3) \bigwedge_{i=1}^u (x_2 \vee x_{i+3}) \wedge \bigwedge_{j=1}^{n-u-3} (x_3 \vee x_{j+u+3}),$$

где $0 \leq u \leq n-3$.

Тогда

$$\begin{aligned} \|f\| &= \|f(x_2=0, x_3=0)\| + \|f(x_2=0, x_3=1)\| + \\ &+ \|f(x_2=1, x_3=0)\| + \|f(x_2=1, x_3=1)\| = \\ &= 0 + 2^{n-u-3} + 2^u + 2^{n-2} \leq 3 \cdot 2^{n-3} + 1. \end{aligned}$$

Лемма доказана. $\square$

Из леммы 2 следует, что далее можно ограничиться исследованием только функций из классов Bi_n''' . При дальнейших рассуждениях будем рассматривать наиболее удобную функцию из класса эквивалентности относительно перестановки переменных. Поэтому рассуждения будем проводить для графа G_f , который в данном случае является неориентированным графом без изолированных вершин, петель и кратных ребер. Основным исследуемым параметром будет величина $v(G_f)$. Сразу можно заметить, что если $v(G_f) = 1$, то $f(x_1, \dots, x_n) \in R_n$ (см. свойство 7). Поэтому далее в доказательстве теоремы 2 будут рассматриваться случаи $v(G_f) \geq 2$.

Лемма 3. Пусть $f \in Bi_n'''$, $v(G_f) = 2$, $n \geq 5$. Тогда $\|f\| \leq w_n$, причем $\|f\| = w_n$ только для функций

$$f(x_1, \dots, x_n) \in \left[\bigwedge_{i=2}^{n-2} (x_1 \vee x_i) \cdot (x_{n-1} \vee x_n) \right]_{\langle S_n \rangle}. \quad (6)$$

Доказательство. Пусть $\{x_1, x_2\}$ — вершинное покрытие графа G_f . В графе G_f выделим двудольный подграф G'_f , одну долю которого составляют вершины $\{x_1, x_2\}$, а другую долю — вершины $\{x_3, \dots, x_n\}$. Ребрами этого графа являются ребра графа G_f , соединяющие вершины из разных долей, и только они. Через V_1 обозначим множество вершин, смежных с x_1 , а через V_2 — множество вершин, смежных с x_2 .

Положим

$$A_1 = V_1 \setminus V_2, \quad A_2 = V_1 \cap V_2, \quad A_3 = V_2 \setminus V_1.$$

Обозначим $k = |A_1|$, $l = |A_2|$, $m = |A_3|$. Из условия леммы вытекает система соотношений

$$\begin{cases} k + l + m = n - 2, \\ k + l \geq 1, \\ l + m \geq 1, \\ k \geq 0, \\ l \geq 0, \\ m \geq 0. \end{cases}$$

Из приведенных рассуждений следует, что функция $f(x_1, \dots, x_n)$ имеет имплиценту

$$h(x_1, \dots, x_n) = \bigwedge_{i \in A_1} (x_1 \vee x_i) \wedge \bigwedge_{j \in A_2} (x_1 \vee x_j) \wedge \bigwedge_{r \in A_2} (x_2 \vee x_r) \wedge \bigwedge_{s \in A_3} (x_2 \vee x_s).$$

Оценим $\|h\|$. По свойству 2

$$\begin{aligned} \|h\| &= \|h(x_1=1, x_2=1)\| + \|h(x_1=0, x_2=1)\| + \\ &+ \|h(x_1=1, x_2=0)\| + \|h(x_1=0, x_2=0)\|. \end{aligned}$$

При этом

$$\begin{aligned} \|h(x_1=1, x_2=1)\| &= 2^{n-2}, \\ \|h(x_1=0, x_2=1)\| &= \left\| \bigwedge_{i \in A_1 \cup A_2} x_i \right\| = 2^{n-2-k-l}, \\ \|h(x_1=1, x_2=0)\| &= \left\| \bigwedge_{i \in A_2 \cup A_3} x_i \right\| = 2^{n-2-l-m}, \\ \|h(x_1=0, x_2=0)\| &= \|x_3 \cdots x_n\| = 1. \end{aligned}$$

Поэтому

$$\|h\| = 2^{n-2} + 2^{n-2-k-l} + 2^{n-2-l-m} + 1.$$

Покажем, что $\|h\| \leq w_n = 3 \cdot 2^{n-3} + 3$. Для этого достаточно доказать, что

$$2^{n-2-k-l} + 2^{n-2-l-m} \leq 2^{n-3} + 2.$$

Пусть l фиксировано. Сначала рассмотрим случай $l = 0$. Тогда

$$\begin{cases} k + m = n - 2, \\ 1 \leq k \leq n - 3, \\ 1 \leq m \leq n - 3. \end{cases}$$

В этом случае $2^{n-2-k-l} + 2^{n-2-l-m} = 2^{n-2-k} + 2^k$. Легко показать, что данная величина принимает максимальное значение при $k = 1$ и что при $k = n - 3$ и это значение равно $2^{n-3} + 2$.

Пусть $l \geq 1$. Обозначим $n' = n - 2 - l \leq n - 3$. Тогда

$$\begin{cases} k + m = n', \\ 0 \leq k \leq n', \\ 0 \leq m \leq n'. \end{cases}$$

В этом случае

$$2^{n-2-k-l} + 2^{n-2-l-m} = 2^{n'-k} + 2^{n'-m} = 2^{n'-k} + 2^k.$$

Данная величина принимает максимальное значение при $k = 0$ и при $k = n'$, и это значение равно $2^{n'} + 1 \leq 2^{n-3} + 1 < w_n$.

Из проведенных рассуждений следует, что

$$\|f\| \leq \|h\| \leq 3 \cdot 2^{n-3} + 3 = w_n. \quad (7)$$

Как указывалось ранее, правая часть (11) достигает максимального значения, равного w_n , при $l = 0$ и $k = 1$ или $k = n - 3$. Значение w_n соответствует функции из класса (9).

Другие функции имеют вес, меньший w_n (см. свойство 4). $\square$

Следующая лемма устанавливает связь между весом функции $f \in Bi_n'''$ и мощностью паросочетания ее графа.

Лемма 4. Пусть $f \in Bi_n''', n \geq 7$, $m(G_f) \geq 3$. Тогда $\|f\| < w_n$.

Доказательство. В условиях леммы без ограничения общности можем считать, что функция f имеет имплиценту

$$(x_1 \vee x_2)(x_3 \vee x_4)(x_5 \vee x_6). \quad (8)$$

Если $m(G_f) \geq 4$, то у функции $f(x_1, \dots, x_n)$ есть имплицента

$$(x_1 \vee x_2)(x_3 \vee x_4)(x_5 \vee x_6)(x_7 \vee x_8). \quad (9)$$

Тогда

$$\|f\| \leq 3^4 \cdot 2^{n-8} = \frac{3^4}{2^5} \cdot 2^{n-3} < 2,6 \cdot 2^{n-3} < w_n.$$

Если же $m(G_f) = 3$, то у функции $f(x_1, \dots, x_n)$ есть имплицента вида (12), но нет имплиценты вида (19). При этом, поскольку $n \geq 7$ и f существенно зависит от всех переменных, существует имплицента вида

$$(x_1 \vee x_2)(x_3 \vee x_4)(x_5 \vee x_6)(x_1 \vee x_7).$$

В этом случае

$$\|f\| = \|f(x_1=0)\| + \|f(x_1=1)\| = 3^2 \cdot 2^{n-3-4} + 3^2 \cdot 2^{n-5} < 2,9 \cdot 2^{n-3}. \quad \square$$

Лемма 5. Пусть $f \in Bi_n'''$, $v(G_f) = 3$, $n \geq 7$. Тогда $\|f\| < w_n$.

Доказательство. Пусть $\{x_1, x_2, x_3\}$ — минимальное вершинное покрытие графа G_f . Аналогично доказательству леммы 3 определим множества V_1, V_2, V_3 по правилу: множество V_1 содержит все вершины, смежные с x_1 , множество V_2 содержит все вершины, смежные с x_2 , а множество V_3 содержит все вершины, смежные с x_3 . Выделим соответствующий двудольный подграф H и по нему построим имплиценту h функции f . В этом случае функция h существенно зависит от всех переменных и имеет вид

$$h(x_1, \dots, x_n) = \bigwedge_{x_i \in V_1} (x_1 \vee x_i) \wedge \bigwedge_{x_j \in V_2} (x_2 \vee x_j) \wedge \bigwedge_{x_k \in V_3} (x_3 \vee x_k).$$

При этом $v(H) = 3$. Рассмотрим множества V_1, V_2, V_3 . По построению $|V_i| \geq 1$, $i = 1, 2, 3$, и $|V_1 \cup V_2 \cup V_3| = |x_4, \dots, x_n| \geq 4$.

Рассмотрим попарные объединения этих множеств. В случае когда все попарные объединения имеют мощность не менее 2, выполняются условия критерия Ф. Холла [7, гл. 3], и тогда семейство множеств (V_1, V_2, V_3) имеет трансверсаль, а следовательно, $m(H) = 3$. В этом случае для функции h , задаваемой графом H и являющейся имплицентой функции f , выполняются условия леммы 4 и $\|f\| < w_n$.

Осталось рассмотреть случай, когда объединение каких-либо двух множеств из семейства (V_1, V_2, V_3) имеет мощность 1. Пусть $|V_1 \cup V_2| = 1$. Без ограничения общности будем считать, что $V_1 = V_2 = \{x_4\}$. Тогда $h(x_1, \dots, x_n) = (x_1 \vee x_4) \wedge (x_2 \vee x_4) \wedge \bigwedge_{x_k \in V_3} (x_3 \vee x_k)$, причем $|V_3| = n - 4 \geq 3$.

Стало быть, при $n \geq 7$

$$\|f\| \leq \|h\| = 5 \cdot (2^{n-4} + 1) = 5 \cdot 2^{n-4} + 2 + 3 < 5 \cdot 2^{n-4} + 2^{n-4} + 3 = w_n. \quad \square$$

Лемма 6. Пусть $n \geq 7$, $f \in Bi_n'''$, $v(G_f) \geq 4$. Тогда $\|f\| < w_n$.

Доказательство. Поскольку $v(G_f) \geq 4$, то $n \geq 8$. Пусть $\{x_1, x_2, x_3, x_4\}$ — вершинное покрытие. Аналогично доказательствам лемм 3 и 5 построим множества V_1, V_2, V_3, V_4 вершин, смежных вершинам из покрытия. Выделим соответствующий двудольный граф H и соответствующую имплиценту h функции f . В этом случае $v(H) = 4$. По свойству 6 мощность паросочетания $m(H) \geq 2$. Если $m(H) \geq 3$, то лемма верна в силу леммы 4. Рассмотрим случай $m(H) = 2$. Пусть $\{x_1, x_5\}$ и $\{x_2, x_6\}$ — ребра, образующие паросочетание мощности 2. Тогда эти ребра смежны со всеми остальными ребрами графа H . Следовательно, любое ребро, инцидентное x_3 или x_4 , инцидентно либо x_5 , либо x_6 . Возможны следующие варианты.

а) Одно ребро инцидентно x_5 , а другое — x_6 . Тогда с точностью до перестановки переменных функция h имеет имплиценту вида

$$g = (x_1 \vee x_5)(x_2 \vee x_5)(x_3 \vee x_6)(x_4 \vee x_6).$$

Поскольку $n \geq 8$, то в графе H есть вершина x_7 , смежная с вершиной $x_i \in \{x_1, \dots, x_4\}$. Если эта вершина инцидентна x_3 или x_4 , то в исходное паросочетание можно добавить соответствующее ребро $\{x_i, x_7\}$, в результате чего получим паросочетание большей мощности, что ведет к противоречию. Поэтому она инцидентна либо x_1 , либо x_2 . Без ограничения общности считаем, что она инцидентна x_1 . Тогда

$$\|f\| \leq \|h\| \leq \|g(x_1 \vee x_7)\| = 40 \cdot 2^{n-7} < 48 \cdot 2^{n-7} + 3 = w_n.$$

б) Ребра, инцидентные вершинам x_3 и x_4 , инцидентны только x_5 . Тогда с точностью до перестановки переменных функция h имеет имплиценту вида

$$g = (x_1 \vee x_5)(x_3 \vee x_5)(x_4 \vee x_5)(x_2 \vee x_6).$$

Рассмотрим вершину x_7 . Как и ранее, эта вершина инцидентна либо x_1 , либо x_2 . Если она инцидентна x_2 , то

$$\|f\| \leq \|(x_1 \vee x_5)(x_3 \vee x_5)(x_4 \vee x_5)(x_2 \vee x_6)(x_2 \vee x_7)\| = 45 \cdot 2^{n-7} < 48 \cdot 2^{n-7} + 3 = w_n.$$

Если же вершина x_7 инцидентна x_1 , то в графе H можно построить паросочетание из ребер $\{x_1, x_7\}, \{x_5, x_3\}, \{x_2, x_6\}$, что ведет к противоречию. Следовательно,

$$\|f\| < w_n. \quad \square$$

Справедливость теоремы 2 следует из лемм 1–6. Объединяя результаты работы [5] и доказанных выше теорем 1, 2, получаем следующие свойства весов бионктивных функций $f(x_1, \dots, x_n), n \geq 7$, существенно зависящих от всех переменных.

1. Функций с весом t , $t > 2^{n-1} + 1$, не существует.
2. Функции из класса R_n (и только они) имеют вес $t = 2^{n-1} + 1$.
3. Функций с весом t при $3 \cdot 2^{n-3} + 3 < t < 2^{n-1} + 1$ не существует.
4. Функции из класса W_n (и только они) имеют вес $t = 3 \cdot 2^{n-3} + 3$.
5. Для любого $t \in \{1, \dots, 2^{\lfloor n/2 \rfloor}\}$ существуют функции с весом t .

Таким образом, пока нет полной ясности относительно функций с весом в диапазоне $2^{\lfloor n/2 \rfloor} < t < 3 \cdot 2^{n-3} + 3$, хотя некоторые результаты в этой области можно сформулировать.

Функция

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^{n-2} (x_1 \vee x_{i+1}) \wedge (x_2 \vee x_n)$$

имеет вес $\|f\| = \|f(x_1=1)\| + \|f(x_1=0)\| = 3 \cdot 2^{n-3} + 2$, а функция

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \wedge (x_2 \vee x_n)$$

имеет вес $\|f\| = \|f(x_1=1)\| + \|f(x_1=0)\| = 3 \cdot 2^{n-3} + 1$. Функции вида

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^{n-k-1} (x_1 \vee x_{i+1}) \wedge \bigwedge_{j=1}^{k-1} (x_{n-k+1} \vee x_{j+n-k+1})$$

имеют вес $\|f\| = (2^{n-k-1} + 1) \cdot (2^{k-1} + 1) = 2^{n-2} + 2^{n-k-1} + 2^{k-1} + 1$, функции вида

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^{n-2k-1} (x_1 \vee x_{i+1}) \wedge \bigwedge_{j=1}^k (x_{n-2k+2j-1} \vee x_{n-2k+2j})$$

имеют вес $\|f\| = (2^{n-2k-1} + 1) \cdot 3^k$.

Гипотеза. Для любых натуральных $n \geq 5$ и t , $1 \leq t \leq 3 \cdot 2^{n-3}$, можно построить бионктивную функцию $f(x_1, \dots, x_n)$, существенно зависящую от всех переменных и имеющую вес, равный t .

2. О функциях максимального веса, представимых в виде 3-КНФ

Как уже отмечалось, среди биюнктивных функций $f(x_1, \dots, x_n)$, существенно зависящих от всех переменных, максимальный вес, равный $\|f\| = 2^{n-1} + 1$, имеют функции из класса R_n . В этом разделе изучаются функции максимального веса из множества $(3)\text{-КНФ} \cap F'_n$.

Рассмотрим k -юнктивную функцию вида

$$f(x_1, \dots, x_n) \equiv \bigwedge_{i=1}^{n-k+1} (x_1 \vee \dots \vee x_{k-1} \vee x_{k-1+i}), \quad (10)$$

где $n \geq k$. Ясно, что функция (15) монотонна и существенно зависит от n переменных. При $k=2$ функция (15) принадлежит классу эквивалентности R_n .

Свойство 8. Функция (15) имеет вес

$$\|f\| = 2^n - 2^{n-k+1} + 1. \quad (11)$$

Доказательство. По свойству 2

$$\|f\| = \sum_{(\alpha_1, \dots, \alpha_{k-1}) \in V_{k-1}} \|f(x_1 = \alpha_1, \dots, x_{k-1} = \alpha_{k-1})\|. \quad (12)$$

При этом $\|f(x_1=0, \dots, x_{k-1}=0)\| = 1$, а если $(\alpha_1, \dots, \alpha_{k-1}) \neq 0_{k-1}$, то $\|f(x_1=\alpha_1, \dots, x_{k-1}=\alpha_{k-1})\| = 2^{n-k+1}$. Поэтому

$$\|f\| = (2^{k-1} - 1) \cdot 2^{n-k+1} + 1 = 2^n - 2^{n-k+1} + 1. \quad \square$$

Следствие 1. При $k=3$ функция (15) имеет вес

$$\|f\| = 0,75 \cdot 2^n + 1. \quad (13)$$

Обозначим

$$m_n(k) = \max_{f \in ((k)\text{-КНФ}) \cap F'_n} \|f\|.$$

При этом $m_n(2) = 0,5 \cdot 2^n + 1$.

Теорема 3. Для любого $n \geq 7$ выполняется соотношение

$$m_n(3) = 0,75 \cdot 2^n + 1. \quad (14)$$

Это значение достигается только на функциях

$$f(x_1, \dots, x_n) \in \left[\bigwedge_{i=1}^{n-2} (x_1 \vee x_2 \vee x_{2+i}) \right]_{\langle Q_n \rangle}. \quad (15)$$

Доказательство разобьем на несколько лемм.

Лемма 7. Пусть $f(x_1, \dots, x_n) \in (3)\text{-КНФ}$ и существует такая 3-КНФ этой функции, что в нее некоторая переменная входит в разных степенях. Тогда

$$\|f\| \leq 0,75 \cdot 2^n. \quad (16)$$

Доказательство. Если функция f имеет имплиценту вида x_i^α , то $\|f\| \leq 0,5 \cdot 2^n$. Если f имеет имплиценту $(x_i^\alpha \vee x_j^\beta)$, то $\|f\| \leq 0,75 \cdot 2^n$. Далее считаем, что все элементарные имплиценты функции f содержат 3 литерала. Без ограничения общности можно считать, что функция f имеет имплиценту

$$(x_1 \vee x_2 \vee x_3)(\bar{x}_1 \vee x_i^\alpha \vee x_j^\beta).$$

Тогда

$$\|f\| = \|f(x_1=0)\| + \|f(x_1=1)\| \leq 3 \cdot 2^{n-3} + 3 \cdot 2^{n-3} = 0,75 \cdot 2^n.$$

Лемма доказана. $\square$

В дальнейшем для нахождения функций с максимальным весом можно ограничиться рассмотрением только монотонных функций.

Лемма 8. Пусть $f(x_1, \dots, x_n) \in (3)\text{-КНФ} \cap M$, функция f имеет имплиценту

$$(x_1 \vee x_2 \vee x_3)(x_4 \vee x_5 \vee x_6)(x_7 \vee x_i \vee x_j). \quad (17)$$

Тогда верно (6).

Доказательство. Предположим, что $\{i, j\} \cap \{1, \dots, 6\} = \emptyset$, тогда

$$\|f\| \leq 7^3 \cdot 2^{n-9} = \frac{7^3}{2^9} \cdot 2^n < 0,67 \cdot 2^n$$

и справедливо (6). Пусть $|\{i, j\} \cap \{1, \dots, 6\}| = 1$, тогда без ограничения общности можно считать, что имплицента (18) имеет вид

$$(x_1 \vee x_2 \vee x_3)(x_4 \vee x_5 \vee x_6)(x_7 \vee x_8 \vee x_1)$$

и поэтому

$$\|f\| = \|f(x_1=0)\| + \|f(x_1=1)\| \leq 3 \cdot 7 \cdot 3 \cdot 2^{n-8} + 7 \cdot 2^{n-4} < 0,69 \cdot 2^n.$$

Наконец, предположим, что $|\{i, j\} \cap \{1, \dots, 6\}| = 2$, тогда без ограничения общности можно считать, что имплицента (18) имеет вид

$$(x_1 \vee x_2 \vee x_3)(x_4 \vee x_5 \vee x_6)(x_7 \vee x_1 \vee x_2) \quad (18)$$

или вид

$$(x_1 \vee x_2 \vee x_3)(x_4 \vee x_5 \vee x_6)(x_7 \vee x_1 \vee x_4). \quad (19)$$

В случае (21)

$$\|f\| = \|f(x_1=0)\| + \|f(x_1=1)\| \leq 5 \cdot 7 \cdot 2^{n-7} + 7 \cdot 2^{n-4} < 0,72 \cdot 2^n,$$

а в случае (22)

$$\begin{aligned} \|f\| &= \|f(x_1=0, x_4=0)\| + \|f(x_1=0, x_4=1)\| + \\ &+ \|f(x_1=1, x_4=0)\| + \|f(x_1=1, x_4=1)\| \leq \\ &\leq 3 \cdot 3 \cdot 2^{n-7} + 3 \cdot 2^{n-4} + 3 \cdot 2^{n-4} + 2^{n-2} < 0,7 \cdot 2^n. \end{aligned}$$

Лемма доказана. $\square$

Замечание 2. Если функция $f(x_1, \dots, x_n)$ имеет имплиценту

$$(x_1 \vee x_2 \vee x_3)(x_4 \vee x_5 \vee x_6) \quad (20)$$

и во все остальные имплиценты входят только переменные из множества $\{x_1, \dots, x_6\}$, то функция f существенно зависит не более чем от 6 переменных.

Далее считаем, что $f(x_1, \dots, x_n) \in (3)\text{-КНФ} \cap M$, функция f существенно зависит не менее чем от 7 переменных и не имеет имплицент вида (23).

Замечание 3. Далее считаем, что функция f имеет имплиценту $x_1 \vee x_2 \vee x_3$. Поскольку f не имеет имплицент вида (23), в каждую элементарную имплиценту функции f входит хотя бы одна из переменных $\{x_1, x_2, x_3\}$.

Лемма 9. Пусть функция f , существенно зависящая не менее чем от 7 переменных, имеет имплиценту

$$(x_1 \vee x_2 \vee x_3)(x_1 \vee x_4 \vee x_5)$$

и выполняются условия замечания 3. Тогда справедлива оценка (6).

Доказательство. В рассматриваемых условиях без ограничения общности можно считать, что функция f имеет одну из следующих имплицентов:

$$(x_1 \vee x_2 \vee x_3)(x_1 \vee x_4 \vee x_5)(x_1 \vee x_6 \vee x_i), \quad (21)$$

$$(x_1 \vee x_2 \vee x_3)(x_1 \vee x_4 \vee x_5)(x_2 \vee x_6 \vee x_i). \quad (22)$$

Пусть f имеет имплиценту (20) и $i = 7$, тогда

$$\|f\| = \|f(x_1=0)\| + \|f(x_1=1)\| \leq 3 \cdot 3 \cdot 3 \cdot 2^{n-7} + 2^{n-1} < 0,72 \cdot 2^n.$$

Далее без ограничения общности в случае (20) можно считать, что $i \in \{2, 4\}$. Предположим, что $i = 2$, тогда (20) примет вид

$$(x_1 \vee x_2 \vee x_3)(x_1 \vee x_4 \vee x_5)(x_1 \vee x_6 \vee x_2),$$

а для веса функции f имеем

$$\begin{aligned} \|f\| &= \|f(x_1=0, x_2=0)\| + \|f(x_1=0, x_2=1)\| + \|f(x_1=1)\| \leq \\ &\leq 3 \cdot 2^{n-6} + 3 \cdot 2^{n-4} + 2^{n-1} < 0,74 \cdot 2^n. \end{aligned}$$

Если $i = 4$, то

$$\begin{aligned} &(x_1 \vee x_2 \vee x_3)(x_1 \vee x_4 \vee x_5)(x_1 \vee x_6 \vee x_4) \in \\ &\in \left[(x_1 \vee x_2 \vee x_3)(x_1 \vee x_4 \vee x_5)(x_1 \vee x_6 \vee x_2) \right]_{\langle Q_6 \rangle}. \end{aligned}$$

Этот случай рассмотрен выше.

Перейдем к рассмотрению случая (24). Если $i = 7$, то

$$\begin{aligned} \|f\| &= \|f(x_1=0, x_2=0)\| + \|f(x_1=0, x_2=1)\| + \\ &+ \|f(x_1=1, x_2=0)\| + \|f(x_1=1, x_2=1)\| \leq \\ &\leq 3 \cdot 3 \cdot 2^{n-7} + 3 \cdot 2^{n-4} + 3 \cdot 2^{n-4} + 2^{n-2} < 0,7 \cdot 2^n. \end{aligned}$$

Вариант $i = 1$ изучен при рассмотрении (20). Осталось рассмотреть два варианта $i \in \{3, 4\}$. Аналогично показывается, что и в этих случаях выполняется (6). Лемма доказана. $\square$

Рассмотрим последний случай, когда

$$f(x_1, \dots, x_n) \equiv (x_1 \vee x_2 \vee x_3) \wedge \bigwedge_{i=1}^t (x_{i_1} \vee x_{i_2} \vee x_{i_3}),$$

где $|\{1, 2, 3\} \cap \{i_1, i_2, i_3\}| = 2$, $i = 1, \dots, t$. Тогда функцию f можно представить в виде

$$f \equiv (x_1 \vee x_2 \vee x_3) \wedge \bigwedge_{i=1}^{t_1} (x_1 \vee x_2 \vee x_{r_i}) \wedge \bigwedge_{j=1}^{t_2} (x_1 \vee x_3 \vee x_{u_j}) \wedge \bigwedge_{l=1}^{t_3} (x_2 \vee x_3 \vee x_{w_l}). \quad (23)$$

Лемма доказана. $\square$

Лемма 10. Пусть функция f имеет вид (25) и существенно зависит не менее чем от 7 переменных. Тогда $\|f\| = 0,75 \cdot 2^n + 1$, если и только если функция f принадлежит классу (5), в противном случае $\|f\| < 0,72 \cdot 2^n$.

Доказательство. Пусть функция f не принадлежит классу (5), тогда без ограничения общности можно считать, что функция f имеет одну из двух имплицентов

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_1 \vee x_2 \vee x_5) \wedge (x_1 \vee x_3 \vee x_6) \quad (24)$$

или

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (x_1 \vee x_3 \vee x_5) \wedge (x_2 \vee x_3 \vee x_6). \quad (25)$$

В случае (24)

$$\begin{aligned} \|f\| &= \|f(x_1=0, x_2=0)\| + \|f(x_1=0, x_2=1)\| + \|f(x_1=1)\| \leq \\ &\leq 2^{n-5} + 3 \cdot 2^{n-4} + 2^{n-1} < 0,72 \cdot 2^n. \end{aligned}$$

В случае (25)

$$\begin{aligned} \|f\| &= \|f(x_1=0, x_2=0)\| + \|f(x_1=0, x_2=1)\| + \\ &+ \|f(x_1=1, x_2=0)\| + \|f(x_1=1, x_2=1)\| \leq \\ &\leq 2^{n-4} + 3 \cdot 2^{n-4} + 3 \cdot 2^{n-4} + 2^{n-2} < 0,69 \cdot 2^n. \end{aligned}$$

Доказательство леммы, а вместе с ним и доказательство теоремы 3 завершены. $\square$

Гипотеза. Для всякого $k \geq 4$ существует такое натуральное t_k , что $m_n(k) = 2^n - 2^{n-k+1} + 1$ при $n \geq t_k$, причем это значение достигается только для функций

$$f(x_1, \dots, x_n) \in \left[\bigwedge_{i=1}^{n-k+1} (x_1 \vee \dots \vee x_{k-1} \vee x_{k-1+i}) \right]_{\langle Q_n \rangle}.$$

Результаты работы [5] и доказанная выше теорема 3 свидетельствуют о том, что данная гипотеза верна при $k = 2$ и $k = 3$.

3. О равновероятных k -ъюнктивных булевых функциях

Равновероятные булевы функции имеют важные приложения в прикладных задачах, поэтому представляет интерес исследование возможности представления равновероятных функций в виде k -КНФ. Всякая функция $f(x_1, \dots, x_n)$ представима в виде n -КНФ, этой записью является совершенная конъюнктивная нормальная форма. Равновероятных биъюнктивных функций, существенно зависящих от $n \geq 5$ переменных, не существует [5]. Приведем некоторые результаты в рассматриваемой области для случая $2 \leq k \leq n-1$.

Теорема 4. Для любого $n \in N$ существуют равновероятные функции $f \in F'_n$, представимые в виде $\lceil \frac{n+1}{2} \rceil$ -КНФ.

Доказательство. Для $n = 1$ это функция x_1 , а для $n = 2$ — любая функция $f \in F'_2$.

Пусть $n \geq 3$, n — нечетное. Тогда функция

$$f(x_1, \dots, x_n) = \bigwedge_{1 \leq i_1 < \dots < i_{(n+1)/2} \leq n} (x_{i_1} \vee \dots \vee x_{i_{(n+1)/2}}) \quad (26)$$

обладает следующими свойствами:

- 1) принадлежит множеству $\left(\frac{n+1}{2}\right)$ -КНФ,
- 2) существенно зависит от всех переменных,
- 3) является равновероятной.

Запись (26) является сокращенной КНФ, поэтому функция f существенно зависит от всех переменных. Также нетрудно видеть, что $f(\alpha) = 0, \alpha \in V_n$, если и только если $\|\alpha\| \leq (n-1)/2$, поэтому $\|f\| = 2^{n-1}$.

Пусть n — четное. Тогда функция

$$f(x_1, \dots, x_n) = \bigwedge_{1 \leq i_1 < \dots < i_{n/2+1} \leq n} (x_{i_1} \vee \dots \vee x_{i_{n/2+1}}) \wedge \bigwedge_{2 \leq j_1 < \dots < j_{n/2-1} \leq n} (x_{j_1} \vee \dots \vee x_{j_{n/2-1}}) \quad (27)$$

обладает следующими свойствами:

- 1) принадлежит множеству $(\frac{n}{2} + 1)$ -КНФ,
- 2) существенно зависит от всех переменных,
- 3) является равновероятной.

Функцию f можно представить в виде

$$f(x_1, \dots, x_n) = \bigwedge_{2 \leq i_1 < \dots < i_{n/2+1} \leq n} (x_{i_1} \vee \dots \vee x_{i_{n/2+1}}) \wedge \bigwedge_{2 \leq j_1 < \dots < j_{n/2-1} \leq n} (x_{j_1} \vee \dots \vee x_{j_{n/2-1}}). \quad (28)$$

Все элементарные имплиценты записи (28) являются простыми, поэтому функция f существенно зависит от всех переменных. Покажем, что функция f является равновероятной. Пусть n — четное число и

$V_n^{(n/2)'} — множество векторов из $V_n^{(n/2)}$ с нулевой первой координатой,$

$V_n^{(n/2)''} — множество векторов из $V_n^{(n/2)}$ с единичной первой координатой.$

Установим соответствие между множествами $V_n^{(n/2)'}$ и $V_n^{(n/2)''}$ по правилу $(\alpha_1, \dots, \alpha_n) \leftrightarrow (\bar{\alpha}_1, \dots, \bar{\alpha}_n)$, где $(\alpha_1, \dots, \alpha_n) \in V_n$. Легко видеть, что при четном n указанное соответствие является взаимно однозначным, откуда следует справедливость соотношений

$$|V_n^{(n/2)'}| = |V_n^{(n/2)''}| = \frac{1}{2} \cdot \binom{n}{n/2}. \quad (29)$$

Функция f принимает значение 0 только на векторах из слоев $V_n^{(i)}$, $i = 0, \dots, n/2 - 1$, и на векторах из множества $V_n^{(n/2)'}$.

Учитывая (29), находим, что функция f является равновероятной. $\square$

Список литературы

- [1] Schaefer T., “Complexity of satisfiability problems”. In: “*Proc. 10 Annu. ACM Symp. Theory of Computing Machinery*”, 1978, 216–226.
- [2] Горшков С. П., Тарасов А. В., *Сложность решения систем булевых уравнений*, М.: Курс, 2017, 192 с.
- [3] Monien B., Speckenmeyer E., “Solving satisfiability in less than 2^n steps”, *Discr. Appl. Math.*, № 10 (1985), 287–295.
- [4] Данцин Е. Я., “Алгоритмика задачи выполнимости”, *Вопросы кибернетики (Проблема сокращения перебора)*, № 131 (1987), 7–29.
- [5] Тарасов А. В., “О свойствах функций, представимых в виде 2-КНФ”, *Дискретная математика*, 13:4 (2001), 99–115.
- [6] Гэри М., Джонсон Д., *Вычислительные машины и труднорешаемые задачи*, М.: Мир, 1982, 416 с.
- [7] Сачков В. Н., *Курс комбинаторного анализа*, М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.