Math-Net.Ru

Общероссийский математический портал

А. В. Тарасов, О методах оценивания веса булевых биюнктивных функций, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 4, 125–142

DOI: <https://doi.org/10.4213/mvk273>

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: 34.229.45.116

26 апреля 2023 г., 16:23:33

**Два метода оценивания
веса булевых биюнктивных функций**

А. В. Тарасов

ООО «Центр сертификационных исследований», Москва

Получено 18.IV.2018

Аннотация. Задача определения веса функции, представимой в виде 2-КНФ (т. е. биюнктивной функции), в общем случае входит в класс труднорешаемых задач перечисления. Однако существуют методы получения верхних и нижних оценок веса таких функций. В работе рассматриваются два метода получения таких оценок: метод включения-исключения и метод, использующий порядковую функцию графа 2-КНФ, представляющей собой биюнктивную функцию. На основе предложенных методов построен ряд полиномиально вычислимых оценок веса биюнктивных функций.

Ключевые слова: булева функция, биюнктивная функция, 2-КНФ, метод включения-исключения, порядковая функция графа

Two methods of estimation of Boolean bijunctive function weights

A. V. Tarasov

Certification Research Center, LLC, Moscow

Abstract. A problem of computation of the weight of function representable as 2-CNF (i. e. bijunctive function) belongs to the class of hard enumeration problems. Nevertheless there exist methods of upper and lower estimation of the weight of such functions. We consider two methods of estimation the weights: inclusion-exclusion method and method using the monotone function on graph corresponding to the 2-CNF representing the bijunctive function. By means of these methods several polynomially computable estimates of the bijunctive functions weights are constructed.

Key words: Boolean function, bijunctive function, 2-CNF, inclusion-exclusion method, monotone function on graph

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 4, pp. 125–142 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Постановка задачи

Пусть V_n — множество двоичных векторов размерности n . Для булевой функции f от n переменных обозначим через E_f множество ее выполняющих векторов (носитель функции f). Булева функция $f(x_1, \dots, x_n)$ называется *бионктивной*, если ее можно представить в виде

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^t (x_{s_{i,1}}^{a_{i,1}} \vee x_{s_{i,2}}^{a_{i,2}}). \quad (1)$$

Такие функции изучались, в частности, в работах [1–6]. Одной из важных задач исследования булевых функций является задача определения веса, т. е. мощности множества выполняющих векторов. В случае бионктивной функции вида (1) данная задача эквивалентна известной задаче определения числа решений системы уравнений

$$\left\{ x_{s_{i,1}}^{a_{i,1}} \vee x_{s_{i,2}}^{a_{i,2}} = 1, \quad i = \overline{1, t}. \right.$$

Последняя задача является частным случаем известной задачи $\#SAT$ и носит название $\#2-SAT$ (см. [4]). В [3] показано, что данная задача в общем случае относится к классу труднорешаемых задач перечисления, а именно является $\#P$ -полной. При этом она полиномиальна, если каждая переменная в КНФ (1) встречается не более двух раз, а также в некоторых других случаях (см., например, [2]). Данной проблеме посвящен ряд работ. Свойства весов бионктивных функций изучались в [2] и [6], а в [4] получена оценка сложности алгоритма нахождения веса бионктивной функции порядка $O(1.2561^n)$. Данный результат показывает, что при определении веса функции вида (1) в настоящее время необходимо использовать переборный алгоритм. Вместе с тем существует возможность получения относительно нетривиальных верхних и нижних оценок веса $\|f\|$ с помощью достаточно эффективных алгоритмов. Нашей целью является разработка методов получения эффективно вычисляемых оценок величины $\|f(x_1, \dots, x_n)\|$ при задании функции формулой вида (1).

Заметим, что задание вида (1), вообще говоря, неоднозначно. Методы описания всех 2-КНФ, задающих одну и ту же функцию, приведены, например, в [2]. Будем считать, что КНФ в правой части (1) — минимальная (такую можно построить с полиномиальной сложностью [2]).

Из формулы (1) следует очевидное соотношение для носителя функции f :

$$E_f = \bigcap_{i=1}^t E_{x_{s_{i,1}}^{a_{i,1}} \vee x_{s_{i,2}}^{a_{i,2}}}. \quad (2)$$

Множества $E_{x_{s_{i,1}}^{a_{i,1}} \vee x_{s_{i,2}}^{a_{i,2}}}$ суть дополнения многообразий пространства V_n , являющихся носителями функций $x_{s_{i,1}}^{a_{i,1} \oplus 1} x_{s_{i,2}}^{a_{i,2} \oplus 1}$. Положим $V(i, j, a, b) = E_{x_i^a x_j^b}$. Тогда (2) можно переписать в виде

$$\overline{E_f} = \bigcup_{i=1}^t V(s_{i,1}, s_{i,2}, a_{i,1} \oplus 1, a_{i,2} \oplus 1). \quad (3)$$

В этом случае для вычисления мощности $|\overline{E_f}| = 2^n - \|f\|$ можно воспользоваться формулой включения-исключения ([7]):

$$\begin{aligned} |\overline{E_f}| &= \sum_{i=1}^t |V(s_{i,1}, s_{i,2}, a_{i,1} \oplus 1, a_{i,2} \oplus 1)| - \\ &\quad - \sum_{1 \leq i_1 < i_2 \leq t} |V(s_{i_1,1}, s_{i_1,2}, a_{i_1,1} \oplus 1, a_{i_1,2} \oplus 1) \cap \\ &\quad \cap V(s_{i_2,1}, s_{i_2,2}, a_{i_2,1} \oplus 1, a_{i_2,2} \oplus 1)| + \dots, \end{aligned}$$

откуда

$$\begin{aligned} \|f\| &= 2^n - \sum_{i=1}^t |V(s_{i,1}, s_{i,2}, a_{i,1} \oplus 1, a_{i,2} \oplus 1)| + \\ &\quad + \sum_{1 \leq i_1 < i_2 \leq t} |V(s_{i_1,1}, s_{i_1,2}, a_{i_1,1} \oplus 1, a_{i_1,2} \oplus 1) \cap \\ &\quad \cap V(s_{i_2,1}, s_{i_2,2}, a_{i_2,1} \oplus 1, a_{i_2,2} \oplus 1)| + \dots + \\ &\quad + (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq t} |V(s_{i_1,1}, s_{i_1,2}, a_{i_1,1} \oplus 1, a_{i_1,2} \oplus 1) \cap \dots \cap \\ &\quad \cap V(s_{i_k,1}, s_{i_k,2}, a_{i_k,1} \oplus 1, a_{i_k,2} \oplus 1)| + \dots + \\ &\quad + (-1)^t |V(s_{1,1}, s_{1,2}, a_{1,1} \oplus 1, a_{1,2} \oplus 1) \cap \dots \cap \\ &\quad \cap V(s_{t,1}, s_{t,2}, a_{t,1} \oplus 1, a_{t,2} \oplus 1)|. \end{aligned} \quad (4)$$

Заметим, что в формуле (4)

$$|V(s_{i,1}, s_{i,2}, a_{i,1} \oplus 1, a_{i,2} \oplus 1)| = 2^{n-2},$$

а для произвольных $k \in \{2, 3, \dots, t\}$ и $1 \leq i_1 < \dots < i_k \leq t$

$$\begin{aligned} &|V(s_{i_1,1}, s_{i_1,2}, a_{i_1,1} \oplus 1, a_{i_1,2} \oplus 1) \cap \dots \cap V(s_{i_k,1}, s_{i_k,2}, a_{i_k,1} \oplus 1, a_{i_k,2} \oplus 1)| = \\ &= \|x_{s_{i_1,1}}^{a_{i_1,1}} x_{s_{i_1,2}}^{a_{i_1,2}} \dots x_{s_{i_k,2}}^{a_{i_k,2}}\|. \end{aligned} \quad (5)$$

Для продолжения рассуждений введем граф для 2-КНФ из правой части (1), следуя, например, [5]. Пусть $X = \{x_1, \dots, x_n\}$, $\bar{X} = \{\bar{x}_1, \dots, \bar{x}_n\}$ и $G = (VG, EG)$ — орграф, в котором

$$VG = X \cup \bar{X}, \quad EG = \{(x_{s_{i,1}}^{a_{i,1} \oplus 1}, x_{s_{i,2}}^{a_{i,2}}), (x_{s_{i,2}}^{a_{i,2} \oplus 1}, x_{s_{i,1}}^{a_{i,1}}), i = 1, 2, \dots, t\}. \quad (6)$$

Пересечению из левой части (5) можно поставить в соответствие набор из $2k$ дуг графа G :

$$M = \{(x_{s_{i_1,1}}^{a_{i_1,1} \oplus 1}, x_{s_{i_1,2}}^{a_{i_1,2}}), (x_{s_{i_1,2}}^{a_{i_1,2} \oplus 1}, x_{s_{i_1,1}}^{a_{i_1,1}}), \dots, (x_{s_{i_k,1}}^{a_{i_k,1} \oplus 1}, x_{s_{i_k,2}}^{a_{i_k,2}}), (x_{s_{i_k,2}}^{a_{i_k,2} \oplus 1}, x_{s_{i_k,1}}^{a_{i_k,1}})\}. \quad (7)$$

Верно следующее утверждение.

Утверждение 1. Для произвольных $k \in \{2, 3, \dots, t\}$, $1 \leq i_1 < \dots < i_k \leq t$ пересечение из левой части (5) непусто тогда и только тогда, когда набор дуг M , определенный в (7), не содержит ориентированных цепей длины больше 1.

Доказательство утверждения очевидным образом следует из формулы (5), определения (6) графа G и того, что конъюнкция $x_{s_{i_1,1}}^{a_{i_1,1} \oplus 1} x_{s_{i_1,2}}^{a_{i_1,2}} \dots x_{s_{i_k,2}}^{a_{i_k,2}}$ обращается в тождественный 0 тогда и только тогда, когда она содержит некоторое переменное вместе со своим отрицанием.

2. Оценки веса монотонной биюнктивной функции

Пусть функция f монотонна. Тогда она представляется в виде

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^t (x_{s_{i,1}} \vee x_{s_{i,2}}). \quad (8)$$

Дополнительно считаем, что КНФ в правой части (8) — минимальная и содержит все переменные $x_1, \dots, x_n$. Многообразия $V(s_{i,1}, s_{i,2}, a_{i,1} \oplus 1, a_{i,2} \oplus 1)$ в этом случае имеют вид $V(s_{i,1}, s_{i,2}, 0, 0)$ и в формуле включения-исключения (4) все пересечения будут непустыми. Рассмотрим вопрос об оценивании веса $\|f\|$ по формуле (4) с помощью неравенств Бонферрони.

По КНФ (8) построим неориентированный граф $H = (VH, EH)$, в котором $VH = \{x_1, \dots, x_n\}$, $EH = \{e_1 = \{x_{s_{1,1}}, x_{s_{1,2}}\}, \dots, e_t = \{x_{s_{t,1}}, x_{s_{t,2}}\}\}$. Тогда задача подсчета веса функции $f(x_1, \dots, x_n)$ превращается в задачу подсчета числа всех вершинных покрытий графа H . В частности, если α — число вершинного покрытия графа H , то очевидно, что

$$\|f\| \geq 2^{n-\alpha}.$$

Введем следующий параметр: для произвольного множества ребер $E' = \{e_{i_1}, \dots, e_{i_k}\}$ обозначим через $N(e_{i_1}, \dots, e_{i_k})$ число вершин в подграфе графа H , порожденном множеством ребер E' .

Теорема 1. Для веса функции $f(x_1, \dots, x_n)$, заданной равенством (8), справедлива формула

$$\|f\| = 2^n \left[\sum_{k=0}^t (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq t} 2^{-N(e_{i_1}, \dots, e_{i_k})} \right]. \quad (9)$$

Доказательство. Для доказательства воспользуемся формулой включения-исключения и равенством (5). Поскольку функция f монотонна, то для любого $l = 1, 2, \dots, t$

$$a_{l,1} = a_{l,2} = 1,$$

откуда, в силу (5), для произвольных $k \in \{2, 3, \dots, t\}$ и $1 \leq i_1 < \dots < i_k \leq t$

$$\begin{aligned} & |V(s_{i_1,1}, s_{i_1,2}, a_{i_1,1} \oplus 1, a_{i_1,2} \oplus 1) \cap \dots \cap V(s_{i_k,1}, s_{i_k,2}, a_{i_k,1} \oplus 1, a_{i_k,2} \oplus 1)| = \\ & = \|x_{s_{i_1,1}} x_{s_{i_1,2}} \dots x_{s_{i_k,2}}\|. \end{aligned}$$

При этом набор вершин $x_{s_{i_1,1}}, x_{s_{i_1,2}}, \dots, x_{s_{i_k,2}}$ состоит из всех вершин графа H , инцидентных ребрам $e_{i_1}, \dots, e_{i_k}$. Их число — $N(e_{i_1}, \dots, e_{i_k})$. Поэтому

$$\|x_{s_{i_1,1}} x_{s_{i_1,2}} \dots x_{s_{i_k,2}}\| = 2^{n-N(e_{i_1}, \dots, e_{i_k})},$$

откуда и следует (9).

После применения к (9) неравенств Бонферрони ([7]) получаем следующее следствие из теоремы.

Следствие 1. В условиях теоремы 1 для любого нечетного $m \leq t-1$ верны неравенства

$$\begin{aligned} & 2^n \left[\sum_{k=0}^m (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq t} 2^{-N(e_{i_1}, \dots, e_{i_k})} \right] \leq \\ & \leq \|f\| \leq 2^n \left[\sum_{k=0}^{m+1} (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq t} 2^{-N(e_{i_1}, \dots, e_{i_k})} \right]. \end{aligned} \quad (10)$$

Таким образом, частичные суммы (9) с четным числом слагаемых дают нижнюю оценку, а с нечетным — верхнюю. Для нахождения оценок необходимо знать величины $N(e_{i_1}, \dots, e_{i_k})$. В частности, для чисел $N(e_{i_1}, \dots, e_{i_k})$ верны очевидные соотношения

$$N(e_i) = 2, \quad 3 \leq N(e_{i_1}, e_{i_2}) \leq 4, \quad 2\lceil\sqrt{k}\rceil \leq N(e_{i_1}, \dots, e_{i_k}) \leq 2k. \quad (11)$$

Поэтому из неравенств (10) можно получить следующие грубые оценки.

Следствие 2. В условиях теоремы 1 для любого нечетного $m \leq t-1$ верны неравенства

$$\begin{aligned} 2^n \left[\sum_{k=0, k \text{ четно}}^m \binom{t}{k} 2^{-2k} - \sum_{k=0, k \text{ нечетно}}^m \binom{t}{k} 2^{-2\sqrt{k}} \right] &\leq \\ &\leq \|f\| \leq 2^n \left[\sum_{k=0, k \text{ четно}}^m \binom{t}{k} 2^{-2\sqrt{k}} - \sum_{k=0, k \text{ нечетно}}^m \binom{t}{k} 2^{-2k} \right]. \end{aligned} \quad (12)$$

Представим формулу (9) в следующем виде:

$$\|f\| = 2^n \sum_{k=0}^t (-1)^k L_k, \quad (13)$$

где

$$L_k = \sum_{1 \leq i_1 < \dots < i_k \leq t} 2^{-N(e_{i_1}, \dots, e_{i_k})}. \quad (14)$$

Для получения оценок по формуле (13) необходимо вычислять значения величин L_k . Эти величины по сути представляют собой вероятности события, состоящего в том, что случайный двоичный вектор с равномерным распределением не лежит ни в одном из множеств

$$V(s_{k,1}, s_{k,2}, 0, 0), \quad k = 1, 2, \dots, t.$$

Для такой модели в дальнейшем удобно пользоваться результатами работы [9].

Обозначим через A_i , $i = 1, 2, \dots, t$, событие, состоящее в том, что случайный вектор $\alpha \in V_n$, имеющий равномерное распределение на V_n , лежит в множестве $V(s_{i,1}, s_{i,2}, 0, 0)$, $i = 1, 2, \dots, t$; тогда $\mathbf{P}\{A_i\} = 1/4$. Через η обозначим случайную величину, равную числу одновременно происходящих событий $A_1, \dots, A_t$.

Тогда очевидно, что

$$\|f\| = 2^n \mathbf{P}\{\eta = 0\},$$

и при $k = 0, 1, 2, \dots, t$

$$\mathbf{P}\{A_{i_1}, \dots, A_{i_k}\} = 2^{-N(e_{i_1}, \dots, e_{i_k})},$$

$$L_k = \sum_{1 \leq i_1 < \dots < i_k \leq t} 2^{-N(e_{i_1}, \dots, e_{i_k})} = \sum_{1 \leq i_1 < \dots < i_k \leq t} \mathbf{P}\{A_{i_1}, \dots, A_{i_k}\}.$$

В этом случае величины L_k представляют собой факториальные моменты случайной величины η , т. е.

$$\begin{aligned} L_k &= \mathbf{E}(\eta_{[k]}) = \mathbf{E}(\eta(\eta - 1) \cdots (\eta - k + 1)) = \\ &= \sum_{j=k}^t A_k^j \mathbf{P}\{\eta = j\}. \end{aligned}$$

Найдем значения величин L_k при малых k . Ясно, что

$$L_0 = 1, \quad L_1 = \frac{t}{4}.$$

Пусть $I\{x_j \in H(e_{i_1}, \dots, e_{i_k})\}$ — индикатор события, состоящего в том, что вершина x_j лежит в подграфе графа H , порожденном ребрами $e_{i_1}, \dots, e_{i_k}$. Степень вершины x_j обозначим через d_j , $j = 1, 2, \dots, n$.

Утверждение 2. Верно равенство

$$L_2 = \frac{1}{16} \left(\binom{t}{2} + \sum_{j=1}^n \binom{d_j}{2} \right). \quad (15)$$

Доказательство. Из (14) следует, что

$$L_2 = \sum_{1 \leq i_1 < i_2 \leq t} 2^{-N(e_{i_1}, e_{i_2})},$$

т. е.

$$L_2 = \sum_{1 \leq i_1 < i_2 \leq t} 2^{-\sum_{j=1}^n I(x_j \in H(e_{i_1}, e_{i_2}))}.$$

Теперь заметим, что

$$N(e_{i_1}, e_{i_2}) = \begin{cases} 3, & \text{если ребра } e_{i_1}, e_{i_2} \text{ смежны,} \\ 4, & \text{если ребра } e_{i_1}, e_{i_2} \text{ не смежны.} \end{cases}$$

Тогда

$$L_2 = \frac{1}{8} \sum_{e_{i_1}, e_{i_2} \text{ смежны}} 1 + \frac{1}{16} \sum_{e_{i_1}, e_{i_2} \text{ не смежны}} 1 = \frac{1}{8} l_2^{(1)} + \frac{1}{16} l_2^{(2)}.$$

Очевидно, что если два ребра инцидентны одной вершине, то для каждой вершины x графа H можно выбрать $\binom{\deg x}{2}$ пар смежных ребер. Поэтому

$$l_2^{(1)} = \sum_{j=1}^n \binom{d_j}{2}.$$

Поскольку в графе H всего $\binom{t}{2}$ неупорядоченных пар ребер, то пары, не учтенные в сумме $l_2^{(1)}$, попадают сумму $l_2^{(2)}$, поэтому

$$L_2 = \frac{1}{8} \sum_{j=1}^n \binom{d_j}{2} + \frac{1}{16} \left(\binom{t}{2} - \sum_{j=1}^n \binom{d_j}{2} \right);$$

отсюда следует формула (15).

Из доказанного утверждения и теоремы Эйлера о рукопожатиях [8] следует очевидный факт.

Следствие 3. Если G — регулярный граф степени d на n вершинах, то

$$L_2 = \frac{nd}{128} (nd + 2d - 4).$$

Пусть $A = (a_{ij})_{n \times n}$ — матрица смежности графа H и $\text{tr} A = \sum_{i=1}^n a_{ii}$. Также обозначим $A^k = (a_{ij}^{(k)})_{n \times n}$, $k \geq 2$. Пусть $J = (1)_{n \times n}$, E — единичная $n \times n$ -матрица.

Утверждение 3. Верно равенство

$$\begin{aligned} L_3 = & \frac{7}{384} \text{tr} (A^3) + \frac{3}{64} \sum_{j=1}^n \binom{d_j}{3} + \\ & + \frac{1}{32} \sum_{j=1}^n \binom{d_j}{2} (t - d_j) + \frac{1}{64} \text{tr} ((J - E)(A^3 - A)). \end{aligned} \quad (16)$$

Доказательство. Для ребер $e_{i_1}, e_{i_2}, e_{i_3}$ возможны следующие варианты:

1. Все три ребра попарно смежны и образуют треугольник в графе H . В этом случае $N(e_{i_1}, e_{i_2}, e_{i_3}) = 3$.
2. Все три ребра инцидентны одной вершине. Тогда $N(e_{i_1}, e_{i_2}, e_{i_3}) = 4$.
3. Ребра образуют цепь длины 3. Тогда опять $N(e_{i_1}, e_{i_2}, e_{i_3}) = 4$.
4. Смежны ровно два ребра из трех. В этом случае $N(e_{i_1}, e_{i_2}, e_{i_3}) = 5$.
5. Ребра попарно не смежны. В этом случае $N(e_{i_1}, e_{i_2}, e_{i_3}) = 6$.

Тогда

$$L_3 = \frac{1}{8} l_3^{(1)} + \frac{1}{16} l_3^{(2)} + \frac{1}{16} l_3^{(3)} + \frac{1}{32} l_3^{(4)} + \frac{1}{64} l_3^{(5)},$$

где $l_3^{(i)}$, $i = 1, \dots, 5$, — число неупорядоченных троек ребер, удовлетворяющих условиям пп. 1)–5). В первом случае (см. [8, с. 187, задача 13.3])

$$l_3^{(1)} = \frac{1}{6} \text{tr} A^3.$$

Во втором случае, аналогично доказательству утверждения 2,

$$l_3^{(2)} = \sum_{j=1}^n \binom{d_j}{3}.$$

В третьем случае заметим, что $a_{ij}^{(3)}$ — число $x_i x_j$ -маршрутов длины 3. Поэтому число простых цепей длины 3 вычисляется как сумма недиагональных элементов матрицы $A^3 - A$, деленная на 2. Таким образом,

$$l_3^{(3)} = \sum_{i=1}^{n-1} \sum_{j=i+1}^n (a_{ij}^{(3)} - a_{ij}) = \frac{1}{2} \text{tr} ((J - E)(A^3 - A)).$$

В четвертом случае два ребра образуют цепь длины 2, а третье с ними не смежно. Поэтому

$$l_3^{(4)} = \sum_{j=1}^n \left[\binom{d_j}{2} (t - d_j) \right].$$

Осталось только заметить, что

$$l_3^{(5)} = \binom{t}{3} - l_3^{(1)} - l_3^{(2)} - l_3^{(3)} - l_3^{(4)},$$

откуда получаем (16).

Теперь, используя результаты [9], получаем следующие оценки.

Утверждение 4. *Во введенных обозначениях верны неравенства*

$$2^n \left(1 - L_1 + \frac{(L_1 + L_2)^2}{3L_1 + 5L_2 + L_3} \right) \leq \|f\| \leq 2^n \frac{2L_2 + L_2^2}{L_1 + L_2}. \quad (17)$$

Доказательство. Обозначим $m_k = \mathbf{E}\eta^k$, $k = 1, 2, \dots, t$. Тогда (см., например, [9]) верны равенства

$$m_k = \sum_{j=1}^k \sigma(k, j) L_j,$$

где $\sigma(k, j)$ — числа Стирлинга второго рода, так что

$$m_1 = L_1, \quad m_2 = L_1 + L_2, \quad m_3 = L_1 + 3L_2 + L_3.$$

Напомним, что η — дискретная неотрицательная случайная величина. Поэтому для нее верны результаты [9], в частности

$$\frac{m_1^2}{m_2} \leq \mathbf{P}\{\eta \geq 1\} \leq m_1 - \frac{L_2^2}{L_3 + 2L_2}.$$

Из равенств $\mathbf{P}\{\eta=0\} = 1 - \mathbf{P}\{\eta \geq 1\}$ и $\|f\| = 2^n \mathbf{P}\{\eta=0\}$ следует (17).

3. Случай немонотонной биюнктивной функции. Порядковая функция

Рассмотрим теперь случай, когда функция f , заданная (1), не содержит аффинных имплицентов, т.е. имплицент вида x_i^a и $x_i \oplus x_j \oplus a$, $i, j \in \{1, 2, \dots, n\}$, $a \in \{0, 1\}$. В этом случае, в соответствии с результатами [2], граф G , определенный в (6), не имеет нетривиальных сильно связанных компонент, а значит, является бесконтурным. Напомним также (см. [2]), что графы всех 2-КНФ, задающих функцию f , отличаются друг от друга наличием дуг, соединяющих начала и концы ориентированных цепей, и имеют одно и то же транзитивное замыкание.

Определим понятие порядковой функции бесконтурного орграфа аналогично [10, гл. 3]. Пусть $H = (VH, EH)$ — бесконтурный орграф. *Порядковой функцией* графа H называется такая функция $\rho: VH \rightarrow \mathbb{N}_0$, что для всякой дуги $(u, v) \in EH$ выполняется неравенство $\rho(u) < \rho(v)$.

В дальнейшем порядковую функцию будем строить методом, описанным в ([10], гл. 3): положим

$$H_0 = H, \quad N_0 = \{u \in VH: d^+(u) = 0\},$$

$$H_1 = H - N_0, \quad N_1 = \{u \in VH_1: d^+(u) = 0\},$$

и т.д. до такого r , что граф H_r не содержит дуг. Тогда множества $N_0, N_1, \dots, N_r$ образуют разбиение множества VH , а функция ρ определяется условием $\rho(u) = i$, если $u \in N_i$. Построенная таким образом функция строится однозначно для любого бесконтурного орграфа (т.е. орграфа без сильно связанных компонент). При этом очевидно, что для произвольной вершины $u \in VG$ значение $\rho(u)$ суть не что иное, как длина максимальной ориентированной цепи (орцепи) из начальной вершины графа G в вершину u , а ее максимальное значение — радиус орграфа G (под длиной ориентированной цепи понимается число дуг в ней, а под радиусом графа — наибольшая из длин орцепей).

Введем обозначения: $n_i = |N_i|$, $i = 0, \dots, r$, а для произвольного множества вершин N графа G положим $\bar{N} = \{\bar{u}, u \in N\}$.

Очевидно следующее утверждение.

Утверждение 5. Пусть $f(x_1, \dots, x_n)$ — бионктивная функция, заданная (18) и не имеющая аффинных имплицентов. Тогда:

- 1) порядковые функции любых двух графов 2-КНФ функции f совпадают,
- 2) для графа G любой 2-КНФ функции f и любого $x_i \in \{x_1, \dots, x_n\}$

$$\rho(\bar{x}_i) = r - \rho(x_i), \text{ где } r = \max\{\rho(u), u \in VG\},$$

- 3) для $i \in \{0, \dots, r\}$ множества N_i не пусты, состоят из попарно не смежных вершин и выполняются равенства

$$N_i = \bar{N}_{r-i}, \quad n_i = n_{r-i}.$$

Таким образом, порядковая функция представляет собой характеристику бионктивной функции, не зависящую от представляющей ее 2-КНФ, а набор величин $(r, n_0, \dots, n_r)$ является инвариантом класса функций $[f]_{Q_n}$. Значение r будем обозначать $r(f)$ и назовем *глубиной* функции f . Очевидно, что $r(f) \leq n-1$. Множества вершин $N_0, \dots, N_r$ будем далее называть *слоями* функции f , а набор чисел $(r(f), n_0, \dots, n_{r(f)})$ — *типом* функции f .

Следствие 4. Пусть функция $f(x_1, \dots, x_n) \in Bi$ не имеет аффинных имплицентов и $r(f) = 1$. Тогда функция f имеет единственную 2-КНФ и найдется такой вектор $\alpha = (a_1, \dots, a_n) \in V_n$, что функция $f(x_1 \oplus a_1, \dots, x_n \oplus a_n)$ монотонна.

Доказательство. Единственность 2-КНФ следует из того, что в графе нет орцепей длины, большей 1. Пусть G — граф 2-КНФ функции f вида (1). Данный граф не имеет сильно связных компонент, и его множество вершин состоит из множеств N_0 (начальных вершин) и N_1 (конечных вершин), вершины в которых попарно не смежны. Это означает, что основание графа G (соответствующий неориентированный граф) является двудольным графом. При этом дуги в графе G идут из вершин множества N_0 в множество N_1 . Ясно, что если x_i — начальная вершина ребра, то $\bar{x}_i$ — конечная, и наоборот. Поэтому $|N_0| = |N_1| = n$ по утверждению 4 и номера переменных в каждом из этих множеств различны и составляют все множество $\{1, 2, \dots, n\}$.

Заметим, что сдвиг переменных на любой вектор $\alpha \in V_n$ означает перестановку вершин x_i и $\bar{x}_i$. Произведем необходимые перестановки так, чтобы выполнялись соотношения $N_0 = \{\bar{x}_1, \dots, \bar{x}_n\}$ и $N_1 = \{x_1, \dots, x_n\}$. Тогда полученный граф будет графом 2-КНФ монотонной биюнктивной функции.

Следствие 4 означает, что монотонная биюнктивная функция имеет всего два слоя, причем $N_0 = \bar{X}$, $N_1 = X$. Поэтому для получения оценок веса такой функции целесообразно применять методы, описанные в разделе 2.

Следствие 5. Пусть $r = r(f)$ нечетно. Тогда

$$n_0 + n_1 + \dots + n_{(r+1)/2} = n$$

и с точностью до инверсий слои $N_0, \dots, N_{(r+1)/2}$ содержат все переменные $x_1, \dots, x_n$.

Если же r четно, то слои $N_0, \dots, N_{r/2}$ содержат все переменные $x_1, \dots, x_n$ с точностью до инверсий.

Доказательство очевидным образом следует из пп. 2)–3) утверждения 5.

Рассмотрим случай, когда функция f лежит в пересечении класса WP слабо положительных и класса WN слабо отрицательных функций: $f \in WP \cap WN$. Свойства таких функций рассмотрены в [1, п. 1.11]. В частности, такая функция f является биюнктивной и представима 2-КНФ вида

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^t (\bar{x}_{s_{i,1}} \vee x_{s_{i,2}}). \quad (18)$$

В этом случае граф G распадается на два подграфа с множествами вершин X и $\bar{X}$. Обозначим их через $G(X)$ и $G(\bar{X})$ соответственно. При этом $(x_i, x_j) \in EG(X)$ тогда и только тогда, когда $(\bar{x}_j, \bar{x}_i) \in EG(\bar{X})$, т. е. эти графы являются обратными друг другу. В частности, если порядковая функция графа $G(X)$ задает слои $N_0, \dots, N_r$, то у графа $G(\bar{X})$ соответствующими слоями будут множества $\bar{N}_r, \dots, \bar{N}_0$.

Поэтому для задания 2-КНФ (18) достаточно графа $G(X)$. Вес функции f , заданной (18), оценим в терминах ее порядковой функции и некоторых характеристик графа $G(X)$. Будем считать, что в этом графе существует s максимальных вершинно не пересекающихся орцепей $P_1, \dots, P_s$, начинающихся в начальных вершинах графа $G(X)$, имеющих длины, соответственно, $t_1 \geq t_2 \geq \dots \geq t_s$. Поскольку в r -м слое есть хотя бы одна вершина, в указанном множестве будет хотя бы одна цепь длины r , т. е. $t_1 = r$. Обозначим $t = t_1 + \dots + t_s$.

Теорема 2. Пусть функция $f(x_1, \dots, x_n) \in WP \cap WN$ существенно зависит от всех переменных, r — глубина графа $G(X)$, а $n_0, \dots, n_r$ — мощности его слоев. Тогда верны неравенства

$$2^{n_0} + 2^{n_1} + \dots + 2^{n_r} - r \leq \|f\| \leq \prod_{i=1}^s (t_i + 2) 2^{n-s-t}. \quad (19)$$

Доказательство. Поскольку f существенно зависит от всех переменных, то $n_0 + \dots + n_r = n$ и $r \geq 1$. Без ограничения общности будем считать, что

$$N_0 = \{x_1, \dots, x_{n_0}\}, N_1 = \{x_{n_0+1}, \dots, x_{n_0+n_1}\}, \dots, N_r = \{x_{n-n_r+1}, \dots, x_n\}.$$

Сначала докажем нижнюю оценку в (19). Граф $G(X)$ — $(r+1)$ -дольный, с долями $N_0, \dots, N_r$. Рассмотрим функцию

$$h_r(x_1, \dots, x_n) = \bigwedge_{t=0}^{r-1} \bigwedge_{i \in N_t, j \in N_{t+1}} (\bar{x}_i \vee x_j).$$

Очевидно, что $\|f\| \geq \|h_r\|$. Индукцией по r докажем, что

$$\|h_r\| = 2^{n_0} + 2^{n_1} + \dots + 2^{n_r} - r.$$

Пусть $r = 1$. Построим для h_1 соответствующий граф $G_{h_1}(X)$. Это полный двудольный граф с множеством дуг

$$EG_{h_1}(X) = \{(x_i, x_j), i \in \{1, \dots, n_0\}, j \in \{n_0 + 1, \dots, n\}\}.$$

Вектор $\alpha = (a_1, \dots, a_n) \in V_n$ будет выполняющим для h_1 тогда и только тогда, когда $a_i \leq a_j$ для всех $i \in \{1, \dots, n_0\}$ и $j \in \{n_0 + 1, \dots, n\}$.

Положим $\alpha = (\alpha', \alpha'')$, где $\alpha' = (a_1, \dots, a_{n_0})$ и $\alpha'' = (a_{n_0+1}, \dots, a_n)$. Тогда выполняющими векторами функции h будут такие векторы $\alpha = (\alpha', \alpha'')$, что либо $\alpha' = (0, \dots, 0)$ и α'' — произвольный, либо вектор α' содержит единицу и $\alpha'' = (1, \dots, 1)$. В итоге получаем $2^{n_0} + 2^{n_1} - 1$ векторов.

Пусть утверждение верно для всех функций h_{r-1} глубины $r-1$ от любого числа переменных. Докажем его для h_r . Построим граф $G_{h_r}(X)$ со слоями $N_0, \dots, N_r$ мощностей $n_0, \dots, n_r$. Выполняющий вектор $\alpha = (a_1, \dots, a_n) \in V_n$ представим в виде $\alpha = (\alpha^{(0)}, \dots, \alpha^{(r)})$, где

$$\alpha^{(0)} = (a_1, \dots, a_{n_0}), \alpha^{(1)} = (a_{n_0+1}, \dots, a_{n_0+n_1}), \dots, \alpha^{(r)} = (a_{n-n_r+1}, \dots, a_n).$$

Определим функцию

$$h_{r-1}(x_1, \dots, x_{n-n_r}) = \bigwedge_{t=0}^{r-2} \bigwedge_{i \in N_t, j \in N_{t+1}} (\bar{x}_i \vee x_j).$$

По предположению индукции

$$\|h_{r-1}\| = 2^{n_0} + 2^{n_1} + \dots + 2^{n_{r-1}} - r + 1.$$

Если $\alpha = (\alpha^{(0)}, \dots, \alpha^{(r)}) \in E_{h_r}$, то $\alpha' = (\alpha^{(0)}, \dots, \alpha^{(r-1)}) \in E_{h_{r-1}}$. Рассмотрим вектор α' . Если $\alpha' = (0, \dots, 0) \in E_{h_{r-1}}$, то, выбирая в качестве $\alpha^{(r)}$ любой вектор длины n_r , получим выполняющий вектор функции h_r . Если же вектор α' содержит хотя бы одну единицу, то единственным возможным вектором, дополняющим его до выполняющего вектора h_r , является вектор $\alpha^{(r)} = (1, \dots, 1)$. Поэтому в итоге получаем, что

$$\|h_r\| = 2^{n_0} + 2^{n_1} + \dots + 2^{n_r} - r,$$

и первое неравенство в (19) доказано.

Докажем второе неравенство. Удалим из графа G все дуги, не входящие в цепи $P_1, \dots, P_s$. Получим граф функции $g(x_1, \dots, x_n)$, причем $\|g\| \geq \|f\|$. Граф 2-КНФ функции g не связный. Поэтому

$$\|g\| = \prod_{i=1}^s (t_i + 2) 2^{n-s-t},$$

откуда следует верхняя оценка в (19).

Первое следствие констатирует тот факт, что в графе $G(X)$ есть как минимум одна цепь длины r .

Следствие 6. Если $r(f) = r$, то

$$\|f\| \leq (r+1) 2^{n-r-1}.$$

Следствие 7. Если в графе $G(X)$ все конечные вершины лежат в слое N_r , то

$$\|f\| \leq (r+1)^s 2^{n-(r+1)s}.$$

Значение верхней оценки из (19) обозначим $\mu(f)$. Эта величина определена, вообще говоря, неоднозначно, поскольку максимальные орцепи в графе можно выбирать различными способами. Однако максимальное число таких цепей может быть получено с помощью алгоритмов построения максимального потока в некоторой сети, получаемой из графа $G(X)$. При этом строится набор орцепей, причем среди них обязательно будет хотя бы одна цепь длины r .

Теорема 3. Для веса функции $f \in WP \cap WN$, не имеющей аффинных имплицентов, существует полиномиальный алгоритм вычисления оценки вида $\mu(f)$.

Доказательство. Пусть $P_1, \dots, P_s$ — наибольшее множество максимальных вершинно не пересекающихся цепей, начинающихся в начальных вершинах графа $G(X)$. По графу $G(X)$ построим сеть $\hat{G}$ следующим образом:

1. Добавим в $\hat{G}$ новые вершины u и v .
2. Для вершины u добавим дуги вида (u, x_i) , $x_i \in N_0$. Тогда $\deg^-(u) = n_0$.
3. Для вершины v добавим дуги вида (x_j, v) для всех конечных вершин x_j графа $G(X)$. Ясно, что тогда $\deg^+(v) \geq n_r$, поскольку множество конечных вершин содержит в себе множество N_r и конечные вершины предыдущих слоев.
4. В результате получаем (u, v) -сеть с источником u и стоком v .
5. Пропускные способности дуг полученной сети зададим равными 1.

В этой сети рассмотрим цепи $P'_1, \dots, P'_s$, полученные из цепей $P_1, \dots, P_s$ добавлением дуг, соединяющих вершину u с их началами, а их концы с вершиной v . Получим цепи, пересекающиеся только по вершинам u и v . По теореме Менгера (вершинная форма) (см. [11, с. 117]) максимальное число таких цепей равно мощности минимального вершинного (u, v) -разреза сети $\hat{G}$.

Для непосредственного вычисления мощности разреза и соответствующих цепей необходимо перейти к рассмотрению реберных разрезов в сетях и построению максимальных потоков. Применим метод, описанный в [11, с. 118]. Каждую проходную вершину x_i сети $\hat{G}$ преобразуем в две вершины $x_i^{(1)}$ и $x_i^{(2)}$. Соединим их дугой $(x_i^{(1)}, x_i^{(2)})$; дуги, входящие в x_i , будут входить в $x_i^{(1)}$, а дуги, выходящие из x_i , будут выходить из $x_i^{(2)}$. Пропускная способность каждой дуги по-прежнему остается равной 1. Получим новую сеть $\tilde{G}$ на $2n + 2$ вершинах.

Очевидно, что любому вершинному разрезу сети $\hat{G}$ однозначно соответствует реберный разрез сети $\tilde{G}$. По теореме Форда–Фалкерсона [11, с. 89] минимальному разрезу $\tilde{G}$ соответствует максимальный поток. Таким образом, для нахождения мощности максимального вершинного разреза в $\hat{G}$ достаточно построить максимальный поток в сети $\tilde{G}$. Данную задачу можно решить со сложностью $O(n^3)$ [11, с. 93]. При этом, поскольку пропускные способности дуг равны 1, т. е. целые, максимальный поток будет целочисленным, т. е. поток через каждую дугу будет равен 0 или 1 (см. [11, с. 91]).

Пусть величина найденного потока равна s . Тогда в точности s дуг, выходящих из u в N_0 , содержат поток, равный 1. Далее, так как поток через каждую дугу равен 0 или 1, то ненулевой поток идет в точности через s реберно не пересекающихся (u, v) -цепей. Проводя обратное преобразование от сети $\tilde{G}$ к сети $\hat{G}$, получим цепи $P'_1, \dots, P'_s$, а из них — вершинно не пересекающиеся цепи $P_1, \dots, P_s$. Легко понять, что хотя бы одна из них имеет длину r .

Замечание. Если выполняется условие следствия 6, то применение метода из доказательства теоремы 3 дает точное значение параметра $s = \mu(f)$. Если же это условие не выполнено, то алгоритм теоремы 3 построит максимально возможное число вершинно не пересекающихся орцепей длины r , поскольку каждая такая орцепь проходит через любой вершинный разрез сети.

Легко доказывается следующее утверждение.

Утверждение 6. Для любой биюнктивной функции $f(x_1, \dots, x_n)$ верно неравенство

$$\|f(x_1, \dots, x_n)\| \leq (r(f) + 2) 2^{n-r(f)-1}. \quad (20)$$

Доказательство. Положим $r = r(f)$. При $f \in WP \cap WN$ оценка (20) представляет собой очевидное следствие верхней оценки из (19). В остальных случаях достаточно заметить, что для любой 2-КНФ функции f в графе G найдется цепь P длины $r(f)$, причем в этой цепи все литералы попарно различны и нет пар литералов вида $x_i, \bar{x}_i$. Без ограничения общности можно считать, что цепь P имеет вид $P = (x_1, \dots, x_{r+1})$. Обратной цепью будет $\bar{P} = (\bar{x}_{r+1}, \dots, \bar{x}_1)$. Удалив из графа вершины $x_{r+2}, \dots, x_n, \bar{x}_{r+2}, \dots, \bar{x}_n$, получим граф 2-КНФ функции

$$g(x_1, \dots, x_n) = (\bar{x}_1 \vee x_2) \cdot \dots \cdot (\bar{x}_r \vee x_{r+1})$$

с несущественными переменными $x_{r+2}, \dots, x_n$. При этом $\|g\| = (r+2) 2^{n-r-1}$. Очевидно, что $g \geq f$, и поэтому $\|f\| \leq \|g\|$.

Обобщением утверждения 7 является следующая теорема, доказательство которой аналогично доказательству теорем 2 и 3.

Теорема 4. Пусть $f(x_1, \dots, x_n)$ — биективная функция, заданная (1) и не имеющая аффинных имплицентов, G — граф ее произвольной 2-КНФ, $r = r(f)$. Пусть, далее, $P_1, \dots, P_s$ — некоторый набор максимальных орцепей в G длин $r = t_1 \geq \dots \geq t_s$, причем эти цепи вершинно не пересекаются и множество всех их вершин не содержит пар вида $(x_i, \bar{x}_i)$. Тогда верна оценка

$$\|f\| \leq \prod_{i=1}^s (t_i + 2) 2^{n-s-t}, \quad (21)$$

где $t = t_1 + \dots + t_s$, и сложность получения параметров верхней оценки в (21) полиномиальна.

Заметим, что параметр s в формулировке теоремы 4 можно вычислить за полиномиальное время методами, изложенными в доказательстве теоремы 3. Если длина максимальной орцепи графа G ограничена снизу, то получаем следующую оценку.

Следствие 8. Если выполнены условия теоремы 4 и $t_s \geq \tau$, то

$$\|f\| \leq (r+2)(\tau+2)^{(s-1)} 2^{n-s-r-(s-1)\tau}. \quad (22)$$

В качестве примера рассмотрим функцию

$$f(x_1, \dots, x_m) = (\bar{x}_1 \vee x_2)(\bar{x}_2 \vee x_3) \cdots (\bar{x}_{n-1} \vee x_n).$$

Легко показать, что $\|f\| = n + 1$, а граф 2-КНФ $G(X)$ состоит из одной орцепи $x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_n$. Поэтому $r(f) = n - 1, n_0 = \dots = n_{n-1} = 1, s = 1, t_1 = n - 1$ и нижняя оценка в (19) дает значение $2n - (n - 1) = n + 1$. Верхняя оценка веса получается по любой из формул (19)–(21) и дает значение $(t_1 + 2) 2^{n-s-t_1} = n + 1$. Таким образом, верхняя и нижняя оценки веса совпадают и равны весу функции. Данный пример показывает, что полученные оценки являются достаточно точными. Вместе с тем у функций с более сложной структурой графа 2-КНФ верхняя и нижняя оценки могут существенно расходиться.

Список литературы

- [1] Горшков С.П., Тарасов А.В., *Сложность решения систем булевых уравнений*, М.: Курс, 2017, 192 с.
- [2] Тарасов А.В., “О свойствах функций, представимых в виде 2-КНФ”, *Дискретная математика*, **13**:4 (2001), 99–115.
- [3] Горшков С.П., “О сложности нахождения числа решений систем булевых уравнений”, *Дискретная математика*, **6**:1 (1996), 72–85.
- [4] Dahl ö ff V., Jonsson P., Wahlstr ö m M., “Counting models for 2SAT and 3SAT formulae”, *Theor. Comput. Sci.*, **332(1-3)** (2005), 265–291.
- [5] Данцин Е.Я., “Алгоритмика задачи выполнимости”, *Вопросы кибернетики*, **131** (1987), 7–21.
- [6] Горшков С.П., Тарасов А.В., “О весе булевых функций, представимых в виде 2-КНФ или 3-КНФ”, *Математические вопросы криптографии*, **1**:1 (2018), 5–26.
- [7] Сачков В.Н., *Курс комбинаторного анализа*, М.-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.
- [8] Харари Ф., *Теория графов*, М.: Мир, 1973, 300 с.
- [9] Зубков А.М., “Неравенства для распределения числа одновременно происходящих событий”, *Обозрение прикл. и промышл. матем.*, **1**:4 (1994), 638–666.
- [10] Кофман А., *Введение в прикладную комбинаторику*, М.: Мир, 1975, 480 с.
- [11] Ловас Л., Пламмер М., *Прикладные задачи теории графов. Теория паросочетаний в математике, физике и химии*, М.: Мир, 1998, 653 с.