ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 2
2020

А. В. Тарасов (Москва, ООО «Центр сертификационных исследований»).
Булевы биюнктивные функции и их графы.
УДК 519.716.5

Резюме: Показана связь задачи $\sharp$2-SAT с задачей нахождения веса булевых биюнктивных функций. Введен орграф 2-КНФ таких функций. Получены оценки веса биюнктивных функций в зависимости от параметров графа.

Ключевые слова: задача $\sharp$2-SAT , булева биюнктивная функция.

Рассмотрим систему уравнений вида:

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

Задача определения совместности такой системы является полиномиальной, но задача определения числа решений таких систем является частным случаем известной задачи $\sharp SAT$ и носит название $\sharp$2-SAT. Данная задача в общем случае относится к классу труднорешаемых задач перечисления, а именно, является $\sharp P$-полной (см. [2]). Очевидно, что задача определения числа решений системы (1) эквивалентна задаче определения веса (числа выполняющих векторов) функции вида

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

Функции вида (2) называются *биюнктивными*, а класс всех таких функций обозначается через Bi и является одним из классов *Шефера*.

Для практического использования может представлять интерес не столько нахождение точного числа решений системы (1), сколько получение верхних и нижних оценок этого числа. Поэтому представляют интерес задачи получения оценок веса булевых биюнктивных функций, спектра значений их весов и иных весовых свойств. Данной проблеме посвящен ряд работ, например, [4, 3].

Введем основные понятия. Пусть V_n — множество двоичных векторов длины n. Для булевой функции f от n символом $\|f\| = |E_f|$ обозначим ее вес. Введем понятие графа 2-КНФ вида (2).

Положим $X = \{x_1, \ldots, x_n\}, \overline{X} = \{\overline{x}_1, \ldots, \overline{x}_n\}$ и $G = (VG, EG)$ — ориентированный граф, в котором:

$$VG = X \cup \overline{X}, \quad EG = \left\{(x_{s_{i,1}}^{a_{i,1}\oplus 1}, x_{s_{i,2}}^{a_{i,2}}),\ (x_{s_{i,2}}^{a_{i,2}\oplus 1}, x_{s_{i,1}}^{a_{i,1}}), \quad i = 1, 2, \ldots, t\right\}. \tag{3}$$

Имплицентой булевой функции f, называется такая не равная константе функция g, что $f \cdot g \equiv f$. Класс биюнктивных функций, существенно зависящих от всех переменных и не имеющих аффинных имплицент, т. е. имплицент вида x_i^a и $x_i \oplus x_j \oplus a$, $i, j \in \{1, 2, \ldots, n\}, a \in \{0, 1\}$, обозначим Bi'. Если $f(x_1, \ldots, x_n) \in Bi'$, то, в соответствии с результатами [1], граф G, определенный в (3), не имеет нетривиальных сильно связных компонент, а значит, является бесконтурным. Величина r, равная максимальной длине ориентированной цепи в орграфе G, является характеристикой

биюнктивной функции, не зависящей от представляющей ее 2-КНФ. Это значение будем обозначать $r(f)$ и назовем *глубиной* функции f (см. [3]).

Введем обозначения для некоторых классов функций:

— M_3 — класс функций, представимых в виде

$$f(x_1,\dots,x_n)=\mathop{\&}_{i=1}^{t}(\overline{x}_{s_{i,1}}\vee x_{s_{i,2}}).$$

— $[M_3]$ — класс функций, получаемых из функций класса M_3 путем навешивания отрицаний на переменные.

Теорема. *Пусть* $n\geqslant 3$, $f(x_1,\dots,x_n)\in Bi'$, $r(f)=r$, l — *остаток от деления* n *на* $r+1$, *а* $q=\lfloor\frac{n}{r+1}\rfloor$ — *неполное частное. Тогда верно неравенство*:

$$\|f\|\leqslant(r+1)\cdot 2^{n-(r+1)}+1. \tag{4}$$

Если, кроме того, $f(x_1,\dots,x_n)\in Bi'\cap[M_3]$, *то верно неравенство*:

$$\|f\|\geqslant(r+l+1)\cdot 2^{q}-r. \tag{5}$$

Обе указанные оценки являются достижимыми.

СПИСОК ЛИТЕРАТУРЫ

1. *Тарасов А. В.* О свойствах функций, представимых в виде 2-КНФ. — Дискретная математика, 2001, т. 13, в. 4, с. 99–115.
2. *Горшков С. П.*, *Тарасов А. В.* Сложность решения систем булевых уравнений, М.: Курс, 2017, 192 с.
3. *Тарасов А. В.* О методах оценивания веса булевых биюнктивных функций. — Математические вопросы криптографии, 2018, т. 8, в. 4, с. 125–142.
4. *Горшков С. П.*, *Тарасов А. В.* О весе булевых функций, представимых в виде 2-КНФ или 3-КНФ. — Математические вопросы криптографии, 2018, т. 9, в. 4, с. 5–26.

УДК 519.716.5

Tarasov A. V. (Moscow, Certification Research Center, LLC). **Boolean bijunctive functions and their graphs**

Abstract: The connection of the problem $\sharp 2\text{-}SAT$ with the problem of finding the weight of Boolean bijunctive functions is shown. Digraph 2-CNF of such functions has been introduced. Estimates for the weight of bijunctive functions in depending on the parameters of the graph.

Keywords: problem $\sharp 2\text{-}SAT$, Boolean bijunctive function.