ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/1/1

УДК 519.7

О СЛОЖНОСТИ НАХОЖДЕНИЯ ПРИВЕДЕННЫХ ПРЕДСТАВЛЕНИЙ СЛАБО ПОЛОЖИТЕЛЬНЫХ И СЛАБО ОТРИЦАТЕЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ

С.П. Горшков

Институт криптографии, связи и информатики Академии ФСБ России, г. Москва

E-mail: spg54@bk.ru

В работе оценивается сложность задачи построения приведенных представлений слабо положительных и слабо отрицательных булевых функций, записанных в совершенной конъюнктивной нормальной форме или многочленом Жегалкина.

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

Булева функция $f(x_1, ..., x_k)$ называется:

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

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

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

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

$$f \equiv \bigwedge_{i=1}^{t} (x_{s_{i1}}^{\alpha_i} \vee \overline{x}_{s_{i2}} \vee ... \vee \overline{x}_{s_{ik_i}}), \quad (2)$$

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

Множество всех функций классов 1 и 2 обозначим соответственно *WP*, *WN*. Формулы (1), (2) соответственно для функций классов *WP*, *WN* будем называть *приведенными представлениями*.

В работах [1, 2] показано, что слабо положительные и слабо отрицательные функции (наряду с мультиаффинными и биюнктивными функциями) порождают полиномиально решаемые классы систем булевых уравнений без ограничений на выбор неизвестных. В англоязычной литературе слабо отрицательные функции часто называются хорновскими функциями, а слабо положительные булевы функции – антихорновскими.

Интерес к задаче оценки сложности нахождения приведенных представлений слабо положительных и слабо отрицательных функций по другим заданиям функций обусловлен следующими моментами.

1. В общем случае задача перевода функций из одного вида в другой (например, построение по многочлену Жегалкина функции совершенной дизъюнктивной нормальной формы этой функции) имеет экспоненциальную сложность.

2. Если все функции левой части системы булевых уравнений

$$\{ f_i(x_1, ...x_n) = 1, i = 1, ..., m, \quad (3)$$

слабо положительные (слабо отрицательные) функции и записаны в приведенном виде, то существует алгоритм линейной сложности (сложности $O(\text{len}(S))$, где $\text{len}(S)$ – длина записи системы (3)) распознавания совместности (3) [3].

3. Если две слабо положительные (слабо отрицательные) функции f_1, f_2 заданы в приведенном виде, то с полиномиальной сложностью можно определить $f_1 \stackrel{?}{\equiv} f_2$.

Напомним некоторые определения. Функция $h(x_1, ..., x_k)$ называется *имплицентой* функции $f(x_1, ..., x_k)$, если

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

Имплиценты вида $x_{s_1}^{\alpha_1} \vee x_{s_2}^{\alpha_2} \vee ... \vee x_{s_r}^{\alpha_r}$, где $s_i \neq s_j$ при $i \neq j$, называются *элементарными имплицентами*. Элементарная имплицента функции f называется *простой*, если никакая ее собственная часть не является имплицентой функции f.

Любая функция $f(x_1,...,x_k)$, не равная тождественно 1, представляется конъюнкцией всех своих простых имплицент. Конъюнктивная нормальная форма функции *f*, в которую входят все простые имплиценты функции *f* и только они, называется *сокращенной* КНФ функции *f*. Любая функция $f(x_1,...,x_k)$ имеет единственную, с точностью до перестановки сомножителей, сокращенную КНФ. Сокращенная КНФ слабо положительной (слабо отрицательной) булевой функции является одной из ее приведенных представлений.

Утверждение 1. Задача построения по совершенной КНФ (СКНФ) слабо положительной функции ее сокращенной КНФ имеет полиномиальную сложность.

Доказательство. Для построения сокращенной КНФ функции $f \in WP$ необходимо найти все простые имплиценты функции *f* вида

$$x_{s_1}^{\alpha} \vee x_{s_2} \vee ... \vee x_{s_q}. \tag{4}$$

Рассмотрим вначале алгоритм поиска всех имплицент (4), в которых $\alpha = 1$. Если функция *f* имеет простую имплиценту $x_{s_1} \vee x_{s_2} \vee ... \vee x_{s_q}$, где $s_1 < ... < s_q$, то

$$f(x_{s_1} = 0,..., x_{s_q} = 0) \equiv 0, \tag{5}$$

и каждая из функций

$$f(x_{s_1} = 0,..., x_{s_{i-1}} = 0, x_{s_{i+1}} = 0,..., x_{s_q} = 0), \ i = 1, ..., q, \tag{6}$$

не равна тождественно нулю. Заметим, что ввиду (5) в СКНФ функции *f* входит элементарная имплицента

$$\bar{x}_1 \vee ... \vee \bar{x}_{s_1-1} \vee x_{s_1} \vee \bar{x}_{s_1+1} \vee ... \vee \bar{x}_{s_q-1} \vee x_{s_q} \vee \bar{x}_{s_q+1} \vee ... \vee \bar{x}_k.$$

Из этих свойств следует, что для поиска всех имплицент (4), в которых $\alpha = 1$, необходимо провести следующие процедуры. Для каждого конъюнкта $x_1^{\delta_1} \vee ... \vee x_k^{\delta_k}$ функции *f* рассматриваем функцию

$$f' \equiv f(x_{j_1} = 0,..., x_{j_q} = 0),$$

где $j_1, ..., j_q$ – номера всех координат вектора $\delta = (\delta_1, ..., \delta_k)$, равных 1. В случае, когда функция *f* имеет имплиценту $(x_{j_1} \vee ... \vee x_{j_q})$, должно выполняться (5) (сложность проверки, очевидно, полиномиальна). Для проверки простоты имплиценты необходимо рассмотреть *q* соотношений вида (6).

Для поиска простых имплицент вида $\bar{x}_{s_1} \vee x_{s_2} \vee ... \vee x_{s_q}$ следует для всякого сомножителя $x_1^{\delta_1} \vee ... \vee x_k^{\delta_k}$ из СКНФ функции *f* рассмотреть $k - q$ функций $f_i' \equiv f(x_{j_1} = 0,..., x_{j_q} = 0, x_i = 1)$, где $j_1, ..., j_q$ – номера всех координат вектора $\delta = (\delta_1, ..., \delta_k)$, равных 1, $i \in \{1, ..., k\} \setminus \{j_1, ..., j_q\}$, и способом, аналогичным описанному выше, определить: является ли функция $\bar{x}_i \vee x_{j_1} \vee ... \vee x_{j_q}$ простой элементарной имплицентой функции *f*, или нет.

Нетрудно видеть, что приведенный алгоритм с полиномиальной сложностью находит сокращенную КНФ (которая является приведенным представлением) слабо положительной функции. Утверждение доказано.

Поскольку

$$f(x_1, ..., x_k) \in WP, \text{ если и только если } f(\bar{x}_1, ..., \bar{x}_k) \in WN, \tag{7}$$

и с полиномиальной сложностью по СКНФ функции $f(x_1, ..., x_k)$ находится СКНФ функции $f(\bar{x}_1, ..., \bar{x}_k)$, то справедлив следующий результат.

Утверждение 2. Существует полиномиальный алгоритм, который по СКНФ слабо отрицательной функции *f* находит сокращенную КНФ функции *f*.

Перейдем к рассмотрению случая, когда функции задаются многочленами Жегалкина.

Утверждение 3. Задача построения по многочлену Жегалкина монотонной функции ее сокращенной (минимальной) КНФ не является полиномиальной.

Доказательство. Нетрудно показать, что для монотонной функции сокращенная КНФ совпадает с минимальной КНФ.

Для доказательства теоремы достаточно показать, что для любого полинома $p(n)$ существует натуральное k_0, такое, что при любом $k > k_0$ найдется монотонная функция $f(x_1, ..., x_k)$, для длины записи которой многочленом Жегалкина $\text{len}(f_{\text{Жег}})$ справедливо соотношение

$$\text{len}(f_{\text{КНФ}}) > p(\text{len}(f_{\text{Жег}})), \tag{8}$$

где $\text{len}(f_{\text{КНФ}})$ – длина записи сокращенной КНФ функции *f*.

Перейдем к построению монотонных функций с требуемыми свойствами. Символом $h^{(r)}(y_1,...,y_r)$ обозначим следующую монотонную функцию:

$$h^{(r)}(y_1,...,y_r) \equiv y_1 \vee ... \vee y_r \equiv \bar{y}_1 \cdot ... \cdot \bar{y}_r \oplus 1. \tag{9}$$

Поскольку запись функции $\bar{y}_1 \cdot \ldots \cdot \bar{y}_r$ многочленом Жегалкина содержит все 2^r мономов, то запись функции $h^{(r)}$ в виде многочлена Жегалкина содержит $2^r - 1$ мономов.

Рассмотрим функцию $h^{(rt)}$, которая является суперпозицией функции $h^{(r)}$ и монотонных функций

$$q^{(i)}(x_{(i-1)t+1},\ldots,x_{it}) \equiv x_{(i-1)t+1} \cdot \ldots \cdot x_{it},$$

$$h^{(rt)}(x_1,\ldots,x_{rt}) = h^{(r)}(q^{(1)}(x_1,\ldots,x_t),\ldots,q^{(r)}(x_{(r-1)t+1},\ldots,x_{rt})).$$

Длина записи функции $h^{(rt)}$ многочленом Жегалкина не более чем

$$\text{len}(h^{(rt)}_{\text{Жег}}) \le 2^r (rt)^2 . \tag{10}$$

Например, $$h^{(2,k/2)}(x_1,\ldots,x_k) \equiv x_1 \cdot \ldots \cdot x_{k/2} \oplus x_{(k/2)+1} \cdot \ldots \cdot x_k \oplus x_1 \cdot \ldots \cdot x_k,$$

где k – четное число.

Ясно, что $h^{(rt)}$ как суперпозиция монотонных функций является монотонной функцией. Кроме того, нетрудно показать, что сокращенная (а значит, и минимальная) КНФ функции $h^{(rt)}$ имеет вид

$$\bigwedge_{\substack{1\le s_1\le t,\\ t+1\le s_2\le 2t,\\ \cdots\\ (r-1)t+1\le s_r\le rt}} (x_{s_1} \vee \ldots \vee x_{s_r}).$$

Поэтому длина записи минимальной КНФ функции $h^{(rt)}$ не менее чем

$$h^{(rt)}_{\text{КНФ}} \ge t^r . \tag{11}$$

Для любого натурального k определим монотонную функцию $f(x_1, \ldots, x_k)$. Положим

$$t = \lfloor k / \log_2 k \rfloor, \quad r = \lfloor \log_2 k \rfloor .$$

Если $t = 0$ или $r = 0$, то считаем $f \equiv 0$. В случае $t \cdot r > 0$ функция $f(x_1, \ldots, x_k)$ существенно зависит от $t \cdot r$ переменных

$$f(x_1,\ldots,x_{rt},\alpha_1,\ldots,\alpha_{k-rt}) = h^{(rt)}(x_1,\ldots,x_{rt}),$$

для любых $(\alpha_1,\ldots,\alpha_{k-rt}) \in B_{k-rt}$.

Для длины записи функции f многочленом Жегалкина из соотношения (10) следует оценка сверху

$$\text{len}(f_{\text{Жег}}) \le 2^{\lfloor \log_2 k \rfloor} (rt)^2 \le 2^{\log_2 k} k^2 = k^3 . \tag{12}$$

С другой стороны, из (11) вытекает

$$\text{len}(f_{\text{КНФ}}) \ge (\lfloor k / \log_2 k \rfloor)^{\lfloor \log_2 k \rfloor} > ((k / \log_2 k) - 1)^{\log_2 k - 1}, \tag{13}$$

откуда, в частности, следует, что при $0 < \varepsilon < 1$ (например, $\varepsilon = 1/2$) справедливо следующее асимптотическое неравенство:

$$\text{len}(f_{\text{КНФ}}) \gtrsim k^{\varepsilon \cdot \log_2 k}. \tag{14}$$

Из (14) и (12) получаем справедливость (8) и теоремы в целом.

Следствие. Задача построения по многочлену Жегалкина слабо положительной функции ее сокращенной (минимальной) КНФ не является полиномиальной.

Замечание. Алгоритмы сложности вида $k^{\varepsilon \cdot \log_2 k}$ называются субэкспоненциальными алгоритмами, их сложность превосходит любой полином от k, но меньше чем 2^{k^ε} для любого $\varepsilon > 0$.

Приведем без доказательства один результат о сложности нахождения приведенного представления слабо отрицательных функций, записанных многочленом Жегалкина.

Утверждение 4. Существует алгоритм построения сокращенной КНФ любой слабо отрицательной функции $f(x_1, \ldots, x_k)$, записанной многочленом Жегалкина, сложность которого не выше чем

$$T' = \text{len}(f_{\text{Жег}})^{c \cdot \log_2 (\text{len}(f_{\text{Жег}}))} + p(\text{len}(f_{\text{КНФ}})), \tag{15}$$

где p – некоторый полином; $c > 0$ – некоторая константа.

Замечание. Таким образом, функция сложности (15) есть сумма двух слагаемых, первое слагаемое является субэкспоненциальной функцией от размера входа, а второе слагаемое – полиномиальная функция от размера выхода.

ЛИТЕРАТУРА

1. *Schaefer T.* Complexity of satisfiability problems // Proceedings of the 10 Annual ACM Symposium on Theory of Computing Machinery. 1978. P. 216 – 226.
2. *Горшков С.П.* Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений // Обозрение прикл. промышл. матем., сер. дискрет. матем. 1995. Т. 2. Вып. 3. С. 325 – 398.
3. *Dowling W.F.*, *Gallier J.H.* Linear-time algorithms for testing the satisfiability of propositional Horn formulae // J. Logic Programming. 1984. No. 3. P. 267 – 284.