Серия «Математика»
2010. Т. 3, № 4. С. 2—6

Онлайн-доступ к журналу:
http://isu.ru/izvestia

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.716.322

О сложности одного класса булевых функций *

С. Ф. Винокуров, А. С. Казимиров
Восточно-Сибирская государственная академия образования

Аннотация. В работе исследуется сложность представления булевых функций в классе полиномиальных нормальных форм, которая определяется по числу слагаемых в минимальном полиноме. Рассматривается класс булевых функций, которые имеют наибольшую сложность среди всех функций от 6 переменных и менее. Получено точное значение сложности функций этого класса, зависящих от 7 переменных.

Ключевые слова: булевы функции; полиномиальные формы; операторные формы; минимизация; сложность.

Полиномиальным представлением булевой функции $f(x_1, \ldots, x_n)$ будем называть следующее представление:

$$f(x_1, \ldots, x_n) = K_1 \oplus K_2 \oplus \cdots \oplus K_s,$$

где $\oplus$ — сложение по модулю 2, K_i — произведения переменных, возможно с отрицанием, или функция 1.

Поскольку для каждой функции существует множество полиномиальных представлений, возникает задача нахождения наименее сложного. Здесь под сложностью $L(\Phi)$ полиномиального представления Φ будем понимать число слагаемых Φ, а под сложностью $L(f)$ функции f — число слагаемых ее наименее сложного представления. Сложность всех функций от n переменных $L(n)$ определяется как максимальная из сложностей таких функций.

Функции $n-1$ переменной, полученные подстановкой константы α вместо переменной x_i в функцию n переменных f, будем называть нулевой (при $\alpha = 0$) и единичной (при $\alpha = 1$) остаточными функциями и обозначать через $f^0_{x_i}$ и $f^1_{x_i}$ соответственно.

На множестве булевых функций n переменных задается класс операторов, которые можно представить в виде последовательностей $\mathbf{a}_1 \ldots \mathbf{a}_n$, где $\mathbf{a}_i \in \{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Число n будем называть размерностью оператора. Действие оператора $\mathbf{a} = \mathbf{a}_1 \ldots \mathbf{a}_n$ на функцию $f(\tilde{x})$ определяется по

* Работа выполнена при финансовой поддержке РФФИ, грант 09-01-00476-а.

правилу: $\mathbf{a}(f(\tilde{x})) = f_n(\tilde{x})$, где $f_0(\tilde{x}) = f(\tilde{x})$ и

$$f_i(\tilde{x}) = \begin{cases} f_{i-1}(\tilde{x}), & \text{если } \mathbf{a}_i = \mathbf{e}; \\ f_{i-1}(x_1, ..., x_{i-1}, \bar{x}_i, x_{i+1}, ..., x_n), & \text{если } \mathbf{a}_i = \mathbf{p}; \\ f_{i-1}(\tilde{x})^0_{x_i} \oplus f_{i-1}(\tilde{x}))^1_{x_i}, & \text{если } \mathbf{a}_i = \mathbf{d}. \end{cases}$$

Представление функции $f(x_1, \ldots, x_n)$ в виде

$$f(\tilde{x}) = \bigoplus_{i=1}^{s} \mathbf{a}^i(h(\tilde{x})),$$

в котором $\mathbf{a}^1, \ldots, \mathbf{a}^s$ — операторы размерности n, называется операторной формой функции f, построенной по функции $h(x_1, \ldots, x_n)$. В дальнейшем изложении будем считать, что $h(\tilde{x}) = x_1 \cdot \ldots \cdot x_n$.

Пусть S — полная группа подстановок на множестве $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$:

$$S = \left\{ \begin{pmatrix} \mathbf{dep} \\ \mathbf{dep} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{dpe} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{ped} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{edp} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{epd} \end{pmatrix}, \begin{pmatrix} \mathbf{dep} \\ \mathbf{pde} \end{pmatrix} \right\}$$

Определим преобразование φ операторов размерности n в виде последовательности $\varphi_1 \ldots \varphi_n$, где $\varphi_i \in S$. Преобразование φ действует на оператор $\mathbf{a} = \mathbf{a}_1 \ldots \mathbf{a}_n$ следующим образом: $\varphi(\mathbf{a}) = \varphi_1(\mathbf{a}_1) \ldots \varphi_n(\mathbf{a}_n)$. Таким образом построенное преобразование φ назовем S-преобразованием.

Действие S-преобразований распространяется на множество функций следующим образом. Пусть $f(x_1, \ldots, x_n) = \sum_{i=1}^{s} \mathbf{a}^i(h)$ — некоторая операторная форма функции f. Тогда $\varphi(f) = \sum_{i=1}^{s} \varphi(\mathbf{a}^i)(h)$. SP-преобразованием назовем комбинацию S-преобразования и перестановки символов в операторах.

Две функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ называются SP-эквивалентными, если существует такое SP-преобразование φ, что $\varphi(f) = g$. Частным случаем SP-эквивалентности является LP-эквивалентность [7].

Все функции n переменных разбиваются на классы SP-эквивалентных функций. Более подробно об операторах и операторных преобразования можно прочитать в [2]. Здесь мы только отметим, что сложности SP-эквивалентных функций совпадают.

Для всех полиномиальных представлений известны следующие нижняя [5] и верхняя [3] оценки:

$$\frac{2^n}{n \log_2 3} \leq L(n) \leq \frac{2^n(2 \log_2 n + 2)}{n}$$

Однако задача нахождения самой сложной функции остается открытой. Известно [6, 7], что самыми сложными при $n \leq 6$ являются функции, SP-эквивалентные функции $p_n(x_1, \ldots, x_n)$:

$$p_n(\alpha_1, \ldots, \alpha_n) = \begin{cases} 0, & \text{если } \overline{\alpha_1 \ldots \alpha_n} = 3k, \\ 1, & \text{иначе,} \end{cases}$$

где $\overline{\alpha_1 \ldots \alpha_n}$ — число, записанное в двоичном виде.

Обозначим через M_n множество всех функций, которые SP-эквивалентны p_n при различных n.

Также среди M_n выделим функции

$$q_n(\alpha_1, \ldots, \alpha_n) = \begin{cases} 0, & \text{если } \overline{\alpha_1 \ldots \alpha_n} = 3k+1, \\ 1, & \text{иначе} \end{cases}$$

$$r_n(\alpha_1, \ldots, \alpha_n) = \begin{cases} 0, & \text{если } \overline{\alpha_1 \ldots \alpha_n} = 3k+2, \\ 1, & \text{иначе} \end{cases}$$

Для p_n известна следующая оценка [1]:

$$\left(\frac{3}{2}\right)^{n-1} \leq L(p_n)$$

Простая верхняя оценка получается из следующего неравенства:

$$L(p_n) \leq 3L(p_{n-2})$$

С помощью вычислительной техники найдены $L(p_5) = 9$ и $L(p_6) = 15$ [7]. В [4] предложен алгоритм, которой позволил получить полиномиальное представление для p_7 сложности 24, то есть было показано, что $L(p_7) \leq 24$. Однако оставался открытым вопрос о точном значении сложности p_7.

В данной работе окончательно решен вопрос о сложности p_7. Результат сформулирован в виде теоремы, хотя в доказательстве использованы компьютерные вычисления.

Теорема. $L(p_7) = 24$.

Доказательство. Предположим, что существует такое полиномиальное представление Φ, реализующее функцию p_7, что $L(\Phi) \leq 23$.

Можно заметить, что $(p_7)^0_{x_1} = \Phi^0_{x_1} = p_6$, $(p_7)^1_{x_1} = \Phi^1_{x_1} = r_6$, $(p_7)^0_{x_1} \oplus (p_7)^1_{x_1} = \Phi^0_{x_1} \oplus \Phi^1_{x_1} = q_6$.

Сгруппируем в Φ слагаемые, содержащие x_1 и $\bar{x}_1$:

$$\Phi = x_1 \cdot \Phi_1 \oplus \bar{x}_1 \cdot \Phi_2 \oplus \Phi_3$$

Пусть $L(\Phi_1) = l_1$, $L(\Phi_2) = l_2$ и $L(\Phi_3) = l_3$. Тогда $l_1 + l_2 + l_3 \leq 23$.

Неравенства

$$l_1 + l_2 = L(\Phi_1) + L(\Phi_2) \geq L(\Phi_1 \oplus \Phi_2) = L(\Phi^0_{x_1}) \geq L(p_6) = 15$$

показывают, что $l_1 + l_2 \geq 15$. Повторяя аналогичные рассуждения для $l_1 + l_2$ и $l_2 + l_3$, получаем систему неравенств:

$$\begin{cases} l_1 + l_2 + l_3 \leq 23 \\ l_1 + l_2 \geq 15 \\ l_1 + l_3 \geq 15 \\ l_2 + l_3 \geq 15, \end{cases}$$

из которых следует выполнение только одного из трех условий:

$$l_1 = 7,\ l_2 = 8,\ l_3 = 8$$
$$l_1 = 8,\ l_2 = 7,\ l_3 = 8$$
$$l_1 = 8,\ l_2 = 8,\ l_3 = 7$$

Пусть, например, $l_1 = 7$, $l_2 = 8$, $l_3 = 8$. Тогда $L(\Phi_1 \oplus \Phi_2) = 15$, то есть $\Phi_1 \oplus \Phi_2$ — минимальное полиномиальное представление для q_6. Аналогично, $\Phi_1 \oplus \Phi_3$ — минимальное представление для r_6.

Но тогда два минимальных представления для q_6 и r_6 должны содержать по крайней мере 7 общих слагаемых, так как $L(\Phi_1) = 7$.

В двух других случаях не менее 7 общих слагаемых должны содержать представления для p_6 и q_6 или p_6 и r_6.

С помощью алгоритма точной минимизации функций 6 переменных [6] были найдены все минимальные формулы для функций p_6, q_6, r_6. Для каждой из этих функций существует по 14581 формуле минимальной сложности.

С помощью компьютерных вычислений все эти формулы были попарно рассмотрены и было показано, что никакие две формулы для разных функций не имеют более 6 общих слагаемых.

Таким образом, $L(p_7) > 23$. С учетом того, что $L(p_7) \leq 24$, получаем следующий результат: $L(p_7) = 24$. □

Функции q_7 и r_7, как SP-эквивалентные функции p_7, тоже имеют сложность 24.

Следствие. $L(7) \geq 24$.

Список литературы

1. Балюк А. С. Нижняя оценка сложности одной последовательности булевых функций в классе полиномиальных нормальных форм / А. С. Балюк // Синтез и сложность управляющих систем : материалы XII междунар. шк.-семинара. – М. : Изд-во ЦПИ при мех.-мат. фак. МГУ, 2001. – Ч. 1. – С. 18–21.
2. Винокуров С. Ф. Перечисление операторных классов булевых функций / С. Ф. Винокуров, А. С. Казимиров// Изв. Иркут. гос. ун-та. Сер.: Математика. – 2009. – Т. 2, № 2. – С. 40–55.
3. Кириченко К. Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций / К. Д. Кириченко // Синтез и сложность управляющих систем : материалы XII междунар. шк.-семинара. – М. : Изд-во ЦПИ при мех.-мат. фак. МГУ, 2001. – Ч. 1. – С. 115–120.
4. Рябец Л. В. Нахождение минимальных полиномов булевых функций с использованием специальной операторной формы / Л. В. Рябец // Технологии Microsoft в теории и практике программирования. – Новосибирск, 2006. – С. 215–217.
5. Even S. On minimal modulo 2 sums of products for switching function / S. Even, I. Kohavi, A. Paz // IEEE Trans. Elect. Comput. – 1967. – P. 671–674.

6. Gaidukov A. Algorithm to derive minimum ESOPs for 6-variable functions / A. Gaidukov // Proceedings of the 5th International Workshop on Boolean Problems 2002, Freiberg, Germany, Sept. 19–20, 2002. – P. 141–148.
7. Koda N. An Upper Bound on the Number of Products in Minimum ESOPs / N. Koda, T. Sasao // Workshop in Application of the Reed-Muller Expansion Apllication in Circuit Design. – Japan, 1995. – P. 94–101.

S. F. Vinokurov, A. S. Kazimirov
On Complexity of a Particular Boolean Functions Class

Abstract. This paper concerns complexity of polynomial forms (exor-sum-of-products) representing Boolean functions. Complexity is defined as a minimal number of summands in exor-sum-of-products for a given function. A class of Boolean functions being the most complex among Boolean functions having 6 or less arguments is considered. The exact complexity for functions of described class having 7 agruments is obtained.

Keywords: boolean function, ESOP, exor-sum-of-products, polynomial, operator, complexity.

Винокуров Сергей Федорович, доктор физико-математических наук, профессор, Восточно-Сибирская государственная академия образования, 664011, Иркутск, ул. Н. Набережная, 6 тел.: (3952) 240435 (servin38@gmail.com)

Казимиров Алексей Сергеевич, кандидат физико-математических наук, Восточно-Сибирская государственная академия образования, 664011, Иркутск, ул. Н. Набережная, 6 тел.: (3952) 240435 (a.kazimirov@gmail.com)

Vinokurov Sergey, East Siberian State Academy of Education, 6, N. Naberezhnaya St., Irkutsk, 664011, professor, phone: (3952) 240435 (servin38@gmail.com)

Kazimirov Alexey, East Siberian State Academy of Education, 6, N. Naberezhnaya St., Irkutsk, 664011, phone: (3952) 240435 (a.kazimirov@gmail.com)