

И.С. СЕРГЕЕВ

**ВЕРХНИЕ ОЦЕНКИ СЛОЖНОСТИ ФОРМУЛ
ДЛЯ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ**

Аннотация. Показано, что сложность реализации оператора подсчета числа единиц в булевом наборе длины n формулами над базисом B_2 двуместных булевых функций не превосходит $n^{3.03}$, а над стандартным базисом B_0 — $n^{4.47}$. Как следствие, такие же оценки справедливы для сложности любой пороговой симметрической функции n переменных, в частности, для функции голосования. Для сложности произвольной симметрической функции n переменных получены оценки $n^{3.04}$ и $n^{4.48}$ над базисами B_2 и B_0 соответственно. Доказательство основано на применении модулярной арифметики.

Ключевые слова: сложность формул, симметрические булевы функции, функция голосования, умножение.

УДК: 519.714

ЛИТЕРАТУРА

- [1] Лупанов О.Б. *Асимптотические оценки сложности управляющих систем* (Изд-во МГУ, М., 1984).
- [2] Нигматуллин Р.Г. *Сложность булевых функций* (Наука, М., 1991).
- [3] Чашкин А.В. *Дискретная математика* (Академия, М., 2012).
- [4] Яблонский С.В. *Введение в дискретную математику* (Наука, М., 1986).
- [5] Dunne P.E. *The complexity of Boolean networks* (Academic Press, San Diego, 1988).
- [6] Jukna S. *Boolean function complexity* (Springer-Verlag, Berlin–Heidelberg, 2012).
- [7] Храпченко В.М. *О сложности реализации симметрических функций алгебры логики формулами в конечных базисах*, в сб. “Проблемы кибернетики” (Наука, М., 1976), вып. 31, с. 231–234.
- [8] Черухин Д.Ю. *Нижние оценки формульной сложности симметрических булевых функций*, Дискр. анализ и исслед. опер. Сер. 1 **7** (3), 86–98 (2000).
- [9] Храпченко В.М. *Об одном методе получения нижних оценок сложности π -схем*, Матем. заметки **10** (1), 83–92 (1971).
- [10] Fischer M.J., Meyer A.R., Paterson M.S. $\Omega(n \log n)$ lower bounds on length of Boolean formulas, SIAM J. Comput. **11** (3), 416–427 (1982).
- [11] Sergeev I.S. *Upper bounds for the formula size of the majority function*, <http://arxiv.org/abs/1208.3874> (2012). [там же русский перевод]
- [12] Paterson M., Zwick U. *Shallow circuits and concise formulae for multiple addition and multiplication*, Comput. Complexity **3** (3), 262–291 (1993).
- [13] Peterson G.L. *An upper bound on the size of formulae for symmetric Boolean function*, Tech. Report 78-03-01 (Univ. Washington, 1978).
- [14] Храпченко В.М. *О сложности реализации симметрических функций формулами*, Матем. заметки **11** (1), 109–120 (1972).

Поступила 07.11.2012

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проекты №№ 11-01-00508, 11-01-00792-а) и программы фундаментальных исследований Отделения математических наук РАН “Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения” (проект “Задачи оптимального синтеза управляющих систем”).

- [15] Paterson M.S., Pippenger N., Zwick U. *Optimal carry save networks*, LMS Lecture Notes Series. Boolean function complexity (Cambridge University Press, 1992), vol. 169, p. 174–201.
- [16] Paterson M.S., Pippenger N., Zwick U. *Faster circuits and shorter formulae for multiple addition, multiplication and symmetric Boolean functions*, Proc. 31st IEEE Symp. Found. Comput. Sci., 642–650 (1990).
- [17] Столяров Г.К. *Способ параллельного умножения в цифровых вычислительных машинах и устройство для осуществления способа*, Авт. свид-во кл. 42 т 14, №126668 (1960).
- [18] Stockmeyer L.J. *On the combinational complexity of certain symmetric Boolean functions*, Math. Syst. Theory **10** (4), 323–336 (1977).
- [19] Demenkov E., Kojevnikov A., Kulikov A., Yaroslavtsev G. *New upper bounds on the Boolean circuit complexity of symmetric functions*, Inf. Proc. Letters **110** (7), 264–267 (2010).
- [20] Лупанов О.Б. *К вопросу о реализации симметрических функций алгебры логики контактными схемами*, в сб. “Проблемы кибернетики” (Наука, М., 1965), вып. 15, с. 85–99.
- [21] Гашков С.Б. *Занимательная компьютерная арифметика. Быстрые алгоритмы операций с числами и многочленами* (Либроком, М., 2012).

И.С. Сергеев

*старший научный сотрудник, кафедра дискретной математики,
Московский государственный университет,
ГСП-1, Ленинские горы, г. Москва, 119991, Россия,*

e-mail: isserg@gmail.com

I.S. Sergeev

Upper bounds on the formula size of symmetric Boolean functions

Abstract. It is proved that complexity of implementation of the counting function of n Boolean variables with binary formulae is at most $n^{3.03}$ and is at most $n^{4.47}$ with respect to DeMorgan formulae. Hence, the same bounds hold for the formula size of any threshold symmetric function of n variables, particularly, for majority function. The following bounds are proved for the formula size of any symmetric Boolean function of n variables: $n^{3.04}$ with respect to binary formulae and $n^{4.48}$ with respect to DeMorgan formulae. A proof is based on modular arithmetic.

Keywords: formula size, symmetric Boolean functions, majority function, multiplication.

I.S. Sergeev

*Senior Researcher, Chair of Discrete Mathematics,
Moscow State University,
GSP-1, Leninskie Gory, Moscow, 119991 Russia,*

e-mail: isserg@gmail.com