Краткий комментарий к работам А. А. Маркова по теории сложности булевых функций

А. А. Разборов
Математический Институт им. В. А. Стеклова
117966, ГСП–1, Москва, ул. Губкина, 8

Исследования Андрея Андреевича в теории сложности булевых функций представлены в настоящем издании работами [1, 2, 3, 4]. Главной целью этой теории (не достигнутой в полном объеме до сих пор) является установление нижних оценок сложности вычисления конкретных, естественных булевых функций с помощью схем из данного класса; иными словами, требуется установить, что та или иная вычислительная задача не допускает эффективного алгоритма в заданной вычислительной модели. Конец 50-х и начало 60-х годов (к которым и относятся обсуждаемые работы) ознаменовались значительным всплеском активности в данном направлении: предложенные в этот период постановки задач и методы их решения во многом определили последующее развитие теории сложности булевых функций, а многие полученные тогда результаты до сих пор не превзойдены. Рассматриваемые работы А. А. Маркова занимают весьма достойное место в этом ряду.

Пожалуй, наиболее важной среди них является работа [1]. В ней А. А. Марков рассмотрел одну из самых популярных в то время вычислительных моделей, *контактно-вентильные схемы*, и для случая *монотонных* схем такого вида (называемых в [1] *положительными двухполюсниками*) совершенно точно вычислил сложность реализации всех пороговых (= монотонных симметрических) функций. В частности, для наиболее важной *функции голосования* MAJ_n ($s_n^{[n/2]}$ в обозначениях [1]) эта сложность оказалась по порядку величины равной n^2.

Как мне кажется, в полной мере оценить значение этого результата можно только сейчас, на основании накопленного в течении прошедших 35 лет опыта. За это время основополагающей концепцией теории сложности вычислений стало понятие *класса сложности*, и, в частности, выяснилось, что контактно-вентильные схемы в некотором стандартном и совершенно строгом смысле соответствуют одному из наиболее важных классов сложностной иерархии, $NLOGSPACE$ (недетерминированные вычисления с логарифмической памятью). Один из наиболее красивых результатов теории, полученный в [12, 15], утверждает, что этот класс замкнут относительно дополнений: его доказательство существенно использует возможность эффективного вычисления пороговых функций контактно-вентильными схемами. Большое число исследований было также посвящено попыткам распространить результат А. А. Маркова на случай немонотонных схем. Довольно скоро выяснилось, что в этом случае ситуация меняется в корне: именно, в работе [6] было показано, что MAJ_n вычисляется *немонотонными* контактно-вентильными схемами существенно меньшей сложности $O(n^{3/2})$. Получение каких-либо нетривиальных *нижних* оценок растянулось еще на 20 лет: они появились только в работах [13, 9, 5, 8]. Эти оценки растут лишь чуть быстрее линейной функции от числа переменных. Сужение имеющегося зазора между верхней и нижней оценками является в немонотонном случае открытой и, по-видимому, крайне трудной задачей. На этом фоне работа [1] приятно выделяется своей законченностью и изяществом: примеры такого рода в теории сложности булевых функций крайне редки.

На самом деле, именно ввиду этой завершенности не так просто указать работы, служащие непосредственным продолжением [1]. Циклу работ [2, 3] в этом отношении повезло больше, хотя с первого взгляда кажется, что рассматриваемая в них задача решена настолько же окончательно, как и в [1]: для любой системы функций $f_1, \ldots, f_m$ в достаточно наглядных терминах вычислена ее *инверсионная сложность* $\mathrm{Inv}(f_1, \ldots, f_m)$. Тем не менее, сразу возник естественный вопрос о том, насколько *сложной* должна быть схема, вычисляющая $f_1, \ldots, f_m$ и использующая лишь сравнительно небольшое число отрицаний; существование такой схемы утверждается теоремой А. А. Маркова. Иными словами, насколько эффективной может быть конструктивная реализация этой теоремы? На этот счет были в частности получены следующие результаты.

Уже из работ [2, 3] легко вытекает, что

$$\max_{f_1,\dots,f_m} \mathrm{Inv}(f_1,\dots,f_m) = \log_2(n+1),$$

где максимум берется по всем системам $f_1,\dots,f_m$ булевых функций от n переменных; этот максимум достигается, например, для системы функций $V_n = \{\neg x_1,\dots,\neg x_n\}$. Более того, система V_n универсальна в том смысле, что обладая схемой, вычисляющей эту систему и использующей минимально возможное число отрицаний $\log_2(n+1)$, можно легко элиминировать все остальные отрицания в *любой* схеме, вычисляющей *произвольную* систему функций от n переменных. По этой причине вычисляющие V_n схемы с $\log_2(n+1)$ отрицаниями заслужили специальное название *инвертеров*; их конструкции последовательно совершенствовались в работах [11, 16, 10]. В последней работе из этого цикла был построен инвертер размера $O(n\log n)$ и глубины $O(\log^2 n)$. Вопрос о существовании инвертера линейного размера $O(n)$ остается открытым.

На другом полюсе находятся монотонные функции, т.е. функции инверсионной сложности ноль. Здесь ситуация кардинально отличается от только что рассмотренной: были построены примеры (немонотонных) схем полиномиального размера, вычисляющих монотонные функции и таких, что для удаления *всех* отрицаний размер схемы неизбежно должен вырасти экспоненциально [7, 17]. Для сравнения отметим, что как мы только что видели, до $\log_2(n+1)$ число используемых отрицаний всегда можно редуцировать эффективно. Вопрос о том, что происходит при допустимом числе отрицаний в промежутке между 0 и $\log_2(n+1)$ в настоящее время открыт, и это, по-видимому, наиболее интересная нерешенная проблема относительно впервые рассмотренной А. А. Марковым инверсионной сложности.

В работе [4] рассматривается задача вычисления функции сложения (или, что с вычислительной точки зрения эквивалентно, вычитания) по $\mathrm{mod}\ n$ двух чисел, записанных либо в *унарной кодировке* (*кодирование с помощью ортов* в [4]) либо в ее слегка более экономной модификации (*кодирование с помощью пар ортов*). Для решения этой задачи строится ряд конкретных схем, имеющих *глубину* (называемую в [4] *высотой*) $O(1)$ и число ребер (*диодов*) $O(n^2)$.

Читателям, желающим ближе познакомиться с предметом, можно порекомендовать главы 2 и 14 книги [18], представляющие собой прекрасное современное введение в иерархию классов сложности и теорию сложности булевых функций соответственно. Обзор [14] посвящен более специфическим вопросам сложности контактно-вентильных и других связанных с ними классов схем.

Литература

[1] А. А. Марков, О минимальных контактно-вентильных двухполюсниках для монотонных симметрических функций, *Проблемы кибернетики*, 1962, вып. 8, стр. 117-121.

[2] А. А. Марков, Об инверсионной сложности систем функций, *ДАН СССР*, 1957, т. 116, N 6, стр. 917-919.

[3] А. А. Марков, Об инверсионной сложности системы булевых функций, *ДАН СССР*, 1963, т. 150, N 3, стр. 477-479.

[4] А. А. Марков, Об однотактных диодных схемах для сложения и вычитания по модулю n, рукопись, 1958.

[5] М. И. Гринчук, О сложности реализации симметрических булевых функций контактными схемами, канд. дисс., МГУ, 1989.

[6] О. Б. Лупанов, К вопросу о реализации симметрических функций алгебры логики контактными схемами, *Проблемы кибернетики*, 1965, вып. 15, стр. 85-99.

[7] А. А. Разборов, Нижние оценки монотонной сложности логического перманента, *Математические Заметки*, 1985, т. 37, N 6, стр. 887-900.

[8] А. А. Разборов, Нижние оценки сложности реализации симметрических булевых функций контактно-вентильными схемами, *Математические Заметки*, 1990, т. 48, N 6, стр. 79-91.

[9] L. Babai, P. Pudlák, V. Rödl, and E. Szemeredi. Lower bounds to the complexity of symmetric Boolean functions. *Theoretical Computer Science*, 74(3):313–323, 1990.

[10] R. Beals, T. Nishino, and K. Tanaka. More on the complexity of negation-limited circuits. In *Proceedings of the 27th ACM Symposium on Theory of Computing*, pages 585–595, 1995.

[11] M. J. Fischer. The complexity of negation-limited networks – a brief survey. In *Lecture Notes in Computer Science,* 33, pages 71–82. Springer-Verlag, Berlin, 1974.

[12] N. Immerman. Nondeterministic space is closed under complementation. In *Proceedings of the* 3*rd Structure in Complexity Theory Annual Conference*, pages 112–115, 1988.

[13] P. Pudlák. A lower bound on complexity of branching programs. In *Proceedings of the* 11*th MFCT, Lecture Notes in Computer Science,* 176, pages 480–489, New York/Berlin, 1984. Springer-Verlag.

[14] A. Razborov. Lower bounds for deterministic and nondeterministic branching programs. In *Proceedings of the 8th FCT, Lecture Notes in Computer Science,* 529, pages 47–60, New York/Berlin, 1991. Springer-Verlag.

[15] R. Szelepcsényi. The method of forcing for nondeterministic automata. *Bulletin of the EATCS*, 33:96–99, 1987.

[16] K. Tanaka and T. Nishino. On the complexity of negation-limited Boolean networks. In *Proceedings of the 26th ACM Symposium on Theory of Computing*, pages 38–47, 1994.

[17] É. Tardos. The gap between monotone and nonmonotone circuit complexity is exponential. *Combinatorica*, 8:141–142, 1988.

[18] Jan van Leeuwen, editor. *Handbook of Theoretical Computer Science, vol. A* (*Algorithms and Complexity*). Elsevier Science Publishers B.V. and The MIT Press, 1990.