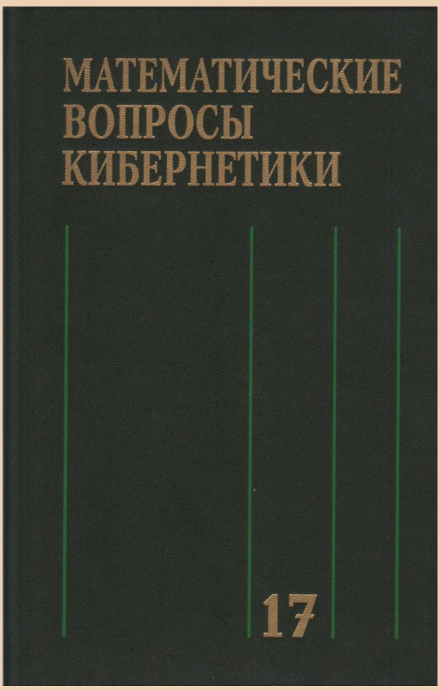

О. Б. Лупанов

А. Н. Колмогоров и теория сложности схем

А. Н. КОЛМОГОРОВ И ТЕОРИЯ СЛОЖНОСТИ СХЕМ

О. Б. ЛУПАНОВ

(МОСКВА)

Статья написана на основе доклада, прочитанного на Международной конференции «Колмогоров и современная математика» (Москва, 16–21 июня 2003 г.) и содержит обзор некоторых результатов по теории сложности схем в тех направлениях исследований, которые интересовали А. Н. Колмогорова или были им инициированы, а также являются продолжением или развитием этих исследований.

Основным объектом исследований являются схемы из функциональных элементов (определение схемы, а также функций, характеризующих сложность схем, см., например в [12–15, 23]).

Напомним кратко некоторые из этих определений:

$L(S)$ — сложность схемы S, т. е. число ее элементов;

$D(S)$ — глубина схемы S — максимальная длина цепи из элементов схемы S от входов до выходов.

Пусть F — булева функция или система функций. Положим

$L(F) = \max\limits_{S \text{ реализует } F} L(S)$;

$D(F) = \max\limits_{S \text{ реализует } F} D(S)$.

Сложение и умножение

Пусть Σ_n — оператор сложения двух n-разрядных двоичных чисел, т. е. система $n+1$ функций, которая по разрядам слагаемых вычисляет разряды их суммы.

Пусть M_n — аналогичный оператор умножения двух n-разрядных чисел.

Сложение. Очевидно, что известный «школьный» алгоритм сложения n-разрядных чисел приводит к схеме S_n^{Σ}, имеющей параметры

$$L(S_n^{\Sigma}) \asymp n, \tag{1}$$
$$D(S_n^{\Sigma}) \asymp n.$$

Более точно, [для базиса $B_0 = \{\&, \vee, {}^{-}\}$]

$$L_{B_0}(\Sigma_n) \leqslant 9n - 5. \tag{2}$$

Схема, доставляющая верхнюю оценку в (2), состоит из n последовательно соединенных ячеек. Одна из них, работающая с младшими разрядами слагаемых, имеет сложность 4; каждая из остальных («типичных») ячеек имеет сложность 9. Доказано, что эти ячейки являются минимальными по сложности. Однако из этого не следует, что минимальная схема для Σ_n имеет сложность $9n-5$. Наилучшая нижняя оценка для $L_{B_0}(\Sigma_n)$ получена Н. П. Редькиным и имеет вид *)

$$L_{B_0}(\Sigma_n) \geqslant 7n - C.$$

Около 1960 г. было установлено, что [11, 26, 27]

$$D(\Sigma_n) \lesssim \log n, \tag{3}$$

и что можно получить оценки (1) и (3) одновременно (в одной и той же схеме).

Очевидно, что с меньшей по порядку глубиной реализовать оператор Σ_n невозможно, так как старший разряд суммы существенно зависит от всех $2n$ разрядов слагаемых.

В. М. Храпченко подробно исследовал вопрос о сложности и глубине схем для Σ_n [20]. Он доказал, что для любого конечного базиса B существует константа C_B такая что

$$D_B(\Sigma_n) \sim C_B \log_2 n.$$

Более того, существуют константа C'_B и схема $S^{\Sigma}_{B,n}$ такие что

$$D_B(S^{\Sigma}_{B,n}) \sim C_B \log_2 n,$$
$$L_B(S^{\Sigma}_{B,n}) \lesssim C'_B n.$$

В частности, для базиса $B_0 = \{\&, \vee, ^-\}$

$$D_{B_0}(S^{\Sigma}_{B_0,n}) \sim \log_2 n,$$
$$L_{B_0}(S^{\Sigma}_{B_0,n}) \lesssim 12n.$$

Умножение. Очевидно, что «школьный» алгоритм для умножения имеет сложность порядка n^2. До недавнего времени считалось, что такая сложность необходима. Однако это было опровергнуто результатом А. А. Карацубы, который доказал, что

$$L(M_n) \lesssim n^{\log_2 3}$$

($\log_2 3 \approx 1,585$) [9]. Метод Карацубы основан на разбиении $2n$-разрядных чисел на n-разрядные. При этом умножение двух $2n$-разрядных чисел сводится к трем (а не четырем!) умножениям n-разрядных чисел и нескольким операциям с линейной относительно n сложностью:

$$L(M_{2n}) \leqslant 3L(M_n) + C'n.$$

Разбиение множителей на большее (конечное) число частей было осуществлено А. Л. Тоомом и привело к следующему результату [18].

Для любого $\varepsilon > 0$ существует число C_ε, такое что

$$L(M_n) < C_\varepsilon n^{1+\varepsilon},$$

*) Буквой C (иногда со штрихами) здесь и далее обозначаются числовые константы, в разных случаях, вообще говоря, различные. — Прим. ред.

а разбиение на растущее (с ростом n) число частей дает оценку

$$L(M_n) \leqslant C' n^{1+\frac{C''}{\sqrt{\log n}}}.$$

Дальнейшее продвижение было получено при применении быстрого преобразования Фурье. По-видимому, первый результат здесь был получен Н. С. Бахваловым, [установившим] оценку

$$L(M_n) \lesssim n(\log n)^3.$$

Наиболее сильный результат в этом направлении был получен А. Шенхаге и В. Штрассеном [28]*):

$$L(M_n) \lesssim n \log n \log\log n.$$

Эта оценка уже близка к линейной (но нелинейная). Заметим, что до настоящего времени не получено никаких нелинейных нижних оценок сложности схем из функциональных элементов в полных булевых базисах для «конкретных» функций или систем функций (нелинейных относительно суммы «число входов» + «число реализуемых функций»).

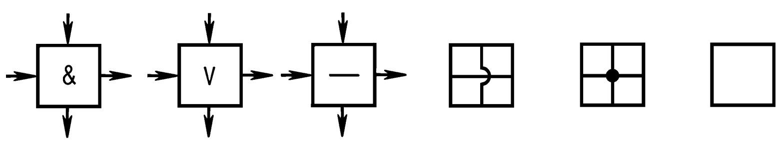

Рис. 1

Значительное различие в сложности реализации операторов сложения и умножения проявляется в другом классе схем (интенсивно изучавшемся в последние десятилетия) — в классе так называемых клеточных схем [11, 22]. Грубо говоря, это схемы, построенные из элементов рис. 1, образующие прямоугольник и удовлетворяющие определению схем из функциональных элементов. Сложность схемы определяется как число всех элементов схемы (т. е. «площадь» прямоугольника). Входы и выходы схемы располагаются на ее периметре. Легко построить такую схему для оператора сложения Σ_n со сложностью порядка n (при подходящем расположении входов и выходов). Для оператора умножения M_n может быть построена схема со сложностью порядка n^2 (например, при использовании «школьного» алгоритма умножения). Однако любая схема для M_n (в классе схем из клеточных элементов) при любом расположении входов и выходов имеет сложность по порядку не менее n^2.

Дискретные приближения непрерывных функций

А. Н. Колмогоров был инициатором исследований в области сложности дискретных приближений непрерывных функций [10].

Пусть $f(x)$ — непрерывная функция, $x \in [0, 1)$, $f(x) \in [0, 1)$. Определим множество F_f булевых (n, n)-функций

$$\widetilde{f}(x_1, \ldots, x_n) = (f^{(1)}(x_1, \ldots, x_n), \ldots, f^{(n)}(x_1, \ldots, x_n)),$$

удовлетворяющих следующим условиям.

) Этот результат недавно существенно усилил М. Фюрер [24] (см. примечания в конце статьи). — Прим. ред.

Для любого булева набора $(\alpha_1, \ldots, \alpha_n)$ длины n положим $a = \sum_{i=1}^{n} \frac{\alpha_i}{2^i}$ и для $(\beta_1, \ldots, \beta_n) = \widetilde{f}(\alpha_1, \ldots, \alpha_n)$ пусть $b = \sum_{i=1}^{n} \frac{\beta_i}{2^i}$. Тогда $\widetilde{f}(x_1, \ldots, x_n) \in F_f$ тогда и только тогда, когда для любого набора $(\alpha_1, \ldots, \alpha_n)$

$$|f(a) - b| \leqslant \frac{1}{2^n}.$$

Для любой непрерывной функции $f(x)$ обозначим через $L(f)$ наименьшую из сложностей функций $\widetilde{f}$ из F_f.

Пусть Φ — некоторый класс непрерывных функций. Введем обозначение

$$L(\Phi, n) = \max_{f \in \Phi} L(f)$$

(это определение корректно, так как число соответствующих функций $\widetilde{f}$ конечно).

Первые результаты в направлении исследования функций $L(\Phi, n)$ для различных классов Φ были получены Ю. П. Офманом [17]. Затем они были продолжены А. В. Тогером [19], [Е. А. Асариным [3], Ю. Маковозом [25], Г. Г. Аманжаевым [1]] и другими. Соответствующие результаты приведены в таблице.

Таблица

Обозначение класса	Определение	Оценки
M^r	[Дифференцируемые r раз] функции, $\lvert f^{(r)}\rvert \leqslant 1$	$L(M^r, n) \asymp \frac{2^{n/r}}{n}$ Ю. П. Офман, 1963 [17]
A	Аналитические функции, $\max\left\lvert\frac{f^{(r)}}{r!}\right\rvert \leqslant \left(\frac{1}{2}\right)^r$	$\frac{n^2}{\log n} \lesssim L(A, n) \lesssim n^{2+\varepsilon}$ Ю. П. Офман, 1963 [17] $L(A, n) \lesssim n^2 \log n \log\log n$ Е. А. Асарин, 1984 [3] $L(A, n) \lesssim n^2 \log n$ Г. Г. Аманжаев, 1996 [1]

Другое направление в этой области — дискретные аналоги непрерывных функций, определяемые внутренним образом.

Г. Г. Аманжаев, используя разделенные разности, построил очень тонкую классификацию дискретных аналогов непрерывных функций, имеющую «почти произвольный» порядок роста числа функций в этих классах [2].

Реализация булевых функций схемами в базисах, элементы которых реализуют непрерывные функции. Очевидно, что любая булева функция может быть продолжена (вне булевых наборов) до некоторой непрерывной функции.

Например,

$$\bar{x} \longrightarrow 1 - x,$$
$$x \& y \longrightarrow xy,$$
$$x \vee y \longrightarrow x + y - xy.$$

Будем теперь рассматривать схемы в базисах, элементы которых реализуют непрерывные функции. Базис будем называть B-полным, если для любой булевой функции $f(x_1, \ldots, x_n)$ можно построить схему, реализующую непрерывную функцию, которая на любом наборе из нулей и единиц $(\sigma_1, \ldots, \sigma_n)$ принимает значение $f(\sigma_1, \ldots, \sigma_n)$. Вопрос о сложности реализации булевых функций схемами в таких базисах подробно исследовался С. Б. Гашковым. Приведем некоторые результаты в этом направлении.

Заметим, что схема, реализующая некоторую булеву функцию из некоторого класса, является кодом этой функции. Этот код «сам себя декодирует». Информация о реализуемой функции содержится, с одной стороны, в структуре схемы и, с другой стороны, в функциях элементов схемы. В случае конечных базисов основная информация содержится в структуре схемы. Возникает вопрос, можно ли, имея базисные функции от ограниченного числа переменных, значительную часть информации о реализуемой функции поместить внутрь элементов схемы.

С. Б. Гашков подробно исследовал различные возникающие здесь ситуации [4]. В частности, установил возможность кодирования булевой функции посредством помещения информации о ней фактически в одну непрерывную функцию (даже в константу) и относительно простого декодирования. Приведем некоторые характерные результаты. Будем называть базис B почти конечным, если он содержит конечное множество функций и все константы из некоторого ограниченного отрезка. С. Б. Гашков установил, в частности, следующее. Существует аналитическая функция $H(x, y)$ такая, что для почти конечного базиса $B = \{H(x, y), x+1, [0, 1]\}$

$$L_B(n) \sim n.$$

В то же время для базисов, содержащих достаточно гладкие функции, это явление не имеет места. Например, для любого почти конечного базиса B, содержащего только функции, удовлетворяющие условию Липшица, или только рациональные функции, имеет место соотношение [4]

$$L_B(n) \gtrsim 2^{\frac{n}{2}}. \tag{4}$$

Впоследствии Туран и Ватан установили, что оценки вида (4) по порядку неулучшаемы [30].

Реализация приближений непрерывных функций в базисах, элементы которых реализуют непрерывные функции. Хорошо известно, что любая непрерывная функция может быть с любой степенью точности приближена полиномом, т. е. схемой над базисом, содержащим сложение, умножение и (все) действительные константы. Очевидно, что можно обойтись и конечным базисом. Например, $\{x+y, x-y, x \cdot y, \frac{1}{2}\}$.

Повидимому, один из первых результатов [в этом направлении — о сложности реализации приближений действительных чисел схемами,] был получен В. Штрассеном [29].

С. Б. Гашков получил много результатов о сложности приближенной реализации непрерывных функций в «непрерывных базисах». Эти результаты учитывают специфику классов реализуемых функций и формулируются достаточно сложно [5, 6]. Ниже приводятся некоторые характерные результаты.

Пусть:

K — компакт,

$H_\varepsilon(K)$ — его ε-энтропия,

B — конечный базис,

$L_B(f, \varepsilon) = \min L(S)$ (минимум берется по всем схемам S, реализующим функцию f с точностью ε),

$L_B(K, \varepsilon) = \max L_B(f, \varepsilon)$ (максимум берется по всем функциям f из K).

Тогда

$$L_B(K,\varepsilon) \geqslant C_B \frac{H_\varepsilon(K)}{\log_2 H_\varepsilon(K)}\left(1+\frac{\log_2\log_2 H_\varepsilon(K)-O(1)}{\log_2 H_\varepsilon(K)}\right),$$

где C_B — константа, зависящая от базиса; [при этом для «достаточно хороших» компактов и базисов (например, $K = M^r$ и $B = \{x+y, x-y, x\cdot y, \frac{1}{2}\}$)]

$$L_B(K,\varepsilon) \leqslant C_B \frac{H_\varepsilon(K)}{\log_2 H_\varepsilon(K)}\left(1+\frac{C\log_2\log_2 H_\varepsilon(K)+O(1)}{\log_2 H_\varepsilon(K)}\right).$$

Для произвольного почти конечного липшицева базиса B [при любом достаточно малом $\varepsilon > 0$] справедлива оценка

$$L_B(K,\varepsilon) \geqslant C'_B \min\left(\sqrt{H_{2\varepsilon}(K)}, \frac{H_{2\varepsilon}(K)}{\log_2\left(\frac{1}{\varepsilon}\right)}\right),$$

[где C'_B — константа, зависящая от базиса. Эта оценка также достижима в «достаточно хороших» случаях [7*]].

Примечания редактора

Подготовка статьи к печати была Олегом Борисовичем практически завершена, потребовалась лишь минимальная заключительная правка (выделена в тексте квадратными скобками) и восстановление литературных ссылок; добавленная при редактировании литература отмечена звездочкой.

Следует заметить, что со времени написания статьи появилось несколько принципиально важных результатов, относящихся к затронутой в ней проблематике.

1) М. Фюрер [24*] получил новую верхнюю оценку сложности умножения n-разрядных чисел

$$L(M_n) \lesssim n \log n 2^{O(\log^* n)},$$

где $\log^* n$ обозначает «сверхлогарифм» числа n.

Результат Фюрера позволяет, в частности, улучшить верхнюю оценку сложности аналитических функций из [1]:

$$L(A,n) \lesssim \frac{n^2 \log n 2^{O(\log^* n)}}{\log\log n}.$$

2) В. М. Храпченко [21*] установил нетривиальную нижнюю оценку глубины схем сложения n-разрядных чисел в базисе $B_0 = \{\&, \vee, ^-\}$

$$D_{B_0}(\Sigma_n) \geqslant \log_2 n + C' \log_2\log_2\log_2 n - C'',$$

а в самое последнее время М. И. Гринчук [8*] получил новую верхнюю оценку глубины схем сложения

$$D_{B_0}(\Sigma_n) \leqslant \log_2 n + \log_2\log_2 n + C.$$

О. М. Касим-Заде

СПИСОК ЛИТЕРАТУРЫ

1. Аманжаев Г. Г. Дискретные аналоги бесконечно гладких функций // Дискретный анализ и исследование операций.— 1996.— Т. 3, №3. — С. 3–39.
2. Аманжаев Г. Г. О классификации дискретных функций различной гладкости // Докл. РАН. — 1999. — Т. 364, № 4. — С. 439–441.
3. Асарин Е. А. О сложности равномерных приближений непрерывных функций // Успехи математических наук. — 1984. — Т. 39, № 3. — С. 157–169.
4. Гашков С. Б. Сложность реализации булевых функций схемами из функциональных элементов и формулами в базисах, элементы которых реализуют непрерывные функции // Проблемы кибернетики. Вып. 37.— М.: Наука, 1980. — С. 57–118.
5. Гашков С. Б. О сложности приближенной реализации непрерывных функций схемами и формулами в полиномиальных и некоторых других базисах // Математические вопросы кибернетики. Вып. 5.— М.: Наука, 1994. — С. 144–207.
6. Гашков С. Б. О сложности приближенной реализации функциональных компактов в некоторых пространствах и о существовании функций с заданной по порядку сложностью // Фундаментальная и прикладная математика. — 1996. — Т. 2, № 3. — С. 675–774.

7*. Гашков С. Б., Вегнер Я. В. О сложности приближенной реализации липшицевых функций // Вестник МГУ. Математика. Механика.— 2008.— №4. — С. 49–51.

8*. Гринчук М. И. Уточнение верхней оценки глубины сумматора и компаратора // Дискретный анализ и исследование операций.— 2008.— Т. 15, №2. — С. 12–22.

9. Карацуба А., Офман Ю. Умножение многозначных чисел на автоматах // Докл. АН СССР. — 1962. — Т. 145, № 2. — С. 293–294.
10. Колмогоров А. Н. Различные подходы к оценке трудности приближенного задания и вычисления функций // Proc. Intern. Congr. Math. Stockholm, 1963. — P. 369–376. (См.: Колмогоров А. Н. Теория информации и теория алгоритмов. — М.: Наука, 1987. — С. 197–204.)
11. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19.— М.: Наука, 1967. — С. 285–293.
12. Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.
13. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10.— М.: Физматгиз, 1963. — С. 63–97.
14. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14.— М.: Наука, 1965. — С. 31–110.
15. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.
16. Офман Ю. Об алгоритмической сложности дискретных функций // Докл. АН СССР. — 1962. — Т. 145, № 1. — С. 48–51.
17. Офман Ю. О приближенной реализации непрерывных функций на автоматах // Докл. АН СССР. — 1963. — Т. 152, № 4. — С. 823–826.
18. Тоом А. Л. О сложности схем из функциональных элементов, реализующих умножение целых чисел // Докл. АН СССР. — 1963. — Т. 150, № 3. — С. 496–498.
19. Тогер А. В. О сложности некоторых функциональных классов // Докл. АН СССР. — 1971 — Т. 199, № 4. — С. 789–791.
20. Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора // Проблемы кибернетики. Вып. 19.— М.: Наука, 1967. — С. 107–122.

21*. Храпченко В. М. Об одной из возможностей уточнения оценок для задержки параллельного сумматора // Дискретный анализ и исследование операций.— 2007.— Т. 14, №1. — С. 87–93.

22. Шкаликова Н. А. О реализации булевых функций схемами из клеточных элементов // Математические вопросы кибернетики. Вып. 2.— М.: Наука, 1989. — С. 177–197.
23. Яблонский С. В. Введение в дискретную математику. — М.: Высш. шк., 2003. (4-е изд., стер.)

24*. Fürer M. Faster integer multiplication // Proc. 39th Annual ACM Symp. on Theory of Computing. — San Diego (California), 2007. — P. 57–66.

25. Makovoz Y. On the Kolmogorov complexity of functions of finite smoothness // Journal of Complexity. — 1986. — V. 2. — P. 121–130.
26. Sklansky J. Conditional sum addition logic // IRE Trans. Electron. Comput. — 1960. — V. EC-9. — P. 213–226.
27. Sklansky J. An evaluation of several two-summand binary adders // IRE Trans. Electron. Comput. — 1960. — V. EC-9. — P. 226–231.

28. Schönhage A., Strassen V. Schnelle multiplikation grosser Zahlen // Computing, Archiv für elektronisches Reichen. — 1971. — V. 7, № 3–4. — P. 281–292. [Имеется перевод: Шенхаге А., Штрассен В. Быстрое умножение больших чисел // Кибернетич. сб. — Новая серия. Вып. 10. — М.: Мир. — 1973. — С. 87–98.]
29. Strassen V. Berechnungen in partiellen Algebren endlichen Typs // Computing. — 1973. — V. 11, № 3. — P. 181–196.
30. Turán G., Vatan F. On the computation of boolean functions by analog circuit of bounded fan-in // Journal of Computer and System Sciences. — 1997. — V. 54, № 1. — P. 199–212.