

Сложность вычислений в моделях схемного типа (обзор)

Сергеев И.С.

2026

Эволюция теории

1955–1975: классические результаты, построение скелета теории, постановка основных задач

- асимптотические методы синтеза булевых функций, алгоритмы БПФ, быстрое умножение чисел

1975–1995: развитие теории в глубину, создание более тонких методов на основных направлениях

- нижние оценки сложности монотонных схем, тензорные методы умножения матриц, переключательная лемма

1995–2015: развитие теории в ширину, новые модели и направления (в т.ч. квантовые вычисления), активная интеграция со смежными областями

- расширенная иерархия классов сложности, теория коммуникационной сложности

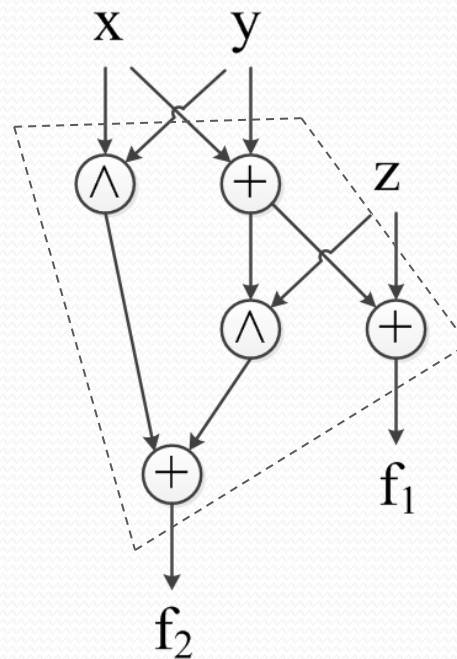
2015–н.в.: углубленное исследование периферийных областей, спецификация комбинаторного и вероятностного инструментария

- методы «подъема» нижних оценок, усиленные варианты леммы о подсолнечнике

Схемы (из ф.э.): булевы, арифметические

базис В

схема S:



сложность
 $C_B(S) = 5$

глубина
 $D_B(S) = 3$

$$x + y + z = 2f_2 + f_1$$

булевы базисы: $B_2 = \{g(x,y)\}$, $B = \{\wedge, \oplus, 1\}$, ...

арифметические базисы: $A = \{+, \times, a \cdot x \mid a \in R\}$, ...

Булевы схемы (нижние оценки)

$\boxed{C(f_n) \geq ?}$ f_n — явно заданная булева функция n переменных
для п.в. функций: $C(f_n) \asymp 2^n/n$ [Muller, 1956; Лупанов, 1958 (асимпт.)]

метод константных подстановок — с 1950-х гг.

в базисе $\mathcal{B}_2 = \{g(x, y)\}$: $C_{\mathcal{B}_2}(f_n) \gtrsim 3n$ [Blum, 1984]

в базисе $\mathcal{U}_2 = \mathcal{B}_2 \setminus \{\oplus, \sim\}$: $C_{\mathcal{U}_2}(f_n) \gtrsim 5n$ [Iwama, Morizumi, 2002]

в базисе $\{\wedge, \neg\}$: $C_{\{\wedge, \neg\}}(f_n) \gtrsim 7n$ [Редькин, 1973]

метод аффинных подстановок [Find, Golovnev, Hirsch, Kulikov, 2015] $\rightarrow$
 $C_{\mathcal{B}_2}(f_n) \gtrsim 3.1n$ [Li, Yang, 2021]

$\boxed{C(F_n) \geq ?}$ F_n — булев (n, n) -оператор

$C_{\mathcal{B}_2}(F_n) \gtrsim C_{\mathcal{B}_2}(f_{n-o(n)}) + 2n \gtrsim 5.1n$ [Сергеев, 2026]

Открытая проблема: $C(f_n) = \omega(n)$ для некоторой последовательности f_n .

Арифметические схемы (нижние оценки)

$$\boxed{C_{\mathcal{A}}(f_n) \geq ?} \quad f_n \in \mathbb{R}[x], \deg f_n = n; \quad \mathcal{A} = \{+, *\} \cup \mathbb{R} \quad (\text{или } \mathbb{C})$$

СЛОЖНОСТЬ ТИПИЧНОГО МНОГОЧЛЕНА:

$\sim n$ сложений, $\sim n/2$ умножений, $\sim \sqrt{n} \dots \sqrt{2n}$ не скалярных операций

[Motzkin; Пан; Белага, 1950-е; Paterson, Stockmeyer, 1973]

Нижние оценки (основаны на приложении алгебраической геометрии):

[Strassen, 1974] ... [Schnorr, Van de Wiele, 1978–80] [Heintz, Sieveking, 1980]

$\rightarrow \sim n$ сложений, $\sim n/2$ умножений, $\Omega(\sqrt{n})$ не скалярных операций

Примеры: $\sum_{k=0}^n 2^{2^{kn^2}} x^k$, $\sum_{k=0}^n e^{2\pi i/p_k} x^k$, $\mathbb{P} = \{p_0, p_1, \dots\}$

Открытая проблема: построить явные примеры трудновычислимых многочленов с 0/1-коэффициентами.

▷ для $f_n \in \mathbb{R}[x_1, \dots, x_n]$, $\deg f = d$: $C_{\mathcal{A}}(f_n) \succeq n \log d$ [Baur, Strassen, 1983] 0/1

Пример: $\sum_{k=1}^n x_i^d$

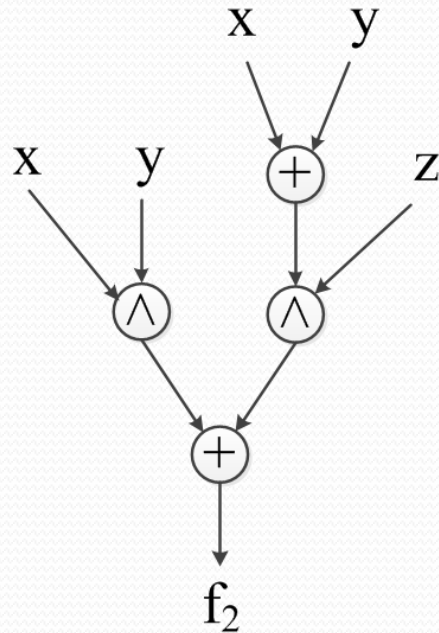
Формулы

формула = схема без ветвлений

$$F = xy \oplus z(x \oplus y)$$



сложность $\Phi_B(F) = 5$



глубина $D_B(F) = 3$

Булевы формулы

$$\boxed{\Phi(f_n) \geq ?}$$

f_n — явно заданная булева функция n переменных

для п.в. функций $\Phi(f_n) \asymp 2^n / \log n$ [Riordan, Shannon, 1942; Лупанов, 1960 (ас.)]

в базисе $\mathcal{B}_2 = \{g(x, y)\}$:

для универсальных функций: $\Phi_{\mathcal{B}_2}(f_n) \succeq \frac{n^2}{\log n}$ [Нечипорук, 1966]

для симметрических функций: $\Phi_{\mathcal{B}_2}(f_n) \succeq n \log n$, $\Phi(f_n) \succeq n \log n$
[Fischer, Meyer, Paterson, 1982]; [Черухин, 2000]

в базисе $\mathcal{B}_0 = \{\wedge, \vee, \neg\}$:

метод случайных подстановок $\rightarrow$ оценки на экспоненту сжатия базиса

для функции Андреева: $\Phi_{\mathcal{B}_0}(f_n) \succeq \frac{n^3}{\gamma(\log n)}$

$\gamma(x) = x^{7/2} \log^3 x$ [Håstad, 1998], $\gamma(x) = x^2 \log x$ [Tal, 2014]

для другой функции: $\Phi_{\mathcal{B}_0}(f_n) \succeq \frac{n^3}{\gamma(\log n)}$, $\gamma(x) = x \log^2 x$ [Tal, 2017]

Открытая проблема: $\mathsf{C}_{\mathcal{B}_2}(\text{Sym}_n) \asymp n^{1+\Theta(1)}$, где Sym_n — симметрические функции n переменных?

Глубина и сложность формул

Открытая проблема: нижние оценки глубины, независимые от сложности формул в полных базисах арифметического типа.

▷ в бинарных базисах тривиально выполнено $D(f) \geq \log_2 \Phi(f)$

$D_{\mathcal{B}}(f) \asymp \log \Phi_{\mathcal{B}}(f)$ в булевых и арифметических базисах $\mathcal{B}$

[Храпченко, 1968] [Brent, Kuck, Maruyama, 1973] [Угольников; Ragaz, 1987]

Примеры:

$\mathcal{B}$ — неарифм. полный: $D_{\mathcal{B}}(f_n) \gtrsim 2 \log_2 \Phi_{\mathcal{B}}(f_n)$, $\mathcal{B} = \{\setminus\}$ [Храпченко, 1967]

мон. арифм. $\mathcal{A}_+ = \{+, *\}$: $D_{\mathcal{A}_+}(f_n) \gtrsim 1.5 \log_2 \Phi_{\mathcal{A}_+}(f_n)$ [Coppersmith, Schieber, 1992]

монот. булев $\mathcal{B}_M = \{\vee, \wedge\}$: $D_{\mathcal{B}_M}(f_n) \gtrsim 1.06 \log_2 \Phi_{\mathcal{B}_M}(f_n)$ [Сергеев, 2019]

Верхние оценки:

для п.в. функций $D(f_n) \asymp n$ [Riordan, Shannon, 1942; Лупанов, 1970 (асимп.)]

Открытая проблема: верно ли $D(\text{НОД}_n) \ll n$, где НОД_n — оператор НОД n -разрядных чисел?

▷ $S(\text{НОД}_n) \leq n \log^2 n$; НОД многочленов вычисляется параллельными схемами

Монотонные булевы схемы (нижние оценки)

$\boxed{C_{\mathcal{B}_M}(f_n) \geq ?}$ f_n — монотонная булева функция n переменных; $\mathcal{B}_M = \{\vee, \wedge\}$

для п.в. функций: $C_{\mathcal{B}_M}(f_n) \asymp 2^n / n^{3/2}$ [Редькин, 1979; Андреев, 1988 (асимпт.)]

метод ДНФ/КНФ приближений [Андреев; Разборов, 1985] $\rightarrow$

$$C_{\mathcal{B}_M}(f_n) \succeq 2^{n^{1/3-o(1)}} \quad [\text{Андреев, 1987}]$$

$$C_{\mathcal{B}_M}(Per_n) \succeq n^{\Omega(\log n)}, \quad Per_n \text{ — логический перманент} \quad [\text{Разборов, 1985}]$$

$$C_{\mathcal{B}_M}(f_n) \succeq 2^{n^{1/6-o(1)}}, \quad C(f_n) = n^{O(1)} \quad [\text{Tardos, 1987}]$$

специальная модификация леммы о подсолнечнике $\rightarrow$

$$C_{\mathcal{B}_M}(f_n) \succeq 2^{n^{1/2-o(1)}} \quad [\text{Cavalar, Kumar, Rossman, 2020}]$$

$$C_{\mathcal{B}_M}(Per_n) \succeq 2^{n^{1/3-o(1)}} \quad [\text{Cavalar, Göös, Riazanov, Sofronova, Sokolov, 2025}]$$

+ метод подъема нижних оценок $\rightarrow$

$$C_{\mathcal{B}_M}(f_n) \succeq 2^{n^{1/3-o(1)}}, \quad C(f_n) = n^{O(1)} \quad [\text{de Rezende, Vinyals, 2025}]$$

Открытая проблема: $C_{\mathcal{B}_M}(Maj_n) \succ n^2$, где Maj_n — функция голосования?

Монотонные арифм. схемы (нижние оценки)

$\boxed{C_{\mathcal{A}_+}(f_n) \geq ?}$ $f_n \in \mathbb{R}_+[x_1, \dots, x_n]$ — мультилинейный многочлен;

$\boxed{C_{\mathcal{A}_+}(g_n) \geq ?}$ $g_n \in \mathbb{R}_+[x]$, $\deg g_n = n$; $\mathcal{A}_+ = \{+, *\} \cup \mathbb{R}_+$

для случайных многочленов: $C_{\mathcal{A}_+}(f_n) \asymp 2^n$, $C_{\mathcal{A}_+}(g_n) \asymp n$.

множество мономов не содержит удобных для вычисления структур $\rightarrow$

$C_{\mathcal{A}_+}(f_n) \succeq 2^{n^{1/2-o(1)}}$ [Schnorr, 1976], [Jerrum, Snir, 1982] 0/1-коэфф.

$\dots$ $C_{\mathcal{A}_+}(f_n) \succeq 2^{n-o(n)}$, $C_{\mathcal{A}_+}(g_n) \succeq n^{1-o(1)}$ [Гашков, Сергеев, 2012] 0/1

$C_{\mathcal{A}_+}(f_n) = 2^{\Omega(\sqrt{n})}$, $C_{\mathcal{A}}(f_n) = n^{O(1)}$ [Valiant, 1980] 0/1

$C_{\mathcal{A}_+}(f_n) = 2^{\Omega(n)}$, $C_{\mathcal{A}}(f_n) = n^{O(1)}$ коэфф. $\in n^{O(1)}$

[Cavalar, Fabris, Mukhopadhyay, Srinivasan, Yehudayoff, 2025]

Открытая проблема: примеры многочленов $C_{\mathcal{A}_+}(f_n) = 2^{\Omega(n)}$, $C_{\mathcal{A}}(f_n) = n^{O(1)}$ с 0/1 коэффициентами, и для одной переменной: $C_{\mathcal{A}_+}(g_n) = n^{\Omega(1)}$, $C_{\mathcal{A}}(g_n) = \log^{O(1)} n$.

Монотонные арифметические схемы

Эффект деления $\mathcal{A}_/ = \{+, *, /\} \cup \mathbb{R}$, $\mathcal{A}_{+,/} = \{+, *, /\} \cup \mathbb{R}_+$

$$C_{\mathcal{A}}(f) \preceq d \log d \cdot C_{\mathcal{A}_/}(f), \quad f \in \mathbb{R}[X], \quad d = \deg f \quad [\text{Strassen, 1973}]$$

(!) в $\mathcal{A}_{+,/}$ вычислимы немонот. многочлены: $x^2 - xy + y^2 = (x^3 + y^3)/(x + y)$

$C_{\mathcal{A}_{+,/}}(ST_n) \preceq n^3$, $C_{\mathcal{A}_+}(ST_n) \succeq 2^{\Omega(\sqrt{n})}$ ST_n — многочлен Кирхгофа
(перечисляющий остовные деревья в полном n -вершинном графе)

[Fomin, Grigoriev, Koshevoy, 2016] [Jerrum, Snir, 1982; Jukna, Seiwert, 2019]

Тропические схемы (алгоритмы динамич. программир.): $\mathcal{T}_+ = \{\min, +\} \cup \mathbb{R}_+$

Открытая проблема: верно ли, что $C_{\mathcal{T}_+}(PATH_n) \asymp n^3$, где $PATH_n$ — тропический многочлен, вычисляющий кратчайший путь между двумя полюсами n -вершинного графа (оптимальность алгоритма Беллмана–Форда–Мура)?

▷ сложность вычисления кратчайших путей между всеми парами равна $\Theta(n^3)$

Глубина и сложность

класс NC^k : (равномерные) схемы сложности $n^{O(1)}$ и глубины $O(\log^k n)$

класс $\text{NC}_{\mathcal{A}}^k$: аналогично для арифметических схем

умножение, деление $\in \text{NC}^1$ [фольклор; Beame, Cook, Hoover, 1986]

« $\text{P}_{\mathcal{A}} = \text{NC}_{\mathcal{A}}^2$ » для арифм. схем [Valiant, Skyum, Berkowitz, Rackoff, 1983]

в частности, определитель $\in \text{NC}_{\mathcal{A}}^2$

[Berkowitz, 1982; Borodin, von zur Gathen, Hopcroft, 1982]

НОД многочленов $\in \text{NC}_{\mathcal{A}}^1$ (кусочно) [Andrews, Wigderson, 2024] $\mathbb{R}, \mathbb{C}$

Открытая проблема: логический перманент $\in \text{NC}^k$?

▷ доказано существование схем сложности $n^{O(1)}$ и глубины $O(\log^2 n)$ [BGH82]

Открытая проблема: можно ли оператор максимума n чисел длины n реализовать булевыми схемами сложности $O(n^2)$ и глубины $O(\log n)$?

Умножение

$$\boxed{C(M_n) \geq ?}$$

M_n — оператор умножения n -разрядных чисел

$$C(M_n) \preceq n^{\log_2 3} \quad [\text{Карацуба, 1960}] \rightarrow$$

+ интерполяция [Тоом], + БПФ [Бахвалов, Карацуба]

$$\rightarrow C(M_n) \preceq n \log n \log \log n \quad [\text{Schönhage, Strassen, 1971}]$$

+ аккуратный выбор кольца для интерполяции $\rightarrow$

$$C(M_n) \preceq n \log n \cdot 2^{O(\log^* n)} \quad [\text{Fürer, 2007}]$$

+ приближение БПФ _{N} при помощи БПФ _{2^n} $\rightarrow$

$$C(M_n) \preceq n \log n \quad [\text{Harvey, van der Hoeven, 2019}]$$

$$\boxed{C_{\mathcal{A}}(M_n^R) \geq ?}$$

M_n^R — оператор умножения многочленов $\deg < n$ из $R[x]$

$$C_{\mathcal{A}}(M_n^{\mathbb{C}}) \preceq n \log n \quad [\text{Cooley, Tukey, 1965}] \quad \text{БПФ}$$

$$C_{\mathcal{A}}(M_n^R) \preceq n \log n \log \log n \quad [\text{Cantor, Kaltofen, 1991}] \quad \text{произв. кольцо } R$$

$$C_{\mathcal{A}}(M_n^R) \preceq n \log n \cdot 2^{O(\log^* n)} \quad [\text{Harvey, van der Hoeven, Lecerf, 2014}]$$

Открытая проблема: $C_{\mathcal{A}}(M_n^R) \preceq n \log n$?

▷ выполняется в $\mathbb{R}, \mathbb{C}$; имеется алгоритм, основанный на допущениях [HvdH19]

Умножение матриц

$$\boxed{C_A(MM_n) \geq ?}$$

MM_n — оператор умножения $n \times n$ -матриц (над R)

$$C_A(MM_n) \preceq n^{\log_2 7} \quad [\text{Strassen, 1968}]$$

1970–1980-е:

- трилинейное представление [Пан]
- приближенные вычисления (граничный ранг) [Bini]
- метод прямых сумм [Schönhage]
- лазерный метод [Strassen]

$$\dots \quad C_A(MM_n) \preceq n^{2.376} \quad [\text{Coppersmith, Winograd, 1986}]$$

анализ степеней тензора Винограда–Копперсмита [Stothers, 2010]

$$\dots \quad C_A(MM_n) \preceq n^{2.372}$$

[Alman, Duan, Vassilevska Williams, Xu, Xu, Zhou, 2024]

Открытая проблема: $C_A(MM_n) = n^{2+o(1)}$?

Умножение $n \times n$ - и $n \times n^\alpha$ -матриц: $C_A(MM_{n,n,n^\alpha}) = n^{2+o(1)}$

$\alpha > 0.294$ [Coppersmith, 1996] $\dots$ $\alpha > 0.321$ [WXXZ, 2023]

Умножение матриц, модулярная композиция

Практически значимые методы (экономные трилинейные декомпозиции):

$$C_A(MM_n) \preceq n^{2.774} \quad [\text{Pan}, 1982], \quad [\text{Schwartz}, \text{Zwecher}, 2025]$$

Альтернативные представления: пример для MM_2 :

стандартное: 7 умножений, 15 сложений [Strassen, Winograd]

альтернативное: 7 умножений, 12 сложений [Bodrato, 2010]

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \rightarrow \begin{bmatrix} x_{11} & x_{12} - x_{21} + x_{22} \\ x_{22} - x_{21} & x_{12} + x_{22} \end{bmatrix}$$

Модулярная композиция

$$C_A(MC_n) = ?, \quad C_A(MC_n^*) = ?$$

MC_n вычисляет $f(g(x)) \bmod h(x)$; MC_n^* вычисляет $f(g(x)) \bmod x^n$, $\deg f, g, h = n$

$$C_A(MC_n) \prec n^{1.7}, \quad C_A(MC_n^*) \preceq C_A(M_n) \cdot \sqrt{n \log n} = n^{1.5+o(1)} \quad [\text{Brent}, \text{Kung}, 1978]$$

идея интерполяции $\rightarrow C_A(MC_n) = n^{1+o(1)} \quad [\text{Umans}, 2008] \quad GF(p^k), \quad p \text{ мало}$

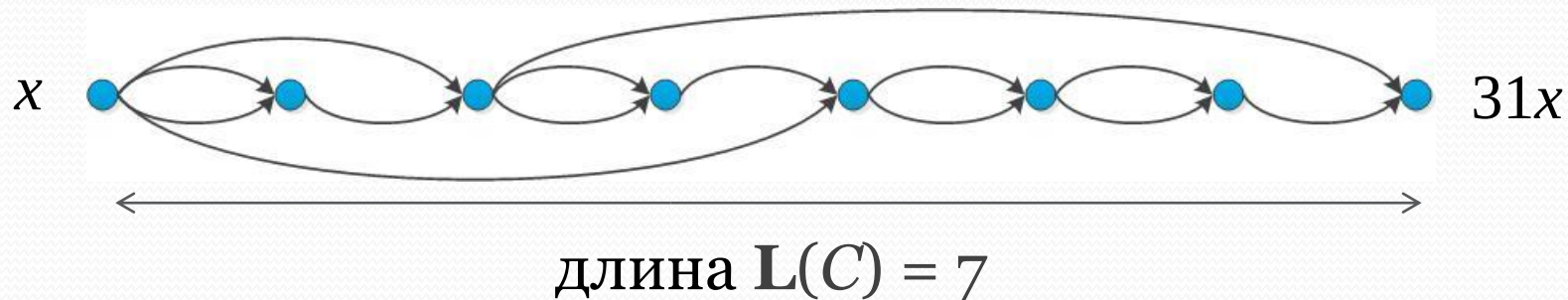
сведение к вычислению члена рекуррентной последовательности $\rightarrow$

$$C_A(MC_n^*) \preceq C_A(M_n) \cdot \log n \quad [\text{Kinoshita}, \text{Li}, 2024]$$

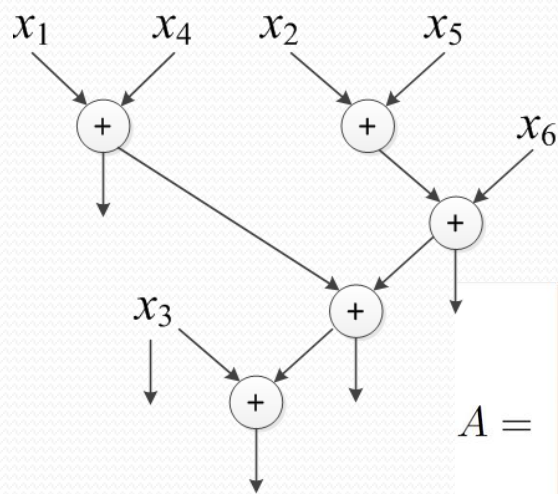
Открытая проблема: $C_A(MC_n) = n^{1+o(1)}$ в общем случае (хотя бы над $\mathbb{R}$ и $\mathbb{C}$)?

Аддитивные цепочки

C: 1, 2, 3, 6, 7, 14, 28, 31



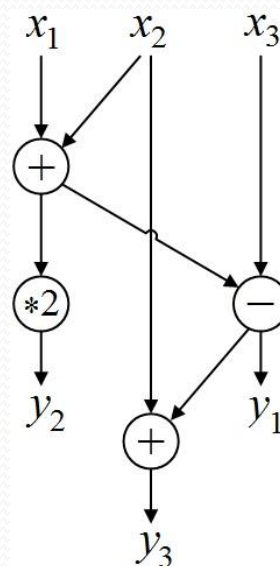
Аддитивные схемы



$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$y = A \cdot x$$

Линейные (арифм.) схемы



$$A = \begin{bmatrix} 1 & 1 & -1 \\ 2 & 2 & 0 \\ 1 & 2 & -1 \end{bmatrix}$$

Линейные схемы (нижние оценки)

аддитивные цепочки: $L(n) \sim \log_2 n$ [Brauer, 1939]

аддитивные схемы: $L(A_n) \asymp n^2 / \log_2 n$ для $0/1$ $n \times n$ -матриц
[Лупанов, 1956; Нечипорук, 1963 (асимпт.)]

линейные схемы: $L(A_n) \asymp n^2$ для $n \times n$ -матриц над $\mathbb{R}$ (или $\mathbb{C}$)

Нижние оценки:

монот. вычисления $0/1$ матриц (в $(\mathbb{B}, \vee)$ или $\mathbb{Z}_+$): $L(A_n) = n^{2-o(1)}$ [Андреев, 1986]

схемы над $\mathbb{C}$: $L(A_n) \gtrsim n^2 / \log n$ [Heintz, Sieveking, 1980]

Открытая проблема: аддитивные цепочки: явно построить множество $\mathbf{m} = \{m_1, \dots, m_n\}$, $m_i \in n^{O(1)}$ сложности $L(\mathbf{m}) = n + \Omega(n)$.

▷ верхняя оценка $L(\mathbf{m}) = n + O(n)$; получено: $L(\mathbf{m}) = n + \Omega(n^{1-\varepsilon})$ [Сергеев, 2024]

Открытая проблема: схемы над $GF(2)$: $L(A_n) = \omega(n)$ для некоторой последовательности матриц $A_n \in GF(2)^{n \times n}$.

▷ известная оценка: $L(A_n) \gtrsim 5n$ [Сергеев, 2025]

Открытая проблема: линейные схемы над $\mathbb{R}$ (или $\mathbb{C}$): $L(A_n) = \omega(n)$ для последовательности $n \times n$ -матриц A_n с $0/1$ -коэффициентами.

▷ есть оценки для схем с ограничениями на константы

Коммуникационная сложность

А



В



... 0 1 0 ... 1 1 0 1 ... 0 1 ...



игра $G[f]$

знает X

знает Y

! должны выяснить $f(X, Y)$ за возможно меньшее число битов коммуникации

$cc(G[f])$ – минимально возможный объём коммуникации

Коммуникационная сложность и глубина

$\boxed{D[f]}$ $A : x \in f^{-1}(1)$ $B : y \in f^{-1}(0)$ найти $i : x_i \neq y_i$.

$\boxed{D_+[f]}$ f — монот., $A : x \in f^{-1}(1)$ $B : y \in f^{-1}(0)$ найти $i : x_i > y_i$.

$$\text{cc}(D[f]) = D_{\mathcal{B}_0}(f), \quad \mathcal{B}_0 = \{\wedge, \vee, \neg\}$$

$$\text{cc}(D_+[f]) = D_{\mathcal{B}_M}(f), \quad \mathcal{B}_M = \{\wedge, \vee\} \quad [\text{Karchmer, Wigderson, 1990}]$$

Применения:

$D_{\mathcal{B}_M}(Stcon_n) \asymp \log^2 n$, $Stcon_n$ — функция st -проводимости n -вершинного графа
[Karchmer, Wigderson, 1990]

$D_{\mathcal{B}_M}(Per_n) \asymp n$, Per_n — логический перманент [Raz, Wigderson, 1992]

$D_{\mathcal{B}_M}(CL_{n,k}) \asymp k \log n$ при $k \leq n^\varepsilon$, $CL_{n,k}$ — функция наличия k -клики в графе
[Raz, McKenzie, 1997]

$\boxed{CIS[G]}$ $A : \text{клика } a \text{ в графе } G$ $B : \text{независ. множ. } b \subset G$ найти $|a \cap b|$

для графа $G = (V, E)$ выполнено $\text{cc}(CIS[G]) \preceq \log^2 |V|$ [Yannakakis, 1991]

метод подъема нижних оценок [Göös, 2015] $\rightarrow$

$\exists G : \text{cc}(CIS[G]) \asymp \log^{2-o(1)} |V|$ [Balodis, 2021]

темы, не вошедшие в доклад:

- машины Тьюринга, программы с памятью
- схемы над бесконечными базисами, схемы ограниченной глубины
- деревья решений, контактные схемы и ветвящиеся программы
- недетерминированные схемы и др. модели
- квантовые вычисления
- вероятностные (рандомизированные) алгоритмы
- средняя сложность / приближенные вычисления
- некоммутативные вычисления
- задачи комбинаторной оптимизации
- теоретико-числовые алгоритмы
- классификационные задачи иерархии сложностных классов