

Complexity of circuit-type computations (survey)

Sergeev I.S.

2026

Evolution of the theory

1955–1975: classical results, construction of the theory's skeleton, formulation of the main problems

- theory of asymptotic synthesis of boolean functions, FFT algorithms, fast integer multiplication

1975–1995: development of the theory in depth, creation of more sophisticated methods in the main areas

- lower bounds for the complexity of monotone circuits, tensor methods of matrix multiplication, switching lemma

1995–2015: development of the theory in breadth, new models and directions (including quantum computing), active integration with related fields

- extended hierarchy of complexity classes, theory of communication complexity

2015–present: in-depth study of peripheral domains, specification of combinatorial and probabilistic tools

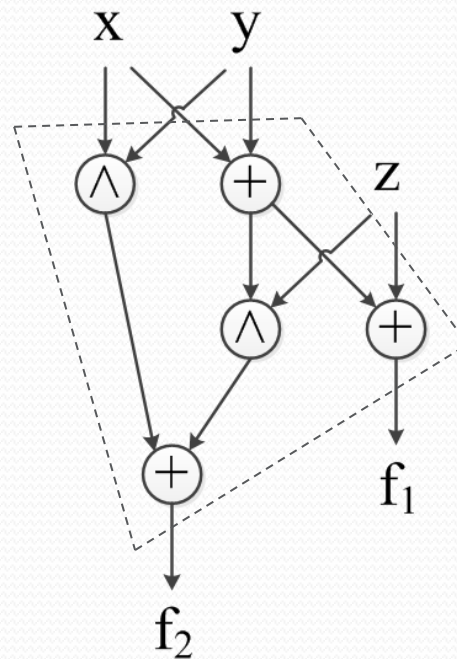
- lower bound “lifting” methods, strengthened versions of the sunflower lemma

Circuits (from f.e.): boolean, arithmetic

basis B

circuit S:

complexity
 $C_B(S) = 5$



depth
 $D_B(S) = 3$

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

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

arithmetic bases: $A = \{+, \times, a \cdot x \mid a \in \mathbb{R}\}$, ...

Boolean circuits (lower bounds)

$\boxed{\mathsf{C}(f_n) \geq ?}$ f_n — explicit boolean function of n variables

for almost all functions: $\mathsf{C}(f_n) \asymp 2^n/n$ [Muller, 1956; Lupanov, 1958 (asympt.)]

method of constant substitutions — since 1950s:

over basis $\mathcal{B}_2 = \{g(x, y)\}$: $\mathsf{C}_{\mathcal{B}_2}(f_n) \gtrsim 3n$ [Blum, 1984]

over basis $\mathcal{U}_2 = \mathcal{B}_2 \setminus \{\oplus, \sim\}$: $\mathsf{C}_{\mathcal{U}_2}(f_n) \gtrsim 5n$ [Iwama, Morizumi, 2002]

over basis $\{\wedge, \neg\}$: $\mathsf{C}_{\{\wedge, \neg\}}(f_n) \gtrsim 7n$ [Red'kin, 1973]

method of affine substitutions [Find, Golovnev, Hirsch, Kulikov, 2015] $\rightarrow$

$\mathsf{C}_{\mathcal{B}_2}(f_n) \gtrsim 3.1n$ [Li, Yang, 2021]

$\boxed{\mathsf{C}(F_n) \geq ?}$ F_n — boolean (n, n) -operator

$\mathsf{C}_{\mathcal{B}_2}(F_n) \gtrsim \mathsf{C}_{\mathcal{B}_2}(f_{n-o(n)}) + 2n \gtrsim 5.1n$ [Sergeev, 2026]

Open problem: $\mathsf{C}(f_n) = \omega(n)$ for some sequence f_n .

Arithmetic circuits (lower bounds)

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

complexity of typical polynomials:

$\sim n$ additions, $\sim n/2$ multiplications, $\sim \sqrt{n} \dots \sqrt{2n}$ nonscalar operations

[Motzkin; Pan; Belaga, 1950s; Paterson, Stockmeyer, 1973]

Lower bounds (based on applications of algebraic geometry):

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

$\rightarrow \sim n$ additions, $\sim n/2$ multiplications, $\Omega(\sqrt{n})$ nonscalar operations

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

Open problem: construct explicit examples of hard-to-compute polynomials with 0/1-coefficients.

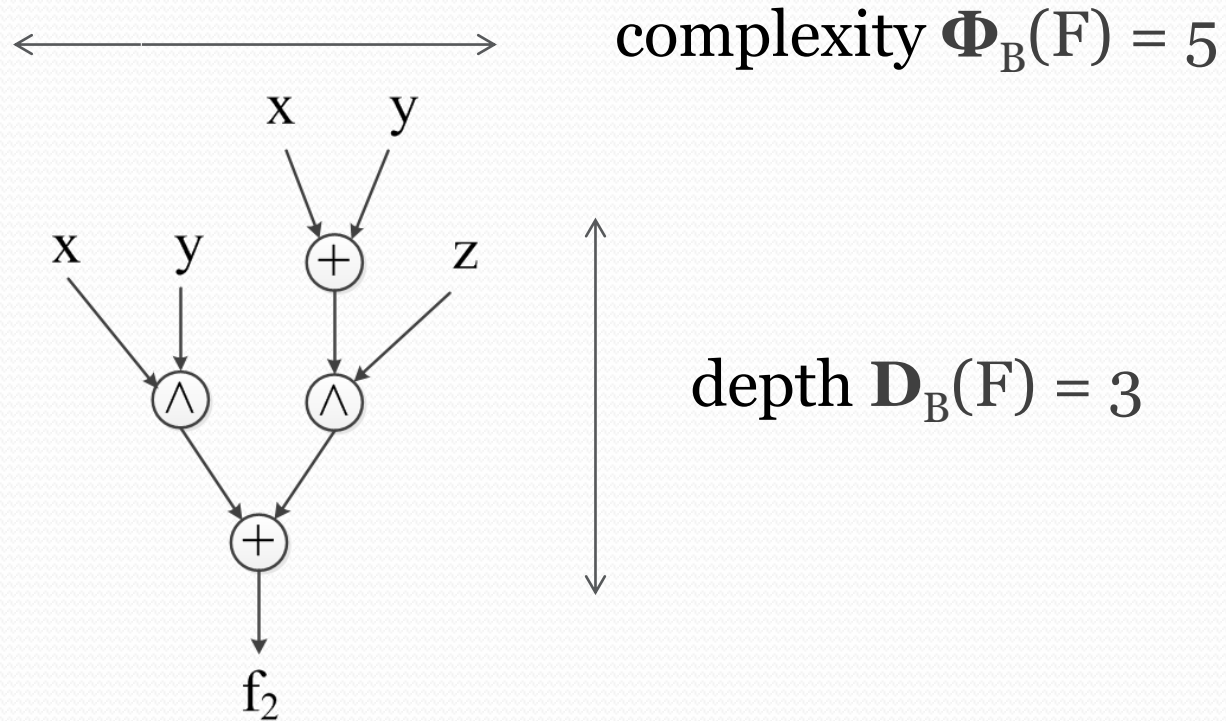
▷ for $f_n \in \mathbb{R}[x_1, \dots, x_n]$, $\deg f = d$: $C_{\mathcal{A}}(f_n) \succeq n \log d$ [Baur, Strassen, 1983] 0/1

Example: $\sum_{k=1}^n x_i^d$

Formulae

formula = circuit with gate fanout 1

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



Boolean formulae

$\boxed{\Phi(f_n) \geq ?}$ f_n — explicit boolean function of n variables

for a.a. functions: $\Phi(f_n) \asymp 2^n / \log n$ [Riordan, Shannon, 1942; Lupanov, 1960 (as.)]

over basis $\mathcal{B}_2 = \{g(x, y)\}$:

for universal functions: $\Phi_{\mathcal{B}_2}(f_n) \succeq \frac{n^2}{\log n}$ [Nechiporuk, 1966]

for symmetric functions: $\Phi_{\mathcal{B}_2}(f_n) \succeq n \log n$, $\Phi(f_n) \succeq n \log n$
[Fischer, Meyer, Paterson, 1982]; [Cherukhin, 2000]

over basis $\mathcal{B}_0 = \{\wedge, \vee, \neg\}$:

method of random substitutions $\rightarrow$ bounds for shrinkage exponents of bases

for Andreev function: $\Phi_{\mathcal{B}_0}(f_n) \succeq \frac{n^3}{\gamma(\log n)}$

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

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

Open problem: $\mathsf{C}_{\mathcal{B}_2}(\text{Sym}_n) \asymp n^{1+\Theta(1)}$, where Sym_n — symmetric functions of n variables?

Depth vs complexity of formulae

Open problem: depth lower bound techniques independent of formula complexity
lower bounds in complete arithmetic-type bases.

▷ in binary bases trivially holds: $D(f) \geq \log_2 \Phi(f)$

$\boxed{D_{\mathcal{B}}(f) \asymp \log \Phi_{\mathcal{B}}(f)}$ in boolean and arithmetic bases $\mathcal{B}$

[Khrapchenko, 1968] [Brent, Kuck, Maruyama, 1973] [Ugol'nikov; Ragaz, 1987]

Examples:

$\mathcal{B}$ — nonarithm. complete: $D_{\mathcal{B}}(f_n) \gtrsim 2 \log_2 \Phi_{\mathcal{B}}(f_n)$, $\mathcal{B} = \{\setminus\}$ [Khrapchenko, 1967]

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

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

Upper bounds:

for a.a. functions: $D(f_n) \asymp n$ [Riordan, Shannon, 1942; Lupanov, 1970 (asympt.)]

Open problem: can we prove $D(\text{GCD}_n) \ll n$, where GCD_n is GCD operator of n -bit integers?

▷ $C(\text{GCD}_n) \preceq n \log^2 n$; polynomial GCD may be implemented by parallel circuits

Monotone boolean circuits (lower bounds)

$\boxed{\mathsf{C}_{\mathcal{B}_M}(f_n) \geq ?}$ f_n — monotone boolean function of n variables; $\mathcal{B}_M = \{\vee, \wedge\}$
for a.a. functions: $\mathsf{C}_{\mathcal{B}_M}(f_n) \asymp 2^n / n^{3/2}$ [Red'kin, 1979; Andreev, 1988 (asympt.)]

method of DNF/CNF approximations [Andreev; Razborov, 1985] $\rightarrow$

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

$$\mathsf{C}_{\mathcal{B}_M}(Per_n) \succeq n^{\Omega(\log n)}, \quad Per_n \text{ — logical permanent} \quad [\text{Razborov, 1985}]$$

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

appropriate modification of the Sunflower lemma $\rightarrow$

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

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

+ lifting lower bounds method $\rightarrow$

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

Open problem: $\mathsf{C}_{\mathcal{B}_M}(Maj_n) \succ n^2$, where Maj_n is the majority function?

Monotone arithmetic circuits (lower bounds)

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

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

for random polynomials: $C_{\mathcal{A}_+}(f_n) \asymp 2^n$, $C_{\mathcal{A}_+}(g_n) \asymp n$.

a set of monomials doesn't contain computationally convenient structures $\rightarrow$

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

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

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

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

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

Open problem: example of multilinear polynomial $C_{\mathcal{A}_+}(f_n) = 2^{\Omega(n)}$, $C_{\mathcal{A}}(f_n) = n^{O(1)}$

with 0/1-coefficients, and of single-variable: $C_{\mathcal{A}_+}(g_n) = n^{\Omega(1)}$, $C_{\mathcal{A}}(g_n) = \log^{O(1)} n$.

Monotone arithmetic circuits

Effect of division $\mathcal{A}_/ = \{+, *, /\} \cup \mathbb{R}$, $\mathcal{A}_{+, /} = \{+, *, /\} \cup \mathbb{R}_+$

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

(!) in $\mathcal{A}_{+, /}$ one can compute nonmon. polynomials: $x^2 - xy + y^2 = (x^3 + y^3)/(x + y)$

$$\mathsf{C}_{\mathcal{A}_{+, /}}(ST_n) \preceq n^3, \quad \mathsf{C}_{\mathcal{A}_+}(ST_n) \succeq 2^{\Omega(\sqrt{n})} \quad ST_n - \text{Kirchhoff polynomial} \\ (\text{enumerating spanning trees in the complete } n\text{-vertex graph})$$

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

Tropical circuits (dynamic programming algorithms): $\mathcal{T}_+ = \{\min, +\} \cup \mathbb{R}_+$

Open problem: is it true that $\mathsf{C}_{\mathcal{T}_+}(PATH_n) \asymp n^3$, where $PATH_n$ is the tropical polynomial computing the shortest path between two poles in an n -vertex graph (optimality of the Bellman–Ford–Moore algorithm)?

▷ computational complexity of shortest paths between all pairs is $\Theta(n^3)$

Depth and complexity

class NC^k : (uniform) circuits of complexity $n^{O(1)}$ and depth $O(\log^k n)$

class $\text{NC}_{\mathcal{A}}^k$: the same for arithmetic setting

multiplication, division $\in \text{NC}^1$ [folklore; Beame, Cook, Hoover, 1986]

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

in particular, determinant $\in \text{NC}_{\mathcal{A}}^2$

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

polynomial GCD $\in \text{NC}_{\mathcal{A}}^1$ (piecewise) [Andrews, Wigderson, 2024] $\mathbb{R}, \mathbb{C}$

Open problem: logical permanent $\in \text{NC}^k$?

▷ the existence of circuits of complexity $n^{O(1)}$ and depth $O(\log^2 n)$ is proven [BGH82]

Open problem: can the operator of maximum of n numbers of length n be implemented by boolean circuits of complexity $O(n^2)$ and depth $O(\log n)$?

Multiplication

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

M_n — operator of multiplication of n -bit integers

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

+ interpolation [Toom], + FFT [Bakhvalov, Karatsuba]

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

+ special choice of interpolation rings $\rightarrow$

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

+ approximation of FFT_N by FFT_{2^n} $\rightarrow$

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

$$\boxed{\mathsf{C}_{\mathcal{A}}(M_n^R) \geq ?} \quad M_n^R \text{ — operator of multiplication of polynomials } \deg < n \text{ from } R[x]$$

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

$$\mathsf{C}_{\mathcal{A}}(M_n^R) \preceq n \log n \log \log n \quad [\text{Cantor, Kaltofen, 1991}] \quad \text{arbitrary ring } R$$

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

Open problem: $\mathsf{C}_{\mathcal{A}}(M_n^R) \preceq n \log n$?

▷ holds for $\mathbb{R}, \mathbb{C}$; there is a conventional algorithm [HvdH19]

Matrix multiplication

$\boxed{\mathcal{C}_{\mathcal{A}}(MM_n) \geq ?}$ MM_n — operator of multiplication of $n \times n$ -matrices (over R)

$$\mathcal{C}_{\mathcal{A}}(MM_n) \preceq n^{\log_2 7} \quad [\text{Strassen, 1968}]$$

1970–1980s:

- trilinear representation [Pan]
- approximate computations (border rank) [Bini]
- method of direct sums [Schönhage]
- laser method [Strassen]

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

analysis of powers of Coppersmith–Winograd tensor [Stothers, 2010]

$$\dots \quad \mathcal{C}_{\mathcal{A}}(MM_n) \preceq n^{2.372}$$

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

Open problem: $\mathcal{C}_{\mathcal{A}}(MM_n) = n^{2+o(1)}$?

Multiplication of $n \times n$ - and $n \times n^\alpha$ -matrices: $\mathcal{C}_{\mathcal{A}}(MM_{n,n,n^\alpha}) = n^{2+o(1)}$

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

Matrix multiplication, modular composition

Practically meaningful methods (economical trilinear decompositions):

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

Alternative representations: example for MM_2 :

standard: 7 multiplications, 15 additions [Strassen, Winograd]

alternative: 7 multiplications, 12 additions [Bodrato, 2010]

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

Modular composition

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

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

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

interpolation idea $\rightarrow C_A(MC_n) = n^{1+o(1)} \quad [\text{Umans, 2008}] \quad GF(p^k), \quad p \text{ is small}$

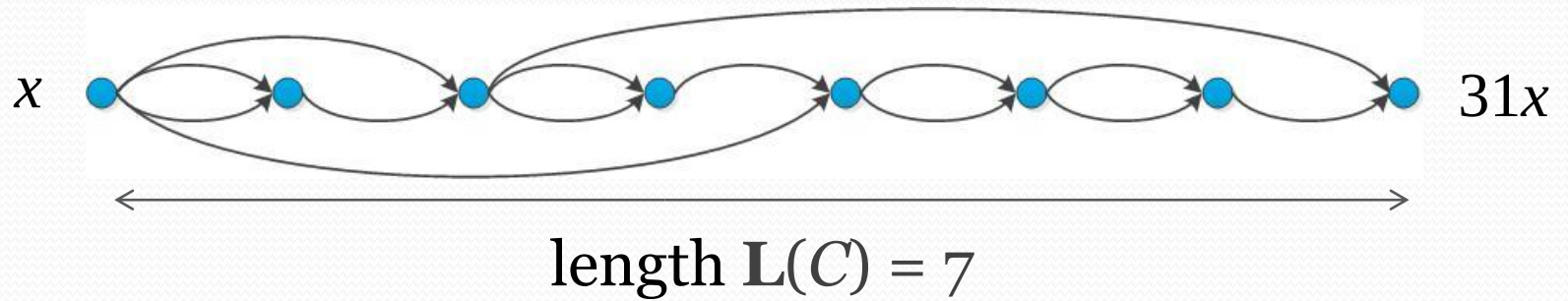
reduction to computing of a member of recurrent sequence $\rightarrow$

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

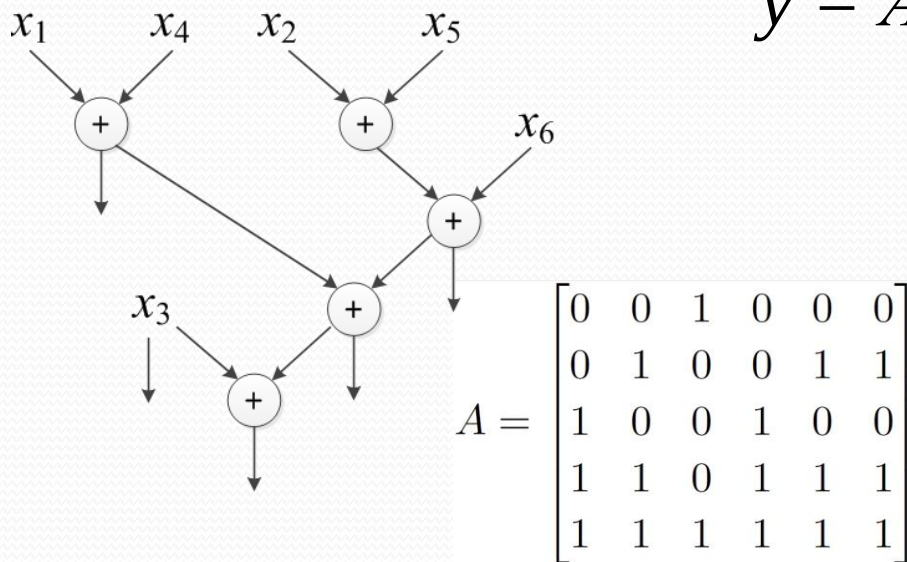
Open problem: $C_A(MC_n) = n^{1+o(1)}$ in general case (at least for $\mathbb{R}$ и $\mathbb{C}$)?

Addition chains

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

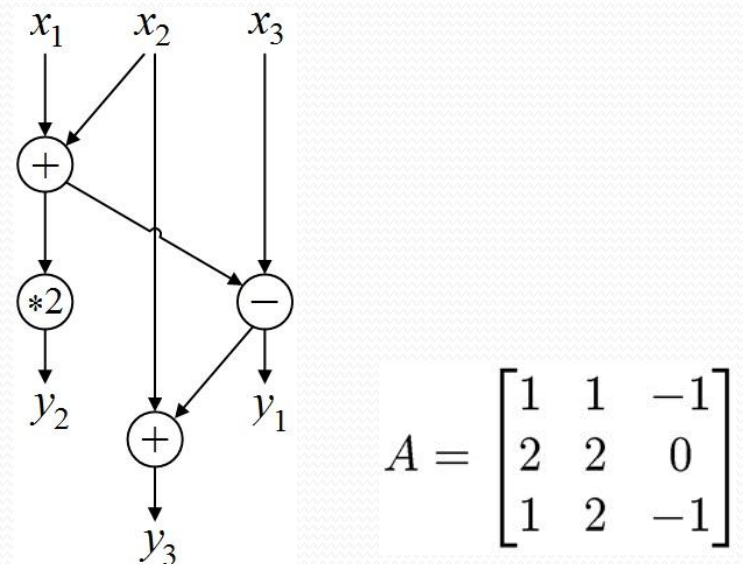


Additive circuits



$$y = A \cdot x$$

Linear (arithmetic) circuits



Linear circuits (lower bounds)

addition chains: $L(n) \sim \log_2 n$ [Brauer, 1939]

additive circuits: $L(A_n) \asymp n^2 / \log_2 n$ for 0/1 $n \times n$ -matrices

[Lupanov, 1956; Nechiporuk, 1963 (asyp.)]

linear circuits: $L(A_n) \asymp n^2$ for $n \times n$ -matrices over $\mathbb{R}$ (or $\mathbb{C}$)

Lower bounds:

monot. comput. of 0/1 matrices (over $(\mathbb{B}, \vee)$ or $\mathbb{Z}_+$): $L(A_n) = n^{2-o(1)}$ [Andreev, 1986]

circuits over $\mathbb{C}$: $L(A_n) \succeq n^2 / \log n$ [Heintz, Sieveking, 1980]

Open problem: addition chains: construct an explicit set $\mathbf{m} = \{m_1, \dots, m_n\}$, $m_i \in n^{O(1)}$, of complexity $L(\mathbf{m}) = n + \Omega(n)$.

▷ upper bound $L(\mathbf{m}) = n + O(n)$; known result: $L(\mathbf{m}) = n + \Omega(n^{1-\varepsilon})$ [Sergeev, 2024]

Open problem: circuits over $GF(2)$: $L(A_n) = \omega(n)$ for some sequence of matrices $A_n \in GF(2)^{n \times n}$.

▷ known bound: $L(A_n) \gtrsim 5n$ [Sergeev, 2025]

Open problem: linear circuits over $\mathbb{R}$ (or $\mathbb{C}$): $L(A_n) = \omega(n)$ for a sequence of $n \times n$ -matrices A_n with 0/1-coefficients.

▷ there are bounds for circuits with bounded constants

Communication complexity

A



B



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



game $G[f]$

knows X

knows Y

! have to determine $f(X,Y)$ via as few communicated bits as possible

$cc(G[f])$ – minimal possible number of communicated bits

Communication complexity and depth

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

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

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

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

Applications:

$D_{\mathcal{B}_M}(Stcon_n) \asymp \log^2 n, \quad Stcon_n - st\text{-connectivity function of an } n\text{-vertex graph}$
[Karchmer, Wigderson, 1990]

$D_{\mathcal{B}_M}(Per_n) \asymp n, \quad Per_n - \text{logical permanent} \quad [\text{Raz, Wigderson, 1992}]$

$D_{\mathcal{B}_M}(CL_{n,k}) \asymp k \log n \quad \text{for } k \leq n^\varepsilon, \quad CL_{n,k} - k\text{-clique function for a graph}$
[Raz, McKenzie, 1997]

$\boxed{CIS[G]}$ $A : \text{clique } a \text{ in a graph } G \quad B : \text{independent set } b \subset G \quad \text{find } |a \cap b|$

for a graph $G = (V, E)$ one has $\text{cc}(CIS[G]) \preceq \log^2 |V| \quad [\text{Yannakakis, 1991}]$

lifting lower bounds method [Göös, 2015] $\rightarrow$

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

topics beyond the scope of the presentation:

- Turing machines, programs with memory
- circuits over infinite bases, circuits of bounded depth
- decision trees, contact circuits, and branching programs
- nondeterministic circuits and other models
- quantum computing
- probabilistic (randomized) algorithms
- average complexity / approximate computations
- noncommutative computations
- combinatorial optimization problems
- number-theoretic algorithms
- classification problems of complexity class hierarchies