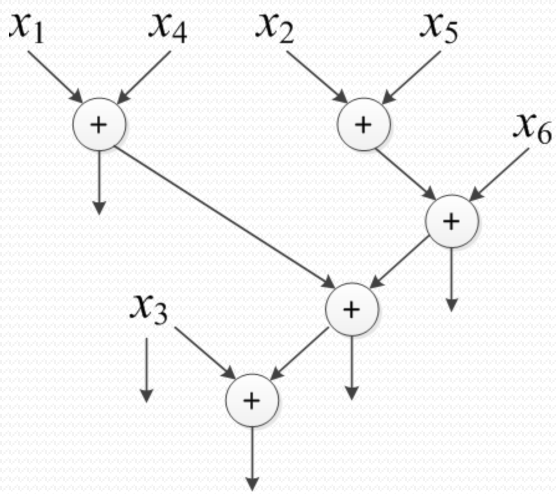
# Lower bounds on the additive complexity of linear operators over GF(2)

I.S. Sergeev, 2024

# Additive circuits




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

$$\left.\begin{array}{ll} 1+1=2 & \text{circuits over } \{\mathbb{Z},+\} \\ 1+1=1 & \text{circuits over } \{\mathbb{B},\vee\} \end{array}\right\} \text{monotone models}$$

$$\boxed{1+1=0 \qquad \text{circuits over } GF(2)}$$

Complexity of a matrix $A$ over $GF(2)$: $\mathsf{L}(A)$

# Preliminary information

$\mathsf{L}(n \times n) \sim \dfrac{n^2}{2\log_2 n}$ (E. I. Nechiporuk, 1963)

In monotone models: $\mathsf{L}_{mon}(A) = n^{2-o(1)}$ for explicit matrices

(A. E. Andreev, 1986; J. Kóllar, L. Rónyai, T. Szabó, 1996)

$\boxed{\text{Open problem: construct an explicit example } \mathsf{L}(A) = \omega(n)}$

# Direct sums of matrices

$$A \boxplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}; \qquad \mathsf{L}_{mon}(A \boxplus B) = \mathsf{L}_{mon}(A) + \mathsf{L}_{mon}(B)$$

$$\frac{1}{2}(\mathsf{L}(A) + \mathsf{L}(B)) \leq \mathsf{L}(A \boxplus B) \leq \mathsf{L}(A) + \mathsf{L}(B)$$

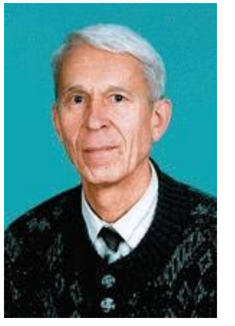
Example (from a paper by W. Paul, 1976): $B \in GF(2)^{n \times n}$, $\mathsf{L}(B) = n^{2-o(1)}$.

$$\mathsf{L}(I_n \otimes B) = \mathsf{L}(B \boxplus \cdots \boxplus B) = \mathsf{L}(B \cdot X) \preceq n^{2.38} \ll n\mathsf{L}(B)$$

# Lower bounds in GF(2). Easy example

Transposition principle (B. S. Mityagin, B. N. Sadovskii, 1965):

**Claim.** *For a matrix* $A \in GF(2)^{m\times n}$ *without zero rows and columns,* $\mathsf{L}(A) + m = \mathsf{L}(A^\top) + n.$



$$\mathcal{Y}_n \in GF(2)^{n\times(2^n-1)}: \qquad \mathcal{Y}_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

$$\Rightarrow \mathsf{L}(\mathcal{Y}_n) \sim 2 \cdot 2^n$$

Example (from a paper by A. V. Chaskin, 1994; modified):

$$m = \log_2 n, \quad U \in GF(2)^{m\times(n-m)}, \quad U \subset \mathcal{Y}_m: \qquad A = \begin{bmatrix} U & 0 \\ 0 & U^\top \end{bmatrix} \in GF(2)^{n\times n}.$$

$$\Rightarrow \mathsf{L}(A) \geq \mathsf{L}(U) + n - 2m = \mathsf{L}(U^\top) + 2n - 4m \geq 3n - 6m \sim 3n.$$

# Extended complexity

Extended circuit:

— may have inputs of additional variables $Y$;

— if an element computes a sum $\langle a, X\rangle + \langle b, Y\rangle$,
then let $b$ be the *type* of the element.

— complexity $\mathsf{L}^* =$
the number of elements $-$ the number of different types of weight $\geq 2$.

By definition, $\mathsf{L}^*(A) \leq \mathsf{L}(A)$.

**Lemma.** *For any pair of boolean matrices $A$, $B$,*

$$\mathsf{L}^*(A \boxplus B) = \mathsf{L}^*(A) + \mathsf{L}^*(B), \qquad \mathsf{L}(A \boxplus B) \geq \mathsf{L}(A) + \mathsf{L}^*(B).$$

**Theorem.** *For any matrix $A \in GF(2)^{m\times n}$, it holds that $\mathsf{L}^*(A) \leq 2m + n$.*

# Main theorem

*Independency index* $\operatorname{ind}(B)$ of a vector set $B \subset GF(2)^m$: maximal number $k \le |B|$, such that any $k$ vectors from $B$ are linearly independent over $GF(2)$.

**Theorem.** *Let* $m \le n$, *a matrix* $B \in GF(2)^{n \times m}$ *does not have rows of weight* $1$, *and* $\operatorname{ind}(B) \ge 2k \ge 6$. *Then*

$$\mathsf{L}^*(B) \ge n + \frac{2k-4}{2k-1} \cdot n^{1-\frac{1}{k}} - m.$$

For $k \gg \log n$, the lower bound is $2n - o(n) - m$.

# Notes to the theorem

$m = n^{8/9}$;

$n \times m$ matrix $B$ of random rows of weight 3:

— has complexity $\mathsf{L}(B) \leq 2n$;

— $\mathrm{ind}(B) \succeq n^{1/9}$ (due to good expanding properties).

$\Rightarrow$ the bound of the theorem is (asymptotically) tight.

Fact: if a linear code with the check matrix $H$ has distance $d$, then $\mathrm{ind}(H^\top) = d - 1$.

# Main corollary

$$p = \log_2 n, \quad s = \sqrt{n}, \quad m = ps \qquad \alpha_1, \dots, \alpha_{n-m} \in GF(2^p),$$

$$U = \begin{pmatrix} \alpha_1^1 & \alpha_1^2 & \dots & \alpha_1^s \\ \alpha_2^1 & \alpha_2^2 & \dots & \alpha_2^s \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-m}^1 & \alpha_{n-m}^2 & \dots & \alpha_{n-m}^s \end{pmatrix} \in GF(2)^{(n-m)\times m}$$

$\mathrm{ind}(U) \geq s.$

**Corollary 1.** $A = U^\top \boxplus U \in GF(2)^{n\times n} \quad \Rightarrow \quad \boxed{\mathsf{L}(A) \geq 5n - o(n).}$

- $\mathsf{L}(A) \geq \mathsf{L}^*(U) + \mathsf{L}(U^\top) \geq \mathsf{L}^*(U) + \mathsf{L}(U) + n - 2m \geq 5n - o(n).$

**Corollary 2.** $A = 1_{m\times(n-m)} \boxplus U \in GF(2)^{n\times n} \quad \Rightarrow \quad \boxed{\mathsf{L}^*(A) \geq 3n - o(n).}$

- $\mathsf{L}^*(A) = \mathsf{L}^*(1_{1\times(n-m)}) + \mathsf{L}^*(U); \qquad \mathsf{L}^*(1_{1\times n}) = \mathsf{L}(1_{1\times n}) = n - 1.$

# Bilinear algorithms

Bilinear form: $\sum a_{ij} x_i y_j$

Bilinear algorithm (for a system of bilinear forms) = circuit over $\{+, \times\}$:

— all multiplications are of the form $(\sum \alpha_i x_i) \cdot (\sum \beta_j y_j)$

# Matrix multiplication

Complexity of a *bilinear algorithm* for a system of bilin. forms $F$ over $GF(2)$:

— $\mathsf{Bil}_+(F)$ — minimal number of additive operations;

— $\mathsf{Bil}_*(F)$ — minimal number of multiplicative operations;

— $\mathsf{Bil}(F)$ — minimal overall number of operations.

$MM_n$ — operator of multiplication of matrices in $GF(2)^{n\times n}$.

Fact: $\mathsf{Bil}_*(MM_n) \geq 3n^2 - o(n^2)$ (A. Shpilka, 2003)

**Lemma.** *For any matrix* $A \in GF(2)^{n\times n}$,

$$\mathsf{Bil}_+(MM_n) \geq n\mathsf{L}^*(A) + n^2 - \nu(A) - O(n).$$

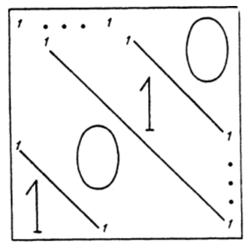
▶ $X \cdot Y \to A \cdot Y$; $\mathsf{L}^*(A \boxplus \cdots \boxplus A) = n\mathsf{L}^*(A)$.

**Corollary.** $\mathsf{Bil}_+(MM_n) \geq (4 - o(1))n^2$, $\mathsf{Bil}(MM_n) \geq (7 - o(1))n^2$.

# Circulant matrices

$S \subset [\![n]\!]$;   $Z_{n,S} \in GF(2)^{n\times n}$: 1s in the 1st row are in positions $S$.

Known bounds for $GF(2)^{n\times n}$:   $\mathsf{L}(Z) \geq 2n - o(n)$.

$Z = \overline{I_n}$ (trivially);   $Z =$  (K. A. Zykov, 1993)

**Claim.** *If a matrix* $B \in GF(2)^{n\times m}$, $n \geq m$, *doesn't contain rectangles, and its every row has weight* $\geq s$, *then* $\mathrm{ind}(B) \geq s$.

$S$ is a Sidon set   $\Rightarrow$   there are no rectangles in $Z_{n,S}$.

Example:   $p \sim \sqrt{n}$,

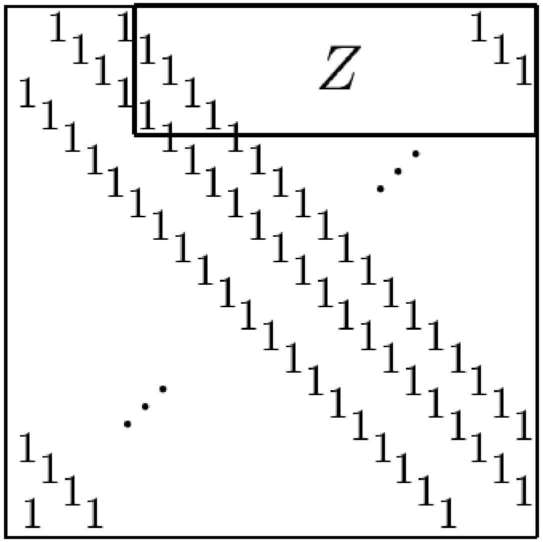
$S_n = [\![n]\!] \cap \{s_k = 2pk + (k^2 \bmod p) \mid k \geq 1\}$

(P. Erdos, P. Turán, 1941)

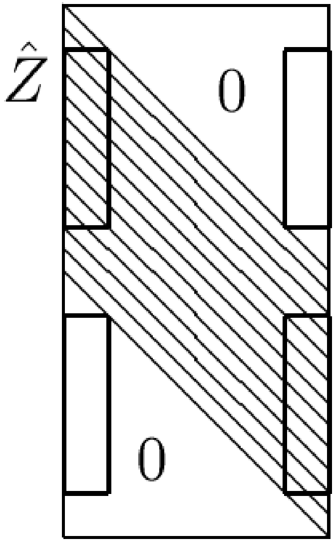
# Circulant matrices

$\hat{Z}_{n,S_n} \in GF(2)^{n\times(2n-1)}$

**Corollary.** $\boxed{\mathsf{L}(Z_{n,S_n}) \geq 3n - o(n),}$ $\mathsf{L}(\hat{Z}^{\top}_{n,S_n}) \geq 4n - o(n).$




$Z_{n,S_n}$



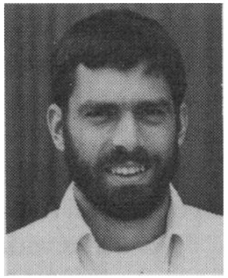

$\hat{Z}^{\top}_{n,S_n}$

# Polynomial multiplication

$M_n$ — operator of multiplication of degree $n-1$ polynomials over $GF(2)$;
$CC_n$ — the order $n$ cyclic convolution over $GF(2)$:

$$CC_n(x_1,\ldots,x_n;y_1,\ldots,y_n)=\left\{\sum_{i+j\equiv k \bmod n} x_i y_j \mid k=1,\ldots,n\right\}.$$

Fact: $\mathsf{Bil}_*(M_n)\geq(3.52-o(1))n$.
(M. R. Brown, D. P. Dobkin, 1980)



**Lemma.** *For any set* $S\subset [\![n]\!]$,

$$\mathsf{Bil}_+(CC_n)\geq \mathsf{L}(Z_{n,S})+n-|S|-O(1),$$
$$\mathsf{Bil}_+(M_n)\geq \mathsf{L}(\hat{Z}^\top_{n,S})+n-|S|-O(1).$$

**Corollary.** $\mathsf{Bil}_+(CC_n)\geq(4-o(1))n,\quad \mathsf{Bil}_+(M_n)\geq(5-o(1))n,$
$\mathsf{Bil}(M_n)\geq(8.52-o(1))n.$

# Complexity of the Sierpinski matrices

Sierpinski matrices (or disjointness matrices) $D_n \in GF(2)^{2^n \times 2^n}$:

$$D_0 = 1, \qquad D_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad D_{k+1} = \begin{bmatrix} D_k & D_k \\ 0 & D_k \end{bmatrix}.$$

Alternatively: $D_n[I, J] = (I \cap J = \varnothing), \quad I, J \subset [\![n]\!]$.

$\boxed{\text{Hypothesis: } \mathsf{L}(D_n) = \omega(2^n)}$

$D_{n,k}$ — a submatrix composed from columns indexed by sets of cardinality $\leq k$.
$D_{n,k}$ has size $2^n \times (C_n^0 + C_n^1 + \ldots + C_n^k)$.
$\mu_{n,k}$ — minimal number of monomials for a nonzero boolean function on $n$ variables, taking value 0 on all inputs of weight $\geq n - k$.

**Lemma.** (1) $\quad \mathrm{ind}(D_{n,k}) \geq \mu_{n,k} - 1, \quad$ (2) $\quad \mu_{n,k} > k^{5/2}/(5n)$.

**Corollary.** $\boxed{\mathsf{L}(D_n) \geq (3 - o(1))2^n.}$

- $k = n/3: \qquad \mathsf{L}(D_n) \geq \mathsf{L}(D_{n,k}^\top) = \mathsf{L}(D_{n,k}) + 2^n - o(2^n) \geq (3 - o(1))2^n.$

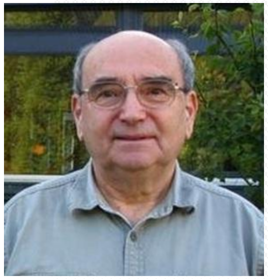
# Open problems

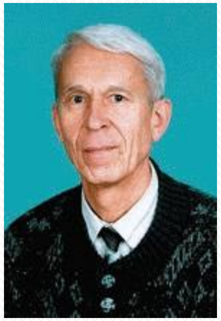
Hystorical:

For a rectangle-free matrix $A \in GF(2)^{n\times n}$:

$\mathsf{L}(A)$ vs $\nu(A) - n$?

(B. S. Mityagin, B. N. Sadovskii, 1965)





First examples $\frac{\mathsf{L}(A)}{\nu(A)-n} < const < 1$:

by depth-3 circuits

(S. B. Gashkov, 1973; K. A. Zykov, 1998)

Finally:

$$\inf_{A\in GF(2)^{n\times n}} \frac{\mathsf{L}(A)}{\nu(A)-n} = n^{o(1)-0.5}$$

on explicit examples

(S. B. Gashkov, I. S. Sergeev, 2010)

# Open problems

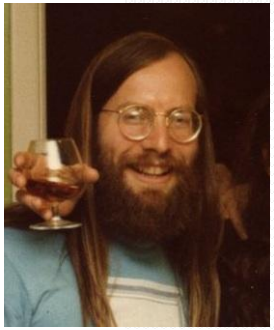
**1.** Construct a pair of explicit matrices $A_1$, $A_2$ with $\mathsf{L}(A_1 \boxplus A_2) < \mathsf{L}(A_1) + \mathsf{L}(A_2)$.

**2.** Construct a matrix $A$: $\mathsf{L}_\vee(A) \ll \mathsf{L}(A)$.

**3.** Do conjunctions allow to reduce the complexity of a linear operator?

*Note:* for circuits over $(\mathbb{B}, \vee)$, yes!

(R. E. Tarjan, 1978)



**4.** Is it true that $\mathsf{L}(D_n) < n2^{n-1}$ as $n \to \infty$?

**5.** Does a circulant matrix $Z$ exist such that $\mathsf{L}(Z) = \omega(n)$?

*Note:* There exist circulant matrices $\mathsf{L}_{mon}(Z) = n^{2-o(1)}$ (M. I. Grinchuk, 1988); moreover, there are explicit examples (S. B. Gashkov, I. S. Sergeev, 2012)