Complexity of additive computations

Sergeev I. S.

2021

Addition chains

$1, 2, 3, 6, 7, 14, 28, 31$ $\qquad a_0 = 1, \quad a_k = a_i + a_j, \quad i, j < k.$

$\lambda(n)$ — minimal length of an a.c. for n; $\qquad \lambda(31) = 7$

$$\lambda(n) \geq \log_2 n$$

$$\lambda(n) \leq \log_2 n + \nu(n) - 1 \leq 2 \log_2 n$$ (Horner's scheme)

$$n = [n_k \; n_{k-1} \; \dots \; n_0]_2 = 2(\dots 2(2n_k + n_{k-1}) + \dots + n_1) + n_0$$

$$\lambda(n) \leq \log_2 n + (1 + \varepsilon_n) \frac{\log_2 n}{\log_2 \log n}$$ (A. Brauer'29)

$$n = \begin{pmatrix} 1 & 2^k & 2^{2k} & \dots & 2^{(t-1)k} \end{pmatrix} \cdot \begin{pmatrix} n_0 & n_1 & \cdots & n_{k-1} \\ n_k & n_{k+1} & \cdots & n_{2k-1} \\ \vdots & \vdots & \ddots & \vdots \\ n_{(t-1)k} & n_{(t-1)k+1} & \cdots & n_{tk-1} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ \dots \\ 2^{k-1} \end{pmatrix}$$

$$k \approx \log_2 t - \log_2 \log_2 t \quad \rightarrow \quad \lambda(n) \leq (k-1) + 2^k + (t-1)(k+1)$$

Addition chains (2)

$$\lambda(n) \le \log_2 n + (1+\varepsilon_n)\frac{\log_2 n}{\log_2 \log n}$$

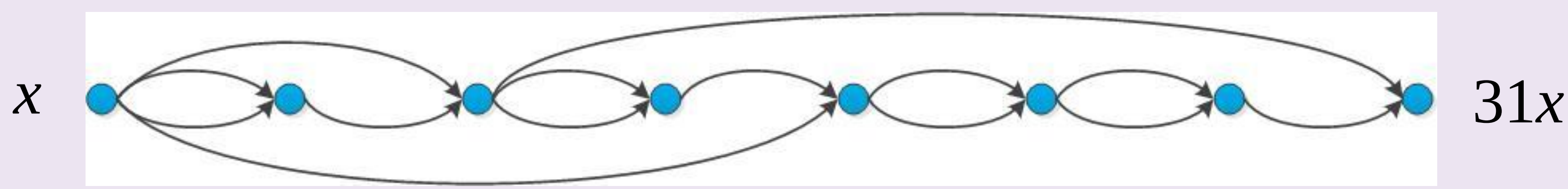
$$\lambda(n) \ge \log_2 n + (1-\delta_n)\frac{\log_2 n}{\log_2 \log n} \quad \text{for alm. all } n$$ (P. Erdös'60)

$$\varepsilon_n, \delta_n \lesssim \frac{2\log_2 \log\log n}{\log_2 \log n}$$ (V.V. & D.V. Kochergin'17)

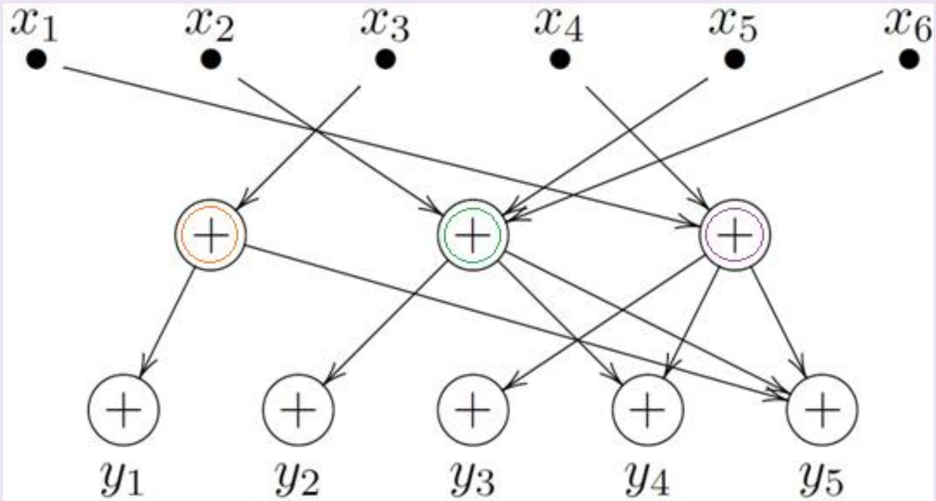
$$\lambda(n) \ge \log_2 n + \log_2 \nu(n) - 2.13$$ (A. Schönhage'75)

The bound $\lfloor \log_2 n \rfloor + \lceil \log_2 \nu(n) \rceil$ is achievable for any $\nu(n)$.

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



Linear circuits



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

$$p_{i,j} = \{\text{number of paths connecting } x_j \text{ and } y_i\}$$

SUM :	$(\mathbb{Z}_{\geq 0}, +)$	$A[i,j] = p_{i,j}$
OR :	$(\mathbb{B}, \vee)$	$A[i,j] = (p_{i,j} \geq 1)$
XOR :	$(\mathbb{B}, \oplus)$	$A[i,j] = p_{i,j} \bmod 2$

Complexity of a circuit = number of edges

Complexity of a matrix: $\mathsf{L}(A)$ = complexity of the minimal circuit

Complexity of a class of matrices: $\mathsf{L}(M) = \max_{A \in M} \mathsf{L}(A)$

Depth of a circuit = length of the longest input-output path

Linear circuits (2)

$\mathsf{L}(q,m,n)$ — complexity of the class of $m \times n$ matrices over $[q]$

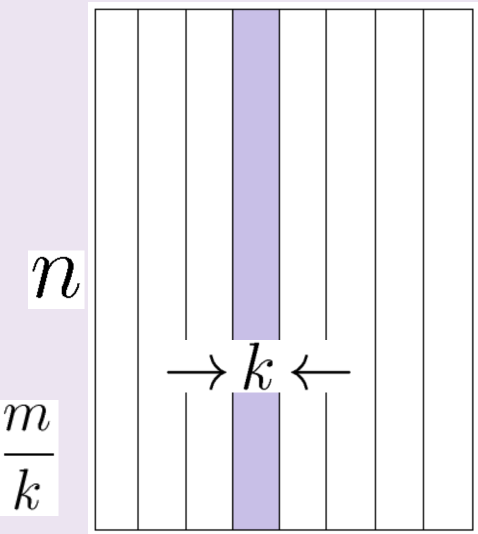
$\mathsf{L}_d(q,m,n)$ — the same with the depth $\leq d$

$\mathsf{L}_d(q,m,n) = \mathsf{L}_d(q,n,m)$ (since $\mathsf{L}(A) = \mathsf{L}(A^T)$); further $m \leq n$

$$\mathsf{L}_2(2,m,n) \sim \frac{mn}{\log_2 n}, \quad m = \omega(\log n)$$

$$\mathsf{L}(2,m,n) \sim \mathsf{L}_2(2,m,n), \quad \log m = o(\log n)$$

(O.B. Lupanov'56)



$$k \approx \log_2 n - 2\log_2\log_2 n \;\to\; \mathsf{L} \leq k2^k \cdot \frac{m}{k} + n \cdot \frac{m}{k}$$

$$\mathsf{L}(2,m,n) \sim \mathsf{L}_3(2,m,n) \sim \frac{mn}{\log_2(mn)}, \quad \log_m n \sim r \in \mathbb{N}$$

(E.I. Nechiporuk'63)

$$\mathsf{L}(2,m,n) \sim \frac{mn}{\log_2(mn)}$$ (N. Pippenger'79)

(I.S. Sergeev'18) $$\mathsf{L}_3(2,m,n) \sim \frac{mn}{\log_2(mn)}$$

Linear circuits (3)

$$\frac{\log n}{\log(mn)} \approx 1 - \frac{1}{r_1}\left(1 - \frac{1}{r_2}\left(1 - \frac{1}{r_3}\left(\dots\left(1 - \frac{1}{r_k}\right)\dots\right)\right)\right), \quad r_i \in \overline{\mathbb{N}}$$

$$\mathsf{L}(q,m,n) \geq 3m\log_3(q-1) + (1-\delta_H)\,\frac{H}{\log H},$$
$$H = mn\log_2 q$$

(Pippenger'79)

$$\mathsf{L}(q,m,n) \leq 3m\log_3(q-1) + (1+\varepsilon_H)\frac{H}{\log H} + n$$

(Sergeev'18)

$$\delta_H \asymp \frac{\log\log H}{\log H}, \qquad \varepsilon_H \asymp \sqrt{\frac{\log\log H}{\log H}}$$

$$A[i,j] = b \cdot D_{i,j} \cdot c^T, \quad b = \left(1,\, 3^k,\, 3^{2k}, \dots,\, 3^{(t-1)k}\right), \quad c = (1,\, 3,\, 3^2, \dots,\, 3^{k-1})$$

$$A = \begin{pmatrix} b & 0 & \cdots & 0 \\ 0 & b & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & b \end{pmatrix} \cdot \begin{pmatrix} D_{1,1} & \cdots & D_{1,n} \\ \cdots & \cdots & \cdots \\ D_{m,1} & \cdots & D_{m,n} \end{pmatrix} \cdot \begin{pmatrix} c^T & 0 & \cdots & 0 \\ 0 & c^T & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & c^T \end{pmatrix}$$

Sierpinski matrices

$$D_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad D_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad D_{2n} = \begin{bmatrix} D_n & 0 \\ D_n & D_n \end{bmatrix}$$

$$\mathsf{SUM}(D_n) \sim \mathsf{OR}(D_n) \sim \frac{1}{2} n \log_2 n$$

(S.N. Selezneva; J. Boyar, M.G. Find'12)

$$n^{1.16} \prec \mathsf{SUM}_2(D_n) \prec n^{1.28}$$

(S. Jukna, I. Sergeev'13)

$$n^{1.16} \prec \mathsf{OR}_2(D_n) \prec n^{1.17}$$

(D. Chistikov, S. Ivan, A. Lubiw, J. Shallit'15)

Sylvester-Hadamard matrices

$$H_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \qquad H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \qquad H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & \overline{H}_n \end{bmatrix}$$

$$2n \log_2 n \lesssim \mathsf{OR}(H_n) \le \mathsf{SUM}(H_n) \lesssim 4n \log_2 n$$

$$\sqrt{2}\, n^{3/2} \lesssim \mathsf{OR}_2(H_n) \le \mathsf{SUM}_2(H_n) \lesssim 2n^{3/2}$$

(D.Yu. Grigoriev'77, T.G. Tarjan'75;
S. Jukna, I. Sergeev'13)

$\mathsf{XOR}(H_n) \sim 4n$ (A.V. Chashkin'94)

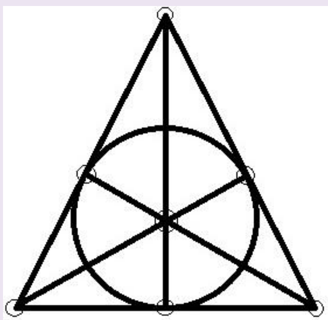
$$H_n = U_n^T \times U_n; \qquad U_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$\mathsf{XOR}_2(H_n) \asymp n \log n$ (N. Alon, W. Maass'90)

Complexity lower bounds

T. A — $(k+1, l+1)$–thin matrix $\Longrightarrow$

$$\mathsf{OR}(A) \geq \frac{|A|}{k \cdot l} \qquad \mathsf{OR}_2(A) \geq \frac{|A|}{\max\{k,l\}}$$



$$S_7 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(E.I. Nechiporuk'64; N. Pippenger'80)

$$\mathsf{OR}(S_n) = |S_n| \sim n^{3/2}$$

$$\mathsf{XOR}(S_n) \preceq n \log^{1+o(1)} n$$

T. $r(A)$ — maximal area of a rectangle in A $\Longrightarrow$

$$\mathsf{OR}(A) \geq \frac{3|A|}{r(A)} \log_3 \frac{|A|}{n} \qquad \mathsf{OR}_d(A) \geq \frac{d|A|}{r(A)} \left(\frac{|A|}{n}\right)^{1/d}$$

(D.Yu. Grigoriev'77; S. Jukna, I. Sergeev'13)

T. A — n^c-Ramsey matrix, $c < 1$

$$\Longrightarrow \quad \mathsf{XOR}_2(A) \succeq n \log n$$

(N. Alon, W. Maass'90)

Extremal separations

$$\frac{\mathsf{OR}(A)}{\mathsf{XOR}(A)}, \frac{\mathsf{OR}_2(A)}{\mathsf{XOR}_2(A)} \succeq \frac{n}{\log^2 n}$$

(P. Pudlák, V. Rödl'94; S. Jukna'06)

$$\frac{\mathsf{SUM}(A)}{\mathsf{OR}(A)} \succeq \frac{\sqrt{n}}{\log n}$$

(M. Find, M. Göös, M. Järvisalo, P. Kaski, M. Koivisto, J. Korhonen'13)

$$\frac{\mathsf{SUM}_2(A)}{\mathsf{OR}_2(A)} \succeq \log n$$

(T. Pinto'12)

$$\frac{\mathsf{XOR}_2(A)}{\mathsf{OR}_2(A)} \succeq \log\log\log n$$

(S. Jukna, I. Sergeev'13)

$$\frac{\mathsf{OR}(\overline{A})}{\mathsf{OR}(A)} \succeq \frac{n}{\log^3 n}$$

(N. Katz'11; S. Jukna, I. Sergeev'13)

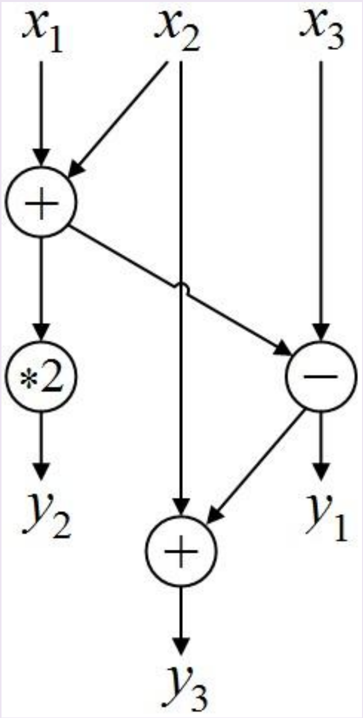
$$\frac{\mathsf{SUM}(\overline{A})}{\mathsf{SUM}(A)} \succeq n^{1/4-o(1)}$$

(S. Jukna, I. Sergeev'21)

Linear arithmetic circuits

$$y = A \cdot x$$

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



basis: $B = \{x + y, x - y, 2x\}$

complexity: $L_B(A) = 4$

complete basis: $B_\infty = \{x \pm y\} \cup \{ax \mid a \in \mathbb{R}\}$

T. $B_C = \{x \pm y\} \cup \{ax \mid |a| \leq C\}$

$$L_{B_C}(A) \geq \log_{\max\{2, C\}} |\det A|$$

(J. Morgenstern'73)

Pascal matrix. I

$$C_n = \begin{bmatrix} C_0^0 & 0 & \cdots & 0 \\ C_1^0 & C_1^1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ C_{n-1}^0 & C_{n-1}^1 & \cdots & C_{n-1}^{n-1} \end{bmatrix}$$

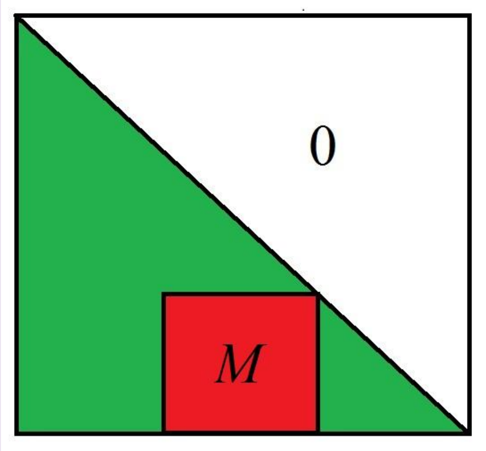
$$C_{n+1}^{k+1} = C_n^{k+1} + C_n^k$$

$$\Rightarrow \quad L_{\{x+y\}}(C_n) \leq n^2/2$$

Pascal matrix. II

1. Matrix C_n has a submatrix M with the determinant of order c^{n^2} for some $c>1$.

$$\Rightarrow \quad L_{B_2}(C_n) = \Theta(n^2)$$



2. $$C_n = \Delta \times \begin{bmatrix} \frac{1}{0!} & 0 & \cdots & 0 \\ \frac{1}{1!} & \frac{1}{0!} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \frac{1}{(n-1)!} & \frac{1}{(n-2)!} & \cdots & \frac{1}{0!} \end{bmatrix} \times \Delta^{-1}$$

$$\Delta = \mathrm{diag}(0!, 1!, \ldots, (n-1)!)$$

$$\Rightarrow \quad L_{B_\infty}(C_n) = O(n \log n)$$ (S.B. Gashkov'14)

Stirling matrices

$$s_n = \| \, s_m^k \, \|_{0 \le k, m < n}, \qquad S_n = \| \, S_m^k \, \|_{0 \le k, m < n}$$

s_m^k - Stirling numbers of the first kind

S_m^k - Stirling numbers of the second kind

$$s_m^k = s_{m-1}^{k-1} - (k-1)s_m^{k-1}, \qquad S_m^k = S_{m-1}^{k-1} + mS_m^{k-1},$$

$$s_0^0 = S_0^0 = 1, \qquad s_0^k = s_k^0 = S_0^k = S_k^0 = 0, \;\; k > 0$$

Fact: $S_n = (s_n)^{-1}$

$$\{1, (x)_1, \ldots, (x)_{n-1}\} \xrightarrow{s_n} \{1, x, \ldots, x^{n-1}\} \xleftarrow{|s_n|} \{1, (x)^1, \ldots, (x)^{n-1}\}$$

$$(x)_k = x(x-1) \cdot \ldots \cdot (x-k+1),$$

$$(x)^k = x(x+1) \cdot \ldots \cdot (x+k-1)$$

Stirling and Vandermonde matrices

1. Matrices s_n and $|s_n|$ have submatrices with determinants of order $2^{\Theta(n^2 \log n)}$.

$$\Rightarrow \quad L_{B_2}(s_n) \asymp L_{\{x \pm y\}}(s_n) = \Theta(n^2 \log n),$$

$$L_{B_2}(|s_n|) \asymp L_{\{x+y\}}(|s_n|) = \Theta(n^2 \log n)$$

(S.B. Gashkov'14)

Vandermonde matrix: $V_n = ||k^m||_{0 \le k,m < n}$

2. $$\det V_n = \prod_{k=1}^{n-1} k! = 2^{\Theta(n^2 \log n)}$$

3. $$V_n = C_n \times \Delta \times S_n^T$$

$$\Rightarrow \quad L_{B_2}(V_n) \asymp L_{\{x+y\}}(V_n) = \Theta(n^2 \log n),$$

$$L_{B_\infty}(V_n),\ L_{B_\infty}(S_n),\ L_{B_\infty}(s_n) = O(n \log^2 n)$$

(S.B. Gashkov'14)

GCD matrix

$$\mathrm{GCD} = \| \gcd(i,k) \|$$

Fact. $\mathrm{GCD} = E \times \phi(D) \times E^T$

E – matrix of divisibility indicators: $E[i,k] = (k \mid i)$

$$D = \mathrm{diag}(1,\ldots,n), \quad f(D) = \mathrm{diag}(f(1),\ldots,f(n))$$

$\phi(x)$ - Euler totient function

(H. Smith'1875)

$$\Rightarrow \quad \log_2 \det \mathrm{GCD} \sim n \log_2 n$$

T. (S.B. Gashkov, I.S. Sergeev'16)

$$L_{B_2}(\mathrm{GCD}) \sim L_{\{x+y\}}(\mathrm{GCD}) \sim n \log_2 n$$

GCD matrix (*)

E – matrix of divisibility indicators: $E[i,k] = (k \mid i)$

M – Möbius matrix: $M[i,k] = \begin{cases} \mu\left(\frac{i}{k}\right), & k \mid i \\ 0, & k \nmid i \end{cases}$

Möbius inversion formula: $M = E^{-1}$

LCM matrix

$$\mathrm{LCM} = \| \operatorname{lcm}(i,k) \|$$

$$\gcd(i,k) \cdot \operatorname{lcm}(i,k) = ik$$

$$\Longrightarrow \quad \mathrm{LCM} = D \times E \times J(D) \times E^T \times D$$

$$J(k) = \frac{1}{k} \prod_{p \in \mathbb{P},\, p|k} (1-p)$$ - Jordan function

$$\Rightarrow \quad \log_2 \det \mathrm{LCM} \sim 2n \log_2 n$$

T. (S.B. Gashkov, I.S. Sergeev'16)

$$L_{B_2}(\mathrm{LCM}) \sim L_{\{\pm\}}(\mathrm{LCM}) \sim 2n \log_2 n$$

$$\mathrm{LCM} = E \times \phi(\gamma(D)) \times \|\phi\,(i/k) \cdot I\{\gamma(i) = \gamma(k)\}\| \times \\ \times [U \times \mu^*(D) \times E^T] \times D$$

$\gamma(k)$ – core of number k $\mu^*(k) = \mu(\gamma(k))$ - unitary Möbius function

$U[i,k] = (k|i \ \wedge \ \gcd(k, i/k) = 1)$ - matrix of unitary divisibility indicators

Discrete Fourier transform

ζ — primitive root of order n in $\mathbb{C}$

$$\boxed{\mathrm{DFT} = \|\zeta^{ik}\|}$$

$$\det\mathrm{DFT} = n^{n/2} \quad \Longrightarrow \quad L^{\mathbb{C}}_{B_2}(\mathrm{DFT}) \geq (1/2) n \log_2 n$$

(J. Morgenstern'73)

$$\mathrm{DFT}_{ST} = \pi \times (I_T \otimes \mathrm{DFT}_S) \times D \times (\mathrm{DFT}_T \otimes I_S)$$

π — permutation matrix; $\qquad D = \mathrm{diag}\{\zeta^{st}\,|_{0\leq s<S,\, 0\leq t<T}\}$

$$n = 2^k : \quad L^{\mathbb{C}}_{B_1}(\mathrm{DFT}) < (3/2) n \log_2 n$$

(J. Cooley, J. Tukey'65)

$$L^{\mathbb{R}}_{B_1}(\mathrm{DFT}) < 4n \log_2 n$$

(P. Duhamel, H. Hollmann, J.-B. Martens, M. Vetterli, H. Nussbaumer'84)

$$L^{\mathbb{R}}_{B_\infty}(\mathrm{DFT}) < 3\tfrac{7}{9} \cdot n \log_2 n$$

(J. van Buskirk'04)

$$L^{\mathbb{R}}_{B_2}(\mathrm{DFT}) \lesssim 3.76875 n \log_2 n$$

(I.S. Sergeev'17)