СЛОЖНОСТЬ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

И. С. СЕРГЕЕВ

2023

I. Симметрические функции

Симметрические булевы функции:

$$f(x_1, x_2, \ldots, x_n) = g(x_1 + x_2 + \ldots + x_n).$$

SYM_n — класс симметрических булевых функций n переменных

$THR_n^k = (x_1 + \ldots + x_n \geq k)$ — монотонная симметрическая функция с порогом k

$MAJ_n = THR_n^{n/2}$ — функция голосования n переменных

$SORT_n = (THR_n^1, THR_n^2, \ldots, THR_n^n)$ — оператор сортировки булева набора

$CNT_n = (x_1 + \ldots + x_n)$ — оператор суммирования n бит

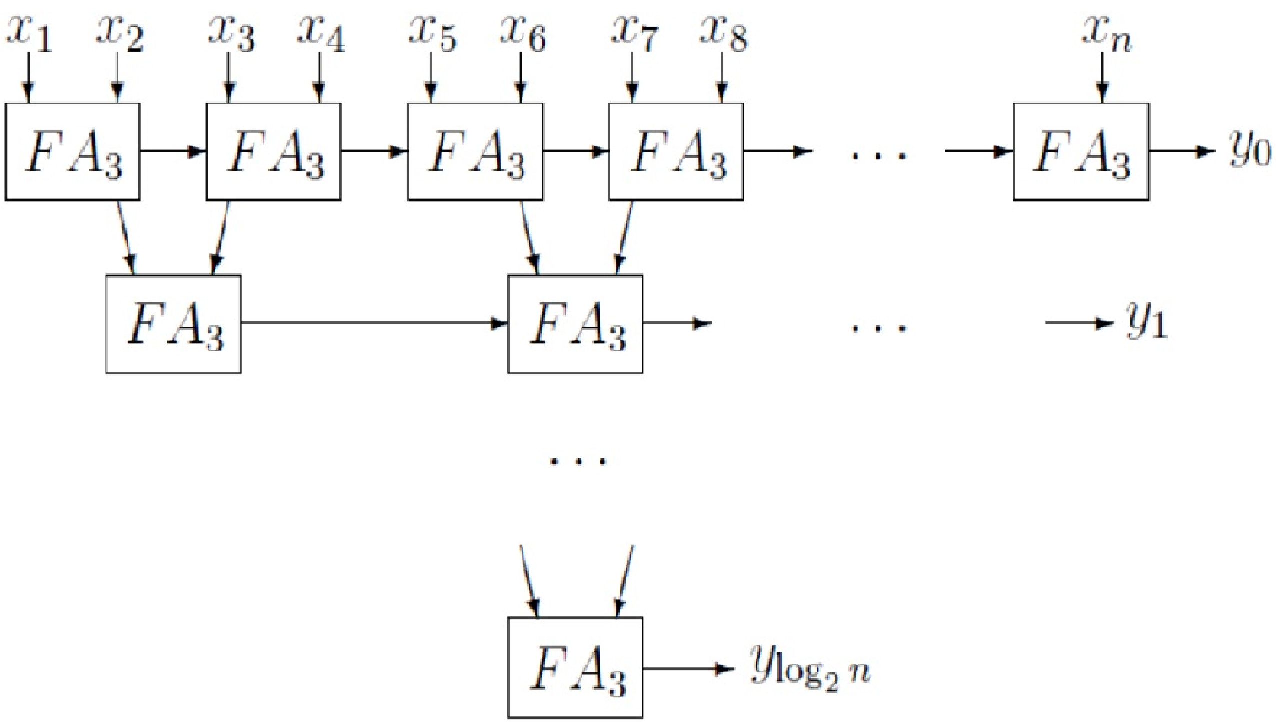
$MOD_n^{m,r} = (x_1 + \ldots + x_n \equiv r \bmod m)$ — элементарная периодическая функция

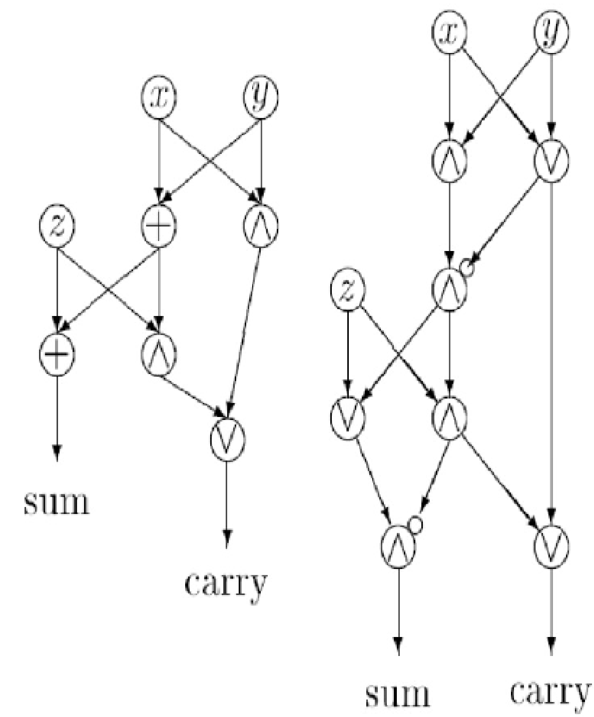
$MOD_n^m = (MOD_n^{m,0}, MOD_n^{m,1}, \ldots, MOD_n^{m,m-1})$ — оператор суммирования по модулю m

II. Сложность булевых схем

$$f(X) \in SYM_n: \qquad X \xrightarrow{O(n)} Y = CNT_n(X) \xrightarrow{O(n/\log n)} g(Y) = f(X)$$

FA_3 — схема суммирования трех бит $\qquad \mathsf{C}_{\mathcal{B}_2}(FA_3) = 5, \quad \mathsf{C}_{\mathcal{U}_2}(FA_3) = 7$



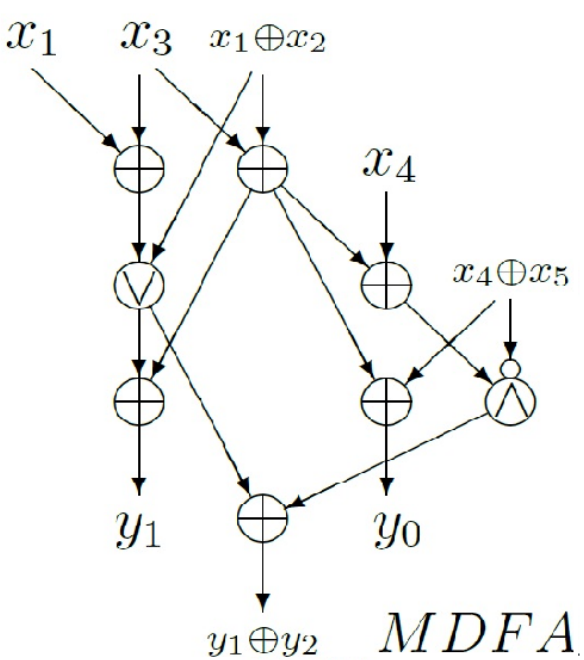


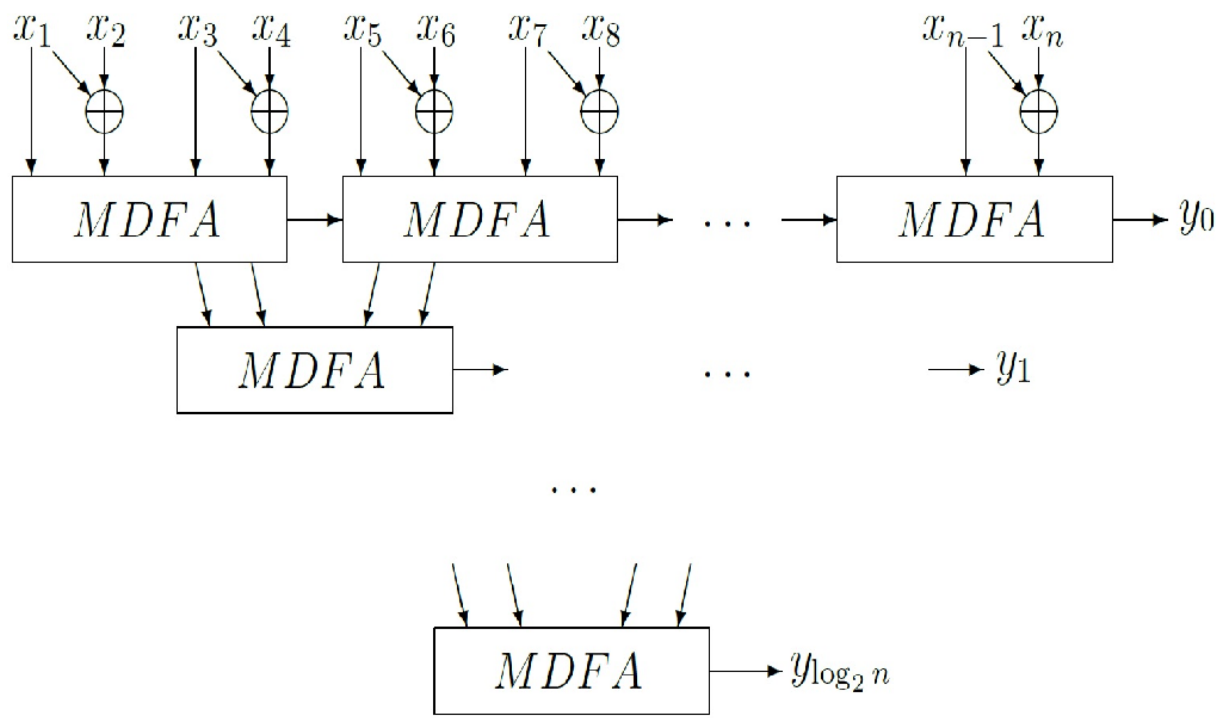
$$\boxed{\mathsf{C}_{\mathcal{B}_2}(SYM_n) \le 5n + o(n), \quad \mathsf{C}_{\mathcal{U}_2}(SYM_n) \le 7n + o(n)}$$

(фольклор)

II. Сложность булевых схем

$\boxed{\mathsf{C}_{\mathcal{B}_2}(SYM_n) \le 4.5n + o(n)}$ (Demenkov E., Kojevnikov A., Kulikov A.S., Yaroslavtsev G., 2010)





Нижние оценки:

$\mathsf{C}_{\mathcal{B}_2}(SYM_n) \ge 2.5n - O(1)$ (L. J. Stockmeyer, 1977) $f = MOD_n^{k,*}$,

$\mathsf{C}_{\mathcal{U}_2}(SYM_n) \ge 4n - O(1)$ (U. Zwick, 1991) $3 \le k = O(1)$

II. Сложность булевых схем

$\mathsf{C}_{\mathcal{B}_2}(MOD_n^{4,*}) = 2.5n - O(1)$ (L. J. Stockmeyer, 1977)

$\mathsf{C}_{\mathcal{U}_2}(MOD_n^{4,*}) \leq 5n - O(1)$ (U. Zwick, 1991)

$\mathsf{C}_{\mathcal{B}_2}(MOD_n^{3,*}) \leq 3n - O(1)$ (KKY, 2009; D. E. Knuth, 2015; A. Kulikov, N. Slezkin, 2021)

$\mathsf{C}_{\mathcal{B}_2}(MOD_n^{2^k,*}) \leq (4.5 - 2^{3-k})n + o(n)$ (DKKY, 2010), $k \geq 3$

$\mathsf{C}_{\mathcal{B}_2}(THR_n^k) \geq 2n + \min\{k, n-k\} - O(1)$ (L. J. Stockmeyer, 1977)

$\mathsf{C}_{\mathcal{B}_2}(THR_n^k) \leq (4.5 - 2^{2-p})n + o(n), \quad 2^{p-1} < k \leq 2^p$ следует из (DKKY, 2010)

Монотонная сложность:

$\mathsf{C}_{\mathcal{B}_M}(SORT_n) = \Theta(n \log n)$ (E.A. Lamagna, 1975; M. Ajtai, J. Komlós, E. Szemerédi, 1983)

$\mathsf{C}_{\mathcal{B}_M}(THR_n^2) = 2n + \Theta(\sqrt{n})$ (Б. М. Клосс, 1965; L. Adleman, 1970-е; И. С. Сергеев, 2020)

$\mathsf{C}_{\mathcal{B}_M}(THR_n^3) = 3n + O(\log n) - O(1)$ (И. С. Сергеев, 2020)

$\mathsf{C}_{\mathcal{B}_M}(THR_n^k) \geq 3n + \min\{k, n-k\} - O(1)$ (P. E. Dunne, 1984; И. С. Сергеев, 2020)

$\mathsf{C}_{\mathcal{B}_M}(THR_n^k) \leq (6 + o(1))n \log_3 n$ (Jimbo S., Maruoka A., 1996)

$\mathsf{C}_{\mathcal{B}_M}(THR_n^k) \leq (\lfloor \log_2 k \rfloor + \lfloor \log_2(4k/3) \rfloor)n + o_k(n)$ (И. С. Сергеев, 2020), $k \ll n$

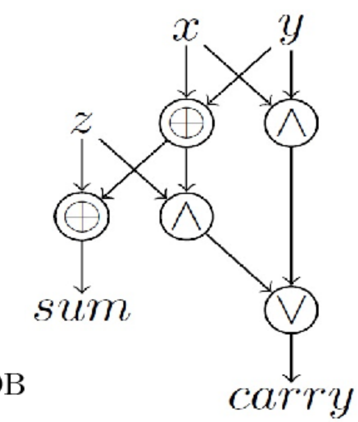
III. Сложность и глубина формул

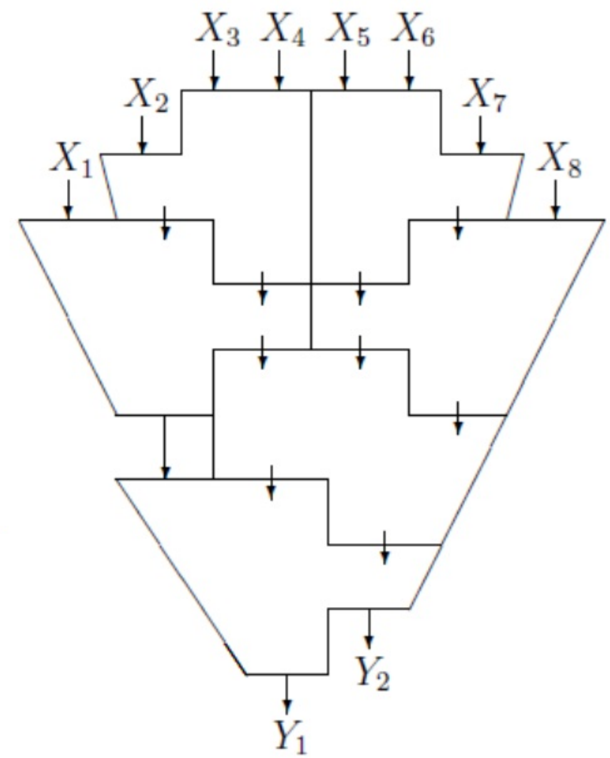
(k,l)-компрессор: $\quad (X_1,\ldots,X_k) \to (Y_1,\ldots,Y_l), \quad \sum_{i=1}^{k} X_i = \sum_{j=1}^{l} Y_j.$

<u>Метод потенциалов:</u>

$p(v) = \lambda^d$ — потенциал вершины v на глубине d.

<u>Утв.</u> При подходящем λ величина $\sum_v p(v)$ не убывает по мере присоединения компрессоров





Для $(3,2)$-компрессора на рис.:
$\lambda \approx 1.2056 \leftarrow \lambda^3 + \lambda^2 = \lambda + 2.$

<u>Сл-е.</u> $D(n \to 2) \geq \log_\lambda(n/2) \approx 3.71 \log_2 n$

<u>Сложность формул</u>

потенциал формулы F: $(\mathsf{L}(F))^\mu$ при подходящем μ

$$\boxed{\mathsf{D}(CNT_n) \leq \log_\lambda n + O(1), \;\; \mathsf{L}(CNT_n) \leq n^{1/\mu + o(1)}}$$

(M. Paterson, N. Pippenger, U. Zwick, 1990–92)

III. Сложность и глубина формул

Общий метод (И. С. Сергеев, 2016)

$\sigma = x_1 + x_2 + \ldots + x_n$

$\boxed{\sigma \bmod 2^k}$ метод компрессоров

$\boxed{\sigma \bmod 3^l}$ троичный метод компрессоров

$\downarrow$

$\boxed{\text{осн. } 3 \to \text{осн. } 3^p}$

$\boxed{\sigma^* :\ |\sigma^* - \sigma| \le T}$ метод Вэльянта для приближений функций THR_n^{tj} , $j = 1..u$

$\boxed{\text{мод. арифм.}}$

$\downarrow$

CNT_n

$\boxed{\text{метод каскадов}}$

$\downarrow$

$f \in SYM_n$

	$\mathsf{L}_{\mathcal{B}_0}$	$\mathsf{L}_{\mathcal{B}_2}$	$\mathsf{D}_{\mathcal{B}_0}$	$\mathsf{D}_{\mathcal{B}_2}$
CNT_n	$n^{3.91}$	$n^{2.84}$	$4.14 \log_2 n$	$3.02 \log_2 n$
SYM_n	$n^{4.01}$	$n^{2.95}$	$4.24 \log_2 n$	$3.10 \log_2 n$

III. Сложность и глубина формул

Нижние оценки:

$\mathsf{L}_{\mathcal{B}_0}(SYM_n) = \Omega(n^2)$, $\mathsf{L}_{\mathcal{B}_0}(THR_n^k) \geq k(n-k+1)$ (В. М. Храпченко, 1971)

$\mathsf{L}_{\mathcal{B}_2}(SYM_n) = \Omega(n \log n)$ (Fischer M. J., Meyer A. R., Paterson M. S., 1982)

$\mathsf{L}_{\mathcal{B}}(SYM_n) = \Omega(n \log n)$, $\mathcal{B}$ — полный базис, (Д. Ю. Черухин, 2000)

Оценки для пороговых функций:

$\mathsf{L}_{\mathcal{B}_0}(THR_n^2) = n\lfloor \log_2 n \rfloor + 2(n - 2^{\lfloor \log_2 n \rfloor})$ (Р. Е. Кричевский, 1964; С. А. Ложкин, 2005)

$\mathsf{L}_{\mathcal{B}_M}(THR_n^k) \preceq k^{4.28} n \log n$ (L. Valiant, 1984; R. Boppana, 1985)

$\mathsf{L}_{\mathcal{B}_M}(THR_n^k) \geq \lfloor k/2 \rfloor n \log(n/k)$, $k \leq n/2$ (J. Radhakrishnan, 1997)

Верхние оценки для MOD_n^m:

m	$\mathsf{L}_{\mathcal{B}_0}$	$\mathsf{L}_{\mathcal{B}_2}$	$\mathsf{D}_{\mathcal{B}_0}$	$\mathsf{D}_{\mathcal{B}_2}$
3	$n^{2.59}$ [Луп65]	n^2 [FMP82]	$2.80 \log_2 n$ [Серг16]	$2 \log_2 n$ [McColl77]
5	$n^{3.22}$ [Серг16]	$n^{2.84}$ [Серг16]	$3.35 \log_2 n$ [Серг16]	$3 \log_2 n$, следует из [VL87]
7	$n^{3.63}$ [Серг16]	$n^{2.59}$ [VL87]	$3.87 \log_2 n$ [Серг16]	$2.93 \log_2 n$ [Серг16]

(О. Б. Лупанов, 1965; W. McColl, 1977; FMP,1982; D. C. van Leijenhorst, 1987; И. С. Сергеев, 2016)

$\mathsf{L}_{\mathcal{B}_2}(MOD_n^{2^k}) \preceq n(\log n)^{k-1}$, $\mathsf{L}_{\mathcal{B}}(MOD_n^{p^k}) \preceq n^{o(k)} \mathsf{L}_{\mathcal{B}}(MOD_n^p)$ (FMP, 1982)

III. Сложность и глубина формул

Формулы для периодических функций:

$$MOD^{m,r}_{n_1+n_2}(X) = \bigvee\nolimits_{k=0}^{m-1} MOD^{m,k}_{n_1}(X^1) \cdot MOD^{m,r-k}_{n_2}(X^2), \qquad X = (X^1,\, X^2)$$

$$MOD^{m,r}_{n_1+n_2}(X) = \bigwedge\nolimits_{k=0}^{m-1} \left(MOD^{m,k}_{n_1}(X^1) \vee \overline{MOD^{m,r-k}_{n_2}(X^2)} \right)$$

$\boxed{\mathsf{L}_{\mathcal{B}_0}(MOD^m_n) \preceq n^{1+\log_2 m}}$ (О. Б. Лупанов, 1965)

$$MOD^{m,r}_{n_1+n_2}(X) = \bigwedge\nolimits_{k=1}^{m-1} \left(MOD^{m,k}_{n_1}(X^1) \sim MOD^{m,r-k}_{n_2}(X^2) \right)$$

$\boxed{\mathsf{L}_{\mathcal{B}_2}(MOD^m_n) \preceq n^{1+\log_2 (m-1)}}$ (W. F. McColl, 1977)

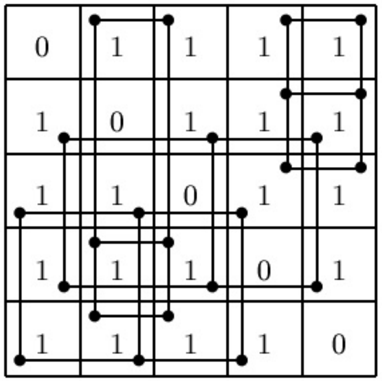
Новые формулы:

$$MOD^{m,S}_n = \left(\sum\nolimits_{i=1}^{n} x_i \bmod m \in S\right)$$

$$MOD^{m,S}_n(X) = \bigvee\nolimits_k MOD^{m,A_k}_{n_1}(X^1) \cdot MOD^{m,B_k}_{n_2}(X^2).$$

Пример: $m = 5, |S| = 4$

$$MOD^{5,S}_n(X) = \bigvee\nolimits_{k=1}^{4} MOD^{5,A_k}_{n_1}(X^1) \cdot MOD^{5,B_k}_{n_2}(X^2).$$



IV. Сложность контактных схем

$\mathsf{K}(MOD_n^m) \leq 2mn$ (C. E. Shannon, 1938)

$\mathsf{K}(MOD_n^m) = 2s_m n - O(1)$, для конст. m (М. И. Гринчук, 1987)

- (s_m — сумма примарных делителей m)

$\mathsf{K}(SYM_n) \leq (2+o(1))n^2/\log_2 n$ (О. Б. Лупанов, 1965)

$\mathsf{K}(SYM_n) \succeq n \log\log\log^* n$ (М. И. Гринчук, 1989; А. А. Разборов, 1990)

$\mathsf{K}(THR_n^k) \preceq \frac{n \log^3 n}{\log\log n \log\log\log n}$ (R. K. Sinha, J. S. Thathachar, 1997)

$\mathsf{K}(MOD_n^{m,*}) \preceq \frac{n \log^4 n}{\log^2 \log n}$ (R. K. Sinha, J. S. Thathachar, 1997)

<u>Монотонные контактные схемы</u>

$\mathsf{K}_+(THR_n^k) \geq k(n-k+1)$ (А. А. Марков, 1962)

$\mathsf{K}_+(THR_n^2) = n\lfloor \log_2 n \rfloor + 2(n - 2^{\lfloor \log_2 n \rfloor})$ (Р. Е. Кричевский; G. Hansel, 1964)

$\mathsf{K}_+(THR_n^k) \preceq k^{3.99} n \log n$ (M. Dubiner, U. Zwick, 1992)

$\mathsf{K}_+(THR_n^{n-1}) \succeq n \log\log\log n$ (M. M. Halldórsson, J. Radh-n, K. V. Subrahmanyam, 1993)

$\mathsf{K}_+(THR_n^k) \succeq kn \log(n/k), \quad k \leq n/2$ (J. Radhakrishnan, 1997)