COMPLEXITY OF SYMMETRIC BOOLEAN FUNCTIONS

I. S. SERGEEV

2023

I. Symmetric functions

Symmetric boolean functions:

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

SYM_n — class of symmetric boolean functions of n variables

$THR_n^k = (x_1 + \ldots + x_n \geq k)$ — threshold-k monotone symmetric function

$MAJ_n = THR_n^{n/2}$ — majority function of n variables

$SORT_n = (THR_n^1, THR_n^2, \ldots, THR_n^n)$ — boolean sorting operator

$CNT_n = (x_1 + \ldots + x_n)$ — n-input counting operator

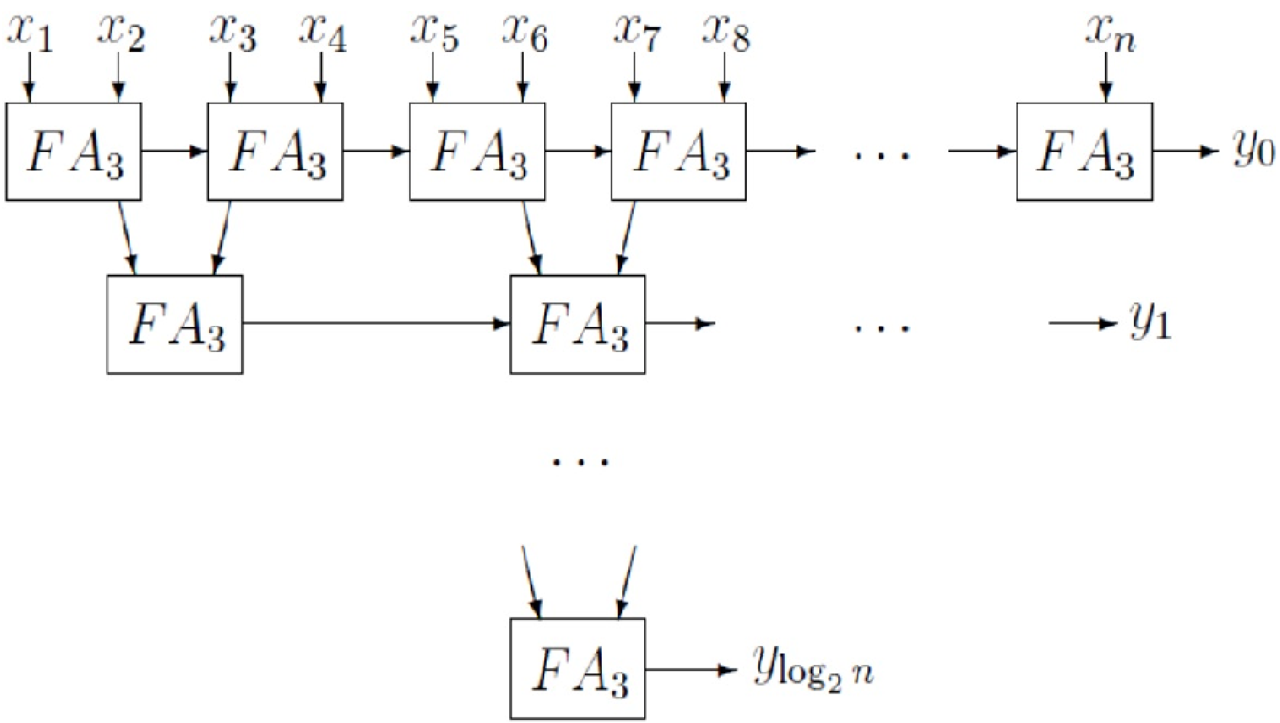
$MOD_n^{m,r} = (x_1 + \ldots + x_n \equiv r \bmod m)$ — elementary periodic function

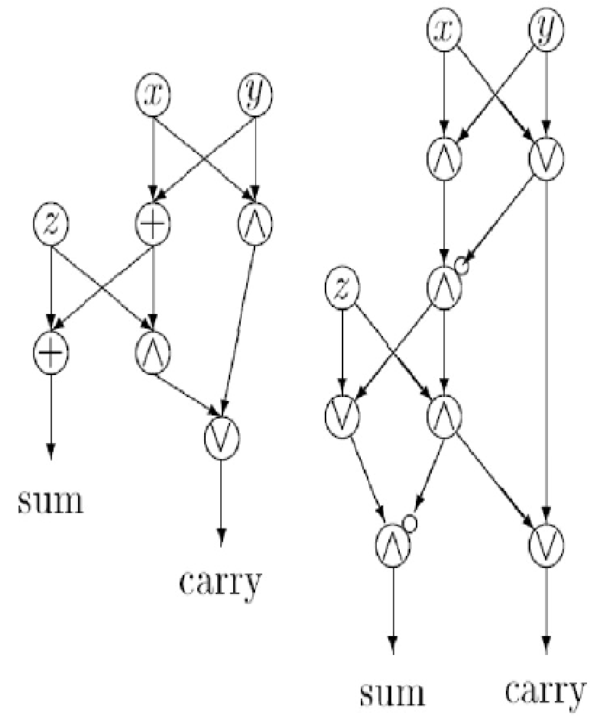
$MOD_n^m = (MOD_n^{m,0}, MOD_n^{m,1}, \ldots, MOD_n^{m,m-1})$ — counting operator modulo m

II. Complexity of boolean circuits

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

FA_3 — a circuit summing 3 bits $\qquad \mathsf{C}_{\mathcal{B}_2}(FA_3) = 5, \quad \mathsf{C}_{\mathcal{U}_2}(FA_3) = 7$



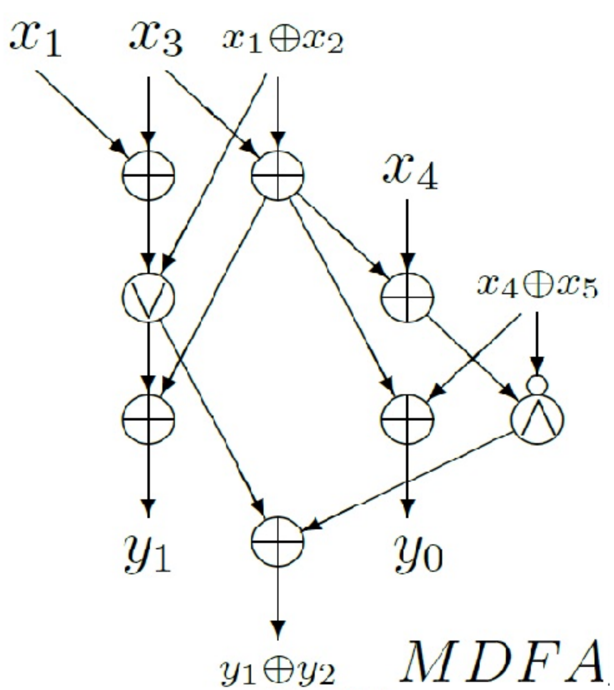


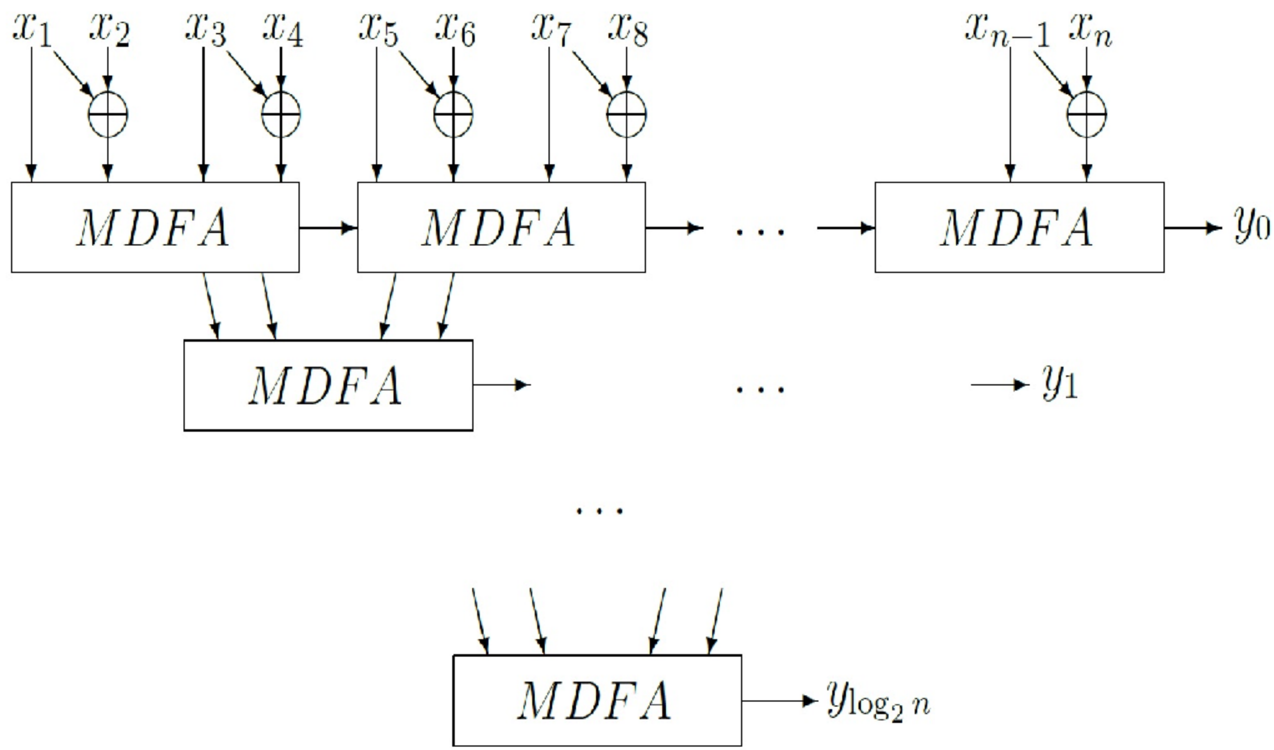
$$\mathsf{C}_{\mathcal{B}_2}(SYM_n) \leq 5n + o(n), \quad \mathsf{C}_{\mathcal{U}_2}(SYM_n) \leq 7n + o(n)$$

(folklore)

II. Complexity of boolean circuits

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





Lower bounds:

$\mathsf{C}_{\mathcal{B}_2}(SYM_n) \ge 2.5n - O(1)$ (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. Complexity of boolean circuits

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

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

Monotone complexity:

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

$\mathsf{C}_{\mathcal{B}_M}(THR_n^2) = 2n + \Theta(\sqrt{n})$ (B. M. Kloss, 1965; L. Adleman, 1970-e; I. S. Sergeev, 2020)

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

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

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

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

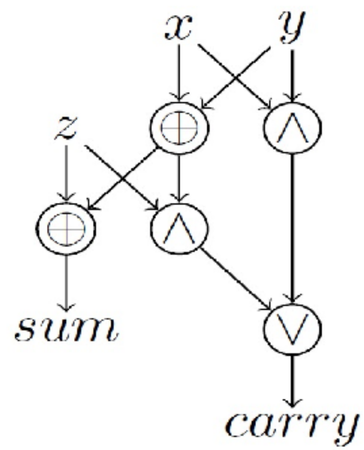
III. Complexity and depth of formulae

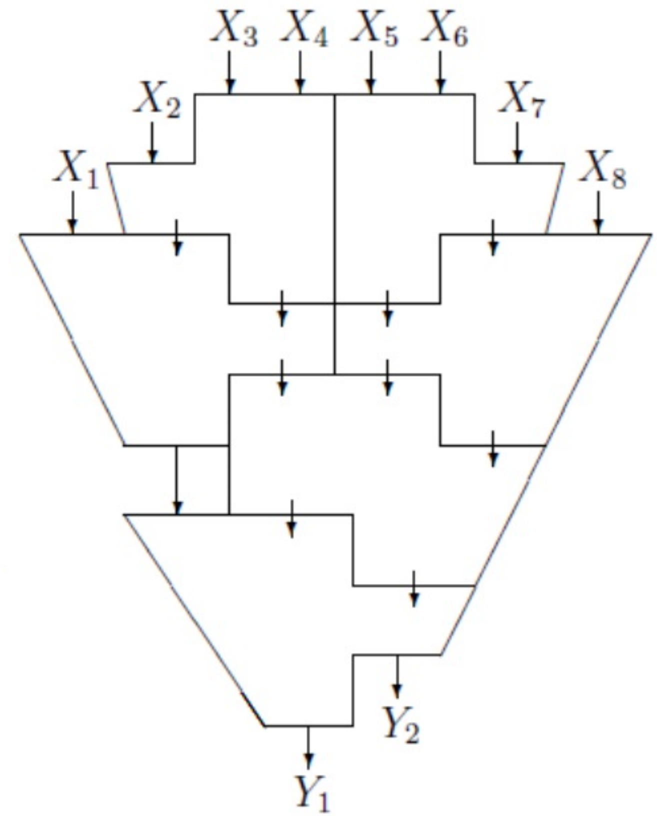
(k,l)-compressor: $(X_1,\ldots,X_k) \to (Y_1,\ldots,Y_l)$, $\sum_{i=1}^{k} X_i = \sum_{j=1}^{l} Y_j$.

Potential method:

$p(v) = \lambda^d$ — potential of a vertex v on depth d.

Claim. For an appropriate λ, $\sum_v p(v)$ does not decrease while adding compressors.





For a $(3,2)$-compressor on fig.: $\lambda \approx 1.2056 \leftarrow \lambda^3 + \lambda^2 = \lambda + 2$.

Corol. $D(n \to 2) \geq \log_\lambda(n/2) \approx 3.71 \log_2 n$

Formula complexity

Potential of a formula F: $(\mathsf{L}(F))^\mu$ for an appropriate μ

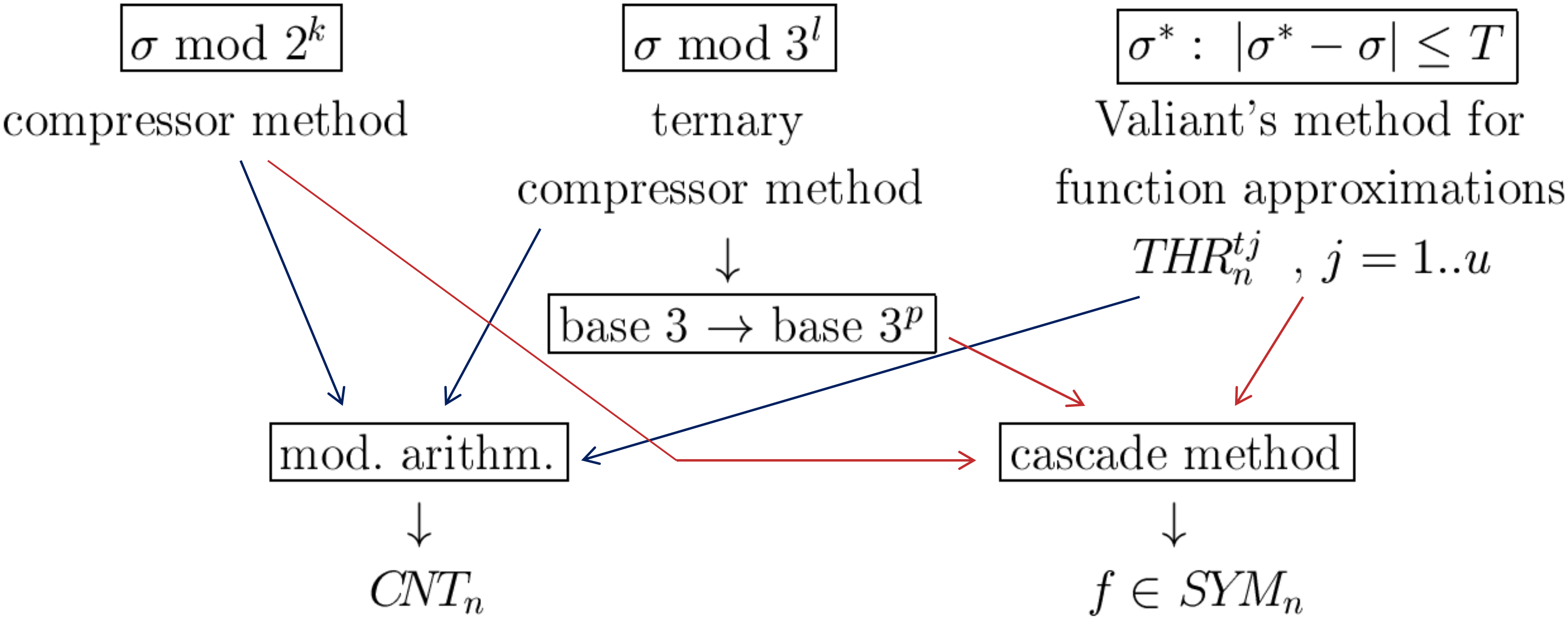
$$\mathsf{D}(CNT_n) \leq \log_\lambda n + O(1), \quad \mathsf{L}(CNT_n) \leq n^{1/\mu + o(1)}$$

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

III. Complexity and depth of formulae

General method (I. S. Sergeev, 2016)

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



	$L_{\mathcal{B}_0}$	$L_{\mathcal{B}_2}$	$D_{\mathcal{B}_0}$	$D_{\mathcal{B}_2}$
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. Complexity and depth of formulae

Lower bounds:

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

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

$\mathsf{L}_{\mathcal{B}}(SYM_n) = \Omega(n \log n)$, $\mathcal{B}$ — complete basis, (D. Yu. Cherukhin, 2000)

Bounds for threshold functions:

$\mathsf{L}_{\mathcal{B}_0}(THR_n^2) = n\lfloor \log_2 n \rfloor + 2(n - 2^{\lfloor \log_2 n \rfloor})$ (R. E. Krichevskii, 1964; S. A. Lozhkin, 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)

Upper bounds for 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	$n^{2.59}$ [Lup65]	n^2 [FMP82]	$2.80 \log_2 n$ [Serg16]	$2 \log_2 n$ [McColl77]
5	$n^{3.22}$ [Serg16]	$n^{2.84}$ [Serg16]	$3.35 \log_2 n$ [Serg16]	$3 \log_2 n$, follows from [VL87]
7	$n^{3.63}$ [Serg16]	$n^{2.59}$ [VL87]	$3.87 \log_2 n$ [Serg16]	$2.93 \log_2 n$ [Serg16]

(O. B. Lupanov, 1965; W. McColl, 1977; FMP,1982; D. C. van Leijenhorst, 1987; I. S. Sergeev, 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. Complexity and depth of formulae

Formulae for periodic functions:

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

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

$$\boxed{\mathsf{L}_{\mathcal{B}_0}(MOD^m_n) \preceq n^{1+\log_2 m}} \qquad \text{(O. B. Lupanov, 1965)}$$

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

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

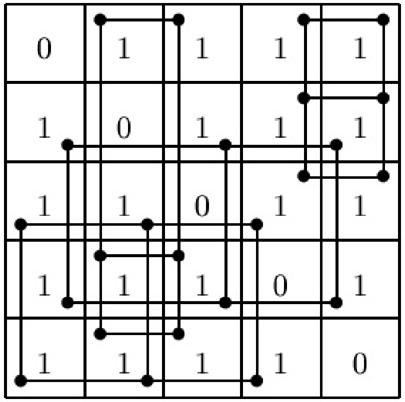
New formulae:

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

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

Example: $m = 5, |S| = 4$

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



IV. Complexity of switching circuits

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

$\mathsf{K}(MOD_n^m) = 2s_m n - O(1)$, for constant m (M. I. Grinchuk, 1987)

(s_m — sum of primary divisors of m)

$\mathsf{K}(SYM_n) \le (2 + o(1))n^2/\log_2 n$ (O. B. Lupanov, 1965)

$\mathsf{K}(SYM_n) \succeq n \log\log\log^* n$ (M. I. Grinchuk, 1989; A. A. Razborov, 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)

Monotone switching circuits

$\mathsf{K}_+(THR_n^k) \ge k(n - k + 1)$ (A. A. Markov, 1962)

$\mathsf{K}_+(THR_n^2) = n\lfloor \log_2 n \rfloor + 2(n - 2^{\lfloor \log_2 n \rfloor})$ (R. E. Krichevskii; 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)

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