A relation between additive and multiplicative complexity of Boolean functions*

Igor S. Sergeev†

Abstract

In the present note we prove an asymptotically tight relation between additive and multiplicative complexity of Boolean functions with respect to implementation by circuits over the basis $\{\oplus, \wedge, 1\}$.

To start, consider a problem of computation of polynomials over a semiring $(K, +, \times)$ by circuits over the arithmetic basis $\{+, \times\} \cup K$.

It's a common knowledge that a polynomial of n variables with nonscalar multiplicative complexity M (i.e. the minimal number of multiplications to implement the polynomial, not counting multiplications by constants) has total complexity $O(M(M+n))$. Generally speaking, the bound could not be improved for infinite semirings. For instance, it follows from results by E. G. Belaga [1] and V. Ya. Pan [8] (there exist 1-variable complex and real polynomials of degree n with additive complexity n; at the same time, each such polynomial has nonscalar multiplicative complexity $O(\sqrt{n})$ [9]).

An analogous standard bound for finite semirings is $O(M(M+n)/\log M)$. Generally speaking, this bound is also tight in order. A result of such sort was proven in [11].[1] We prove a similar but asymptotically tight result.

Theorem 1. *If a Boolean function of n variables can be implemented by a circuit over the basis $\{\oplus, \wedge, 1\}$ of multiplicative complexity $M = \Omega(n)$, then it can be implemented by a circuit of total complexity $(1/2 + o(1))M(M + 2n)/\log_2 M$ over the same basis. The bound is asymptotically optimal.*

*Research supported in part by RFBR, grants 11–01–00508, 11–01–00792, and OMN RAS "Algebraic and combinatorial methods of mathematical cybernetics and information systems of new generation" program (project "Problems of optimal synthesis of control systems").

†e-mail: isserg@gmail.com

[1] [11] deals with monotone Boolean circuits.

The stated result is nearly folklore, since it's an immediate corollary of results by E. I. Nechiporuk of early 1960s. However, these results are little known, and the corollary is even less known. Thus, it seems appropriate to give a proof.

The second claim of the theorem (the bound optimality) holds since almost all Boolean functions of n variables have multiplicative complexity $\sim 2^{n/2}$ [5][2] and total complexity $\sim 2^n/n$ [4].

Let us prove the first claim.

Let A be a Boolean matrix of size $m \times n$ (m rows, n columns). Assign 1 to each entry of matrix which is located at most $\log_2 m$ positions from a one of matrix A in the same row. We denote by $S(A)$ a weight[3] of the obtained matrix and name it an *active square* of matrix A.

The following lemma is an appropriate reformulation of particular case of a result due to Nechiporuk [6, 7]. In what follows, under an implementation of a matrix we understand an implementation of a linear operator with that matrix.

Lemma 1. *Any Boolean matrix A of size $m \times n$ can be implemented by an additive circuit*[4] *of complexity* $\frac{S(A)}{2\log_2 m} + o\left(\frac{(m+n)^2}{\log m}\right)$.

Proof. Divide a set of n variables into groups of $s < \log_2 m$. All possible sums in every group can be trivially computed with complexity $< 2^s$.

Regard the computed sums as new variables and note that the problem is now reduced to implementation of a matrix of size $m \times 2^s\lceil n/s\rceil$ and weight $\leq S(A)/s$.

Divide the new matrix into horizontal sections of height p. Implement each section independently. For this, in each column of a section group all ones into pairs. Denote by $y_{i,j}$ a sum of (new) variables corresponding to columns with paired ones from i-th and j-th rows.

Compute all $y_{i,j}$ independently. Next, implement an i-th row of a section as $y_{i,1}+\ldots+y_{i,p}+z_i$, where z_i is a sum of variables corresponding to positions with odd ones.

Note that the total complexity of computation of all $y_{i,j}$ in all sections is at most as large as the half of matrix weight, that is, $S(A)/(2s)$, and the number of odd ones in each section is at most as large as the number of columns, i.e. $2^s\lceil n/s\rceil$. Therefore, the complexity of the described circuit is

[2] Instead of this result of Nechiporuk a trivial upper bound $\frac{3}{\sqrt{2}} \cdot 2^{n/2}$ from the later paper [2] is often cited.

[3] Weight of a matrix is the number of nonzero entries in it.

[4] Over any associative and commutative semigroup $(G, +)$.

bounded from above by

$$\frac{n2^s}{s} + \frac{S(A)}{2s} + mp + \left\lceil \frac{m}{p} \right\rceil 2^s \left\lceil \frac{n}{s} \right\rceil .$$

Assuming $p \sim m/\log^2 m$ and $s \sim \log_2 m - 3\log_2\log_2 m$, we obtain the required bound. $\square$

The bound of lemma is asymptotically tight. More general results of that sort established by N. Pippenger [10] and V. V. Kochergin [3].

Now we complete the proof of the theorem. Let a circuit S to implement a Boolean function f with multiplicative complexity M. Number all conjunction gates in the circuit in an order not contradicting the orientation. Denote by h_{2i-1}, h_{2i} input functions of i-th conjunction gate, and denote by g_i its output function.

Each function h_j is a linear combination of variables and functions g_i, where $1 \le i < j/2$. The function f itself is a linear combination of variables and all functions g_i.

Computation of all functions h_j, $j = 1, \ldots, 2M$, together with the function f as linear combinations of variables and functions g_i can be performed by a linear operator with matrix of size $(2M+1) \times (M+n)$ and active square $\le (2M+1)(n + M/2 + \log_2 M)$. To obtain the desired bound, implement this operator via the method of Lemma 1.

References

[1] Belaga E. G. Evaluation of polynomials of one variable with preliminary processing of the coefficients. Problems of Cybernetics. **5**. Pergamon Press, 1961, 1–13.

[2] Boyar J., Peralta R., Pochuev D. On the multiplicative complexity of Boolean functions over the basis $(\wedge, \oplus, 1)$. Theor. Comp. Sci. 2000. **235**, 43–57.

[3] Kochergin V. V. On the complexity of computations in finite Abelian groups. Matematicheskie Voprosy Kibernetiki. 1992. **4**, 178–217.

[4] Lupanov O. B. A method of circuit synthesis. Izvestiya VUZ, Radiofizika. 1958. **1**, 120–140 (in Russian).

[5] Nechiporuk E. I. On the complexity of schemes in some bases containing nontrivial elements with zero weights. Problemy Kibernetiki. 1962. **8**, 123–160 (in Russian).

[6] Nechiporuk E. I. Rectifier networks. Soviet Physics Doklady. 1963. **8**, 5–7.

[7] Nechiporuk E. I. On topological principles of self-correction. Problemy Kibernetiki. 1969. **21**, 5–102 (in Russian).

[8] Pan V. Ya. Some schemes for the evaluation of polynomials with real coefficients. Problems of Cybernetics. **5**. Pergamon Press, 1961, 14–32.

[9] Paterson M. S., Stockmeyer L. J. On the number of nonscalar multiplications necessary to evaluate polynomials. SIAM J. Comp. 1973. **2**, 60–66.

[10] Pippenger N. The minimum number of edges in graphs with prescribed paths. Math. System Theory. 1979. **12**, 325–346.

[11] Zwick U. On the number of ANDs versus the number of ORs in monotone Boolean circuits. Inf. Proc. Letters. 1996. **59**(1), 29–30.