On the multiplicative complexity of some Boolean functions

Svetlana N. Selezneva

Lomonosov Moscow State University

3rd Russian-Finnish Symposium
on Discrete Mathematics,
Petrozavodsk, September, 15–18, 2014

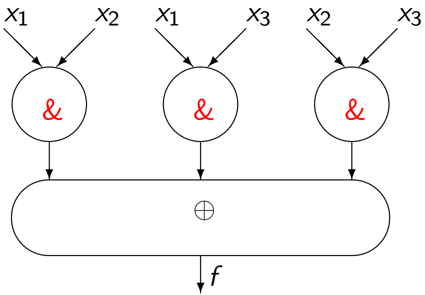
What is "the multiplicative complexity"?

We study the multiplicative complexity of Boolean functions.
What is this?

The multiplicative complexity $\mu(f)$ of a Boolean function $f(x_1, \ldots, x_n)$ is the minimal number of &-gates in circuits over the basis $\{x \& y, x \oplus y, 1\}$ which compute the function f.

Explanations

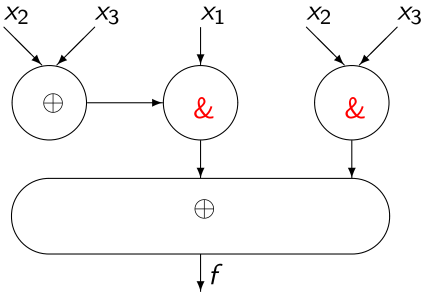
Consider the major function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$.
We can construct the following circuit by this expression:



We can conclude that $\mu(f) \leq 3$.

Explanations

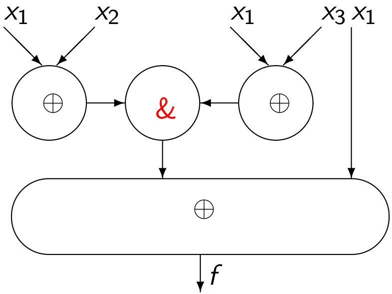
We can rewrite the major function $f(x_1, x_2, x_3)$ by the expression $x_1(x_2 \oplus x_3) \oplus x_2x_3$ and construct the circuit:



Therefore, $\mu(f) \leq 2$.

Explanations

At last, we can represent the major function $f(x_1, x_2, x_3)$ in the form $(x_1 \oplus x_2)(x_1 \oplus x_3) \oplus x_1$ and construct the circuit:



Thus, $\mu(f) \leq 1$, and it can be proved that $\mu(f) = 1$.

Motivations

- Studying complexity of circuits over bases with gates of zero weights

  A.A. Markov (1957 y.) studied the basis $\{x\&y, x \vee y, \bar{x}\}$ where &-gates and $\vee$-gates have the zero weights.

  E.I. Nechiporuk (1962 y.) studied different bases with gates of zero weights, in particular, the basis $\{x\&y, x \oplus y, 1\}$ where $\oplus$-gates have the zero weights.

Motivations

- Finding relations between different types of circuit complexity for Boolean functions

A. Kojevnikov, A.S. Kulikov (2012 y.) obtained a relation between the multiplicative complexity of some Boolean functions and lower bounds of circuits over the basis of all Boolean functions of two variables which compute these functions.

I.S. Sergeev (2013 y., by results of E.I. Nechiporuk) found the relation between the multiplicative complexity and the additive complexity, namely:
If there exists a circuit over the basis $\{\&, \oplus, 1\}$ with M, $M = \Omega(n)$, &-gates which computes a Boolean function f; then there exists a circuit over the same basis with $(1/2 + o(1))M(M + 2n)/\log_2 M$ gates which computes the function f.

Motivations

- More wide problems: studying number of multiplications to compute a function or a set of functions over arithmetic bases

  For example, the problem of mumber of arithmetic operations for matrix multiplication:
  V. Strassen (1970 y.) showed how to compute the product of two matrixes of the size 2×2 by 7 multiplications.

Boolean functions and polynomials

A **Boolean function** f of n variables is a mapping $B^n \to B$ where $B = \{0, 1\}$, $n = 0, 1, \ldots$.

Each Boolean function can be uniquely represented by its **Zhegalkin polynomial**, namely:

$$f(x_1, \ldots, x_n) = \bigoplus_{\alpha \in B^n : c_f(\alpha) = 1} K_\alpha$$

where $c_f(\alpha) = \bigoplus_{\beta \le \alpha} f(\beta) \in B$, $K_\alpha = \prod_{a_i = 1} x_i$, $\alpha = (a_1, \ldots, a_n) \in B^n$, and $K_{(0,\ldots,0)} = 1$.

The **degree** $\deg(f)$ of a Boolean function f:
$\deg(f) = \max_{\alpha \in B^n : c_f(\alpha) = 1} |\alpha|$.

Boolean functions and circuits

A **circuit** over the basis $\{x\&y, x \oplus y, 1\}$ is a directed acyclic graph with nodes of in-degree 0 or 2.

Nodes of in-degree 0 are marked by a variable of the set $\{x_1, \ldots, x_n\}$ or by the constant 1; they are called **inputs**.

Nodes of in-degree 2 are marked by & or by $\oplus$; they are called **gates**.

Denote the number of &-gates in a circuit S by $\mu(S)$.

For each node, a certain Boolean function is naturally computed in this node.

We say that a circuit S **computes** a Boolean function f, iff there exists a node in the circuit S such that f is computed in this node.

Quadratic and multi-affine functions

A Boolean function f is **quadratic**, iff $\deg(f) = 2$.

A Boolean function f is **affine**, iff $\deg(f) \leq 1$.

A Boolean function f is **multi-affine**, iff there exist affine functions $g_1, \ldots, g_l$ such that

$$f = \prod_{i=1}^{l} g_i.$$

Some known results

- **C.P. Schnorr** (1989 y.) showed that $\mu(f) \geq \deg(f) - 1$ for an arbitrary Boolean function $f(x_1, \ldots, x_n)$.
- **J. Boyar, R. Peralta, D. Pochuev** (2000 y.) proved that $\mu(f) \leq n + O(\sqrt{n})$ for an arbitrary symmetric Boolean function $f(x_1, \ldots, x_n)$.
- **T.I. Krasnova** (2012 y.) obtained the value of $\mu(f)$ where $f(x_1, \ldots, x_n)$ is the Boolean function with the threshold 2.

Quadratic functions

C.P. Schnorr (1989 y.), *R. Mirwald* (1992 y.) proved that if $q(x_1, \ldots, x_n)$ is a quadratic Boolean function; then $\mu(q) \leq \lfloor n/2 \rfloor$.

We obtain further results and prove

Theorem. *If a Boolean function $f(x_1, \ldots, x_n)$ can be represented in the form $x_1 \ldots x_n \oplus q(x_1, \ldots, x_n)$ where q is a quadratic function; then $\mu(f) = n - 1$ $(n \geq 3)$.*

Multi-affine functions

C.P. Schnorr (1989 y.) showed that if $f(x_1, \ldots, x_n)$ is a multi-affine Boolean function; then $\mu(f) = \deg(f) - 1$.

We obtain further results and prove

Theorem. *If a Boolean function $f(x_1, \ldots, x_n)$ can be represented in the form $f_1(x_1 \ldots x_n) \oplus f_2(x_1, \ldots, x_n)$ where f_1, f_2 are multi-affine Boolean functions; then*

1) $\mu(f) = n - 2$ *in the case of* $\deg(f_1) = \deg(f_2) = n$;

2) $\mu(f) = n - 1$ *in the case of* $\deg(f_1) = n$, $\deg(f_2) < n$;

3) $\mu(f) \leq n - 1$ *in the case of* $\deg(f_1) < n$, $\deg(f_2) < n$.

Technique of proofs

We use an algebraic technique and the following result

Theorem. *There exists a circuit over the basis* $\{x\&y, x \oplus y, 1\}$ *which computes both functions* $x_1 \ldots x_n$ *and* $\bar{x}_1 \ldots \bar{x}_n$*, and has* $(n-1)$ *&-gates* $(n \geq 1)$*.*

Methods (algorithms) to construct circuits

Let $f(x_1, \ldots, x_n)$ be an arbitrary Boolean function:

J. Boyar, R. Peralta, D. Pochuev (2000 y.) showed how to construct a circuit S'_f such that S'_f computes f, and
$\mu(S'_f) \leq \mathbf{2} \cdot \mathbf{2^{n/2}} - O(n)$ holds, if n is even, and
$\mu(S'_f) \leq (\mathbf{3}/\sqrt{\mathbf{2}}) \cdot \mathbf{2^{n/2}} - O(n)$ holds, if n is odd.

E.I. Nechiporuk (1962 y.) showed how to construct a circuit S''_f such that S''_f computes f, and $\mu(S''_f) \leq \mathbf{2^{n/2}} + o(2^{n/2})$. But his method is very complicated that he said himself in his paper.

We propose a quite simple method to construct a circuit S_f such that S_f computes f, and
$\mu(S_f) \leq (\mathbf{3}/\mathbf{2}) \cdot \mathbf{2^{n/2}} + o(2^{n/2})$ *holds, if n is even, and*
$\mu(S_f) \leq \sqrt{\mathbf{2}} \cdot \mathbf{2^{n/2}} + o(2^{n/2})$ *holds, if n is odd.*

Thank you for attention!