COMPLEXITY OF BOOLEAN FUNCTIONS IN A CLASS OF CANONICAL POLARIZED POLYNOMIALS

A. N. Alekseichuck

Relationships for the maximum of a minimal number of summands among all canonical polarized polynomials of a Boolean function are obtained.

Keywords: Boolean function, canonical polarized polynomial, complexity.

By a canonical polynomial of a Boolean function \( f = f(x_1, \ldots, x_n) \) polarized with respect to a Boolean vector \( \sigma = (\sigma_1, \ldots, \sigma_n) \) will be meant a polynomial whose terms have variable functions \( f \) corresponding to unit components of the vector \( \sigma \), only with negation, and variables corresponding to zero components of the vector \( \sigma \) only without negations. The complexity \( l(f) \) of the Boolean function \( f \) of \( n \) variables in a class of canonical polarized polynomials is determined by the minimum length (the number of terms) of all \( 2^n \) canonical polarized polynomials of the function \( f \). The Shannon function for the complexity of Boolean functions in a class of canonical polarized polynomials is determined as

\[
L(n) = \max_l(f),
\]

where the maximum is taken over all the functions \( f \) of \( n \) variables.

The canonical polarized polynomials are very important for the design of digital devices based on programmed logic matrices [1] and for the classification of Boolean functions [2], which explains, in particular, the substantial interest in the development of various algorithms for the construction of the mentioned polynomials and their minimization [3–8].

The function \( L(n) \) was studied and its estimates were obtained in [1, 8]. (It was shown in [1] that \( 2 \cdot 2^{n/2} - 2 \leq L(n) \) for even \( n \), the inequalities \( C_{n/2}^n \leq L(n) < 3 \cdot 2^{n-2} \), \( n \geq 2 \), are established, and the values of \( L(n) \) for \( n = 3, 4 \) are found in [8].)

In the present paper, the exact value of \( L(n) \) for all \( n \geq 1 \) is obtained and the method of construction of Boolean function \( f^{(n)} \) depending on \( n \) variables and such that \( L(n) = l(f^{(n)}) \) is obtained for each \( n \geq 2 \).

**THEOREM.** For \( n \geq 1 \), the following equalities hold:

\[
L(n) = \begin{cases} 
\frac{1}{3} (2^{n+1} - 1), & \text{if } n \text{ is odd;} \\
\frac{1}{3} (2^{n+1} - 2), & \text{if } n \text{ is even.}
\end{cases}
\]

Here, for each \( n \geq 2 \), the function \( f^{(n)} \) determined using the relations

\[
f^{(2)}(x_1, x_2) = \bar{x}_1 \bar{x}_2 \oplus 1,
\]

\[
f^{(n+1)}(x_1, \ldots, x_{n+1}) = x_1 f^{(n)}(x_2, \ldots, x_{n+1}) \oplus f^{(n)}(\bar{x}_2, \ldots, \bar{x}_{n+1}),
\]

\( n \geq 2 \).
satisfies the condition

\( l(f^{(n)}) = L(n) \). \hspace{1cm} (3)

To prove the formulated theorem, let us establish a number of auxiliary statements.

Denote by \( V_n \) a set of binary vectors of length \( n \). For any Boolean function \( f = f(x_1, \ldots, x_n) \) and vector \( \sigma = (\sigma_1, \ldots, \sigma_n) \), denote by \( f_{\sigma} \) the function \( f(x_1 \oplus \sigma_1, \ldots, x_n \oplus \sigma_n) \). We will denote by \( d(f) \) the length of the Zhegalkin polynomial of the function \( f \). It is shown in [8] that

\[
\min_{\sigma \in V_n} d(f_{\sigma}) = 0
\]

for any Boolean function \( f = f(x_1, \ldots, x_n) \).

**Lemma 1.** For any \( n \geq 1 \), the following inequality holds:

\[
L(n+1) \leq 2^n + \frac{1}{2} L(n). \hspace{1cm} (5)
\]

**Proof.** Let \( h = h(x_1, \ldots, x_{n+1}) \) be an arbitrary Boolean function of \( n+1 \) variables. Let us present the function \( h \) as

\[
h(x_1, \ldots, x_{n+1}) = x_1 f(x_2, \ldots, x_{n+1}) \oplus g(x_2, \ldots, x_{n+1}), \hspace{1cm} (6)
\]

where \( f \) and \( g \) are functions of \( n \) variables.

For any vector \( \sigma = (\sigma_2, \ldots, \sigma_{n+1}) \in V_n \), put \( \sigma(0) = (0, \sigma_2, \ldots, \sigma_{n+1}), \sigma(1) = (1, \sigma_2, \ldots, \sigma_{n+1}) \). Denote by \( d_{\sigma} \) the length of the polynomial, whose each term appears both in the Zhegalkin polynomial of the function \( f_{\sigma} \) and in the Zhegalkin polynomial of function \( g_{\sigma} \).

In view of (6), the following equalities hold:

\[
d(h_{\sigma(0)}) = d(f_{\sigma}) + d(g_{\sigma}), \hspace{1cm} (7)
\]

\[
d(h_{\sigma(1)}) = d(f_{\sigma}) + d(f_{\sigma} \oplus g_{\sigma}) = d(f_{\sigma}) + d(g_{\sigma}) - 2d_{\sigma}. \hspace{1cm} (8)
\]

Since the number of terms appearing in the Zhegalkin polynomial of at least one of the functions \( f_{\sigma}, g_{\sigma} \) does not exceed \( 2^n \), the following inequality is true:

\[
d(f_{\sigma}) + d(g_{\sigma}) - d_{\sigma} \leq 2^n. \hspace{1cm} (9)
\]

Based on (7)–(9), we obtain the following inequalities, true for any vector \( \sigma \in V_n \):

\[
d(h_{\sigma(0)}) \leq 2^n + d_{\sigma}, \hspace{1cm} (10)
\]

\[
d(h_{\sigma(1)}) \leq 2^n + d(f_{\sigma}) - d_{\sigma}. \hspace{1cm} (11)
\]

The existence of the vector \( \sigma = (\sigma_2, \ldots, \sigma_{n+1}) \in V_n \) for which the value of \( d(f_{\sigma}) \) does not exceed \( L(n) \) follows from the definition of \( L(n) \). If \( d_{\sigma} \leq \frac{1}{2} L(n) \), then \( d(h_{\sigma(0)}) \leq 2^n + \frac{1}{2} L(n) \) in view of (10), if \( d_{\sigma} \geq \frac{1}{2} L(n) \), then \( d(h_{\sigma(1)}) \leq 2^n + L(n) - \frac{1}{2} L(n) = 2^n + \frac{1}{2} L(n) \) in view of (11).

Thus, for any Boolean function \( h(x_1, \ldots, x_{n+1}) \), there exists a vector \( \tilde{\sigma} \in V_{n+1} \) such that the length of the Zhegalkin polynomial of the function \( h_{\tilde{\sigma}} \) does not exceed \( 2^n + \frac{1}{2} L(n) \). Hence, on the strength of (4), (5) holds. The lemma is proved.

**Lemma 2.** For any \( n \geq 1 \), the following inequalities hold:

\[
L(n) \leq \begin{cases} 
\frac{1}{3} (2^{n+1} - 1), & \text{if } n \text{ is odd;} \\
\frac{1}{3} (2^{n+1} - 2), & \text{if } n \text{ is even.}
\end{cases} \hspace{1cm} (12)
\]