Two canonical polynomial representations of Boolean functions are introduced: polynomial perfect normal form and polynomial derivative positive form in the Boolean function \( g \). We derive the necessary and sufficient conditions on the function \( g \) for the existence of such representations for any Boolean function.

One of the main stages in discrete logic design is the representation of Boolean functions by various forms \([1, 2]\). The widespread use in electronics of integrated circuits that include "modulo 2 adders" \([3]\) focuses the attention on the representation of Boolean functions by polynomial forms. In this paper, we introduce two types of canonical polynomial representations of Boolean functions: polynomial perfect normal form and polynomial derivative positive form in the Boolean function \( g \). We obtain necessary and sufficient conditions on the function \( g \) for the existence of such representations for any Boolean function. The proposed forms are a generalization of standard representations: the polynomial perfect normal form \([4]\) and the Zhegalkin polarized polynomial \([5]\). These standard representations are obtained from the new forms by taking the conjunction of variables as the function \( g \). An algorithm for minimization of the representation of functions by these forms is described.

Recall that a mixed derivative of Boolean function \( f(x_1, \ldots, x_n) \) with respect to variables \( x_{i_1}, \ldots, x_{i_m} \) \((1 \leq i_1 \leq \ldots \leq i_m \leq n)\) is the function \( \left. \frac{\partial^{m}}{\partial x_{i_1} \cdots \partial x_{i_m}} f(x_1, \ldots, x_n) \right|_{x_{i_1}=0, \ldots, x_{i_m}=0} \) of \((n-m)\) variables defined by equality \( f^{(m)}_{x_{i_1}, \ldots, x_{i_m}}(x_1, \ldots, x_n) = \sum f(x_{i_1}, \ldots, x_{i_m}, x_{i_1}, \ldots, x_{i_m}) \) where summation is over all the combinations \((a_1, \ldots, a_{i_m})\). Denote by \( f^{(\tau)}(x_1, \ldots, x_n) \) the mixed derivative of the function \( f(x_1, \ldots, x_n) \) with respect to the variables corresponding to 1s in the binary expansion \( \tau = 2^{n-1} \tau_1 + \ldots + 2^{0} \tau_n \), \( 0 \leq \tau \leq 2^{n} - 1 \). For simplicity, a mixed derivative will be called a derivative.

A function is called degenerate iff 
\[ f(x_1, \ldots, x_n) = 0 \] and nondegenerate otherwise. In other words, the vector of values of a degenerate function has an even number of 1s.

1. Polynomial Perfect Normal Forms in Boolean Functions

We say that the Boolean function \( f(x_1, \ldots, x_n) \) has a polynomial perfect normal form (PPNF) in the Boolean function \( g(x_1, \ldots, x_n) \) if it is uniquely representable in the form
\[
f(x_1, \ldots, x_n) = \sum_{s=0}^{p} a_s g(x_1^s, \ldots, x_n^s),
\]
where \( \tau = \tau_{m}2^0 + \ldots + \tau_12^{n-1}, a_s \in \{0, 1\} \).

**THEOREM** (on the existence of PPNF). Any Boolean function \( f(x_1, \ldots, x_n) \neq 0 \) has a PPNF in the Boolean function \( g(x_1, \ldots, x_n) \) if and only if \( g(x_1, \ldots, x_n) \) is a nondegenerate function, and \( a_s = (g(x_1^s, \ldots, x_n^s))^{(\tau)} \).

**Proof** is by the method of undetermined coefficients. To find the coefficients \( a_0, \ldots, a_p \), transform the expression (1) into a system of \( 2^n \) equations in \( 2^n \) unknowns, where each equation is the expression (1) for a particular combination of the variables \((x_1, \ldots, x_n)\):
\[
\begin{align*}
a_{0} & \oplus a_{1} (1, \ldots, 1) \oplus a_{1} (1, \ldots, 1, 0) \oplus \ldots \oplus a_{p} (0, \ldots, 0) = f(0, \ldots, 0), \\
a_{0} & \oplus a_{1} (1, \ldots, 1, 0) \oplus a_{1} (1, \ldots, 1) \oplus \ldots \oplus a_{p} (0, \ldots, 0, 1) = f(0, \ldots, 0, 1),
\end{align*}
\]

or equivalently in matrix notation

$$G \cdot A = F,$$  

(2)

where $G$ is the matrix of values of the function $g(x_1, x_2, \ldots, x_n)$ according to the system, $A = (\alpha_0, \alpha_1, \ldots, \alpha_p)^T$, $F = (f(0, 0, 0, \ldots, 0), f(0, 0, 1, \ldots, 1), \ldots, f(1, 1, 1, \ldots, 1))^T$. Note that the matrix $G$ satisfies the equality

$$G = G^T$$

(3)

because of the obvious identity $g(\alpha_1, \ldots, \alpha_n) = g(\alpha_1^T, \ldots, \alpha_n^T)$. Consider the product $G^T \cdot G$. By equality (3), it suffices to consider all possible products of the columns of $G$, i.e., the sums

$$s_{ij} = \sum g(\delta_1^i, \ldots, \delta_n^i) \cdot g(\delta_1^j, \ldots, \delta_n^j),$$

(4)

where summation is over all the combinations $(\delta_1, \ldots, \delta_n)$ and the combinations $(\sigma_1, \ldots, \sigma_n)$ and $(\tau_1, \ldots, \tau_n)$ are binary representations of the numbers $i$ and $j$, respectively.

For $i = j$, the combinations $(\sigma_1, \ldots, \sigma_n)$ and $(\tau_1, \ldots, \tau_n)$ are identical and (4) is transformed as follows:

$$s_{ii} = \sum g(\delta_1^i, \ldots, \delta_n^i) \cdot g(\delta_1^i, \ldots, \delta_n^i) = \sum g(\delta_1^i, \ldots, \delta_n^i) = \sum g(\delta_1^i, \ldots, \delta_n^i) = g^{(0)}(x_1, \ldots, x_n).$$

Hence it follows that $s_{ii} = 1$ if and only if the function $g(x_1, \ldots, x_n)$ is nondegenerate.

Let $i \neq j$. We will show that in this case $s_{ij} = 0$. To prove this fact, define the functions $\varphi_l, l \in \{0, \ldots, p\}$, on the columns of the matrix $G$. Let $A = (\alpha_0, \alpha_1, \ldots, \alpha_p)$ be a column of the matrix $G$. Then let $\varphi_l(A) = (\varphi_l(\alpha_0), \ldots, \varphi_l(\alpha_p)) = (\alpha_{l(0)}, \ldots, \alpha_{l(p)})$. For natural $k, l \leq p$ such that $k = \beta_n - 2^{n-1} - \cdots - 2^0 \beta_0, l = \gamma_n - 2^{n-1} - \cdots - 2^0 \gamma_0$, where $\beta_n, \gamma_n \in \{0, 1\}$, define $\varphi_l(k)$ as $\varphi_l(k) = (\beta_{n-1} \oplus \gamma_{n-1}) 2^{n-1} + \cdots + 2^0 (\beta_0 \oplus \gamma_0)$. These functions obviously act as permutations of the elements of the column $A$.

Note simple properties of these functions:

1) $\varphi_l(\varphi_l(A)) = A$, 2) $\varphi_l(\varphi_l(A)) = \varphi_l(\varphi_l(A))$, 3) $\varphi_l(A_0) = A_0$, 4) $A_0 = \varphi_l(\varphi_l(A_0))$,

where $A$ is any column of the matrix $G$ and $A_0$ is the $i$-th column of the matrix $G$ (the indexing starts with 0).

The first two properties follow directly from definitions. To prove the third property, consider an arbitrary element $a_r$ of the column $A_0$. In our indexing, $a_r = g(\tau_1, \ldots, \tau_n)$, where $\tau = 2^{n-1} \tau_1 + \cdots + 2^0 \tau_n$. Let $a = 2^{n-1} \sigma_1 + \cdots + 2^0 \sigma_n$. Then by definition of the functions $\varphi$

$$\varphi_\sigma(a) = 2^{n-1} (\tau_1 + \sigma_1) + \cdots + 2^0 (\tau_n + \sigma_n),$$

$$\varphi_\sigma(a_0) = g((\tau_1 + \sigma_1)^0, \ldots, (\tau_n + \sigma_n)^0) = g((\delta_1^i, \ldots, \delta_n^i)).$$

By construction of the matrix $G$, the right-hand side of this equality is the $\tau$-th element of the column $A_0$.

The last property easily follows from properties 1-3.

To complete examination of case $i \neq j$, note that if sum (4) contains the term $g(\delta_1^i, \ldots, \delta_n^i) \cdot \varphi_j(g(\delta_1, \ldots, \delta_n))$, then it also contains the term $\varphi_j(g(\delta_1^i, \ldots, \delta_n^i)) \cdot g(\delta_1, \ldots, \delta_n)$. which is equal to the former by properties 1-4. The sum $s_{ij}$ thus contains an even number of 1s, i.e., $s_{ij} = 0$.

The determinant of the matrix $G$ thus does not vanish if and only if the function $g(x_1, \ldots, x_n)$ is nondegenerate. Hence follows existence and uniqueness of the coefficients in the expansion ($1$).

Left-multiply by $G$ the equality (2) for a nondegenerate function: $G \cdot G \cdot A = G \cdot F$. We have proved that $G \cdot G = E$. Then $\alpha = 1$ if and only if $\sum g(\delta_1^i, \ldots, \delta_n^i) \cdot f(\delta_1, \ldots, \delta_n) = 1$, where the sum is over all the combinations $(\delta_1, \ldots, \delta_n)$ and $\tau = 2^{n-1} \tau_1 + \cdots + 2^0 \tau_n$. This is equivalent to nondegeneracy of the function $g(x_1, \ldots, x_n) \& f(x_1, \ldots, x_n)$. Q.E.D.