POLYNOMIAL EXPANSIONS OF BOOLEAN FUNCTIONS WITH RESPECT TO NONDEGENERATE FUNCTIONS

S. F. Vinokurov and N. A. Peryazev

UDC 519.95

Results on the representation of functions by terms over systems of functions are basic in the theory of Boolean functions [1]. Canonical expansions are of special interest. For example, the following polynomial expansion of Boolean functions is well known:

$$f(x_1,\ldots,x_n)=\sum x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m}\cdot f(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n), \tag{1}$$

where the summation is carried over all the sets $(\sigma_1,\ldots,\sigma_m)$. Let us observe that this expansion is obtained from the Shennon expansion by the simple replacement of disjunction by addition module 2. A survey of the results, based on this polynomial expansion, is given in [2].

Let us recall that the function $f^{(m)}_{x_{i_1}\ldots x_{i_m}}(x_1,\ldots,x_n)$ of $(n-m)$ number of variables, defined by the equation

$$f^{(m)}_{x_{i_1}\ldots x_{i_m}}(x_1,\ldots,x_n)=\sum f(x_1,\ldots,\sigma_{i_1},\ldots,\sigma_{i_m},\ldots,x_n),$$

where the summation is carried over all the sets $(\sigma_1,\ldots,\sigma_m)$. is called the mixed derivative of the Boolean function $f(x_1,\ldots,x_n)$ with respect to the variables $x_{i_1},\ldots,x_{i_m}$ $(1\leq i_1\leq\ldots\leq i_m\leq n)$. Further, for brevity, we will call a mixed derivative simply a derivative.

We call a function degenerate if $f^{(n)}_{x_1\ldots x_n}(x_1,\ldots,x_n)=0$ and nondegenerate in the contrary case. It is obvious that the derivatives preserve (non)degeneracy.

We will say that a Boolean function $f(x_1,\ldots,x_n)$ has a polynomial expansion with respect to a Boolean function $g(x_1,\ldots,x_m,y)$ for $m\leq n$ if the following equation is valid:

$$f(x_1,\ldots,x_n)=\sum g(x_1^{\tau_1},\ldots,x_m^{\tau_m},f^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)), \tag{2}$$

where $\tau=g^{(m)}_{x_1\ldots x_m}(x_1,\ldots,x_m,1)$, and the summation is carried over all the sets $(\sigma_1,\ldots,\sigma_m)$ and $(\tau_1,\ldots,\tau_m)$, for which $g'_y(\sigma_1^{\tau_1},\ldots,\sigma_m^{\tau_m},y)=1$.

<u>THEOREM 1 (on the Polynomial Expansions of Functions).</u> Each Boolean function $f(x_1,\ldots,x_n)$ has a polynomial expansion with respect to the Boolean function $g(x_1,\ldots,x_m,y)$, $m\leq n$, if and only if the function $g(x_1,\ldots,x_m,y)$ is nondegenerate.

Irkutsk State University, Irkutsk. Translated from Algebra i Logika, Vol. 30, No. 6, pp. 631-637, November-December, 1991. Original article submitted March 11, 1991.

Proof. Let the function $g(x_1,\ldots,x_m,y)$ be nondegenerate. By expansion (1), we have

$$g(x_1,\ldots,x_m\ y)=y\cdot g(x_1,\ldots,x_m\ 1)\oplus\bar{y}\cdot g(x_1,\ldots,x_m,0).$$

By virtue of this equation, we transform the sum in the right-hand side of (2):

$$\sum g(x_1^{\tau_1},\ldots,x_m^{\tau_m},f^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n))=$$

$$=\sum(f^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\cdot g(x_1^{\tau_1},\ldots,x_m^{\tau_m},1)\oplus$$

$$\oplus\bar{f}^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\cdot g(x_1^{\tau_1},\ldots,x_m^{\tau_m},0))=$$

$$=\sum(f^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\cdot g'_y(x_1^{\tau_1},\ldots,x_m^{\tau_m},y))\oplus\sum g(x_1^{\tau_1},\ldots,x_m^{\tau_m},0).$$

On each set $(\tau_1,\ldots,\tau_m)$ there exist an odd number of sets $(\sigma_1,\ldots,\sigma_m)$ such that $g'_y(\sigma_1^{\tau_1},\ldots,\sigma_m^{\tau_m},y)=1$ since this derivative is a nondegenerate function. Therefore,

$$\sum g(x_1^{\tau_1},\ldots,x_m^{\tau_m},0)=\sum_{(\tau_1,\ldots,\tau_m)}g(x_1^{\tau_1},\ldots,x_m^{\tau_m},0).$$

Here in the left-hand side of the equation the summation is carried over the sets $(\tau_1,\ldots,\tau_m)$ and $(\sigma_1,\ldots,\sigma_m)$, such that $g'_y(\sigma_1^{\tau_1},\ldots,\sigma_m^{\tau_m},y)=1$, and the summation in the right-hand side is carried only over all the sets $(\tau_1,\ldots,\tau_m)$. Further, since the summation in the right-hand side is carried over all the sets $(\tau_1,\ldots,\tau_m)$, it is independent of $x_1,\ldots,x_m$ and therefore the following chain of equations holds:

$$\sum_{(\tau_1,\ldots,\tau_m)}g(x_1^{\tau_1},\ldots,x_m^{\tau_m},0)=\sum_{(\tau_1,\ldots,\tau_m)}g(\tau_1,\ldots,\tau_m,0)=$$

$$=g^{(m)}_{x_1\ldots x_m}(x_1,\ldots,x_m,0)=g^{(m)}_{x_1\ldots x_m}(x_1,\ldots,x_m,1)\oplus 1=\bar{\tau}.$$

We continue transformation of the right-hand side of Eq. (2):

$$\sum(f^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\cdot g'_y(x_1^{\tau_1},\ldots,x_m^{\tau_m},y))\oplus\bar{\tau}=$$

$$=\sum_{(\sigma_1,\ldots,\sigma_m)}f^{\tau}(\sigma_1,\ldots,\sigma_m,x_{m+1},\ldots,x_n)\cdot\Big[\sum_{(\tau_1,\ldots,\tau_m)}g'_y(x_1^{\tau_1},\ldots,x_m^{\tau_m},y)\Big]\oplus\bar{\tau},$$

where the first sum is carried over all the sets $(\sigma_1,\ldots,\sigma_m)$, and the second one is carried over those $(\tau_1,\ldots,\tau_m)$, for which $g'_y(\sigma_1^{\tau_1},\ldots,\sigma_m^{\tau_m},y)=1$ for a fixed set $(\sigma_1,\ldots,\sigma_m)$.

We prove the equality

$$\sum_{(\tau_1,\ldots,\tau_m)}g'_y(x_1^{\tau_1},\ldots,x_m^{\tau_m},y)=x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m},\qquad(3)$$

where the summation is carried over all the sets $(\tau_1,\ldots,\tau_m)$, for which $g'_y(\sigma_1^{\tau_1},\ldots,\sigma_m^{\tau_m},y)=1$. The right-hand side of (3) is equal to 1 for $x_i = \sigma_i$, $i \in \{1,\dots,m\}$. Since the function $g(x_1,\dots,x_m, y)$ is nondegenerate, the sum in the left-hand side is also equal to 1. Let the right-hand side be equal to 0. Then $x_i=\bar{\sigma}_i$ for a certain i (without loss of generality, we can assume that $i=1$ and $x_j=\sigma_j$ for the remaining variables). If there are no sets $(\tau_1,\dots,\tau_m)$ such that $g'_y(\sigma_1^{\tau_1},\dots,\sigma_m^{\tau_m}, y)=g'_y(\bar{\sigma}_1^{\tau_1},\dots,\sigma_m^{\tau_m}, y)=1$, then the left-hand side of Eq. (3) is a sum of zeros. In the contrary case, for a set $(\tau_1,\dots,\tau_m)$ with the property $g'_y(\sigma_1^{\tau_1},\dots,\sigma_m^{\tau_m}, y) = g'_y(\bar{\sigma}_1^{\tau_1},\dots,\sigma_m^{\tau_m}, y)=1$ the set $(\bar{\tau}_1,\dots,\tau_m)$ satisfies the equation $g'_y(\sigma_1^{\bar{\tau}_1},\dots,\sigma_m^{\tau_m} y)=1$. Consequently, we carry out the summation over it. Thus, the sum over these two sets is equal to zero. Therefore, the left-hand side of (3) is equal to zero.

Considering the obtained equation, we transform the right-hand side as follows:

$$\sum_{(\sigma_1,\dots,\sigma_m)} f^{\tau}(\sigma_1,\dots,\sigma_m, x_{m+1},\dots,x_n)\cdot x_1^{\sigma_1}\cdot\dots\cdot x_m^{\sigma_m} \oplus \bar{\tau} =$$

$$= \sum_{(\sigma_1,\dots,\sigma_m)} (f^{\tau}(\sigma_1,\dots,\sigma_m, x_{m+1},\dots,x_n) \oplus \bar{\tau})\cdot x_1^{\sigma_1}\cdot\dots\cdot x_m^{\sigma_m} =$$

$$= \sum_{(\sigma_1,\dots,\sigma_m)} f(\sigma_1,\dots,\sigma_m, x_{m+1},\dots,x_n)\cdot x_1^{\sigma_1}\cdot\dots\cdot x_m^{\sigma_m} = f(x_1,\dots,x_n).$$

The last equality follows from (1), which completes the proof of the existence of expansion (2).

In the reverse direction, the proof of the theorem follows from the degeneracy of a sum of degenerate functions.

We will say that a Boolean function $f(x_1,\dots,x_n)$ has canonical polynomial form with respect to a Boolean function $g(x_1,\dots,x_n)$ if it can be represented uniquely (up to permutation of terms) in the form

$$f(x_1,\dots,x_n) = \sum g(x_1^{\tau_1},\dots,x_n^{\tau_n}), \tag{4}$$

where the summation is carried over all the sets $(\tau_1,\dots,\tau_n)$, for which the function $g(x_1^{\tau_1},\dots,x_n^{\tau_n})\cdot f(x_1,\dots,x_n)$ is nondegenerate.

<u>COROLLARY (on Canonical Polynomial Forms).</u> Each Boolean function $f(x_1,\dots,x_n)\neq 0$ has a canonical polynomial form with respect to a Boolean function $g(x_1,\dots,x_n)$ if and only if $g(x_1,\dots,x_n)$ is a nondegenerate function.

<u>Proof.</u> By virtue of Theorem 1, we have the expansion of $f(x_1,\dots, x_n)$ with respect to the nondegenerate function $h(x_1,\dots,x_n,y)=g(x_1,\dots,x_n)\cdot y$ in the form

$$f(x_1,\dots,x_n) = \sum h(x_1^{\tau_1},\dots,x_n^{\tau_n}, f^{\tau}(\sigma_1,\dots,\sigma_n)),$$

where the summation is carried over all the sets $(\sigma_1,\dots,\sigma_n)$ and $(\tau_1,\dots,\tau_n)$, that satisfy the condition $h'_y(\sigma_1^{\tau_1},\dots,\sigma_n^{\tau_n} y)=1$ and $\tau=h^{(n)}_{x_1\dots x_n}(x_1,\dots,x_n, 1)$. By the definition of a derivative, τ is computed immediately:

$$\tau = \sum h(\sigma_1,\dots,\sigma_n,1) = \sum g(\sigma_1,\dots,\sigma_n)\cdot 1 = 1,$$

where the summation is carried over all the sets $(\sigma_1,\dots,\sigma_n)$. Let us observe that

$$h'_y(\sigma_1^{\tau_1},\dots,\sigma_n^{\tau_n},y) = g(\sigma_1^{\tau_1},\dots,\sigma_n^{\tau_n})\cdot 0 \oplus g(\sigma_1^{\tau_1},\dots,\sigma_n^{\tau_n})\cdot 1.$$

Thus, we get the canonical polynomial form

$$f(x_1,\dots,x_n) = \sum g(x_1^{\tau_1},\dots,x_n^{\tau_n}),$$

in which the summation is carried over all the sets $(\tau_1,\dots,\tau_n)$, for which there exist an odd number of sets $(\sigma_1,\dots,\sigma_n)$ such that $g(\sigma_1^{\tau_1},\dots,\sigma_n^{\tau_n})=1$ and $f(\sigma_1,\dots,\sigma_n)=1$. This is equivalent to the equation

$$\sum g(\sigma_1^{\tau_1},\dots,\sigma_n^{\tau_n})\cdot f(\sigma_1,\dots,\sigma_n) = 1,$$

where the summation is carried over all the sets $(\sigma_1,\dots,\sigma_n)$, which is equivalent to the nondegeneracy of the function $g(x_1^{\tau_1},\dots,x_n^{\tau_n})\cdot f(x_1,\dots,x_n)$.

The uniqueness of form (4) follows from the equality of the number of different functions and different canonical forms in the same number of variables.

The proof of the corollary in the reverse direction is as simple as that of the theorem.

We often need specification of Boolean functions by terms over fixed systems of functions. In this case, for the application of the decompositions theorem the term presentation of nondegenerate functions is useful.

We call a term $t(x_1,\dots,x_n)$ complete if each variable x_i occurs at least once in its expression and elementary if it occurs at most once, and, moreover, constants do not occur in its composition.

THEOREM 2 (Term Presentation of Nondegenerate Functions). The Boolean function $f(x_1,\dots,x_n)$, defined by a term $t(x_1,\dots,x_n)$ over a system of functions S, is nondegenerate if $t(x_1,\dots,x_n)$ has the form

$$t(x_1,\dots,x_n) = \sum_{i=1}^{2m+1} t_i(x_1,\dots,x_n) \oplus \sum_{j=1}^{k} h_j(x_1,\dots,x_n), \tag{5}$$

where $t_i(x_1,\dots,x_n)$ are complete elementary terms over nondegenerate functions from S, and $h_j(x_1,\dots,x_n)$ are incomplete terms over S.

Conversely, each nondegenerate Boolean function $f(x_1,\dots,x_n)$ can be represented over the system S, containing only one nondegenerate function of at least two (exactly two) variables, in the form

$$f(x_1,\dots,x_n)=t(x_1,\dots,x_n)\oplus\sum_{j=1}^{k}h_j(x_1,\dots,x_n), \tag{6}$$

where $t(x_1,\dots,x_n)$ is a complete (complete elementary) term over a nondegenerate function from $\mathcal{S}$ and $h_j(x_1,\dots,x_n)$ are incomplete terms over $\mathcal{S}$.

Proof. Each complete elementary term over nondegenerate functions defines a nondegenerate function. Indeed, nondegeneracy of the functions $u(x_1,\dots,x_\ell)$ and $v(x_1,\dots,x_\rho)\ (\ell,\rho\geq 1)$ implies the nondegeneracy of the function

$$w(x_1,\dots,x_{\ell+\rho-1})=u(x_1,\dots,x_i,v(x_{i+1},\dots,x_{i+\rho}),x_{i+\rho+1},\dots,x_{\ell+\rho-1}),$$

since, by virtue of (1), we get

$$w(x_1,\dots,x_{\ell+\rho-1})=\bar{v}(x_{i+1},\dots,x_{i+\rho})\cdot u(x_1,\dots,x_i,0,x_{i+\rho+1},\dots,x_{\ell+\rho-1})\oplus$$

$$\oplus v(x_{i+1},\dots,\overline{x}_{i+\rho})\cdot u(x_1,\dots,x_i,1,x_{i+\rho+1},\dots,x_{\ell+\rho-1})=$$

$$=v(x_{i+1},\dots,x_{i+\rho})\cdot u'_y(x_1,\dots,x_i,y,x_{i+\rho+1},\dots,x_{\ell+\rho-1})\oplus u(x_1,\dots,x_i,0,x_{i+\rho+1},\dots,x_{\ell+\rho-1}).$$

Hence

$$w^{(\ell+\rho-1)}_{x_1\dots x_{\ell+\rho-1}}(x_1,\dots,x_{\ell+\rho-1})=$$

$$=\sum_{(\sigma_1,\dots,\sigma_{\ell+\rho-1})}\Big[v(\sigma_{i+1},\dots,\sigma_{i+\rho})\cdot u'_y(\sigma_1,\dots,\sigma_i,y,\sigma_{i+\rho+1},\dots,\sigma_{\ell+\rho-1})\oplus$$

$$\oplus u(\sigma_1,\dots,\sigma_i,0,\sigma_{i+\rho+1},\dots,\sigma_{\ell+\rho-1})\Big]=\sum_{(\sigma_{i+1},\dots,\sigma_{i+\rho})}\Big[v(\sigma_{i+1},\dots,\sigma_{i+\rho})\times$$

$$\times\Big[\sum_{(\sigma_1\dots\sigma_i\dots\sigma_{i+\rho+1}\dots\sigma_{\ell+\rho-1})}u'_y(\sigma_1,\dots,\sigma_i,y,\sigma_{i+\rho+1},\dots,\sigma_{\ell+\rho-1})\Big]\Big]\oplus$$

$$\oplus\sum_{r=1}^{2^\rho}\Big[\sum_{(\sigma_1\dots\sigma_i\dots\sigma_{i+\rho+1}\dots\sigma_{\ell+\rho-1})}u(\sigma_1,\dots,\sigma_i,0,\sigma_{i+\rho+1},\dots,\sigma_{\ell+\rho-1})\Big]=$$

$$=v^{(\rho)}(x_{i+1},\dots,x_{i+\rho})\cdot u^{(\ell)}_y(x_1,\dots,x_i,y,x_{i+\rho+1},\dots,x_{\ell+\rho-1})\oplus 0=$$

$$=v^{(\rho)}(x_1,\dots,x_\rho)\cdot u^{(\ell)}(x_1,\dots,x_\ell)=1\cdot 1=1.$$

To prove the theorem in forward direction, we observe that each sum of two (non)degenerate functions is (non)degenerate and each sum of a nondegenerate function and a degenerate function is nondegenerate. Therefore, the term in the right-hand side of (5) is a nondegenerate function.

We show that the converse state is also valid. By the substitution of $\bar{x}$ and x (or constants) in a nondegenerate function of more than two variables, we can obtain a nondegenerate function of two variables $g(x,y)$. By what we have proved above, the complete elementary term $t(x_1,\dots,x_n)$ over this function defines a nondegenerate function. We represent $f(x_1,\dots,x_n)$ by the canonical polynomial form (4) with respect to the function corresponding to this term, and the terms in this form are odd in number since f is nondegenerate. Further, we transform the terms containing the variable $\bar{x}_i$ by the formula

$$h(x_1,\dots,\bar{x}_i,\dots,x_k)=h(x_1,\dots,x_i,\dots,x_k)\oplus h'_{x_i}(x_1,\dots,x_i,\dots,x_k).$$

Applying this transformation the necessary number of times and then cancelling pairs of identical terms, we get the desired expansion (6).

An obvious corollary characterizes nondegenerate functions in terms of the Zhegalkin polynomial.

COROLLARY. Precisely those functions are nondegenerate Boolean functions whose Zhegalkin polynomial contains a complete elementary conjunction.

In conclusion we give an application of the obtained results for the determination of canonical forms in the propositional algebra, which can however be obtained immediately. For the formulation we use the logical terminology, adopted in propositional algebra. As usual, the operations $\neg,\wedge,\vee,\rightarrow$, and $\equiv$ are defined in the propositional algebra. We call a formula $\varphi(X_1,\dots,X_n)$ simple if the expression $\equiv$ does not occur in it, and all variables occur just once. A formula of the form

$$\varphi(Y_{11},\dots,Y_{1n})\equiv\dots\equiv\varphi(Y_{21},\dots,Y_{2n})\equiv\dots\equiv\varphi(Y_{k1},\dots,Y_{kn}),$$

where Y_{ij} is either X_j or $\bar{X}_j$ and all $\varphi(Y_{i1},\dots,Y_{in})$ are different, that is equivalent to a formula $\psi(X_1,\dots,X_n)$ is called the canonical normal form of $\psi(X_1,\dots,X_n)$ with respect to $\varphi(X_1,\dots,X_n)$; moreover, this form is unique up to the associativity $\equiv$.

THEOREM 3 (on Canonical Normal Forms of the Propositional Algebra). For each formula $\psi(X_1,\dots,X_n)$, not identically equal to zero, of the propositional algebra, there exists canonical normal forms with respect to each simple formula $\varphi(X_1,\dots,X_n)$.

Proof. This theorem follows immediately from the statements on the canonical polynomial forms and the term presentation of nondegenerate Boolean functions if we note that $\neg$, $\wedge$, $\vee$, and $\rightarrow$ are nondegenerate Boolean functions and $\equiv$ is dual to $\oplus$.

LITERATURE CITED

1. S. V. Yablonskii, G. P. Gavrilov, and V. B. Kudryavtsev, Functions of Algebra of Logic and Post Classes [in Russian], Nauka, Moscow (1966).
2. É. K. Machikenas and V. P. Suprun, On the Polynomial Expansion of Boolean Functions [in Russian], Deposited in the All-Union Institute of Scientific and Technical Information at No. 1899-V88 on March 9, 1988.