REPORTS ON MATHEMATICAL LOGIC
38 (2004), 61–64

Jerzy KOTAS

SELF–DUAL BOOLEAN FUNCTIONS

A b s t r a c t. We define a simple method for finding polynomials over Z_2 which realize self-dual Boolean functions.

Self–dual Boolean functions were defined by E. Post in *Introduction to a general theory of elementary propositions*, American Journal of Mathematics, 4 (1921), 163–185. They turned out to be essential for the checking test if a given class of Boolean functions is complete (i.e. its closure under the superposition is the class of all Boolean functions). Self-dual functions realized by polynomials over Z_2 found also applications in coding theory.

Let $E_2 = \{0,1\}$. The set ${E_2}^n$, $n < \omega$, is called the n–dimensional Boolean cube. Elements of the cube are called nodes. The number $k = k_1 + 2k_2 + \ldots + 2^{n-1}k_n$ is called the number of the node $\overline{k} = (k_1, k_2, \ldots, k_n)$ in ${E_2}^n$. The node $-\overline{k} = (1 - k_1, \ldots, 1 - k_n)$ is said to be opposite to $\overline{k}$. A mapping $f : {E_2}^n \to E_2$ is called an n-argument Boolean functions. The function is said to be self-dual if

$$f(-\overline{k}) = 1 - f(\overline{k}) \tag{1}$$

Received July 6, 1999
1991 AMS *Subject Classification* 06E30

for each node $\overline{k}$. It follows from (1) that any n-argument self-dual function is determined uniquely by its values on the nodes with $0 \leq k \leq 2^{n-1} - 1$. Then $l = f(\overline{0}) + 2f(\overline{1}) + \ldots + 2^{2^{n-1}-1} f(\overline{2^{n-1}-1})$ is called the number of the function f. Clearly, $0 \leq l \leq 2^{2^{n-1}} - 1$.

The set of the operators $\{\cdot, +, 0, 1\}$ of the field Z_2 is a complete set of Boolean functions. Then each Boolean function f can be given as a polynomial w_f over Z_2. Let w_f^p be the sum of all components of w_f of the degree p, $0 \leq p \leq n$. Obviously, if f is a n–argument self-dual function, then $w_f^p = 0$.

For each node $\overline{k}$ in E_2^n with $0 \leq k \leq 2^{n-1} - 1$ we define a function $\underline{k} : {E_2}^n \to E_2$ as follows

$$\underline{k}(\overline{x}) = \begin{cases} 1 & \text{if } \overline{x} \in \{\overline{k}, -\overline{k}\}, \\ 0 & \text{otherwice.} \end{cases} \tag{2}$$

Theorem 1. *For every n–argument self-dual function f*

$$f(\overline{x}) = \sum \{\underline{k}(\overline{x}); f(\overline{k}) = 0\} + x_n + 1. \tag{3}$$

Corollary 2. *For every n–argument self-dual function f*

$$w_f(\overline{x}) = \sum \{w_{\underline{k}}(\overline{x}) : f(\overline{k}) = 0\} + x_n + 1. \tag{4}$$

Assume that the components of the polynomial $w_{\underline{k}}^p$ are ordered and the order coincides with a lexicographical ordering of the variables. Let $(w_{\underline{k}}^p)$ be the sequence of the coefficients of $w_{\underline{k}}^p$. By $L_m(n), m \leq n$, we denote the set of all increasing sequences of the length m in the set $\{1, \ldots, n\}$. Clearly, $card(L_m(n)) = \binom{m}{n}$.

Let $F_m : E_2^n \to E_2^{\binom{n}{m}}$ be the mapping defined by

$$F_m(\overline{k}) = (c_m(k_{j_1}, \ldots, k_{j_m}) : (j_1, \ldots, j_m) \in L_m(n)), \tag{5}$$

where C_m is the m–argument Boolean function such that

$$C_m(x_1,\ldots,x_m)=\begin{cases}1 & \text{if}\quad x_1=\ldots=x_m,\\ 0 & \text{otherwice.}\end{cases}$$

By $\vec{F}_m(\overline{k})$ we denote the node of the cube $E_2^{\binom{n}{m}}$ received form $F_m(\overline{k})$ by the reversal of its coordinates.

Theorem 3. *For every* $0\le k\le 2^{n-1}-1$ *and every* $0\le p\le n-1$ *the following holds*

$$\left(w^p_{\underline{k}}\right)=\vec{F}_{n-p}(\overline{k}). \tag{6}$$

It follows from (4) and (6) that for each n-ary self-dual function f

$$\left(w^p_f\right)=\begin{cases}\sum\{\vec{F}_{n-p}\overline{k}:f(\overline{k})=0\} & \text{if}\quad 2\le p\le n-1,\\ \sum\{\vec{F}_{n-1}(\overline{k};f(\overline{k})=0\}+(0\ldots01) & \text{if}\quad p=1,\\ (f(\overline{0}))+(1) & \text{if}\quad p=0,\end{cases} \tag{7}$$

where the symbols $\sum$ and $+$ denote the addition (mod 2) of the coordinates of the nodes involved.

To determine $\left(w^p_f\right)$ for the n-argument self-dual function f with the number l, it suffices:

1. Find a binary representation of l in the form $(l_0l_1\ldots l_{2^{n-1}-1})$;
2. Determine the set $T_l=\{k;l_k=0\}$;
3. Calculate $\vec{F}_{n-p}(\overline{k})$ for each $k\in T_l$;
4. Calculate $\left(w^p_f\right)$ using the formula (7).

The sequence (w_f) of the coefficients of the polynomial w_f is the concatenations of the sequences $\left(w^{n-1}_f\right),\left(w^{n-2}_f\right),\ldots,\left(w^1_f\right),\left(w^0_f\right)$.

Example Let us try to determine, according to the above procedure, the polynomials (over Z_2) for the self-dual Boolean function f with the number $l=111$. We get

1. $111 = (10110110)$,
2. $T_{111} = \{1, 4, 7\}$.
3.

$$
\begin{array}{lll}
\overline{1} = (0100) & (w_{\underline{1}}) = & (1111), (111000), (1000), (0), \\
\overline{4} = (0010) & (w_{\underline{4}}) = & (1111), (010101), (0010), (0), \\
\overline{7} = (1110) & (w_{\underline{7}}) = & (1111), (001011), (0001), (0), \\
 & (x_4 + 1) = & \qquad\qquad\qquad\quad (0001), (1) \\
\hline
 & (w_f) = & (1111), (100110), (1010), (1).
\end{array}
$$

So, we receive

$$
\begin{aligned}
w_f(x_1, x_2, x_3, x_4) = {} & x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + \\
& + x_2x_3x_4 + x_1x_2 + x_2x_3 + x_2x_4 + x_1 + x_3 + 1.
\end{aligned}
$$

Mathematical Institute
Pedagogical University
Plac Weyssenhoffa 11
Bydgoszcz 85-720, Poland