PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 37 (51), 1985, pp. 3–6

SOME REMARKS ON THE CANONICAL FORMS FOR PSEUDO-BOOLEAN FUNCTIONS

Radomir S. Stanković

Abstract. We consider some canonical forms for pseudo-Boolean functions and give a fast algorithm for the determination of these forms. We also show that the coefficients of all m^n possible different canonical forms may be computed simultaneously by using the fast convolution algorithms.

In order to make this note self-contained we shall briefly repeat some definitions.

Let $P = \{0, 1. \dots , p-1\}$, and let "+" and "$\cdot$" denote addition and multiplication modulo p.

A pseudo-Boolean function f is defined as a mapping $f : L^n \to P$, where $L \subseteq P$, and L^n stands for the n-th Cartesian power of L.

In the set L we introduce the relations

$$[x_i, q] = \begin{cases} 1, & x_i = q \\ 0, & x_i \neq q \end{cases} \quad x_i, q \in L \ \ (i = 1, \dots , n)$$

for the variables $x_1, \dots , x_n$.

By a pseudo-Boolean expression we mean a well-formed expression made up of the following symbols:

a) the elements $0, 1, \dots , p-1$

b) the variables $[x_{i_k}, q_{i_k}]$

c) the two operations "+" and "$\cdot$".

The set P_n of pseudo-Boolean expressions is a module on the ring $(P, +, \cdot)$ [**1**]. In [**2**] it is proven that for all $(a_1 \cdots a_n) \in L^n$ the set

$$B_{a_{1,\dots,a_n}} = \{1, [x_{i_1}, q_{i_1}] \cdot [x_{i_2}, q_{i_2}] \cdot \ldots \cdot [x_{i_m}, q_{i_m}]\} \tag{1}$$

$$1 \leq m \leq n;\ i_1, i_2, \dots , i_m \in \{1, 2, \dots , n\};\ q_{i_k} \in L \backslash \{a_k\} (1 \leq k \leq n)$$

AMS Subject Classification (1980): Primary 03 B 50.

is a set of linearly independent expressions in P_n.

It is clear that if L consist of m elements, then there are m^n sets $B_{a_1,\dots a_n}$, and, also, it can be easily proven that these sets are bases in P_n.

Using the bases described by (1) some canonical forms for pseudo-Boolean function may be defined. Here, by a canonical form of an m-valued n-variable pseudo-Boolean function we mean an expression of the form:

$$\begin{aligned} f(x_1,\dots,x_n) &= c_0 + c_1[x_{i_1},q_{i_1}] + \cdots + c_m[x_{i_m},q_{i_m}] \\ &+c_{m+1}[x_{i_1},q_{i_1}]\cdot[x_{i_2},q_{i_2}] + \cdots + c_{m^n-1}[x_{i_1},q_{i_1}]\cdot\ldots\cdot[x_{i_m},q_{i_m}] \end{aligned} \tag{2}$$

Since there are m^n bases, it follows that a given pseudo-Boolean function f may be represented in m^n different ways, i.e., there are m^n different canonical forms. In what follows, a canonical form corresponding to the base $B_{a_1,\dots a_n}$ will be denoted by $CF(j)$ where $j = \sum_{i=1}^{n} a_i p^{i-1}$.

In what follows, the coefficients of the canonical forms will be noted by two parameters, $c_{j,i}$; the first parameter denotes the base, and the second denotes the order of the coefficients in (2).

In [**2**] some formulas for determination of these canonical forms are derived. But being given in an analytical form, the results obtained are very cumbersome for practical applications. Written in a matrix form these results may be expressed as follows.

THEOREM. *Let a pseudo-Boolean function $f : L^n \to P$ be given by its value vector $[F] = [f(00\dots0),\dots,f(p-1,p-1,\dots,p-1)]^T$.*

The canonical form $CF(m^n-1)$ correspond in to the base $B_{(p-1)\dots(p-1)}$ may be obtained as:

$$f(x_1,\dots,x_n) = \left(\bigotimes_{i=1}^{n}[A_i]\right)\left(\bigotimes_{i-1}^{n}{}'\,[B_i]\right)\cdot[F] \tag{3}$$

where $\otimes$ denotes the Kronecker product operation, and $\otimes'$ denotes the Kronecker product operation with modulo p reduction. The matrices $[A_i]$ and $[B_i]$ are defined as follows.

The matrix $[A_i]$ is a $(1\times p)$ matrix of the form:

$$[1[x_{i_{p-2}},q_{i_{p-2}}][x_{i_{p-3}},q_{i_{p-3}}]\cdots[x_{i_0},q_{i_0}]]$$

and $[B_i]$ is a $(p\times p)$ matrix of the form

$$\begin{bmatrix} 0 & 0\dots0 & 0 & 1 \\ 0 & 0\dots0 & 1 & p-1 \\ 0 & 0\dots1 & 0 & p-1 \\ \vdots & & & \\ 0 & 1\dots0 & 0 & p-1 \\ 1 & 0\dots0 & 0 & p-1 \end{bmatrix} \tag{4}$$

Proof. The proof of (3) is easily obtained by induction and, hence, it is omitted.

Note that the canonical forms corresponding to each of the remaining bases $B_{a_1 \dots a_n}$ may be obtained by a simple modification of (3). The modification is achieved using the cyclic shift operation.

For a basis $B_{a_1 \dots a_n}((a_1 \dots a_i \dots a_n) \in L^n)$, where $a_1 \dots a_i \dots a_n$ are not all equal $p-1$, we have the first element in the matrix $[A_i]$ $(i = 1, \dots, n)$ in (3) is equal 1. The remaining elements of $[A_i]$ may be obtained by a cyclic shift of the elements of the sequence $\{[x_{i_{p-1}}, q_{i_{p-1}}], [x_{i_{p-2}}, q_{i_{p-2}}], \dots, [x_{i_0}, q_{i_0}]\}$ for $(p-1-a_i)$ places to left and keeping the last $p-1$ elements.

The matrix $[B_i]$ in this case may be obtained by a cyclic shift of the columns of the matrix (4) for $(p-1-a_i)$ places to left.

Expressed in this form the results form [**2**] are obviously equal to those published by Kodandapani and Setlur in [**3**].

When one works with this type of expansions one very important question is the search for the optimal point about which the expansion is to be done in order to obtain the series with the minimal number of terms. This is particularly important in the case of pseudo-Boolean functions, since we use mod$\cdot p$ adders, which is not simple to realize in hardware. A direct way to determine the minimal canonical forms is to compute all the m^n canonical forms and find the form with the least number of nonzero terms. To compute these forms one needs to compute m^n coefficients in each of these forms. There are altogether $m^n \times m^n = m^{2n}$ coefficients. The direct computation of these coefficients using (3) requires a great number of modular operations. This problem has been studied in [**4**]. In [**4**] it is shown that there are only $(m(m+1)^n)/2$ distinct coefficients and a matrix technique to compute them is presented. Also a matrix equation is given which can be conveniently used for computing the minimal expansion. Here, we disclose a fast algorithm for the determination of the coefficients $c_{j,i}$ from (2). The application of this algorithm considerably reduces the number of the required modular operations.

Due to the Kronecker product operation, we immediately have from (3) that the construction of a fast algorithm is possible. The method of construction is completely analogons to that used for obtaining the FFT algorithms (see, for example [**5, 6**]), and no special techniques need be included here. We simply illustrate this statement by the following example.

x	0	0	0	1	1	1	2	2	2
y	0	1	2	0	1	2	0	1	2
f	4	0	1	3	0	0	2	4	0

Table 1

Example. Let $f : \{0,1,2\}^2 \to \{0,1,2,3,4\}$ be given by Table 1.

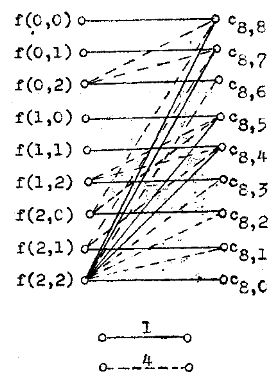
From (3) we have that $CF(m^n-1)$ is given by

$$
\begin{aligned}
f(x,y) &= c_{8,0} + c_{8,1}[y,1] + c_{8,2}[y,0] + c_{8,3}[x,1] + c_{8,4}[x,1][y,1] \\
&\quad + c_{8,5}[x,1][y,0] + c_{8,6}[x,0] + c_{8,7}[x,0][y,1] + c_{8,8}[x,0][y,0] \\
&= ([1[x,1][x,0]] \otimes [1[y,1][y,0]]) \\
&\qquad \left(\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 4 \\ 1 & 0 & 4 \end{bmatrix} \oplus' \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 4 \\ 1 & 0 & 4 \end{bmatrix} \right) \cdot [F].
\end{aligned}
$$

Since $[F] = [4\ 0\ 1\ 3\ 0\ 0\ 2\ 4\ 0]^T$ we otain

$$f(x,y) = 4[y,1] + 2[y,0] + [x,1][y,1] + [x,1][y,0] + [x,0] + [x,0][y,0].$$

For the calculation of the coefficients $c_{8,i} (i = 0,1,\ldots,8)$ in this expansion we use the fast algorithm given in Fig. 1., where a dotted line inducates multiplication by 4 mod 5 before addition mod 5 takes place. It is apparent that this algorithm has a complexity similar to that of one step of a FFT algorithm [**5, 6**], and, moreover, only real arithmetic operations are required. The algorithm is applicable for any p and n. It is obvious that the proposed algorithm is very simple and fast.



If we want to calculate all m^{2n} coefficients of the m^n possible canonical forms $CF(j)$, then the following observation may be very useful.

Let $[R(m^n-1)] = \bigotimes_{i-1}^{n}{}' [B_i]$ be the matrix corresponding to $CF(m^y-1)$, and let $r(s)$ be the s-th row of $[R(m^n-1)]$. The only difference between $[R(m^n-1)]$ and the matrices $[R(j)]$ correspooding to the other canonical forms is in the ordering of their columns. This is a natural consequence of the definition of $[B_i]$.

Now, let $[C]$ be the vector of the coefficients inpexed by k in all m^n possible canonical forms, i. e.,

$$[C] = [c_{0,k}\, c_{l,k} \ldots c_{m^{n-1},k}]^T.$$

Then, one has

$$[C] = [r(k) * [F] \tag{5}$$

where $*$ denotes the cyclic convolution in P_n defined as

$$(f_1 * f_2)(t) = \sum_{x=0}^{p^{n-1}} f_1(x) f_2(t+x), \qquad f_1, f_2 \in P_n.$$

Due to the fast convolution algorithm (see, for example [**8**]) the implementation of (5) is very efficient.

Conclusion. The proposed fast algorthm as well as the relation (5) may be used as a good starting point for the formulation of a procedure for the determination of a minimal canonical form of a given pseudo-Boolean function.

REFERENCES

[1] M. Davio, J. P. Deshapms, A. Thayse, *Discrete and Switching Functions*, Gorgi, St. Saphorin, Switzerland, 1978.

[2] K. Gilezan, B. Čanak, *Quelques formes génerales des fonctions pseudo-booléenes*, Publ. Inst. Math. (Beograd) (N. S.) **24**(**38**) (1978), 45–52.

[3] K. L. Kodandapani, R. V. Setlur, *Reed-Muller canonical forms in multivalued logic*, IEEE Trans. Comput. **C–24** (1975), 627–638.

[4] K. L. Kodandapani, D. K. Pradhan, *Further results on m-RMC expansions for m-valued functions*, Proc. 6th ISMVL, Losan, Uteh. USA, IEEE Press, 1976, 88–92.

[5] F. Theilhemer, *A matrix version of the fast Fourier transform*, IEEE Trans. (1969), 158–161.

[6] I. J. Good, *The relationship between two fast Fourier transforms*, IEEE Trans. **C–20** (1971), 310–317.

[7] M. G. Karpovsky, *Finite Ortogonal Series in the Desing of Digital Devices*, Wiley. New York, IUP Jerusalem, 1976.

[8] R. C. Agarwal, J. W. Cooley, *New algorithms for digital convolution*, IEEE Trans. **ASSP–25** (1975), 392–410.

ETŠC “Mija Stanimirović”
Bulevar Veljka Vlahovića b.b.
18000 Niš, Yugoslavia

(Received 16 05 1984)