Università di Pisa

Dipartimento di Informatica

Technical Report : TR-00-02

The characterization of the sub-pseudocubes of a pseudocube

Valentina Ciriani

March 08, 2000

ADDR: Corso Italia 40,56125 Pisa,Italy. TEL: +39-50-887111. FAX: +39-50-887226

The characterization of the sub-pseudocubes of a pseudocube

Valentina Ciriani
Dipartimento di Informatica, Università di Pisa
ciriani@di.unipi.it

Abstract

Recently introduced pseudocubes and SPP forms have made possible to represent Boolean functions with a more compact expression than in the SP form. In this report we present new properties of pseudocubes. In order to study and manipulate pseudocubes we count and characterize sub-pseudocubes. Letting P be a pseudocube, we derive a normal form and the canonical expression of any sub-pseudoproduct of P.

1 Pseudocubes and pseudoproducts

In the Boolean space the characteristic function of a cube can be expressed as the product (AND) of the variables having constant value in the cube, either in direct or complemented form. Any Boolean function can be expressed in SP form that is as a sum (OR) of products. pseudocubes, pseudoproducts and SPP forms introduced in [LP97] and [LP99] are generalizations of the above. All the definitions and properties of this section are taken from those papers. All vectors are Boolean vectors.

Definition 1 *A vector u of 2^m elements, $m \geq 0$, is **normal** if*

1. *$m = 0$, or*

	$\mathbf{c}_0$	$\mathbf{c}_1$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\mathbf{c}_4$	$\mathbf{c}_5$
$\mathbf{r}_0$	0	1	0	1	0	1
$\mathbf{r}_1$	0	1	0	1	1	0
$\mathbf{r}_2$	0	1	1	0	0	1
$\mathbf{r}_3$	0	1	1	0	1	0
$\mathbf{r}_4$	1	1	0	0	0	0
$\mathbf{r}_5$	1	1	0	0	1	1
$\mathbf{r}_6$	1	1	1	1	0	0
$\mathbf{r}_7$	1	1	1	1	1	1

Figure 1: A canonical matrix with 2^3 rows and $n = 6$ columns. The canonical columns are c_0, c_2, and c_4.

2. *$m > 0$, and $u = v\widehat{v}$ with v (hence $\widehat{v}$) normal. ($\widehat{v}$ denotes v or its elementwise complement $\overline{v}$).*

Definition 2 *A vector u is **constant** if $u = \mathbf{0}$ or $u = \mathbf{1}$ ($\mathbf{0}$ and $\mathbf{1}$ denote vectors of all 0's or all 1's respectively); otherwise u is **divided**. u is **balanced** if it is constant or half of its elements are 0 and half are 1. Two balanced vectors u, v are **concordant** if $u = v$ or $u = \overline{v}$; otherwise u, v are **discordant**.*

In the following definitions a matrix will always have 2^m rows $r_0, \ldots, r_{2^m-1}$ and n columns $c_0, \ldots, c_{n-1}$, with $n \geq 1$ and $0 \leq m \leq n$.

Definition 3 *A matrix M is **normal** if $r_i \neq r_j$ for $i \neq j$, and all the columns are normal. A normal matrix is **canonical** if its rows, interpreted as binary numbers, are arranged in increasing order.*

Figure 1 shows a canonical matrix.

Definition 4 *A normal vector $u = v_0 \ldots v_{2^{m-k}-1}$ is **k-normal**, $0 \leq k \leq m$. A k-normal vector is **k-canonical** if $v_i = 0$ for i even, and $v_i = 1$ for i odd.*

A restriction of a matrix M, composed of the rows whose elements in column c_i are equal to 1 (respectively equal to 0) is denoted by M_i (respectively $M_{\overline{i}}$).

Definition 5 *A matrix M is **balanced** if all its rows are pairwise different, all its columns are balanced, and each M_i (hence $M_{\bar{i}}$) is balanced, $0 \leq i \leq n-1$.*

Proposition 6 *A canonical matrix M contains m columns $c_{i_0}, \ldots c_{i_{m-1}}$ of increasing indices, such that c_{i_j} is $(m-j-1)$-canonical for $0 \leq j \leq m-1$.*

In a canonical matrix M the columns $c_{i_0}, \ldots c_{i_{m-1}}$ of proposition 6 are called *canonical columns* of M. The other columns are the *non canonical* ones (see figure 1). The following propositions show that balanced and normal matrix are the same up to permutation of rows.

Proposition 7 *Any normal (in particular, canonical) matrix M is balanced.*

Proposition 8 *Any balanced matrix M can be transformed into the corresponding canonical one by rearranging the rows, interpreted as binary numbers, in increasing order.*

A set of m points of the Boolean space B^n can be arranged in a $m \times n$ matrix whose rows correspond to the points and the columns correspond to the variables describing B^n. For example the matrix of figure 1 represents eight points in B^6.

Definition 9 *A **pseudocube** of degree m is a set of 2^m points whose matrix is balanced, or equivalently is canonical up to a row permutation.*

The matrix of figure 1 represents a pseudocube.

Pseudo cubes maintain same of the basic properties of cubes. Two halves of a pseudocube of order $m > 0$ are not necessarily pseudocubes. An interesting property of sub-pseudocubes is the following:

Proposition 10 *Let R be a pseudocube of order m, and P a pseudocube of order $m-1$, $P \subset R$. Then $Q = R - P$ is a pseudocube of order $m-1$, and $Q \in \alpha(P)$.*

We now pose:

Definition 11 *For a point $s \in B^n$ and a subset of variables α, the transformed point $\alpha(s)$ is obtained from s by complementing the variables in α. For a set of points S, the transformed set $\alpha(S)$ is the set $\{\alpha(s) : s \in S\}$.*

Proposition 12 *Let P be a pseudocube of degree m and α be a subset of variables. Then $\alpha(P)$ is a pseudocube of degree m, with $\alpha(P) = P$ or $\alpha(P) \cap P = \emptyset$.*

Let M_1, M_2 be the canonical matrices of P_1, P_2 respectively and $P_2 = \alpha(P_1)$. The two following properties hold:

Proposition 13 *M_1 and M_2 have the same canonical variables $x_{p_0}, \ldots, x_{p_{m-1}}$, and non-canonical variables $x_{p_m}, \ldots, x_{p_{n-1}}$.*

Proposition 14 *Let M be the canonical matrix of $P = P_1 \cup P_2$. The canonical variables of M are the same of M_1, M_2, plus the variable $x_k \in \alpha$ of minimum index.*

The characteristic function of a pseudocube is called *pseudoproduct*, and has the concise algebraic expression introduced in the following definition:

Definition 15 *Let P be a pseudocube of degree m in B^n; let M be the canonical matrix of P; and let $x_{p_0}, \ldots, x_{p_{m-1}}$ and $x_{p_m}, \ldots, x_{p_{n-1}}$ be the canonical and non-canonical variables respectively, with these two sets ordered for increasing values of the indices. The **canonical expression** associated with P, $\mathbf{CEX(P)}$, is given by $f_0 \cdot f_1 \cdot \ldots \cdot f_{n-m-1}$, where each f_i, $0 \leq i \leq n-m-1$, is an EXOR-factor containing the following variables:*

1. *the canonical variables x_{p_j}, $0 \leq j \leq m-1$, such that $M[0, p_{m+1}] \neq M[2^{m-j-1}, p_{m+1}]$; these variables are ordered for increasing indexes;*
2. *the non-canonical variable $x_{p_{m+i}}$, if $M[0, p_{m+i}] = 1$; or $\overline{x}_{p_{m+i}}$, if $M[0, p_{m+i}] = 0$.*

In figure 1 column c_i correspond to variable x_i ($0 \leq i \leq 5$). The canonical expression for the pseudocube is:

$$CEX = x_1 \cdot (x_0 \oplus x_3) \cdot (x_0 \oplus x_4 \oplus x_5)$$

In general, an arbitrary function can be expressed as a disjunction of pseudoproducts, giving rise to a sum of pseudoproducts (**SPP**) form. The SPP method is a direct generalization of the one for SP where pseudoproducts are substituted for products.

The concept of prime implicant extend to the one of *prime pseudoproduct* that is a pseudo product implying f, and not implying any other pseudoproduct of f. There is an immediate extension of the classic SP minimization methods to construct SPP form with minimal number of pseudo products or minimal number of literals, composed of prime pseudo products only.

The number of literals in a minimal SPP expression is less equal then in the minimal SP expression for the same function. On the negative side the SPP circuit has three levels, and requires a big effort to be produced in minimal form due to the high number of prime pseudoproducts.

2 The number of distinct sub-pseudocubes

We now evaluate the number of sub-pseudoproducts of degree $m-1$ of a pseudo product of degree m. The following lemmas 16 and 17 contain some properties of normal vectors useful to prove the results reported in the following.

Lemma 16 *The number of distinct normal vectors of* 2^m *elements is* 2^{m+1}.

Proof. By induction on m.

Basis. $m = 0$. The normal vectors of just one element are 0 and 1.

Inductive step. $m > 0$. Assuming that the hypothesis holds for all $n < m$, we prove that it holds for m. Let u be a normal vector and $u = v\widehat{v}$ ($\widehat{v}$ denotes v or $\overline{v}$, and $v\widehat{v}$ is the concatenation of v and $\widehat{v}$). Inductively assume that v is one of 2^m normal vectors with 2^{m-1}elements. Since $\widehat{v}$ can be v or $\overline{v}$, u can be composed in $2 \times 2^m = 2^{m+1}$ ways. ■

Lemma 17 *If* $x_1, x_2, \ldots, x_n$ *are normal vectors of* 2^m *elements,* $x = x_1 \oplus x_2 \oplus \ldots \oplus x_n$ *is a normal vector.*

Proof. By induction on n.

Basis. $n = 2$. We proof that $x = x_1 \oplus x_2$ is normal by induction on the dimension (k) of the vectors x_1 and x_2.

Basis. $k = 1$. Every vector of just one element is normal.

Inductive step. $k > 1$. Let $x_1 = x_1^1 x_1^2 \dots x_1^k$ and $x_2 = x_2^1 x_2^2 \dots x_2^k$, we define $x_1^l = x_1^1 x_1^2 \dots x_1^{k/2}$, $x_1^h = x_1^{k/2+1} x_1^{k/2+2} \dots x_1^k$, $x_2^l = x_2^1 x_2^2 \dots x_2^{k/2}$ and $x_2^h = x_2^{k/2+1} x_2^{k/2+2} \dots x_2^k$. We have:

$$x = \begin{pmatrix} x^l \\ x^h \end{pmatrix} = \begin{pmatrix} x_1^l \\ x_1^h \end{pmatrix} \oplus \begin{pmatrix} x_2^l \\ x_2^h \end{pmatrix} = \begin{pmatrix} x_1^l \oplus x_2^l \\ x_1^h \oplus x_2^h \end{pmatrix}$$

The inductive hypothesis holds for $x_1^l \oplus x_2^l$ and $x_1^h \oplus x_2^h$. We now prove that $x_1^l \oplus x_2^l = x_1^h \oplus x_2^h$ or $x_1^l \oplus x_2^l = x_1^h \oplus \overline{x_2}^h$. By hypothesis x_1 and x_2 are normal, then we have:

$$x_1^l = \widehat{x}_1^h \text{ and } x_2^l = \widehat{x}_2^h \quad (\widehat{x} \text{ denotes } x \text{ or } \overline{x})$$

and the thesis follows immediately using EXOR proprieties.

Inductive step. $n > 1$. Assuming that the hypothesis holds for $n - 1$, we prove that it holds for n. Inductively assume that $y = x_2 \oplus \dots \oplus x_n$ is normal, and note that by hypothesis x_1 is normal. We have just to proof that $x = x_1 \oplus y$ is normal. By the proof of $n = 2$, the thesis follows immediately. ■

An easy extension of proposition 14 is that:

Lemma 18 *Let R be a pseudocube of degree m, and canonical matrix M_R; P be a pseudocube of degree $m - 1$, and canonical matrix M_P; and $P \subset R$. The canonical variables of M_P are the same of M_R except for one.*

Proof. By proposition 10 there exists a pseudocube $Q = R - P$ with $Q \in \alpha(P)$. By proposition 13 we have that P and Q have the same canonical variables. By proposition 14 we have that R has the same canonical variables of P and Q plus one. ■

Let us now count the number of distinct sub-pseudocubes of degree $m-1$ of a pseudocube of degree m.

Proposition 19 *Let R be a pseudocube of degree m. The number of distinct pseudocubes P of degree $m - 1$, with $P \subset R$, is $2^{m+1} - 2$.*

Proof. By lemma 18, the canonical variables of R are the same canonical variables of every P plus one. We first count the number of distinct matrices M' that we can compose with the canonical variables of R except for one. We then prove that all matrices M' correspond to pseudocubes. Denote by M, and $x_1, x_2, \ldots, x_m$ the canonical matrix of R and the canonical variables of M. Note that every row in M is univocally represented by the sub-vector of canonical variables. Consider the canonical variables $x_1, x_2, \ldots, x_{m-1}$. The variable x_m is non canonical for P. For any P, the column of x_m can be chosen as a normal vector of length 2^{m-1}. By lemma 16 there are 2^m normal vectors. Consider now the canonical variables $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m$ and suppose to have already counted all the different combination of normal vectors from x_m to x_{i+1}. Note that in the last but one step (x_{i+1} non canonical) x_i is a canonical variable and x_{i-1} is $(i-1)$-canonical. Now $x_{i-1} = v_0 \ldots v_{2^{i-1}-1}$ is still $(i-1)$-canonical since $v_i = \mathbf{1}$ for i odd and $v_i = \mathbf{0}$ for i even. We now choose normal vectors for x_i that are not already used in the previous combinations. For any v_i the corresponding values of x_i must be all 1 or all 0. In fact if the values of x_i are half 1 and half 0 they can be rearranged to make x_i a canonical variable. Since $\forall v_i$ x_i is $\mathbf{1}$ or $\mathbf{0}$, then x_i can be chosen in $2 \times 2^{i-1} = 2^i$ ways. If we sum all the possible combinations we obtain:

$$\sum_{i=1}^{m} 2^i = 2^{m+1} - 2$$

We finally prove that all these matrices correspond to pseudocubes, that is all non-canonical columns are normal. Note that in matrix M all non-canonical variables are constant or an EXOR combination of canonical variables. In fact, in the CEX representation of matrix M, every non canonical variable x_k is in a EXOR factor $(x_{p_1} \oplus x_{p_2} \oplus \ldots \oplus x_{p_h} \oplus \widehat{x}_k)$ with $x_{p_i} \in \{x_1, x_2, \ldots, x_m\}$ and $0 \leq h \leq m$. By proprieties of EXOR:

$$x_k = (x_{p_1} \oplus x_{p_2} \oplus \ldots \oplus \widehat{x}_{p_h})$$

Since $x_{p_1}, x_{p_2}, \ldots, x_{p_h}$ are normal, by lemma 17, x_k is normal. ■

3 Characterization of sub-pseudocubes

There are numerous ways to represent Boolean function with the form of sum of products of EXOR factors. Luccio and Pagli in [LP97] and [LP99] describe a canonical CEX form. In this report we first characterize all the sub-pseudocubes of a pseudocube representing every distinct sub-pseudocube in a *normal form*. Then we give a canonical CEX expression corresponding to the normal form.

Let R be a pseudocube of degree m. The following lemma 20 shows that every sub-pseudocubes $P \subset R$ of degree $m-1$ has a particular expression in the form of product of EXOR factors (shortly PP). We denote such an expression as *normal form* of P.

Lemma 20 *Let $A_1 A_2 \dots A_q$ be the CEX expression of a pseudocube R, of degree m; and let $x_1, x_2, \dots, x_m$ the canonical variables of R. If P is a pseudo product of degree $m-1$ and $P \subset R$, then exists an expression PP of P of the form:*

$$A_1 A_2 \dots A_q A_{q+1}$$

with $A_{q+1} = y_1 \oplus y_2 \oplus \dots \oplus y_k$ and $\forall i \in [1, \dots, k] : y_i \in \{x_1, x_2, \dots, x_m\}$

*We denote this expression as **normal form** of P.*

Proof. By lemma 18, P has the same canonical variables then R except for one. Let $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m$ the canonical variables of P. A PP expression of P can be $A_1 A_2 \dots A_q A_{q+1}$ with $A_{q+1} = y_1 \oplus y_2 \oplus \dots \oplus y_{k-1} \oplus x_i$ and $\forall i \in [1, \dots, k-1] : y_i \in \{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m\}$. ■

Indeed the inverse implication also holds.

Lemma 21 *Let $A_1 A_2 \dots A_q$ be a CEX expression of a pseudocube R, of degree m; and let $x_1, x_2, \dots, x_m$ the canonical variables of R. Any PP expression $A_1 A_2 \dots A_q A_{q+1}$ with $A_{q+1} = y_1 \oplus y_2 \oplus \dots \oplus \widehat{y}_k$ and $\forall i \in [1, \dots, k] : y_i \in \{x_1, x_2, \dots, x_m\}$ represents a pseudo product P of degree $m-1$ with $P \subset R$.*

Proof. Observe that, as shown in lemma 20, every $P \subset R$ has an PP expression $A_1 A_2 \dots A_q A_{q+1}$ with $A_{q+1} = y_1 \oplus y_2 \oplus \dots \oplus y_k$ and $\forall i \in [1, \dots, k]$:

$y_i \in \{x_1, x_2, \ldots, x_m\}$. By proposition 19 the number of distinct pseudocubes $P \subset R$, of degree $m-1$, is $2^{m+1}-2$. All the possible distinct $A_{q+1} = y_1 \oplus y_2 \oplus \ldots \oplus \widehat{y}_k$ with $\forall i \in [1, \ldots, k] : y_i \in \{x_1, x_2, \ldots, x_m\}$, they are $2^{m+1}-2$. In fact their number is given by:

$$2 \times \sum_{i=1}^{m} \binom{m}{i} = 2^{m+1} - 2$$

Then, by observing that the expressions $A_1 A_2 \ldots A_q A_{q+1}$ are all distinct, we have that every such an expression represents a pseudocube $P \subset R$ of degree $m-1$. ■

The following lemma shows that a sub-pseudoproduct P can have a more general expression.

Proposition 22 *Let $A_1 A_2 \ldots A_q$ be a CEX expression of a pseudocube R, of degree m. Any PP expression $A_1 A_2 \ldots A_q A_{q+1}$ represents a pseudo product P, with $P \subseteq R$.*

Proof. By examining all possible cases:

1. $\exists i \in [1, \ldots, q] : A_{q+1} = \overline{A}_i$. Then $A_1 A_2 \ldots A_q A_{q+1}$ is identically $false$, hence is contained in R.

2. $\exists i \in [1, \ldots, q] : A_{q+1} = A_i$. Then $A_1 A_2 \ldots A_q A_{q+1} = R \subseteq R$.

3. $\forall i \in [1, \ldots, q] : A_{q+1} \neq \overline{A}_i$, $A_{q+1} \neq A_i$, and $A_{q+1} = y_1 \oplus y_2 \oplus \ldots \oplus y_k$ with $y_i \in \{x_1, x_2, \ldots, x_m\}$ $(\forall i \in [1, \ldots, k])$. By lemma 21, $A_1 A_2 \ldots A_q A_{q+1}$ represent a pseudo product $P \subset R$.

4. $\forall i \in [1, \ldots, q] : A_{q+1} \neq \overline{A}_i$, $A_{q+1} \neq A_i$, and $\exists\ y_i \notin \{x_1, x_2, \ldots, x_m\} : A_{q+1} = y_1 \oplus y_2 \oplus \ldots \oplus y_k$. We now prove that the expression $A_1 A_2 \ldots A_q A_{q+1}$ is equivalent (that is denotes the same points in the space B^n, symbol $\cong$) to an expression of the form described in case 3. Observe that if $y_i \notin \{x_1, x_2, \ldots, x_m\}$ then $\exists A_j$ $(j \in [1, \ldots, q])$ such that $A_j = (z_1 \oplus z_2 \oplus \ldots \oplus z_h \oplus \widehat{y}_i)$ and $z_1, \ldots, z_h \in \{x_1, \ldots, x_m\}$ $(0 \leq h \leq m)$. From $A_j = true$ we have: $\widehat{y}_i = z_1 \oplus z_2 \oplus \ldots \oplus \overline{z}_h$. If we substitute every non-canonical $\widehat{y}_i$ in A_{q+1} with the correspondent $z_1 \oplus z_2 \oplus \ldots \oplus \overline{z}_h$,

we obtain a new A'_{q+1} with $A_1A_2\ldots A_qA_{q+1} \cong A_1A_2\ldots A_qA'_{q+1}$, and $A_1A_2\ldots A_qA'_{q+1}$ is in the form described in case 3.

■

An easy extension of proposition 22 is the following:

Corollary 23 *Let $A_1A_2\ldots A_q$ be a CEX expression of a pseudocube R, of degree m, and let $A_i = x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus\widehat{x}_{i_h}$. Any PP expression $A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_qB_1\overline{B_2}$ (or $A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_q\overline{B_1}B_2$) with $B_1 = x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_j}$ and $B_2 = x_{i_{j+1}}\oplus x_{i_{j+2}}\oplus\ldots\oplus x_{i_k}$, represents a pseudoproduct P, with $P\subseteq R$.*

Proof. We prove that the expression $A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_qB_1\overline{B_2}$ is equivalent to an expression $A_1A_2\ldots A_qB$ that, by proposition 22, represents a pseudo product P, with $P\subseteq R$. We have two cases:

1. Expression $A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_qB_1\overline{B_2}$. Note that

$$A_iB_1 = (x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_j}\oplus x_{i_{j+1}}\oplus x_{i_{j+2}}\oplus\ldots\oplus\widehat{x}_{i_k})(x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_j}) =$$
$$= (x_{i_{J+1}}\oplus x_{i_{j+2}}\oplus\ldots\oplus\overline{\widehat{x}}_{i_k})(x_{i_1}\oplus x_{i_2}\oplus\ldots\oplus x_{i_j}) = B_1\overline{B_2}$$

   Then we have:$A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_qB_1\overline{B_2} \cong A_1A_2\ldots A_qB_1$

2. Expression $A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_q\overline{B_1}B_2$. For the same reason we obtain:

$$A_1A_2\ldots A_{i-1}A_{i+1}\ldots A_q\overline{B_1}B_2 \cong A_1A_2\ldots A_qB_2$$

   In both cases we have an expression $A_1A_2\ldots A_qB$.

■

We can now generalize all the previous results with the following proposition:

Proposition 24 *Let A and B be two pseudocubes in B^n, and let $A_1A_2\ldots A_m$ be a CEX expression of A. We have $B\Rightarrow A$ (or $B\subseteq A$) if and only if there exists a PP representation of B of the form $A_1A_2\ldots A_mB_1\ldots B_k$ $(0\leq k)$.*

Proof. *If part.* Immediate. $B = A \wedge C$ for some C, and $A \wedge C \Rightarrow A$.

Only if part. By induction on k.

The basis $k = 1$ holds by proposition 22. Let the assertion hold for $k-1$, and let $B = A_1A_2 \ldots A_nB_1 \ldots B_k$. Given $B' = A_1A_2 \ldots A_nB_1 \ldots B_{k-1}$, by induction we have: $B' \Rightarrow A$. Note that $B = B'B_k$, then, by proposition 22, $B \Rightarrow B' \Rightarrow A$. ■

By corollary 23, any PP expression $A_1A_2 \ldots A_{i-1}A_{i+1} \ldots A_qB_1\overline{B_2}$ (or $A_1A_2 \ldots A_{i-1}A_{i+1} \ldots A_q\overline{B_1}B_2$) with $B_1 = x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_j}$ and $B_2 = x_{i_{J+1}} \oplus x_{i_{j+2}} \oplus \ldots \oplus x_{i_k}$, represents a pseudoproduct P, with $P \Rightarrow R$. A immediate extension of proposition 24 and corollary 23 is the following theorem.

Theorem 25 *Let A and B be two pseudocubes, and let $A_1A_2 \ldots A_n$ be a CEX expression of A. We have $B \Rightarrow A$ (or $B \subseteq A$) if and only if there exists a PP representation, $B_1B_2 \ldots B_k$ of B, and there is a partition of $\{A_1A_2 \ldots A_n\}$ into two subset $\{A_{i_1} \ldots A_{i_s}\}$ and $\{A_{i_{s+1}} \ldots A_{i_n}\}$ (where $0 \leq s \leq n$), such that:*

1) $\forall A_j \in \{A_{i_1} \ldots A_{i_s}\}, \exists B_i \in \{B_1B_2 \ldots B_k\} : A_j = B_i$ *and*

2) $\forall A_j \in \{A_{i_{s+1}} \ldots A_{i_n}\}$ *with* $A_j = x_1 \oplus x_2 \oplus \ldots \oplus \widehat{x}_r$

$$\exists B_{j_1}, \ldots, B_{j_t} \in \{B_1B_2 \ldots B_k\}\ (t \leq k) :$$

$$B_{j_1} = x_1 \oplus \ldots \oplus \widehat{x}_{r_1}$$

$$B_{j_2} = x_{r_1+1} \oplus \ldots \oplus \widehat{x}_{r_2}$$

$$\vdots$$

$$B_{j_t} = x_{r_{t-1}+1} \oplus \ldots \oplus \widehat{x}_r$$

and the number of negations on $x_{r_1} \ldots x_r$ is $\begin{cases} \text{even}, & \text{if } h \text{ is odd} \\ \text{odd}, & \text{if } h \text{ is even} \end{cases}$

$$\text{where } h = \begin{cases} t+1, & \text{if } A_j = x_1 \oplus x_2 \oplus \ldots \oplus \overline{x}_r \\ t, & \text{if } A_j = x_1 \oplus x_2 \oplus \ldots \oplus x_r. \end{cases}$$

We finally have:

Proposition 26 *Any normal form can be transformed in an equivalent CEX expression.*

Proof. Let $A_1A_2 \ldots A_q$ be a CEX expression of a pseudocube R, of degree m and let P be a sub-pseudocube of R. Note that the normal form $A_1A_2 \ldots A_qA_{q+1}$ of P is not a CEX expression. Let $x_1, x_2, \ldots, x_m$ be the canonical variables of R and $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m$ the canonical variables of P. Since $A_1A_2 \ldots A_q$ is a CEX expression of R, then $A_j = x_{r_1} \oplus x_{r_2} \oplus \ldots \oplus x_{r_k} \oplus y_j$ with $x_{r_1}, x_{r_2}, \ldots, x_{r_k}$ canonical variables and y_j non canonical. If $x_i \in \{x_{r_1}, x_{r_2}, \ldots, x_{r_k}\}$ then in the expression $A_1A_2 \ldots A_qA_{q+1}$of P there is a factor (A_j) with two non canonical variables (y_j and x_i). Therefore the normal form $A_1A_2 \ldots A_qA_{q+1}$ is not a CEX expression. By the proof of lemma 20, $A_{q+1} = x_{r_1} \oplus x_{r_2} \oplus \ldots \oplus x_{r_k} \oplus \widehat{x}_i$ with $x_{r_1}, x_{r_2}, \ldots, x_{r_k} \in \{x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m\}$. Hence $x_i = x_{r_1} \oplus x_{r_2} \oplus \ldots \oplus \widehat{x}_{r_k}$. We shall now replace x_i with $x_{r_1} \oplus x_{r_2} \oplus \ldots \oplus \widehat{x}_{r_k}$ in every $A_j \in \{A_1, A_2, \ldots A_q\}$ and we obtain a CEX expression for P. ■

References

[LP97] F. Luccio and L. Pagli. Normal matrices, pseudo-cubes and pseudo-products. *Congressus Numerantium* 127 (1997) 33-56.

[LP99] F. Luccio and L. Pagli. On a new Boolean Function with applications. *IEEE transactions on computers* 48, 3 (1999).