Discrete Applied Mathematics 32 (1991) 263-273
North-Holland

Transformation completeness properties of SVPC transformation sets*

S.C. Tai**

Institute of Computer Science, National Tsing-Hua University, Hsinchu, Taiwan, People's Rep. of China

M.W. Du

GTE Laboratories, Waltham, MA, USA

R.C.T. Lee

National Tsing-Hua University, Hsinchu, Taiwan; and Academia Sinica, Taipei, Taiwan, People's Rep. of China

Received 15 March 1988
Revised 13 November 1989

Abstract

Tai, S.C., M.W. Du and R.C.T. Lee, Transformation completeness properties of SVPC transformation sets, Discrete Applied Mathematics 32 (1991) 263-273.

A set T of permutations of a finite set $\mathfrak{D}$ is said to be transformation complete if the orbits of $\langle T\rangle$, the group generated by T, acting on $\mathfrak{F}(\mathfrak{D})$, the power set of $\mathfrak{D}$, are exactly the set of subsets of $\mathfrak{D}$ having the same cardinality, where the orbit of $x\in\mathfrak{F}(\mathfrak{D})$ is $\{\alpha(x)\mid\alpha\in\langle T\rangle\}$. This paper studies the transformation completeness properties of suppressed variable permutation and complementation (SVPC) transformations which act on Boolean variables with domain being $\mathfrak{D}=\{0,1\}^n$. An SVPC transformation with r control variables is an identity on the n-cube except on an $(n-r)$-subcube where the acting is like a variable permutation and complementation (VPC) transformation on $n-r$ variables, $0\le r<n$. Let P_r^n be the set of all SVPC transformations on n variables with r control variables. It is shown that P_r^n is transformation complete for $n>r\ge 1$. In particular, it is shown that $S_{2^n}=\langle P_{n-1}^n\rangle=\langle P_{n-2}^n\rangle\supset\langle P_{n-3}^n\rangle=\langle P_{n-4}^n\rangle=\cdots=\langle P_1^n\rangle=A_{2^n}\supset\langle P_0^n\rangle$, where S_{2^n} and A_{2^n} are the symmetric group and alternating group of degree 2^n, respectively. P_0^n, i.e., the VPC transformation group on n variables, is not transformation complete, however. Thus, one control variable is necessary and sufficient to make P_r^n transformation complete.

* This research work was partially supported by the National Science Council of the People's Rep. of China under contract NSC78-0408-E007-06.

** Present address: Institute of Electrical Engineering, National Cheng-Kung University, Tainan, Taiwan, People's Rep. of China.

1. Introduction

Consider the transformation scheme shown in Fig. 1, where f_i's are n-variable Boolean functions and t_i's are transformations of Boolean variables (the coordinates of the n-cube). Each transformation t_i corresponds to a substitution of the Boolean variable (coordinate of the n-cube) x_j by a Boolean function $g_j(x_1, \dots, x_n)$, $1 \le j \le n$. That is,

$$t_i = \{x_1 \leftarrow g_{i1}(x_1, \dots, x_n), \dots, x_n \leftarrow g_{in}(x_1, \dots, x_n)\}$$

and

$$f_{i+1}(g_{i1}(x_1, \dots, x_n), \dots, g_{in}(x_1, \dots, x_n)) = f_i(x_1, \dots, x_n),$$

where each g_{ij} is a Boolean function of $x_1, \dots, x_n$. A transformation of the n-cube, t_i, has the result of function transformation. By successive applications of transformations, the Boolean function f_1 can be transformed to another function f_{k+1}.

$$f_1 \xrightarrow{t_1} f_2 \xrightarrow{t_2} f_3 \longrightarrow \cdots \longrightarrow f_{k+1}$$

Fig. 1. Transformation scheme with each t_i transforming f_i to f_{i+1}.

Since in the transformation scheme, each transformation t_i corresponds to n Boolean functions, it can be realized by combinational circuits. Let f_1 be the Boolean function to be realized by combinational circuits. Then f_1 can be accomplished by connecting a cascade realization of the sequence of transformations $t_1, t_2, \dots, t_k$ and the realization of f_{k+1}. To obtain an economical realization of f_1, we require that each transformation can be realized economically. It is also very desirable that the set of transformations provided be powerful enough such that any Boolean function can be transformed to a very simple one. In the next section, we shall propose a special class of transformations, which can be realized economically, called suppressed variable permutation and complementation (SVPC) transformations. Its transformation power is studied throughout this paper.

2. Notations and preliminaries

Let us relax temporarily from the Boolean functions and consider the general form of a binary valued function. An n-variable Boolean function is a special case of a map $f : \mathfrak{D} \to \{0, 1\}$ where $\mathfrak{D}$ is a finite domain, in fact $\mathfrak{D}$ is the set $\{0, 1\}^n$ whose elements are the n-binary vectors which can be assimilated, via the binary coding, to integers, so that $\mathfrak{D}$ is the set $\{0, 1, \dots, 2^n - 1\}$. Thus, the binary valued function $f : \{0, 1, \dots, k\} \to \{0, 1\}$ becomes an n-variable Boolean function when $k = 2^n - 1$. Moreover, such a map f may be assimilated to a subset $\mathfrak{J} \subseteq \mathfrak{D}$ where $\mathfrak{J}$ is the set of integers that have function values true under f. For example, the binary valued function $f(0)=f(2)=1$ and $f(1)=0$ is assimilated to the set $\mathfrak{J}=\{0,2\}$, where f is defined on the domain $\mathfrak{D}=\{0,1,2\}$.

Given any permutation t of $\mathfrak{D}$ this extends to the set of all maps $f:\mathfrak{D}\to\{0,1\}$. Since f can be assimilated to a subset $\mathfrak{J}\subseteq\mathfrak{D}$, this extension can be viewed as the power set extension. That is, $t(\mathfrak{J})$ is the image of subset $\mathfrak{J}$. Evidently, this extension shall preserve the cardinality. Conventionally, the cardinality of $\mathfrak{J}$, i.e., $|\mathfrak{J}|$, is said to be the *weight* of the function f. Therefore, t induces a function transformation that preserves the weight of the function it acts on.

The problem is: let T be a set of permutations of $\mathfrak{D}$ and $\langle T\rangle$ be the group generated by T. What are the necessary and sufficient conditions on T, in order that the orbits of $\langle T\rangle$ acting on $\mathfrak{F}(\mathfrak{D})$, the power set of $\mathfrak{D}$, are exactly the set of all subsets of $\mathfrak{D}$ having the same cardinality, where the orbit of $x\in\mathfrak{F}(\mathfrak{D})$ is $\{\alpha(x)\mid\alpha\in\langle T\rangle\}$? In this case, T is said to be *transformation complete*. It can be easily checked that if $\langle T\rangle=A_{\mathfrak{D}}$, the alternating group on $\mathfrak{D}$ whose cardinality is at least 3, or $\langle T\rangle=S_{\mathfrak{D}}$, the symmetric group on $\mathfrak{D}$, then T is transformation complete. That is,

Lemma 2.1 (Sufficient condition). *Let T be a set of permutations of $\mathfrak{D}$. If $\langle T\rangle=S_{\mathfrak{D}}$, or $A_{\mathfrak{D}}$ when $|\mathfrak{D}|\geq 3$, then T is transformation complete.*

The sufficient condition shown in Lemma 2.1 is not necessary, however. For example, the set $\{(01234),(0132)\}$ is transformation complete on the set $\mathfrak{D}=\{0,1,2,3,4\}$, but $\langle T\rangle$ is a subgroup of order 20 which is less than that of $A_{\mathfrak{D}}$. Note that $\langle T\rangle$ is not a subgroup of $A_{\mathfrak{D}}$, as (0132) is of odd parity.

Let T be a transformation complete set of permutations. Since the orbits of $\langle T\rangle$ acting on $\mathfrak{F}(\mathfrak{D})$ are exactly the set of subsets of $\mathfrak{D}$ having the same cardinality i and thus each orbit contains $\binom{|\mathfrak{D}|}{i}$ subsets of $\mathfrak{D}$, we have the following weak necessary condition [3]:

Lemma 2.2 (Necessary condition). *Let T be a transformation complete set of permutations. Then $\langle T\rangle$ has order a multiple of* $\mathrm{lcm}[\binom{|\mathfrak{D}|}{i}, i=1,2,\ldots,|\mathfrak{D}|]$.

Since a Boolean function is a special case of a binary valued function, the conditions shown in Lemma 2.1 and Lemma 2.2 also hold for Boolean functions. We are thus ready to define the suppressed variable permutation and complementation (SVPC) transformations:

Definition 2.3. In an SVPC transformation, a number of Boolean variables are selected to control the permutation and complementation of the remaining Boolean variables. Let the Boolean variable set be $X=\{x_1,\ldots,x_n\}$. Without loss of generality, we assume that x_1 to x_r are selected to control the permutation and complementation of x_{r+1} to x_n. Then an SVPC transformation t can be expressed as

$$[x_1 \leftarrow x_1, \ldots, x_r \leftarrow x_r, x_{r+1} \leftarrow x_1^{c_1} \ldots x_r^{c_r} x_{p(r+1)}^{c_{r+1}} + \overline{x_1^{c_1}} \ldots \overline{x_r^{c_r}} x_{r+1}, \ldots, x_n \leftarrow x_1^{c_1} \ldots x_r^{c_r} x_{p(n)}^{c_n} + \overline{x_1^{c_1}} \cdots \overline{x_r^{c_r}} x_n\},$$

where $x_j^{c_i}$ is equal to either x_j ($c_i = 0$) or $\bar{x}_j$ ($c_i = 1$), and p is a permutation on letters $r+1, \ldots, n$.

For the sake of convenience, t in Definition 2.3 is described as "When $x_1 x_2 \ldots x_r = b_1 b_2 \ldots b_r$, where

$$b_j = \begin{cases} 0, & \text{if } x_j^{c_i} = \bar{x}_j, \\ 1, & \text{if } x_j^{c_i} = x_j, \ 1 \le j \le r, \end{cases}$$

then $x_i \leftarrow x_{p(i)}^{c_i}$, $r+1 \le i \le n$".

Definition 2.4. The set of all SVPC transformations on n variables with r control variables is denoted as P_r^n. We use L_r^n to denote the subset of P_r^n that contains all the SVPC transformations of variables $x_1, x_2, \ldots, x_n$ that use $x_1, x_2, \ldots, x_r$ as control variables.

Recall that P_0^n is just the classical isometry group of the n-cube, i.e., the variable permutation and complementation (VPC) transformation group on n variables which has been extensively studied in the literature [2]. Consider the transformations of P_r^n. Each transformation in P_r^n can be viewed as the identity on the n-cube except on an $(n-r)$-subcube (defined by r fixed coordinates) where it acts like a VPC transformation on $n-r$ variables (the free variables). By now, it is clear that each SVPC transformation induces a permutation of the vertices on the n-cube.

3. The permutation groups generated by P_r^n and the transformation completeness properties of P_r^n

Let us first consider the transformation power of VPC, i.e., P_0^n, which seems to be the least powerful. In fact, since VPC transformation group has order $n! \times 2^n$ [2] which is less than $\text{lcm}[\binom{2^n}{i}, i = 1, 2, \ldots, 2^n]$ for $n \ge 2$, we have, by Lemma 2.2, the following lemma:

Lemma 3.1. *The set* VPC, *i.e.*, P_0^n, *is not transformation complete for* $n \ge 2$.

It is because that VPC is not transformation complete that SVPC is introduced.

Theorem 3.2. $\langle P_{n-1}^n \rangle = \langle P_{n-2}^n \rangle = S_{2^n}$ *for* $n \ge 3$. *Thus* P_{n-1}^n *and* P_{n-2}^n *are both transformation complete.*

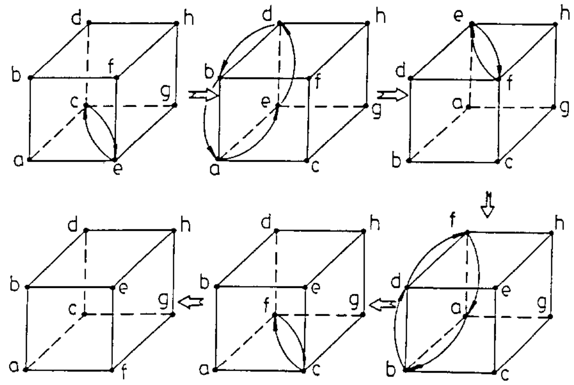

Fig. 2. A sequence of transformations to exchange two adjacent vertices e and f on a 3-cube.

Proof. $\langle P^n_{n-1}\rangle = S_{2^n}$ because by controlling $n-1$ variables, we can exchange any two adjacent vertices of the n-cube.

Figure 2 shows a five-step transformation sequence of P^3_1 to exchange two adjacent vertices on a 3-cube. Similarly we can control $n-2$ variables and allow two variables to permute and complement to exchange any two adjacent vertices on an n-cube. Thus, $\langle P^n_{n-2}\rangle = S_{2^n}$. We thus complete our proof. □

When $n-r\geq 3$, P^n_r does not generate S_{2^n}, however. In fact, the transformations from P^n_r are of even parity for $n-r\geq 3$.

Lemma 3.3. *Every permutation of* P^n_0, $n\geq 3$, *is of even parity.*

Proof. Let the n variables be $x_1, x_2, \ldots, x_n$. Then VPC is generated by variable permutation (VP) set and $(x_1, x_2, \ldots, x_n) \leftarrow (x_1, x_2, \ldots, \bar{x}_n)$, where VP is generated in turn by $\{(x_1x_2), (x_1x_3), \ldots, (x_1x_n)\}$.

The permutation induced by $(x_1, x_2, \ldots, x_n) \leftarrow (x_1, x_2, \ldots, \bar{x}_n)$ is $(01)(23)\cdots(2^n-2\ 2^n-1)$ and there are totally $\frac{1}{2}(2^n-2)+1 = 2^{n-1}$ transpositions contained in this permutation. Hence it is of even parity when $n\geq 2$.

It suffices to show now that any permutation induced by (x_1x_i) is of even parity.

The vertices on the n-cube are permuted only when their x_1 and x_i are different. If they both contain "0" or "1", then they are fixed by transposition (x_1x_i). The transposition (x_1x_i) corresponds to the product of all transpositions induced by fixing the other $n-2$ variables for binary codes ranging from 00...0 to 11...1 and exchanging the contents of x_1 and x_i, i.e., b_1 and b_i. The number of transpositions to be producted is 2^{n-2}, which is even for $n\geq 3$. Hence, we complete our proof. □

Theorem 3.4. *Every transformation of* P^n_r, $n-r\geq 3$, *is of even parity.*

Proof. The parity of a transformation in P_r^n is the same as that of a corresponding transformation in P_0^{n-r}. Since $n-r \geq 3$, by Lemma 3.3, we have that every transformation of P_r^n, $n-r \geq 3$, is of even parity. This completes our proof. □

It is intuitively true that the more variables used as control variables, the more powerful the SVPC transformation group $\langle P_r^n \rangle$ will be. In the following, we shall show that a chain relation does exist.

Lemma 3.5. VPC $\subset \langle P_r^n \rangle$, *for* $n > r \geq 1$.

Proof. Let the n variables be $x_1, x_2, \ldots, x_n$. Then VPC is generated by variable permutation (VP) set and $(x_1, x_2, \ldots, x_n) \leftarrow (x_1, x_2, \ldots, \bar{x}_n)$, where VP is generated in turn by $\{(x_1x_2), (x_1x_3), \ldots, (x_1x_n)\}$. It is evident that any element of these generators can be generated by P_r^n if $n \geq r+2$, i.e., at least two variables are not used as control variables. For the special case that $r = n-1$, it evidently holds since $\langle P_{n-1}^n \rangle = S_{2^n}$.

It suffices to show that $\langle P_r^n \rangle \not\subseteq$ VPC. This is evident since $P_r^n \not\subseteq$ VPC. Hence, we complete our proof. □

Lemma 3.6. $\langle$VPC$, L_r^n \rangle = \langle P_r^n \rangle$, *for* $n > r \geq 1$.

Proof. By Lemma 3.5, it is evident that $\langle$VPC$, L_r^n \rangle \subseteq \langle P_r^n \rangle$.

We prove that any element of P_r^n can be generated by a combination of VPC and L_r^n. This is evident since we can first use VPC (as a matter of fact, we use variable permutations only) to transform the r control variables to $x_1, x_2, \ldots, x_r$, then do the desired suppressed variable permutation and complementation transformation of L_r^n. After that, we use VPC to transform the r control variables back to their original locations. Hence $\langle$VPC$, L_r^n \rangle \supseteq \langle P_r^n \rangle$. We thus complete our proof. □

Lemma 3.7. $\langle P_r^n \rangle \subseteq \langle P_{r+s}^n \rangle$, *where* $s \geq 1$ *and* $n > r$.

Proof. By Lemma 3.6, we suffice to show that $L_r^n \subseteq \langle P_{r+s}^n \rangle$.

A transformation of L_r^n is of the form:

$$\text{if } x_1x_2\ldots x_r = b_1b_2\ldots b_r, \text{ then VPC } x_{r+1}, \ldots, x_n$$

and a transformation of P_{r+s}^n is of the form:

$$\text{if } x_1x_2\ldots x_r = b_1b_2\ldots b_r, \text{ then } P_s^{n-r} x_{r+1}, \ldots, x_n$$

where $b_i = 0$ or 1. Since VPC of $n-r$ variables is a proper subset of $\langle P_s^{n-r} \rangle$ by Lemma 3.5, we thus complete our proof. □

By Theorem 3.2, Lemma 3.5 and Lemma 3.7, we have the following power chain relation:

Theorem 3.8. $\langle P_{n-1}^n\rangle = \langle P_{n-2}^n\rangle \supseteq \langle P_{n-3}^n\rangle \supseteq \langle P_{n-4}^n\rangle \supseteq \cdots \supseteq \langle P_1^n\rangle \supset \langle P_0^n\rangle$.

Since every transformation of P_r^n, $n-r\geq 3$, is of even parity, $\langle P_r^n\rangle$ is a subgroup of A_{2^n}. In the following, we shall show that $\langle P_1^n\rangle$, $n\geq 4$, is exactly A_{2^n}. Thus, by the power chain relation and the fact that every transformation of P_{n-3}^n is of even parity, we shall conclude that $\langle P_r^n\rangle = A_{2^n}$ for $n-r\geq 3$ and $r\geq 1$. Let us start from some well-known results about permutations:

Lemma 3.9. *Let p be a permutation then*

$$p(i_1\, i_2 \ldots i_r)p^{-1} = (p(i_1)\ p(i_2) \ldots p(i_r)).$$

Proof. See [3, p. 51, Exercise]. □

Lemma 3.10. $(ab)(cd) = (cd)(ab)$.

Proof. See [1, p. 14, Exercise]. □

Lemma 3.11. *Two circular permutations which have no letter in common are commutative.*

Proof. This result comes directly from Lemma 3.10 and the fact that

$$(a_1a_2\ldots a_{n-1}a_n) = (a_1a_n)(a_1a_{n-1})\ldots(a_1a_3)(a_1a_2). \qquad \square$$

Lemma 3.12. *If* $p\in P_1^n$, *then* $p\cdot\tilde{p}\in P_1^{n+1}$, *where* $\tilde{p}=qpq^{-1}$, $q=(0\ 2^n)(1\ 2^n+1)\cdots(i\ 2^n+i)\cdots(2^n-1\ 2^{n+1}-1)$. *That is,* $\tilde{p}$ *and* p *have similar cycle forms except that* p *has* i *in its cycle form if and only if* $\tilde{p}$ *has* 2^n+i *in its cycle form.*

Proof. Let p be the permutation induced from $t\in P_1^n$. Also, let $x_n, x_{n-1}, \ldots, x_2, x_1$ be the n Boolean variables with x_n being the most significant bit of the corresponding binary code. Since $t\in P_1^n$, there is a variable that is selected as the control variable. Let it be x_r and let the constraint be $x_r=B$, where $1\leq r\leq n$ and $B=0$ or 1. Then

$$t(x_i)=\begin{cases} x_{\alpha(i)}^{c_i}, & \text{if } x_r=B \text{ and } i\neq r,\\ x_i, & \text{otherwise,}\end{cases}$$

where $x_{\alpha(i)}^{c_i}=x_{\alpha(i)}$ or $\bar{x}_{\alpha(i)}$ and α is a permutation on letters $n, n-1, \ldots, r+1, r-1, \ldots, 2, 1$.

Thus, if $b_r=B$ then

$$\begin{aligned} p(i) &= p(b_nb_{n-1}\ldots b_{r+1}Bb_{r-1}\ldots b_2b_1)\\ &= b_{\alpha(n)}^{c_n}b_{\alpha(n-1)}^{c_{n-1}}\ldots b_{\alpha(r+1)}^{c_{r+1}}Bb_{\alpha(r-1)}^{c_{r-1}}\ldots b_{\alpha(2)}^{c_2}b_{\alpha(1)}^{c_1}=j, \end{aligned}$$

where $b_n b_{n-1} \dots B \dots b_2 b_1$ is the binary code of i and

$$b_{\alpha(n)}^{c_n} b_{\alpha(n-1)}^{c_{n-1}} \dots b_{\alpha(r+1)}^{c_{r+1}} B b_{\alpha(r-1)}^{c_{r-1}} \dots b_{\alpha(2)}^{c_2} b_{\alpha(1)}^{c_1}$$

is the binary code of j; otherwise, if $b_r = \bar{B}$ then $p(i) = i$.

Now, let q be the permutation that is induced from t' of P_1^{n+1} as:

$$t'(x_i) = \begin{cases} x_{\alpha(i)}^{c_i}, & \text{if } x_r = B \text{ and } i \neq r \text{ and } i \neq n+1, \\ x_i, & \text{otherwise.} \end{cases}$$

Thus, if $b_r = B$ then

$$q(b_{n+1} b_n b_{n-1} B b_{r-1} \dots b_2 b_1)$$
$$= b_{n+1} b_{\alpha(n)}^{c_n} b_{\alpha(n-1)}^{c_{n-1}} \dots b_{\alpha(r+1)}^{c_{r+1}} B b_{\alpha(r-1)}^{c_{r-1}} \dots b_{\alpha(2)}^{c_2} b_{\alpha(1)}^{c_1};$$

else

$$q(b_{n+1} b_n b_{n-1} \dots b_{r+1} \bar{B} b_{r-1} \dots b_2 b_1) = b_{n+1} b_n b_{n-1} \dots b_{r+1} \bar{B} b_{r-1} \dots b_2 b_1.$$

That is, if $b_r = B$ then

$$q(i) = q(0 b_n b_{n-1} \dots b_{r+1} B b_{r-1} \dots b_2 b_1)$$
$$= 0 b_{\alpha(n)}^{c_n} b_{\alpha(n-1)}^{c_{n-1}} \dots b_{\alpha(r+1)}^{c_{r+1}} B b_{\alpha(r-1)}^{c_{r-1}} \dots b_{\alpha(2)}^{c_2} b_{\alpha(1)}^{c_1} = j$$

and

$$q(i + 2^n) = q(1 b_n b_{n-1} \dots b_{r+1} B b_{r-1} \dots b_2 b_1)$$
$$= 1 b_{\alpha(n)}^{c_n} b_{\alpha(n-1)}^{c_{n-1}} \dots b_{\alpha(r+1)}^{c_{r+1}} B b_{\alpha(r-1)}^{c_{r-1}} \dots b_{\alpha(2)}^{c_2} b_{\alpha(1)}^{c_1} = 2^n + j,$$

but if $b_r = \bar{B}$ then $q(i) = i$ and $q(2^n + i) = 2^n + i$.

Hence, $p(i) = j$ iff $q(i) = j$ and $q(2^n + i) = 2^n + j$, where $i, j \in [0, 2^n - 1]$. Thus, we can express q as the product of permutations p and $\tilde{p}$ such that for any letter i in p we have letter $2^n + i$ in $\tilde{p}$, i.e., $q = p \cdot \tilde{p}$. We thus complete our proof. □

Lemma 3.13. *If $p \in \langle P_1^n \rangle$, then $p \cdot \tilde{p} \in \langle P_1^{n+1} \rangle$, where $\tilde{p}$ is as in Lemma* 3.12.

Proof. Since $p \in \langle P_1^n \rangle$, there exists a sequence of permutations $p_1, p_2, \dots, p_k \in P_1^n$ such that $p = p_1 \cdot p_2 \cdot \dots \cdot p_k$. Thus, by Lemma 3.12, we have $\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_k$ such that $p_1 \cdot \tilde{p}_1, p_2 \cdot \tilde{p}_2, \dots, p_k \cdot \tilde{p}_k \in P_n^{n+1}$. Thus $(p_1 \cdot \tilde{p}_1) \cdot (p_2 \cdot \tilde{p}_2) \cdot \dots \cdot (p_k \cdot \tilde{p}_k) \in \langle P_1^{n+1} \rangle$. But, by Lemma 3.11, we have

$$\begin{aligned} (p_1 \cdot \tilde{p}_1) \cdot (p_2 \cdot \tilde{p}_2) \cdot \dots \cdot (p_k \cdot \tilde{p}_k) &= p_1 \cdot p_2 \cdot \tilde{p}_1 \cdot \tilde{p}_2 \cdot \dots \cdot p_k \cdot \tilde{p}_k \\ &\vdots \\ &= \\ &= (p_1 \cdot p_2 \cdot \dots \cdot p_k) \cdot (\tilde{p}_1 \cdot \tilde{p}_2 \cdot \dots \cdot \tilde{p}_k) \\ &= p \cdot \tilde{p} \in \langle P_1^{n+1} \rangle. \end{aligned}$$

Thus, we complete our proof. □

Lemma 3.14. *If* $(pqr) \in \langle P_1^n \rangle$, *then* $(pqr)(2^n+p\ 2^n+q\ 2^n+r) \in \langle P_1^{n+1} \rangle$.

Proof. This comes directly from Lemma 3.13. □

Lemma 3.15. $\langle P_1^n \rangle \supseteq A_{2^n}$, *for* $n \geq 3$.

Proof. We prove it by induction.

(1) For $n=3$, $\langle P_1^3 \rangle = S_8 \supseteq A_{2^3}$ by Theorem 3.2.

(2) Suppose that $\langle P_1^k \rangle \supseteq A_{2^k}$. We prove that $\langle P_1^{k+1} \rangle \supseteq A_{2^{k+1}}$.

Since $\langle P_1^k \rangle \supseteq A_{2^k}$, $(abc) \in \langle P_1^k \rangle$ and thus by Lemma 3.14, we have $(abc) \times (2^k+a\,2^k+b\,2^k+c) \in \langle P_1^{k+1} \rangle$ for all $a, b, c \in [0, 2^k-1]$.

Consider the following transformation of P_1^{k+1}:

$$\text{if } x_{k+1}=1, \quad \text{then} \quad x_3 \leftarrow x_1,$$
$$x_1 \leftarrow x_3.$$

Let p be the permutation thus induced. Then $p(0)=0$, $p(1)=1$, $p(2)=2$, $p(2^k)=2^k$, $p(2^k+1)=2^k+4$ and $p(2^k+2)=2^k+2$. Then

$$q_1 = p(012)(2^k\ 2^k+1\ 2^k+2)p^{-1} = (012)(2^k\ 2^k+4\ 2^k+2) \in \langle P_1^{k+1} \rangle$$

since $(012)(2^k\ 2^k+1\ 2^k+2)$ is an element of P_1^{k+1}.

Thus,

$$\begin{aligned}(024)(2^k\ 2^k+2\ 2^k+4)q_1 &= (024)(2^k\ 2^k+2\ 2^k+4)(012)(2^k\ 2^k+4\ 2^k+2)\\ &= (024)(012)(2^k\ 2^k+2\ 2^k+4)(2^k\ 2^k+4\ 2^k+2)\\ &= \mathbf{(014)} \in \langle P_1^{k+1} \rangle\end{aligned}$$

since $(024)(2^k\ 2^k+2\ 2^k+4)$ is an element of P_1^{k+1}.

Let $(abc)=(42i) \in \langle P_1^k \rangle$. Then $p=(42i)(2^k+4\ \ 2^k+2\ \ 2^k+i) \in \langle P_1^{k+1} \rangle$, where $i \in [3, 2^k-1]-\{4\}$.

Let $q=(014)$. Then $pqp^{-1} = \mathbf{(012)} \in \langle P_1^{k+1} \rangle$.

Let $q=(012)$, $p=(42i)(2^k+4\ \ 2^k+2\ \ 2^k+i)$. Then $pqp^{-1} = \mathbf{(01}\boldsymbol{i}\mathbf{)} \in \langle P_1^{k+1} \rangle$, $\forall i \in [3, 2^k-1]-\{4\}$.

Thus, $(01i) \in \langle P_1^{k+1} \rangle$, $\forall i \in [2, 2^k-1]$. We suffice to show that $(01i) \in \langle P_1^{k+1} \rangle$, $\forall i \in [2^k, 2^{k+1}-1]$.

Consider the following transformation of P_1^{k+1}:

$$\text{if } x_1=0 \quad \text{then} \quad x_{k+1} \leftarrow x_k,$$
$$x_k \leftarrow x_{k+1}.$$

Let p be the permutation thus induced. Then $p(0)=0$, $p(1)=1$, $p(2^{k-1})=2^k$, $p(2^{k-1}+2)=2^k+2$. Thus $p(0\ 1\ 2^{k-1})p^{-1} = \mathbf{(0\ 1\ 2^k)} \in \langle P_1^{k+1} \rangle$ and $p(0\ 1\ 2^{k-1}+2)p^{-1} = \mathbf{(0\ 1\ 2^k+2)} \in \langle P_1^{k+1} \rangle$.

Consider the following transformation of P_1^{k+1}:

$$\text{if } x_1 = 1 \quad \text{then} \quad x_{k+1} \leftarrow x_k,$$
$$x_k \leftarrow x_{k+1}.$$

Let p be the permutation thus induced. Then $p(0)=0$, $p(1)=1$, $p(2^{k-1}+1)=2^k+1$. Thus $p(0\ 1\ 2^{k-1}+1)p^{-1}=(\mathbf{0\ 1\ 2^k+1})\in\langle P_1^{k+1}\rangle$.

Let q be $(0\ 1\ 2^k+2)$, $p=(23i)(2^k+2\ 2^k+3\ 2^k+i)$, where $i\in[4,2^k-1]$. Then

$$pqp^{-1}=(\mathbf{0\ 1\ 2^k+3})\in\langle P_1^{k+1}\rangle$$

and

$$p(0\ 1\ 2^k+3)p^{-1}=(\mathbf{0\ 1\ 2^k+}\boldsymbol{i})\in\langle P_1^{k+1}\rangle,\ \forall i\in[4,2^k-1].$$

Thus $(01i)\in\langle P_1^{k+1}\rangle$, $\forall i\in[2,2^{k+1}-1]$. Since $\{(01i)\mid 2\le i\le 2^{k+1}-1\}$ is a set of generators of $A_{2^{k+1}}$ [4], we have $A_{2^{k+1}}\subseteq\langle P_1^{k+1}\rangle$. This completes our proof. □

Theorem 3.16. *$\langle P_1^n\rangle=A_{2^n}$, for $n\ge4$. Thus, P_1^n is transformation complete.*

Proof. By Lemma 3.15, we have $A_{2^n}\subseteq\langle P_1^n\rangle$ for $n\ge4$. By Theorem 3.4, we have $\langle P_1^n\rangle\subseteq A_{2^n}$ for $n\ge4$. Thus, $\langle P_1^n\rangle=A_{2^n}$. By Lemma 2.1, P_1^n is thus transformation complete. This completes our proof. □

Corollary 3.17.

$$\langle P_r^n\rangle=\begin{cases} S_{2^n}, & \text{if } n-r=1,2 \text{ and } r\ge1,\\ A_{2^n}, & \text{if } n-r\ge3 \text{ and } r\ge1.\end{cases}$$

Proof. We suffice to show that $\langle P_r^n\rangle=A_{2^n}$ for $n-r\ge3$.

By Theorem 3.16 and Theorem 3.2, we have

$$A_{2^n}=\langle P_1^n\rangle\subseteq\langle P_2^n\rangle\subseteq\cdots\subseteq\langle P_r^n\rangle\subseteq\cdots\subseteq\langle P_{n-3}^n\rangle.$$

But $\langle P_{n-3}^n\rangle\subseteq A_{2^n}$ by Theorem 3.4. Thus we have

$$A_{2^n}=\langle P_1^n\rangle\subseteq\langle P_2^n\rangle\subseteq\cdots\subseteq\langle P_r^n\rangle\subseteq\cdots\subseteq\langle P_{n-3}^n\rangle\subseteq A_{2^n}.$$

This concludes that $\langle P_r^n\rangle=A_{2^n}$ if $n-r\ge3$. □

Since $\langle P_r^n\rangle=A_{2^n}$, for $n-r\ge3$ and $r\ge1$, P_r^n is transformation complete. The following theorem summarizes the results.

Theorem 3.18.

(1) $S_{2^n}=\langle P_{n-1}^n\rangle=\langle P_{n-2}^n\rangle\supset\langle P_{n-3}^n\rangle=\langle P_{n-4}^n\rangle=\cdots=\langle P_r^n\rangle=\cdots=\langle P_1^n\rangle=A_{2^n}\supset\langle P_0^n\rangle$.

(2) *P_r^n is transformation complete for $n>r\ge1$.*

The results of this section are interesting. We now know that SVPC is very powerful because one control variable is necessary and sufficient for it to induce function transformations that will transform a Boolean function to any other Boolean function of the same weight in stages. Since P_0^n is not transformation complete, we thus conclude that the minimal value of r to make P_r^n transformation complete is 1.

Acknowledgement

We would like to thank Professor Ming-Chang Kang of the Department of Mathematics, National Taiwan University for many helpful discussions. We would also like to thank one of the referees for many helpful suggestions on how to rewrite this paper.

References

[1] R.D. Carmichael, Introduction to the Theory of Groups of Finite Order (Dover, New York, 1956).
[2] M.A. Harrison, Introduction to Switching and Automata Theorey (McGraw-Hill, New York, 1965).
[3] N. Jacobson, Basic Algebra I (Freeman, San Francisco, CA, 1974).
[4] H.S. Stone, Discrete Mathematical Structures and Their Applications (Science Research Associates, Chicago, IL, 1973).