Algebra and Discrete Mathematics
Volume 14 **(2012)**. Number 1. pp. 71 – 83
© Journal “Algebra and Discrete Mathematics”

RESEARCH ARTICLE

Matrix characterization of symmetry groups of boolean functions

Pawel Jasionowski

Communicated by V. I. Sushchansky

Abstract. We studies symmetry groups of boolean functions and construct new way of description of this problem in matrices language. Some theorems about constructions of symmetry groups with using matrices are presented. Some properties of this approach are given.

Introduction

The main objects of study of this paper are symmetry groups of boolean functions. We want to provide some algorithms to describe special kinds of permutation groups and use groups theoretic techniques to show which features of constructed boolean functions are important in determining the representability of this permutation groups.

The starting point of this paper is [3] and [4] where basic structures and some specific constructions of boolean functions are given. In [7] author show first known example of permutation groups which is 3 representable but is not 2 representable. Moreover in [5], [7] and [8] analysis of direct sum and wreath product of permutation groups is presented.

The problem of symmetry group of boolean functions is important not only from algebraic point of view. One of the application is associated with computer science. We take a device (or "module") M with n inputs, each of which can be in one of two possible states 0 or 1. An outputs

2010 MSC: 05E05.
Key words and phrases: Boolean function, invariance group, symmetry group.

of M can assume 0 or 1 too. That kind of device can be represented by boolean function f which n variables (we can consider generalized modules M which have outputs from the set $\{0, 1, ..., k-1\}$). In general a value of that function depends on order of inputs. Of course there could exist some permutation which leave f invariant. For example when f is invariant under any permutation of inputs then we say that module M is symmetric. In this paper we consider a partial-symmetric functions. It is possible that study of this problem could help in optimizing module positioning on integrated circuit in VLSI design technology.

There are many articles related to this problem. In this paper the main is [3] where authors study boolean functions invariance groups and show how we can construct examples of boolean functions which represent some special kinds of permutation groups. Another important work is [7] where the first known example of permutation groups which is 3 representable but is not 2 representable is given.

1. Preliminaries

Let $\{0,1\}^n$ is a set of all boolean vectors of length n. A mapping

$$f : \{0,1\}^n \to \{0, 1, ..., k-1\}, k \geq 2$$

is called k valued boolean function. A set of all k valued boolean functions with n variables is denoted as a $B_{n,k}$. We put B_n for a set of all boolean functions with n variables and two possible values 0 and 1.

Let $f \in B_{n,k}$ and let σ is a permutation from a symmetric group S_n of set $\{1, ..., n\}$. We define an action σ on $f(x_1, ..., x_n)$ in the following way:

$$f^{\sigma}(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

Let

$$S(f) = \{\sigma \in S_n : f = f^{\sigma}\}$$

It is easy to see that $S(f)$ is a subgroup of group S_n. A group $S(f)$ of all permutation $\sigma \in S_n$ such, that

$$f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

is called a symmetry group of k valued boolean function f. Moreover the function f is called an invariant of the group $S(f)$. Equivalently the group $S(f)$ is called an invariant group of boolean function f. We put 0^i or 1^i to denote i consecutive 0 or 1.

A permutation group $G \leq S_n$ such, that $G = S(f)$ for some boolean function $f : \{0,1\}^n \to \{0,1,...,k-1\}$ is called a group representable by the k valued boolean function f (or k representable). A permutation group G is called representable if it is k representable for some k.

Now let $G \leq S_n$. The main point of research on permutation groups and its representability as a symmetry group of some k valued boolean function is to check how G act on the set $\{0,1\}^n$ of all boolean vectors of length n. We can see that any permutation group (G, X) where $|X| = n$ could be seen as a group which act on the set $\{0,1\}^n$. An action is given by the following condition:

$$x \to x^\sigma : (x_1, x_2, ..., x_n) \to (x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

An orbit of element $x \in X$ is defined as $x^G = \{x^\sigma, \sigma \in G\}$.

We see that if $G = S(f)$ for some $f \in B_{n,k}$ then: (a) if $x, y \in \{0,1\}^n$ are in the same G-orbit, then $f(x) = f(y)$; (b) for every $\tau \notin G$ there have to exist element $x \in X$ such, that x and x^τ are in different G-orbits and $f(x) \neq f(x^\tau)$.

For example a group S_n for some n is 2 representable. $S_n = S(f)$ for the constant boolean function f with n variables. A group $\{id\}$ is 2 representable. The group $\{id\} = S(f)$ where $f(x) = 1$ for x in the form $0^i 1^{n-i}$ and $f(x) = 0$ in other case (symbols 0^i and 1^i denote i consecutive 0 or 1). Interesting and unexpected example is $S_2 \times S_2 = \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ which is 3 representable but is not 2 representable. It was presented in [7]. We can ask which permutation groups are representable (or 2 representable) as symmetry groups of boolean functions. It is important that we work only with permutation groups and we do not consider abstract groups at all. It is easy to proof, that every abstract group is representable as a symmetry group of some boolean function.

2. Matrix characterization

Let n is a positive integer number. Now we would like to consider a module M which is represented by boolean function $f : \{0,1\}^n \to \{0,1\}$. Every mapping at that form can be represented as a vector

$$X = (f(00...0), f(00...1), ..., f(11...1)) = (x_1, ..., x_{2^n})$$

of value of that function. We say that this vector is the vector of value of function f and we denote it by X_f. We consider an order given by the following rule: $x_i = f(y_{i1}, y_{i2}, ..., y_{in})$ iff $i = 2^{n-1}y_{i1} + 2^{n-2}y_{i2} + ... + y_{in} + 1$ for $i = 1, 2, ..., 2^n$.

Let V_{2^n} is a set of that kind of vector. So

$$V_{2^n} = \{X = (x_1, ..., x_{2^n}), x_i \in \{0, 1\}, i = 1, 2, ..., 2^n\}$$

Let $Per(2^n)$ is a set of all permutation matrices of size 2^n. An action of a permutation $\sigma \in S_n$ at the boolean function f given by the rule

$$f^\sigma(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$$

can be considered as the matrices action in the following way

$$AX_f = X_f \tag{1}$$

where $X_f \in V_{2^n}$ is a vector of value of function f. Here the vector X_f is given, and we try to find every matrices $A \in Per(2^n)$ which preserve that equality. First of all it is easy to see that if matrix A preserve the rule (1) then A is an element of stabilizer $Stab_{Per(2^n)}X_f$.

We can characterize the stabilizer of element X_f. We know that $X_f \in V_{2^n}$ so we can notice that there exist sets of indexes $I = \{i_1, i_2, ..., i_k\}$, $J = \{j_1, j_2, ..., j_m\}$, $k, m \leq 2^n$ (I or J can be empty) such that $|I| + |J| = 2^n$ and

$$x_i = \begin{cases} 1 & i \in I \\ 0 & i \in J \end{cases}$$

So we see that

$$Stab_{Per(2^n)}X_f \cong S(i_1, i_2, ..., i_k) \oplus S(j_1, j_2, ..., j_m) \tag{2}$$

Now the question is which permutation matrices from $Stab_{Per(2^n)}X_f$ correspond to permutations from S_n in following way: permutation $\sigma \in S_n$ correspond to matrix $A^\sigma \in Per(2^n)$ iff $\sigma \in S(f) \Leftrightarrow A^\sigma X_f = X_f$ where $f : \{0, 1\}^n \to \{0, 1\}$ is some boolean function.

Let $f : \{0, 1\}^n \to \{0, 1\}$. Let X_f is a vector of value of that function. Now we construct a mapping $\psi : S_n \to Per(2^n)$ such that

$$\psi^{-1}(Stab_{Per(2^n)}X_f \cap \psi(S_n)) = S(f)$$

A positive integer number k which is presented in binary form is denoted as a $(k)_2$. Let $\sigma \in S_n$. Now we consider a vector $c = ((0)_2, (1)_2, ..., (2^n - 1)_2)$. This vector can be considered as a matrix H of size $2^n \times n$ where a row with number i is the i coordinate of the vector c, $i = 1, 2, ..., 2^n$. We denote an element of matrix H by $h_{i,j}, 1 \leq i \leq 2^n, 1 \leq j \leq n$ and say that this is a generalized Hamming's matrix.

We transform a matrix H to $H^{\sigma} = [h_{i,\sigma^{-1}(j)}]_{1 \leq i \leq 2^n, 1 \leq j \leq n}$. Now we can create a vector $h^{\sigma} = [h_i]_{1 \leq i \leq 2^n}$ in the following way:

$$h_i = h_{i,\sigma^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma^{-1}(n)}$$

for $1 \leq i \leq 2^n$. We consider a vector h^{σ} in vertical form. In finally step we create a matrix $A^{\sigma} \in Per(2^n)$, $A^{\sigma} = [a_{ij}]$:

$$a_{ij} = \begin{cases} 1 & \text{dla} \quad h_i = j - 1 \\ 0 & \text{dla} \quad h_i \neq j - 1 \end{cases} \quad i, j \in \{1, 2, ..., 2^n\}$$

Now we can define a mapping $\psi : S_n \to Per(2^n)$ as $\psi(\sigma) = A^{\sigma}$. It is easy to see that it is an injection.

When we have mapping ψ we can answer for a question about construction of group $S(f)$.

Theorem 1. *Let n is a positive integer number and $f : \{0,1\}^n \to \{0,1\}$ is a boolean function. Let X_f is a vector of value of function f and $\psi : S_n \to Per(2^n)$ is a mapping which we construct before. Then*

$$S(f) = \psi^{-1}(Stab_{Per(2^n)} X_f \cap \psi(S_n))$$

Proof. When we have boolean function $f : \{0,1\}^n \to \{0,1\}$ we can find a vector X_f (vector of value of function f) and a group

$$Stab_{Per(2^n)} X_f \cong S(i_1, i_2, ..., i_k) \oplus S(j_1, j_2, ..., j_m)$$

as we show in (2). It is easy to see, that a set $\psi(S_n) \cap Stab_{Per(2^n)} X_f$ is a set of matrices which hold the rule $AX_f = X_f$ on one hand, and correspond to some permutation $\sigma \in S_n$ which preserve f on the other hand. Moreover we see, that there are no other permutations $\tau \in S_n$ which preserve f, so

$$\psi^{-1}(Stab_{Per(2^n)} X_f \cap \psi(S_n)) = S(f)$$

□

Now we have a good looking for a problem of 2-representability of permutation groups. There are no big differences between this situation and a k-representability for $k \geq 2$. Let $f : \{0,1\}^n \to \{0, 1, ..., k-1\}$. Now a vector X_f correspond to the boolean function f can be consider in the following way: there exist sets of indexes $I_0 = \{i_1^0, i_2^0, ..., i_{m_0}^0\}, I_1 = \{i_1^1, i_2^1, ..., i_{m_1}^1\}, ..., I_{k-1} = \{i_1^{k-1}, i_2^{k-1}, ..., i_{m_{k-1}}^{k-1}\}, m_j < 2^n, j = 0, 1, ..., k-1$ (I_j can be empty) and $\sum_{j=0}^{k-1} |I_j| = 2^n$ such that

$$x_i = \begin{cases} 0 & i \in I_0 \\ 1 & i \in I_1 \\ ... & ... \\ k-1 & i \in I_{k-1} \end{cases}$$

So

$$Stab_{Per(2^n)} X_f \cong S(i_1^0, ..., i_{m_0}^0) \oplus S(i_1^1, ..., i_{m_1}^1) \oplus ... \oplus S(i_1^{k-1}, ..., i_{m_{k-1}}^{k-1})$$

Then $\psi^{-1}(Stab_{Per(2^n)} X_f \cap \psi(S_n)) = S(f)$.

As we could see before it is easy to construct a group $Stab_{Per(2^n)} X_f$ for some k-valued boolean function f. The most difficult problem is to decide which matrices from $Stab_{Per(2^n)} X_f$ correspond to some permutations from S_n and how we can construct the group $S(f)$. So now we try to answer for question how we can construct w permutation $\sigma \in S_n$ from $A^\sigma \in Per(2^n)$ and which matrices $A \in Per(2^n)$ do not correspond to any $\sigma \in S_n$.

Let $M_{n\times n}$ is a set of all matrices of size n.

Definition 1. A matrix $X_\sigma \in M_{n\times n}$ correspond to the permutation $\sigma \in S_n$ in the natural way if elements x_{ij} of this matrix hold following condition:

$$x_{ij} = \begin{cases} 1 & \text{for} \quad \sigma(i) = j \\ 0 & \text{for} \quad \sigma(i) \neq j \end{cases} \quad i, j \in \{1, 2, ..., n\}$$

Let $A \in M_{n\times n}$ be a matrix which elements are only 0 or 1.

Definition 2. Matrix $B \in M_{n\times n}$ obtain from a matrix A through changing an element 0 to α and 1 to β ($\alpha, \beta \in R$) is called a matrix (α, β)-associate with A. If we know α and β then we simply say that A and B are associate (and we write A *ass* B).

Let $\psi : S_n \to Per(2^n)$ is the same mapping which we construct before. Now with using Hamming's generalized matrix we proof association of matrices X_σ and A^σ.

Theorem 2. *Let $\sigma \in S_n$ and X_σ is a matrix which correspond to permutation σ in the natural way. Let $\psi(\sigma) = A^\sigma$. Then there exists matrix H of size $2^n \times n$ such that matrix $\Gamma := H^T A^\sigma H$ and X_σ are $(2^{n-2}, 2^{n-1})$-associate.*

Proof. Let $\sigma \in S_n$, $A^\sigma \in Per(2^n)$. We have $A^\sigma = [a_{ij}]$, $1 \leq i,j \leq 2^n$. Let $H \in M_{2^n \times n}$ is a generalized Hamming's matrix, that is $H = [h_{ij}]$, $1 \leq i \leq 2^n, 1 \leq j \leq n$ and $h_{i,1} \cdot 2^{n-1} + h_{i,2} \cdot 2^{n-2} + ... + h_{i,n} = i - 1$.

Moreover we put $H^T A^\sigma = [\omega_{i,j}]$, $1 \leq i \leq n, 1 \leq j \leq 2^n$. Because of construction of matrix A^σ we have, that $a_{ij} = 1$ if and only if

$$h_{i,\sigma^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma^{-1}(n)} = j - 1$$

From that condition we get $\omega_{\sigma^{-1}(i),j} = h_{ji}$ what is equivalent to

$$\omega_{ij} = h_{j,\sigma(i)} \tag{3}$$

Let $h_1, h_2, ..., h_n$ denote successive rows of matrix H^T, while $\omega_1, \omega_2, ..., \omega_n$ denote successive rows of matrix $H^T A^\sigma$. From (3) we get that $\omega_i = h_{\sigma(i)}$, $1 \leq i \leq n$.

Because the matrix H is a generalized Hamming's matrix and $A^\sigma \in Per(2^n)$ then the matrix $\Gamma := H^T A^\sigma H = [\gamma_{ij}]$ $1 \leq i,j \leq n$ is consist from elements in form $\gamma_{ij} = \alpha = 2^{n-2}$ or $\gamma_{ij} = \beta = 2^{n-1}$.

Let $i,j \in \{1,2,...,2^n\}$. If there exists $m \in \{1,2,...,2^n\}$ such that $\omega_{im} \neq h_{mj}$ then $\gamma_{ij} = \alpha$. If for all $m \in \{1,2,...,2^n\}$ we have $\omega_{im} = h_{mj}$ then $\gamma_{ij} = \beta$.

So the matrix Γ is in the form

$$\gamma_{ij} = \begin{cases} \alpha & j \neq \sigma(i) \\ \beta & j = \sigma(i) \end{cases}$$

for $1 \leq i,j \leq n$.

When we consider the mapping $0 \to \alpha, 1 \to \beta$ we see, that matrix Γ is $(2^{n-2}, 2^{n-1})$-associate with X_σ. □

It is easy to see that if matrix $A \in Per(2^n)$ and there in no permutation $\sigma \in S_n$ such that $\psi(\sigma) = A$ then matrix $\Gamma_1 := H^T A H$ where H is a generalized Hamming's matrix is not associate with any permutation matrix X of size n.

We can see that the mapping ψ and the matrix $\Gamma := H^T A^\sigma H$ create correspondence between S_n and $Per(2^n)$. Now we ask what we can say about this correspondence. A next theorem shows it's two properties.

Theorem 3. *Let n be a positive integer number. For any permutation $\sigma, \sigma_1, \sigma_2 \in S_n$ we have:*

a. $(A^\sigma)^T = A^{\sigma^{-1}} = (A^\sigma)^{-1}$;

b. $A^{\sigma_1 \sigma_2} = A^{\sigma_2} A^{\sigma_1}$.

Proof. a. We know, that $H^T A^\sigma H$ and X_σ are associate and

$$H^T(A^\sigma)^T H = (H^T A^\sigma H)^T \ ass \ X_\sigma^T = X_{\sigma^{-1}} \ ass \ H^T A^{\sigma^{-1}} H$$

So $(A^\sigma)^T = A^{\sigma^{-1}}$. We show, that$(A^\sigma)^T = (A^\sigma)^{-1}$. This equality is equivalent to $A^\sigma (A^\sigma)^T = E$.

Let

$$A^\sigma = [a_{ij}], \ a_{ij} = \begin{cases} 1 & h_i = j-1 \\ 0 & h_i \neq j-1 \end{cases}$$

where $h_i = h_{i,\sigma^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma^{-1}(n)}$. Moreover

$$(A^\sigma)^T = [b_{ij}], \ b_{ij} = \begin{cases} 1 & h'_i = j-1 \\ 0 & h'_i \neq j-1 \end{cases}$$

where $h'_i = h_{i,\sigma(1)} \cdot 2^{n-1} + h_{i,\sigma(2)} \cdot 2^{n-2} + ... + h_{i,\sigma(n)}$ (because of $(A^\sigma)^T = A^{\sigma^{-1}}$).

Let $A^\sigma (A^\sigma)^T = [c_{ij}]$ where $c_{ij} = \sum_{\alpha=1}^{2^n} a_{i\alpha} b_{\alpha j}$. We know, that $a_{ij} = b_{ji}$ so

$$c_{ij} = \sum_{\alpha=1}^{2^n} a_{i\alpha} b_{\alpha j} = \sum_{\alpha=1}^{2^n} a_{i\alpha} a_{j\alpha}$$

That sum is equal 1 iff $a_{i\alpha} = 1$ and $a_{j\alpha} = 1$. We have $a_{i\alpha} = 1$ so $h_{i,\sigma^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma^{-1}(n)} = \alpha - 1$ and $a_{j\alpha} = 1$. So $h_{j,\sigma^{-1}(1)} \cdot 2^{n-1} + h_{j,\sigma^{-1}(2)} \cdot 2^{n-2} + ... + h_{j,\sigma^{-1}(n)} = \alpha - 1$. From that two conditions we have $i = j$ so $c_{ij} = 1$ iff $i = j$.

b. To show, that $A^{\sigma_1 \sigma_2} = A^{\sigma_2} A^{\sigma_1}$ we put

$$A^{\sigma_1 \sigma_2} = [a_{ij}], a_{ij} = \begin{cases} 1 & h_i = j-1 \\ 0 & h_i \neq j-1 \end{cases}$$

where $h_i = h_{i,\sigma_2^{-1}\sigma_1^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma_2^{-1}\sigma_1^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma_2^{-1}\sigma_1^{-1}(n)}$. Moreover

$$A^{\sigma_2} = [b_{ij}], b_{ij} = \begin{cases} 1 & h'_i = j-1 \\ 0 & h'_i \neq j-1 \end{cases}$$

where $h'_i = h_{i,\sigma_2^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma_2^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma_2^{-1}(n)}$ and

$$A^{\sigma_1} = [c_{ij}], c_{ij} = \begin{cases} 1 & h''_i = j-1 \\ 0 & h''_i \neq j-1 \end{cases}$$

where $h''_i = h_{i,\sigma_1^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma_1^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma_1^{-1}(n)}$. Let $A^{\sigma_2} A^{\sigma_1} = [d_{ij}], d_{ij} = \sum_{\alpha=1}^{2^n} b_{i\alpha} c_{\alpha j}$. That sum can be reduce to only one component i.e. $d_{ij} = 1$ iff $b_{i\alpha} = 1$ and $c_{\alpha j} = 1$. Let $d_{ij} = 1$. Then

$$b_{i\alpha} = 1 \Rightarrow h'_i = h_{i,\sigma_2^{-1}(1)} \cdot 2^{n-1} + h_{i,\sigma_2^{-1}(2)} \cdot 2^{n-2} + ... + h_{i,\sigma_2^{-1}(n)} = \alpha - 1 \quad (4)$$

$$c_{\alpha j} = 1 \Rightarrow h''_i = h_{\alpha,\sigma_1^{-1}(1)} \cdot 2^{n-1} + h_{\alpha,\sigma_1^{-1}(2)} \cdot 2^{n-2} + ... + h_{\alpha,\sigma_1^{-1}(n)} = j - 1 \quad (5)$$

Moreover from definition of H we have

$$h_{\alpha,1} \cdot 2^{n-1} + h_{\alpha,2} \cdot 2^{n-2} + ... + h_{\alpha,n} = \alpha - 1 \quad (6)$$

From (4) and (6) $\sum_{k=1}^{2^n} h_{i,\sigma_2^{-1}(k)} \cdot 2^{n-k} = \sum_{k=1}^{2^n} h_{\alpha,k} \cdot 2^{n-k}$ so

$$h_{i,\sigma_2^{-1}(k)} = h_{\alpha,k}, \; 1 \le k \le n \quad (7)$$

From (5) and (7)

$$h_{\alpha,\sigma_1^{-1}(k)} = h_{i,\sigma_2^{-1}\sigma_1^{-1}(k)}, \; 1 \le k \le n \quad (8)$$

So from (5) and (8) we have, that

$$h_{\alpha,\sigma_1^{-1}(1)} \cdot 2^{n-1} + ... + h_{\alpha,\sigma_1^{-1}(n)} = h_{i,\sigma_2^{-1}\sigma_1^{-1}(1)} \cdot 2^{n-1} + ... + h_{i,\sigma_2^{-1}\sigma_1^{-1}(n)} = j - 1$$

so $a_{ij} = 1$ □

In that way we create a new language to describe symmetry groups of boolean functions which represent module M. Now when we have module M and boolean function f of M is given then we can create a group $S(f)$ in a following way: when we consider a boolean function $f : \{0,1\}^n \to \{0,1,...,k-1\}$ then in natural way we can construct a vector X_f of value of that function and a set $Stab_{Per(2^n)} X_f$. Then because of definition of mapping $\psi : S_n \to Per(2^n)$ the group $S(f)$ is equal to $\psi^{-1}(Stab_{Per(2^n)} X_f \cap \psi(S_n))$. From theorems 2 and 3 we have, that it is not necessary to know all matrices $\psi(\sigma)$ for all $\sigma \in S_n$ because we can consider only a matrices from $Stab_{Per(2^n)} X_f$ and then through the construction described in theorem 3 i.e. $\Gamma := H^T A^\sigma H$ we can create a group $S(f)$.

3. Application of matrix characterization to constructions of symmetry groups of boolean functions

In this section we construct a boolean function which represent direct sum and wreath product of symmetric groups.

Let (G,X) and (H,Y) are two permutation groups and $|X| = n$, $|Y| = m$. For $X \cap Y = \emptyset$ we construct a new group $(G \times H, X \cup Y)$. An action is given by the following condition:

$$z^{(g,h)} = \begin{cases} z^g & \text{if } z \in X \\ z^h & \text{if } z \in Y \end{cases}$$

where $z \in X \cup Y, g \in G, h \in H$. We say that permutation group $(G \times H, X \cup Y)$ is a direct sum of permutation groups (G,X) and (H,Y) and denote it as $G \oplus H$.

There are papers ([3], [7]) where direct sum of two permutation groups are considered. Although, it is interesting to construct exact boolean functions for some special kind of groups. Here we present construction of 2 valued boolean function which represent direct product of two symmetric groups.

Let n_1, n_2 are any positive integer numbers, $n_1 + n_2 = n$. We construct boolean function f in the following way:

$$X_f = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{2^{n_2}} \\ v_{2^{n_2}+1} \\ \vdots \\ v_i \\ \vdots \\ v_{2^n} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ v_i \\ \vdots \\ 1 \end{bmatrix} \tag{9}$$

where $v_i = 1$ iff $i = s \cdot 2^{n_2}$, $s = 1, 2, ..., 2^{n_1}$ and 0 otherwise, $i = 2^{n_2} + 1, ..., 2^n$.

Theorem 4. *For any positive integer n_1, n_2 the 2 valued boolean function f constructed in (9) hold the following condition*

$$S(f) = S_{n_1} \oplus S_{n_2}$$

Proof. Let n_1, n_2 are any positive integer numbers, $n_1 + n_2 = n$. We put $A_1 = \{1, 2, ..., n_1\}, A_2 = \{n_1 + 1, ..., n_1 + n_2\}$. Now we take a boolean function f defined in (9). Let's a vector X_f is a vector of value of that boolean function. Now we show that $S(f) = S_{n_1} \oplus S_{n_2}$. If $\sigma \in S_{n_1} \oplus S_{n_2}$ then obviously matrix $\psi(\sigma)$ preserve vector X_f so $\sigma \in S(f)$. This situation take places because permutation σ can be thought as a pair (ρ, τ) where ρ act inside block A_1 and τ act inside block A_2 so matrix $\psi(\sigma)$ preserve X_f.

We show that if there exist element $i \in A_2$ such that $\sigma(i) \notin A_2$ then $\sigma \notin S(f)$. So let there exists such element. We consider a boolean vector $\underline{x}$ in the form $0^{n_1}\underline{x}_2$ such that coordinate $x_i = 1$.

The element v in the vector X_f corresponds to $\underline{x}$ is equal 1. Under an action of matrix $\psi(\sigma)$ on the X_f this vector can be transform to the following elements: (a) v_{i_1} which corresponds to vector of type $1^{n_1}\underline{x}_2$; (b) v_{i_2} which corresponds to vector of type $\underline{x}_1 0^{n_2}$; (c) any element v_{i_3} where $i \neq s \cdot 2^{n_2}$, $s = 1, 2, ..., 2^{n_1}$. In situations (a),(b),(c) we have that

$$A^\sigma X_f \neq X_f$$

Moreover element v which corresponds to vector $\underline{x}$ can not be transform to element v' which correspond to the vector of type $\underline{x}_1 1^{n_2}$. So $S(f) = S_{n_1} \oplus S_{n_2}$. □

Another natural construction is wreath product of two permutation groups. Let (G, X) and (H, Y) are permutation groups where $|X| = n$, $|Y| = m$. We take a group $(G \times H, X \times Y)$. An action on the set $X \times Y$ is given by the rule

$$(x, y)^{(g_1,...,g_m;h)} = (x^{g_y}, y^h)$$

where $g_i \in G$, for $i = 1, 2, ..., m$,$h \in H$. We can see this action as an action on the set $A = \{1, 2, ..., nm\}$. This set is divided into sets $A_i = \{(i - 1)n + 1, ..., in\}$, for $i = 1, 2, ..., m$. Group G act inside A_i independently, H act on the indexes of A_i.

As before in [3] and [7] authors consider wreath product of two permutation groups, but we are interested in exact boolean function which represent this product. Here we present construction of 2 valued boolean function which represent wreath product of two symmetric groups.

Let's take

$$X_f = \begin{bmatrix} v_1 \\ \vdots \\ v_i \\ \vdots \\ v_{2^n} \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ v_i \\ \vdots \\ 1 \end{bmatrix} \tag{10}$$

where $v_i = 1$ iff vector $\underline{x}$ which corresponds to v_i is in the form $\underline{x}_1\underline{x}_2...\underline{x}_{n_2}$, $\underline{x}_i = 0^{n_1}$ or $\underline{x}_i = 1^{n_1}, i = 1, 2, ..., n_2$.

Theorem 5. *For any positive integer n_1, n_2 the 2 valued boolean function f constructed in (10) hold following condition*

$$S(f) = S_{n_1} \wr S_{n_2}$$

Proof. Let n_1, n_2 are any positive integer numbers, $n_1n_2 = n$. We put $A_1 = \{1, 2, ..., n_1\}, A_2 = \{n_1+1, ..., 2n_1\}, ..., A_{n_2} = \{(n_2-1)n_1+1, ..., n_1n_2\}$. Let's take a boolean function f defined in (10) and a vector X_f of value of that boolean function. Now we show that $S(f) = S_{n_1} \wr S_{n_2}$. It is easy to see that for every permutation $\sigma \in S_{n_1} \wr S_{n_2}$ we have $X_f = A^\sigma X_f$. From the other hand if $\sigma \notin S_{n_1} \wr S_{n_2}$ there exist positive integer i such that $\sigma(A_i^1) \neq A_j^1$, for $j = 1, 2, ..., n_2$. Without loose of generality we can assume that $i = 1$. Now we consider an element $v_k = 1$ which corresponds to the boolean vector $\underline{x} = 1^{n_1}0^{n_1}...0^{n_1}$. An action $A^\sigma X_f$ give us a new vector where element $v_k = 0$. This situation take place because operation A^σ change elements from different blocks, but not all block is changed by another block. We have

$$A^\sigma X_f \neq X_f$$

so $S(f) = S_{n_1} \wr S_{n_2}$ □

4. Final remarks

The results of this paper show that we can construct the matrix characterization of symmetry groups of boolean functions. In the section 2 we give some properties of this characterization. We show how we can create permutations from $S(f)$ when we have matrices which satisfy the equation $AX = X$ where X is a vector of value of function f. In the section 3 using linearization techniques we give a special construction of boolean functions which represent direct sum and wreath product of symmetric groups. Interesting question is to apply this characterization of symmetry groups of boolean functions to construct boolean functions which represent other well known permutation groups.

References

[1] N.L. Biggs, A.T. White *Permutation groups and combinatorial structures*, London Math. Soc., Lecture Notes Series 33, Cambridge Univ. Press. Cambridge, 1979.

[2] P. Cameron.: *Permutation Groups.*, Cambridge University Press, Cambridge , 1999.

[3] P. Clote, E. Kranakis, *Boolean function invariance groups, and parallel complexity.*, J. Comput., Vol. 20, No. 3, 1991, 553-590.

[4] P. Clote, E. Kranakis, *Boolean function and Computation Models* , Springer, Berlin , 2002

[5] M. Grech, A. Kisielewicz, *Direct product of automorphism groups of colored graphs*, Discrete Math., **283**, 2004, 81-86.

[6] M. Grech, *Regular symmetric groups of boolean function*, Discrete Math., **310**, 2010, 2877-2882.

[7] A. Kisielewicz, *Symmetry groups of Boolean functions and constructions of permutation groups*, Journal of Algebra., **199** , 1998, 379-403.

[8] W. Peisert, *Direct product and uniqueness of automorphism groups of graphs*, Discrete Math., **207**, 1999, 189-197.

[9] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1864.

[10] W. Xiao, *Linear symmetries of Boolean functions*, Discrete Applied Math., **149**, 2005, 192-199.

Contact information

P. Jasionowski
Institute of Applied Mathematics
Silesian University of Technology
ul. Kaszubska 23, 44-100 Gliwice, Poland
E-Mail: pawel.jasionowski@polsl.pl

Received by the editors: 27.02.2012
and in final form 25.04.2012.