European Journal of Combinatorics 40 (2014) 1–10

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Symmetry groups of boolean functions

Mariusz Grech, Andrzej Kisielewicz

University of Wrocław, Institute of Mathematics, pl. Grunwaldzki 2, 50-384 Wrocław, Poland

ARTICLE INFO

Article history:
Received 25 February 2013
Accepted 30 January 2014
Available online 21 February 2014

ABSTRACT

We prove that every abelian permutation group, but known exceptions, is the symmetry group of a boolean function. This solves the problem posed in the book by Clote and Kranakis. In fact, our result is proved for a larger class of permutation groups, namely, for all subgroups of direct sums of regular permutation groups.

1. Prerequisites

We consider finite permutation groups up to permutation isomorphism. Thus, generally, we assume that a permutation group G is a subgroup of the symmetric group S_n of the set $X = \{1, 2, \ldots, n\}$. If it is clear from the context that we speak of a permutation group we often omit the attribute "permutation". We adopt general terminology of permutation groups as given, for example, in [6,15]. Yet, the problem of representability of permutation groups we consider involves three approaches that have their own special notions and notations. We recall these in the corresponding subsections.

1.1. Boolean functions

For a permutation group $G \leq S_n$ we consider its natural action on the set $\{0, 1\}^n$ given by

$$x^\sigma = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

where $\sigma \in S_n$ and $x = (x_1, \ldots, x_n) \in \{0, 1\}^n$.

The *symmetry* (or *invariance*, or *automorphism*) *group* of a boolean function $f : \{0, 1\}^n \to \{0, 1\}$ is the group $G(f) \leq S_n$ defined as follows

$$G(f) = \{\sigma \in S_n : f(x^\sigma) = f(x)\}.$$

E-mail addresses: mariusz.grech@math.uni.wroc.pl (M. Grech), andrzej.kisielewicz@math.uni.wroc.pl (A. Kisielewicz).

http://dx.doi.org/10.1016/j.ejc.2014.01.011
0195-6698/

A permutation group $G \leq S_n$ is representable as the symmetry group of a boolean function, or in short, *representable*, if there exists a boolean function f such that $G = G(f)$.

Not all permutation groups are representable. For example, alternating groups A_n are not [2,10]. The problem of representability by the invariance groups of boolean functions was first considered by Clote and Kranakis [2] in connection with parallel complexity of formal languages and the upper bounds for complexity of boolean circuits (see [3], chapter 3). They established the representability conditions for cyclic groups and for maximal subgroups of S_n. In the book [3] they asked for similar results for abelian groups (Exercise 3.11.15 (Open Problem), p. 197).

They considered also the following generalization of boolean functions. By a *k-valued boolean function* we mean a map of the form $f : \{0, 1\}^n \to \{0, 1, \ldots, k-1\}$. The definition of the symmetry group $G(f)$ is the same as in the 2-valued case above. By $BGR(k)$ we denote the set of all permutation groups that are symmetry groups of k-valued boolean functions. Such functions are called *k-representable* (thus "representable" means "2-representable"). In [2], Clote and Kranakis has formulated a result implying that $BGR(k) = BGR(2)$ for any $k \geq 2$. Yet, the proof of this result turned out to be false. Kisielewicz [10] has observed that the group $K_4 \leq S_4$ generated by two permutations $(1, 2)(3, 4)$ and $(1, 3)(2, 4)$ (isomorphic abstractly to the Klein four-group) is in $BGR(3)$, but not in $BGR(2)$. No other counterexample of this kind has been found so far. On the other hand, there are some results confirming the conjecture by Clote and Kranakis. Since we apply these results in the sequel, we recall them in a precise form.

By $C_n \leq S_n$ we denote the permutation group generated by the cycle $\sigma = (1, 2, \ldots, n)$. It is not difficult to check (see [2,10]) that $C_i \in BGR(2)$ for $i \neq 3, 4, 5$, while $C_3, C_4, C_5 \notin BGR(k)$ for any $k \geq 2$. The problem of representability of arbitrary cyclic permutations groups (i.e., those generated by a single permutation) has been solved in [2]:

Theorem 1.1 (*Clote, Kranakis [2]*)**.** *If $G \leq S_n$ is a permutation group generated by a single permutation σ, then either $G \in BGR(2)$ or $G \notin BGR(k)$ for any $k \geq 2$. Moreover, if σ is a product of k disjoint cycles of length $l_1, l_2, \ldots, l_k \geq 2$, respectively, then $G \in BGR(2)$ if and only if for all $s = 3, 4, 5$ and $i \leq k$ the equality $l_i = s$ implies that there is $j \neq i$ such that $\gcd(l_i, l_j) \neq 1$.*

1.2. Relation groups

A closely connected topic is research on defining permutation groups by relations, and especially that concerning unordered relations (see [4,5,14] and the references given therein). An *unordered relation* $\mathbf{R}$ is simply a set of subsets of a given set X. We consider the natural action of the symmetric group $S(X)$ of X on the subsets of X, and given a subset $S \subseteq X$ and a permutation $\sigma \in S(X)$, we denote by S^σ the image of the set S under σ. Then, $G(\mathbf{R})$ is defined as the subgroup of $S(X)$ consisting of those permutations σ which leave $\mathbf{R}$ invariant, that is, $S^\sigma \in \mathbf{R}$ for all $S \in \mathbf{R}$. Such permutation groups are called *relation groups* (cf. [15]).

There is a natural one-to-one correspondence between unordered relations and boolean functions. Given a subset S of an n-element set X by x_S we denote the n-tuple corresponding to the characteristic function of S (under a fixed linear ordering of elements of X). Then the function given by

$$f(x_S) = \begin{cases} 1, & \text{if } S \in \mathbf{R} \\ 0, & \text{otherwise,} \end{cases}$$

is a boolean function on $\{0, 1\}^n$ (determining the relation $\mathbf{R}$). In particular, a group G is representable if and only if $G = G(\mathbf{R})$ for some unordered relation $\mathbf{R}$ (i.e., G is a relation group).

In [4,5], Dalla Volta and Siemons have used results on regular sets in permutation groups to obtain further results on representability. For a permutation group G on a set X a set $S \subseteq X$ is called *regular in G* if for all $\sigma \in G$, $S^\sigma = S$ implies $\sigma = 1$. In [5] it is proved that if a permutation group $H = G(\mathbf{R})$ and H has a regular set S such that there is no set of cardinality $|S|$ in $\mathbf{R}$, then *every* subgroup of H is representable. In particular, it is proved that if G is a subgroup of a primitive group other than A_n and S_n, then with a few possible exceptions, G is representable.

For a broader context of problems of representability of permutation groups we refer the reader to [1,11,15].