BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 78–82
ISSN 1024–7696

Doubly transitive sets of even permutations

Gábor P. Nagy

Abstract. In this paper we investigate doubly transitive sets of permutations which consist of even permutations.

Mathematics subject classification: 20N05, 51E05.
Keywords and phrases: Sharply transitive set, finite projective plane, alternating group.

Dedicated to the 90th anniversary of Prof. V. D. Belousov

1 Introduction

Let S be a set of permutations of some fixed set Ω of n symbols. We say that S is *sharply t–transitive* if for any two tuples $(x_1, \ldots, x_t)$, $(y_1, \ldots, y_t)$ of distinct symbols, there is a unique element $s \in S$ with $x_1^s = y_1, \ldots, x_t^s = y_t$. It is well known that sharply 1– and 2–transitive sets of permutations correspond to Latin squares and affine planes, respectively, cf.[3]. One of the main motivation for the study of finite sharply 2–transitive sets is the famous Prime Power Conjecture for projective planes. (Both parts of the PPC are *folklore,* and it is surprisingly hard to find them in printed literature. The second part of the PPC is mentioned in [4, p. 276].)

Problem 1. (Prime Power Conjecture (PPC) for projective planes)

(1) *Finite projective planes have prime power order.*

(2) *Finite projective planes of prime order are desarguesian.*

The classical construction of a sharply 2–transitive set is the group

$$AGL(1, F) = \{x \mapsto ax + b \mid a \in F^*, b \in F\}$$

of affine linear transformations of the field F. The corresponding projective plane is the desarguesian plane $PG(2, F)$ over F. A wider class of sharply 2–transitive sets is based on the concept of *quasifields.* The set Q endowed with two binary operations $+, \cdot$ is called a (right) quasifield if

(Q1) $(Q, +)$ is an abelian group with neutral element $0 \in Q$,

(Q2) any two of the elements $x, y, z \in Q \setminus \{0\}$ determine the third when $x \cdot y = z$,

Research supported by OTKA Grant No. NN.114614.

(Q3) the right distributive law $(x+y)z = xz + yz$ holds, and,

(Q4) for each $a, b, c \in Q$ with $a \neq b$, there is a unique $x \in Q$ satisfying $xa = xb + c$.

The connection between affine and projective planes and their coordinatizing algebraic structures as plenary ternary rings and mutually orthogonal latin squares are given in [2, Chapter VIII], [4, Chapter 8]. One finds details on the concept of quasifields and translation planes in [4, Section 8.4], and, using the language of sharply transitive sets in [7, 12]. Notice that for the structures considered in [1], two-sided distributivity is assumed; such objects are now called *nearfields.*

It is immediate to show that for a quasifield Q, the set

$$\Lambda(Q) = \{v \mapsto u \cdot v + w \mid u \in H^*, w \in H\}$$

of $Q \to Q$ maps forms a sharply 2–transitive set on Q.

Let $\Omega^{(t)}$ denote the set of t–tuples of distinct symbols of Ω. The permutation group $G \leq \mathrm{Sym}(\Omega)$ has a natural action on $\Omega^{(t)}$, let $G^{(t)}$ denote the corresponding permutation group. It is immediate that the existence of a sharply t–transitive set in G is equivalent with the existence of a sharply 1–transitive set in $G^{(t)}$. In the 1970's, P. Lorimer started the systematic investigation of the question of existence of sharply 2–transitive sets in finite 2–transitive permutation groups. This program was continued by Th. Grundhöfer, M. E. O'Nan, P. Müller, see [6] and the references therein. Some of the 2–transitive permutation groups needed rather elaborated methods from character theory in order to show that they do not contain sharply 2–transitive sets of permutations.

In the paper [10], the authors presented a combinatorial method to show that a given permutation group cannot contain sharply 1–transitive sets. An important implication of this method was the following

Proposition 1 ([10, Theorem 3])**.** *If $n \equiv 2, 3 \pmod 4$ then the alternating group A_n does not contain a sharply 2–transitive set of permutations.*

Recently, Gyula Károlyi [9] asked the question concerning the existence of a sharply 2–transitive set of A_n in the remaining cases, that is, when $n \equiv 0, 1 \pmod 4$. The main result of this paper gives a partial answer to this problem. In particular, we show that for infinitely many integers $n \equiv 0, 1 \pmod 4$, A_n does contain a sharply 2–transitive set.

Theorem 1. *(1) If $n = 2^m$ with $m \geq 2$, or $n = p^{2m}$ with odd prime p, then A_n contains a sharply 2–transitive set of permutations.*

(2) Let p be an odd prime, $n = p^{2m+1}$. If A_n contains a sharply 2–transitive set of permutations, then $p \equiv 1 \pmod 4$ and the corresponding projective plane is nondesarguesian.

The formulation of the theorem shows that no attempts are made to attack the Prime Power Conjecture. We notice that the existence of a sharply 2–transitive set in A_p with a prime p would deliver a nondesarguesian plane of prime order, hence a counterexample to part (b) of Problem 1.

2 Proof of the theorem

In this section, $\mathrm{Alt}(X)$ denotes the group of even permutations of the finite set X. Furthermore, H^* denotes the set of nonzero elements of the quasifield H.

Lemma 1. *Let $q = p^m$ be a prime power. $AGL(1,q) \le A_q$ if and only if $p = 2$ and $m \ge 2$.*

Proof. Clearly, the only nontrivial element of $AGL(1,2)$ is the transposition $(0,1)$ which is odd. Let us assume $q > 2$. Let g be a primitive element in $\mathbb{F}_q$. $AGL(1,q)$ is generated by an elementary abelian p–group N of order q and the permutation $\gamma : x \mapsto gx$. While the elements of N consist of q/p cycles of length p, the permutation γ acts on $\mathbb{F}_q^*$ as a cycle of length $q-1$. Hence, $N \le A_q$ and $\gamma \in A_q$ if and only if $2 \mid q-1$. $\square$

We recall the construction of Hall quasifields from [8, Section IX.2.]. Let F be a field and $f(s) = s^2 - as - b$ an irreducible polynomial over F. Let H be the two-dimensional right vector space over F, with basis elements 1 and λ so that H consists of all elements of the form $x + \lambda y$ as x and y vary over F. The multiplication on H is defined by

$$x \circ (z + \lambda t) = xz + \lambda(xt) \tag{1}$$

and

$$(x + \lambda y) \circ (z + \lambda t) = xz - y^{-1} t f(x) + \lambda(yz - xt + at) \tag{2}$$

for $y \ne 0$. As the right hand sides of (1) and (2) are linear in z, t, one can write the left translation maps $L_u : v \mapsto uv$ in the F-basis $\{1, \lambda\}$ as matrices:

$$L_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, \qquad L_{x+\lambda y} = \begin{pmatrix} x & -y^{-1} f(x) \\ y & -x + a \end{pmatrix}.$$

The determinants are $\det(L_x) = x^2$ and $\det(L_{x+\lambda y}) = -b$.

Lemma 2. *Let p be an odd prime, $r = p^m$, and $\varepsilon \in \mathbb{F}_r$ a nonsquare. Define the Hall quasifield $H = (H, +, \circ)$ with irreducible polynomial $f(s) = s^2 - as - b$, where*

$$a = \frac{\varepsilon + 1}{2}, \qquad b = -\left(\frac{\varepsilon - 1}{4}\right)^2.$$

Then the set

$$\Lambda(H) = \{v \mapsto u \circ v + w \mid u \in H^*, w \in H\}$$

of $H \to H$ maps forms a sharply 2–transitive set in $\mathrm{Alt}(H)$.

Proof. Since the discriminant of f is $a^2 + 4b = \varepsilon$ and is a non-square, the polynomial f is irreducible. Hence, the Hall quasifields is well defined and $\Lambda(H)$ is a sharply 2–transitive set of permutations. Each element of $\Lambda(H)$ is the composition of a translation $v \mapsto v + w$ and an H-multiplication L_u. Since the former is an even permutation, it suffices to show that the H-multiplication L_u is in $\mathrm{Alt}(H^*)$. By the choice of the parameters, all H-multiplications are contained in the subgroup

$$S = \{A \in GL(2,r) \mid \det(A) \text{ is a square in } \mathbb{F}_r\}$$

of index 2 of $GL(2,r)$. Since $GL(2,r)/GL(2,r)'$ is cyclic, $GL(2,r)$ has a unique subgroup of index 2. As the subgroup $GL(2,r) \cap \mathrm{Alt}(H^*)$ has index at most 2 in $GL(2,q)$, it must contain S. This proves the lemma. $\square$

Lemma 2 implies the first part, while Lemma 1 and Proposition 1 imply the second part of Theorem 1.

We finish the paper with a

Conjecture 1. *Let $p \equiv 1 \pmod 4$ be a prime and m a positive integer. The linear group*

$$S = \{A \in GL(2m+1,p) \mid \det(A) \textit{ is a square in } \mathbb{F}_p\}$$

does not contain sharply transitive sets.

Using the command `OneLoopTableInGroup` of the LOOPS package [11] of the computer algebra system GAP4 [5], the conjecture can be verified for $p = 5$, $m = 1$.

References

[1] Belousov V. D. *On the definition of the concept of a quasi-field.* Bul. Akad. Stiince RSS Moldoven., 1964, **6**, 3–10.

[2] Belousov V. D. *Algebraic nets and quasigroups.* Kishinev, Ştiinţa, 1971 (in Russian).

[3] Dembowski P. *Finite geometries.* Ser. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Berlin, Springer-Verlag, 1968.

[4] Dénes J., Keedwell A. D. *Latin squares and their applications.* Academic Press, New York–London, 1974.

[5] *GAP – Groups, Algorithms, and Programming, Version 4.7.9*, (http://www. gap-system.org), The GAP Group, 2015.

[6] Grundhöfer T., Müller P. *Sharply 2-transitive sets of permutations and groups of affine projectivities.* Beiträge zur Algebra und Geometrie. Contributions to Algebra and Geometry, 2009, **50**, No. 1, 143–154.

[7] Hall M. *Projective planes.* Trans. Amer. Math. Soc., 1943, **54**, 229–277.

[8] Hughes D. R., Piper F. C. *Projective planes.* New York, Springer-Verlag, 1973, Graduate Texts in Mathematics, Vol. 6.

[9] Károlyi G. Private communication, 2015.

[10] Müller P., Nagy G. P. *On the non-existence of sharply transitive sets of permutations in certain finite permutation groups.* Advances in Mathematics of Communications, 2011, **5**, No. 2, 303–308.

[11] Nagy G. P., Vojtechovsky P. *LOOPS, computing with quasigroups and loops in GAP, Version 3.1.0* (http://www.math.du.edu/loops). Refereed GAP package, 2015.

[12] Nagy G. P. *Semifields in loop theory and in finite geometry.* Quasigroups and Related Systems, 2011, **1 9**, No. 1, 109–122.

Gábor P. Nagy
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged, Hungary

MTA-ELTE Geometric and Algebraic Combinatorics
Research Group
Pázmány P. sétány 1/c
H-1117 Budapest, Hungary

E-mail: *nagyg@math.u-szeged.hu*

Received January 12, 2016