Journal of Algebraic Combinatorics 4 (1995), 99–102
© 1995 Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

The Uniformly 3-Homogeneous Subsets of $PGL(2, q)$

JÜRGEN BIERBRAUER
Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931

Received July 13, 1992; Revised May 16, 1994

Abstract. We use the character-table of PGL$(2, q)$ to determine the subsets of that group acting uniformly 3-homogeneously on the projective line.

Keywords: authentication, secrecy, permutation, group, character-table, perpendicular array

1 Introduction

A set S of permutations on n letters is *μ-uniformly t-homogeneous* if for every pair A, B of unordered t-subsets, the same number $\mu \neq 0$ of permutations in S carry A into B. If the parameter $\mu \neq 0$ is not specified, we speak of a uniformly t-homogeneous set of permutations. The set S is also called an $APA_\mu(t, n, n)$, where "APA" stands for "authentication perpendicular array." This stems from an application in the cryptographical theory of unconditional secrecy and authentication (see [1, 2, 8]). In this paper we determine completely the subsets of PGL$(2, q)$, which are uniformly 3-homogeneous on the projective line.

Theorem 1 *The S be a uniformly 3-homogeneous proper subset of the group $PGL(2, q)$, $q \geq 4$. Then one of the following holds:*

(i) $S = PSL(2, q)$ *or* $S = PGL(2, q) - PSL(2, q)$, $q \equiv 3 (\mathrm{mod}\ 4)$.
(ii) $q \in \{5, 7, 8\}$, *S is 3-uniformly 3-homogeneous.*

The proof is based on properties of the characters of PGL$(2, q)$ and will be given in Section 2. It is essentially a corollary of the following:

Theorem 2 *Let ρ be the permutation character of PGL$(2, q)$ on unordered 3-subsets of the projective line, where $q > 8$. Then the following holds:*
If $q \not\equiv 3 (\mathrm{mod}\ 4)$, then every irreducible character of PGL$(2, q)$ is a constituent of ρ.
If $q \equiv 3 (\mathrm{mod}\ 4)$, then sgn *(where* $\mathrm{sgn}(g) = 1$ *if* $g \in PSL(2, q)$, $\mathrm{sgn}(g) = -1$ *otherwise) is the only irreducible character which is not a constituent of ρ.*

It is well-known and easily checked that PSL$(2, q)$ is a uniformly 3-homogeneous proper subgroup of PGL$(2, q)$ if and only if $q \equiv 3 (\mathrm{mod}\ 4)$. This explains Theorem 1, (i). It also shows that the case $q = 7$ of Theorem 1 is not very interesting. The exceptional cases $q = 5$ and $q = 9$ deserve attention: In [1] a 3-uniformly 3-homogeneous subset of $PGL(2, 8)$ has been constructed. It was shown that this leads to the construction of authentication perpendicular arrays

$$APA_3(3, 9, 8^f + 1), f \geq 1,$$

and to cryptocodes achieving perfect 3-fold secrecy, which are also 2-fold secure against spoofing . The situation in case $q = 5$ is quite interesting:

Theorem 3

(i) *Let F be a subgroup of order* 5 *of* $PSL(2, 5)$. *Then* $PSL(2, 5)$ *contains a* 2*-uniformly* 2*-homogeneous subset* S_0 (*an* $APA_2(2, 6, 6)$), *which is the union of two double cosets of F* (*see* [1, *Theorem* 12]).
(ii) *Let* $g \in PGL(2, 5) - PSL(2, 5)$. *Then* $S = S_0 \cup S_0 g$ *is* 3*-uniformly* 3*-homogeneous* (*an* $APA_3(3, 6, 6)$).

Proof: (i) was proved in [1]. The group PGL(2, 5) is transitive on the 3-subsets of the projective line, but PSL(2, 5) has two orbits, each of length 10. It is easily checked, that the number of permutations from S_0 mapping the 3-set A onto the 3-set B is exactly 3 if A and B are in the same PSL(2, 5)-orbit (the number is of course 0 otherwise). As g maps the two PSL(2, 5)-orbits on 3-sets onto each other, (ii) follows. □

An $APA_3(3, 6, 6)$ has already been constructed in [6]. The author wants to thank G. Hiß for a number of helpful discussions.

2 Proof of Theorems 1 and 2

Let $G = \mathrm{PGL}(2, q)$, $D^{(3)}$ the complex permutation representation of G on unordered 3-subsets of the projective line, and V the complex vector-space of elements $f = \sum_{g \in G} a_g g \in [G]$ satisfying

$$(*) \qquad D(f) = 0 \text{ for every irreducible non-principal constituent } D \text{ of } D^{(3)}.$$

Let $S \subset G$ and $\overline{S} = \sum_{g \in G} g$ the corresponding element in $\mathbb{Z}[G]$. It has been shown in [1] that S is uniformly 3-homogeneous if and only if $\overline{S} \in V$. It follows from the Schur relations ([5, p. 32]) that

$$\dim(V) = |G| - \sum \deg(D)^2,$$

where D runs through the similarity classes of non-principal irreducible constituents of $D^{(3)}$.

Let $q > 8$ and assume Theorem 2 is proved. As the sign-character is linear, we get

$$\dim(V) = \begin{cases} 1 & \text{if } q \not\equiv 3(\text{mod } 4), q > 8, \\ 2 & \text{if } q \equiv 3(\text{mod } 4), q > 8. \end{cases}$$

If $\dim(V) = 1$, then G is the only subset S of G satisfying $\overline{S} \in V$. In case $q \equiv 3(\text{mod } 4), q > 8$ a basis of V is given by $\overline{\mathrm{PSL}(2, q)}$ and $\overline{G - \mathrm{PSL}(2, q)}$. Thus Theorem 2 implies Theorem 1 if $q > 8$. We turn to the proof of Theorem 2. For the convenience of the reader, we reproduce the character-table of PGL(2, q). Let α and β be primitive $(q-1)^{\text{st}}$ and $(q+1)^{\text{st}}$ roots of unity, a and b elements of orders $(q-1)$ and $(q+1)$, respectively. In case $q = 2^f$, G has $q+1$ conjugacy-classes with representatives $1, z, a^r, b^s (r = 1, 2, \ldots, (q-2)/2, s = 1, 2, \ldots, q/2)$, where z is an involution.

Table 1. The character table of $SL(2, 2^f)$.

	1	z	a^r	b^s
1	1	1	1	1
St	q	0	1	-1
χ_i	$q+1$	1	$\alpha^{ir}+\alpha^{-ir}$	0
Θ_j	$q-1$	-1	0	$-(\beta^{js}+\beta^{-js})$

Here $i = 1, 2, \ldots, (q-2)/2$; $j = 1, 2, \ldots, q/2$.

This can be found in [4].

For q odd, the character table of PGL$(2, q)$ is not as easy to be found in the literature. Steinberg's paper [7] is not correct. The easiest way is to use Deligne-Lusztig theory, even in this smallest of all cases.

PGL$(2, q)$, q odd, has $q + 2$ conjugacy classes with representatives $1, u, a^r, b^s, z_-, z_+$ $(r = 1, 2, .., (q-3)/2,\ s = 1, 2, .., (q-1)/2)$, where u is unipotent of order p, $z_- = a^{(q-1)/2}$, $z_+ = b^{(q+1)/2}$ are involutions. We have

$$|C_G(u)| = q, |C_G(a^r)| = q - 1, |C_G(b^s)| = q + 1,$$
$$|C_G(z_-)| = 2(q-1), |C_G(z_+)| = 2(q+1).$$

Table 2. The character table of PGL$(2, q)$, q odd.

	1	u	a^r	z_-	b^s	z_+
1	1	1	1	1	1	1
sgn	1	1	$(-1)^r$	$(-1)^{(q-1)/2}$	$(-1)^s$	$(-1)^{(q+1)/2}$
St	q	0	1	1	-1	-1
sgn $\cdot$ St	q	0	$(-1)^r$	$(-1)^{(q-1)/2}$	$(-1)^{s+1}$	$(-1)^{(q-1)/2}$
χ_i	$q+1$	1	$\alpha^{ir}+\alpha^{-ir}$	$2(-1)^i$	0	0
Θ_j	$q-1$	-1	0	0	$-(\beta^{js}+\beta^{-js})$	$2(-1)^{j+1}$

Here $r, i = 1, 2, .., (q-3)/2$; $s, j = 1, 2, .., (q-1)/2$. Thus χ_i are the characters $R_{T,\Theta}$, where T is the maximal split torus and Θ is in general position, $\Theta_j = -R_{T,\Theta}$, where T is the unique maximal non-split torus and Θ is in general position (see [3]). Let ρ be the character of $D^{(3)}$, $H \cong S_3$, and χ an irreducible character of G. It is clear, by Frobenius reciprocity, that χ is a constituent of ρ if and only

$$\sum_{h \in H} \chi(h) \neq 0.$$

It is now a trivial task to check that Theorem 2, and with it Theorem 1 for $q > 8$, are true. The exceptional cases $q = 5$ and $q = 8$ have been dealt with in the introduction. Only the case PGL(2, 7) remains to be considered. We know that PSL(2, 7) is 3-uniformly 3-homogeneous. Consider the character table of PGL(2, 7). It follows from case 6 above that sgn and χ_1 are the only irreducible characters of PGL(2, 7) which are not constituents of ρ. Let S be a μ-uniformly 3-homogeneous subset of PGL(2, 7). We want to show $\mu \geq 3$.

We can and will assume $1 \in S$. Let $a_7, a_6, a_3, a_{2-}, a_{8A}, a_4, a_{8B}, a_{2+}$ be the numbers of elements in S which belong to the conjugacy-classes of $u, a, a^2, z_-, b, b^2, b^3, z_+$, respectively. Property (*) implies in particular

$$\sum_{g \in G} \chi(g) = 0,$$

where χ is the character of an irreducible constituent $D \neq 1$ of $D^{(3)}$. Thus each non-principal constituent of $D^{(3)}$ yields a linear equation for the above parameters:

$$a_7 = 6 + 2a_4 - 2a_{2+} \qquad (\Theta_2)$$

$$a_{8A} = a_{8B}, \quad a_7 = 6 + 2a_{2+} \qquad (\Theta_3)$$

It follows $a_4 = 2a_{2+}$.

$$a_3 = 3a_{2+} - 7 \qquad (St) + (\text{sgn} \cdot St)$$

In conjunction with (χ_2) this shows

$$a_6 = 21 - a_{2+} + 2a_{2-}$$

$(St) - (\text{sgn} \cdot St)$ yields then

$$a_8 = 21 - a_{2+} + 2a_{2-}.$$

Thus all the parameters are expressed in terms of a_{2+} and a_{2-}. Summing up we get

$$\begin{aligned} |S| = \mu\binom{8}{3} = 56\mu &= 1 + a_7 + a_6 + a_3 + a_{2-} + a_{8A} + a_4 + a_{8B} + a_{2+} \\ &= 42 + 6a_{2+} + 6a_{2-}. \end{aligned}$$

It follows $\mu \equiv 0 (\text{mod } 3)$ and we are done.

References

1. J. Bierbrauer and Tran van Trung, "Some highly symmetric authentication perpendicular arrays," *Designs, Codes and Cryptography* **1** (1992), 307–319.
2. J. Bierbrauer, Tran van Trung, "Halving $PGL(2, 2^f)$, f odd: a series of cryptocodes," *Designs, Codes and Cryptography* **1** (1991), 141–148.
3. Roger W. Carter, *Finite groups of Lie type,* Wiley, 1985.
4. L. Dornhoff, *Group representation theory,* Dekker, New York, 1971.
5. I. Martin Isaacs, *Character theory of finite groups,* Academic Press, 1976.
6. E.S. Kramer, D. L. Kreher, R. Rees, and D.R Stinson, "On perpendicular arrays with $t \geq 3$," *Ars Combinatoria* **28** (1989), 215–223.
7. N. Steinberg, "The representations of $GL(3, q)$, $GL(4, q)$, $PGL(3, q)$, and $PGL(4, q)$," *Canadian Journal of Mathematics* **3** (1951), 225–235.
8. D.R. Stinson, "The combinatorics of authentication and secrecy codes," *Journal of Cryptology* **2** (1990), 23–49.