Halving $PSL(2, q)$

Jürgen Bierbrauer and Yves Edel

We show that $PSL_2(q)$, $q \not\equiv 3(mod\, 4)$, contains a subset of half the cardinality of $PSL_2(q)$ which is uniformly 2-homogeneous on the projective line.

1 Introduction

The group $PSL_2(q)$ is 2-transitive, in particular 2-homogeneous on the $q+1$ points of the projective line $\mathcal{P}_1(q)$. A set $\mathcal{S}$ of permutations will be called $\mu-$**uniformly** 2-**homogeneous** if for any unordered pairs A, B of the letters, exactly μ permutations in $\mathcal{S}$ map A onto B. If the number $\mu \neq 0$ is not specified, we speak of a uniformly 2-homogeneous set of permutations. We are interested in the question, when there is a subset $\mathcal{S} \subset PSL_2(q)$ of cardinality $|\mathcal{S}| = |PSL_2(q)|/2$, which is uniformly 2-homogeneous on the projective line. If q is odd, then $\mu = (q-1)/2$, if q is even, then $\mu = q-1$.

Theorem 1 *$PSL_2(q)$ contains a subset $\mathcal{S}$ of cardinality $|\mathcal{S}| = |PSL_2(q)|/2$, which is uniformly 2-homogeneous on the projective line, if and only if $q \not\equiv 3(mod\, 4)$.*

If $q \equiv 3(mod\, 4)$, then $\mu = (q-1)/2$ would be an odd number. This contradicts [2],Lemma 2. In case $q \equiv 1(mod\ 4)$ we construct a $(q-1)/2-$uniformly 2-homogeneous subset $\mathcal{S} \subset PSL_2(q)$. More precisely we prove the following:

Theorem 2 *Let $G = PSL_2(q)$, $q \equiv 1(mod\ 4)$, $i \in \mathbb{F}_q$ such that $i^2 = -1$, $U = \{\tau \longrightarrow \tau + \gamma \mid \gamma \in \mathbb{F}_q\}$, F a cyclic subgroup of order $(q+1)/2$ such that ∞ and 0 are in different orbits under F. Then the following hold:*

- *Let* $t_\alpha = (\tau \longrightarrow \alpha^2\tau)$, *and* $w_\alpha = (\tau \longrightarrow \frac{1}{\alpha^2\tau})$. *Let* $R \subset \mathbb{F}_q^*$ *such that*

  $$\alpha \in R \Longleftrightarrow -\alpha \notin R$$

  Then t_α, $\alpha \in R$ *and* w_α, $\alpha \in R$ *together form a set of representatives of the double cosets for* F *and* U.

- *Choose a subset* X *of these representatives such that*

  $$t_\alpha \in X \iff t_{i\alpha} \notin X,$$

  $$w_\alpha \in X \iff w_{i\alpha} \notin X.$$

  Set $\mathcal{S} = \cup_{x\in X} FxU$. *Then* $\mathcal{S}$ *is* $(q-1)/2-$*uniformly* 2*-homogeneous on the projective line.*

It was shown in [1] that $PSL_2(2^f)$, f odd, may be halved in the sense of Theorem 1: If ϕ is the Frobenius automorphism of $\mathbb{F}_q$ and σ_0 is an involution in $PSL_2(2^f)$, which commutes with ϕ, then the set of commutators

$$\mathcal{S} = \{[\sigma_0\phi, g] \mid g \in PSL_2(2^f)\}$$

is (2^f-1)-uniformly 2-homogeneous (f odd).

We show here that $PSL_2(2^f)$ may be halved in the sense of Theorem 1. Our proof works for all f.

Theorem 3 *Let* $G = PSL_2(q)$, $q = 2^f$, $F = <\rho>$ *a cyclic subgroup of order* $q+1$, *where the generator* ρ *is chosen such that* $\rho : 0 \longrightarrow \infty \longrightarrow 1$, $T = \{m_\lambda \mid \lambda \in \mathbb{F}_q^*\} \cong Z_{q-1}$, *where* $m_\lambda = (\tau \longrightarrow \lambda\cdot\tau)$. *Then the following hold:*

- *The elements* $u_\gamma = (\tau \longrightarrow \tau+\gamma)$ *are representatives of the double cosets for* T *and* F, *i.e.*

  $$G = \cup_{\gamma\in F_q} Tu_\gamma F$$

- *Choose a subset* X *of these representatives such that*

  $$u_\gamma \in X \iff u_{\gamma+1} \notin X.$$

  Set $\mathcal{S} = \cup_{x\in X} TxF$. *Then* $\mathcal{S}$ *is* $(q-1)$*-uniformly* 2*-homogeneous on the projective line.*

Observe that the proof of [1],Lemma 2.1 is valid for all $q = 2^f$. This shows that $PSL_2(2^f)$ does not contain a uniformly 2-homogeneous subset with less than $|PSL_2(2^f)|/2$ elements.

2 Proof of the Theorems

2.1 Proof of Theorem 2

We use the notation introduced in the statement of the Theorem. Operation on the projective line will be written from the right. The generic element of the unipotent group U is $(\tau \longrightarrow \tau+\gamma)$. Because of the double transitivity of G the group F may be chosen as in the statement of Theorem 2. Recall that the non-split torus F (in other words the cyclic subgroup F of order $(q+1)/2$) acts semi-regularly. Observe $t_\alpha^{-1} = t_{1/\alpha}$, $w_\alpha^{-1} = w_\alpha$. Assume $t_\beta \in Ft_\alpha U$, equivalently $t_\alpha U t_\beta^{-1} \cap F \neq \emptyset$, or

$$\tau \longrightarrow \frac{1}{\beta^2}(\alpha^2\tau + \gamma) \in F$$

for some $\gamma \in \mathbb{F}_q$. As ∞ is fixed and F acts semi-regularly, we conclude that $\gamma = 0$, $\beta = \pm\alpha$. Assume $w_\beta \in Fw_\alpha U$; equivalently $w_\alpha U w_\beta \cap F \neq \emptyset$, or

$$\tau \longrightarrow \frac{\alpha^2\tau}{\beta^2(1+\alpha^2\gamma\tau)} \in F$$

for some $\gamma \in \mathbb{F}_q$. As 0 is fixed and F acts semi-regularly, we conclude $\gamma = 0$, $\beta = \pm\alpha$. Let $\mathcal{A}_\alpha = Ft_\alpha U$, $\mathcal{B}_\alpha = Fw_\alpha U$. We have seen that the $\mathcal{A}_\alpha$ and $\mathcal{B}_\alpha$ each form $(q-1)/2$ different double cosets. Assume $w_\beta \in Ft_\alpha U$, equivalently $t_\alpha U w_\beta \cap F \neq \emptyset$, or

$$\tau \longrightarrow \frac{1}{\beta^2(\alpha^2\tau + \gamma)} \in F$$

for some $\gamma \in \mathbb{F}_q$. As this element maps ∞ onto 0, we get a contradiction. The first statement of Theorem 2 is proved. Let unordered pairs A and B of elements of the projective line be given, let T be the set of $q-1$ elements of G mapping A onto B. We shall show that for every $\alpha \in \mathbb{F}_q$ there is a bijection between $T \cap \mathcal{A}_\alpha$ and $T \cap \mathcal{A}_{i\alpha}$ and likewise a bijection between $T \cap \mathcal{B}_\alpha$ and $T \cap \mathcal{B}_{i\alpha}$. We have to distinguish several cases:

1. $A = \{\infty, b\}$, $B = \{\infty, d\}$. There is exactly one element in $\mathcal{A}_\alpha$ (and exactly one in $\mathcal{A}_{i\alpha}$) mapping $\infty \longrightarrow \infty$, $b \longrightarrow d$, and likewise there is exactly one element in each of the double cosets of type $\mathcal{A}$ mapping $b \longrightarrow \infty \longrightarrow d$. Consider the double cosets of type $\mathcal{B}$. No element in a double coset of type $\mathcal{B}$ can fix ∞, as otherwise we would have an element of F mapping $\infty \longrightarrow 0$. Which elements of a double coset of type $\mathcal{B}$ afford the operation $b \longrightarrow \infty \longrightarrow d$? The typical element of $\mathcal{B}_\alpha$ is $gw_\alpha u(\gamma)$, where $g \in F$. This element will afford the operation if and only if g maps b to 0, and $\gamma = d - \frac{1}{\alpha^2\infty^g}$. This is feasible if and only if b and 0 are in the same F-orbit. If this is the case, every double coset of type $\mathcal{B}$ will contain exactly one such element.

2. $A = \{\infty, b\}$, $B = \{c, d\}$. There is an element $gt_\alpha u(\gamma) \in \mathcal{A}_\alpha$ mapping $\infty \longrightarrow c$, $b \longrightarrow d$ if and only if there is an element $gt_{i\alpha}u(\gamma') \in \mathcal{A}_{i\alpha}$ mapping $\infty \longrightarrow d$, $b \longrightarrow c$. Here γ and γ' are uniquely determined. The situation is the same for double cosets of type $\mathcal{B}$. There

is an element $gw_\alpha u(\gamma) \in \mathcal{B}_\alpha$ mapping $\infty \longrightarrow c$, $b \longrightarrow d$ if and only if there is an element $gw_{i\alpha}u(\gamma') \in \mathcal{B}_{i\alpha}$ mapping $\infty \longrightarrow d$, $b \longrightarrow c$. Here γ and γ' are uniquely determined.

3. $A = \{a, b\}$, $B = \{\infty, d\}$. As in the second case, there is an element $gt_\alpha u(\gamma) \in \mathcal{A}_\alpha$ mapping $a \longrightarrow \infty$, $b \longrightarrow d$ if and only if there is $gt_{i\alpha}u(\gamma') \in \mathcal{A}_{i\alpha}$ affording the operation $a \longrightarrow d$, $b \longrightarrow \infty$, likewise for the double cosets of type $\mathcal{B}$.

4. $A = \{a, b\}$, $B = \{c, d\}$. The typical element $gt_\alpha u(\gamma) \in \mathcal{A}_\alpha$ will afford the operation $a \longrightarrow c$, $b \longrightarrow d$ if and only if $\alpha^2 = \frac{c-d}{a^g - b^g}$, $\gamma = c - \alpha^2 a^g$. This is the case if and only if a corresponding element $gt_{i\alpha}u(\gamma') \in \mathcal{A}_{i\alpha}$ affords $a \longrightarrow d$, $b \longrightarrow c$, where $\gamma' = c + \alpha^2 b^g$. An analogous computation leads to the same conclusion for double cosets of type $\mathcal{B}$.

2.2 Proof of Theorem 3

The generator ρ of F is chosen such that $u_1 = (\tau \longrightarrow \tau + 1)$ inverts F. Write the elements of the projective line as a_i, with subscripts written mod $q+1$, such that $a_0 = \infty$ and $a_i^\rho = a_{i+1}$. The operation of u_1 shows $a_{-i} = a_i + 1$.

Let a pair $\{a, b\}$ of elements of the projective line be given, and let $g = m_\lambda u_\gamma \rho^\nu$ be the generic element of $Tu_\gamma F$, where $u_\gamma \in X$. Then

$$a^g = (\lambda \cdot a + \gamma)^{\rho^\nu}$$

$$b^g = (\lambda \cdot b + \gamma)^{\rho^\nu}.$$

Set $\lambda \cdot a + \gamma = a_i$, $\lambda \cdot b + \gamma = a_j$. We define a mapping $\Phi = \Phi_{a,b} : \mathcal{S} \longrightarrow G - \mathcal{S}$ by

$$\Phi(g) = m_\lambda u_{\gamma+1} \rho^{\nu+i+j}.$$

Clearly $\Phi(g) \in G - S$ and Φ is a bijective mapping. Compare the action of g to the action of $\Phi(g)$ on $\{a, b\}$. By the choice of i, j we have

$$a^g = a_i^{\rho^\nu} = a_{\nu+i}, \quad b^g = a_j^{\rho^\nu} = a_{\nu+j}.$$

We calculate:

$$a^{\phi(g)} = (a_i + 1)^{\rho^{\nu+i+j}} = a_{-i}^{\rho^{\nu+i+j}} = a_{\nu+j},$$

and similarly $b^{\phi(g)} = a_{\nu+i}$. This shows that the images of the pair $\{a, b\}$ under g and $\Phi(g)$ are the same.

References

[1] J.Bierbrauer and Tran van Trung: *Halving $PGL(2, 2^f)$, f odd: a series of cryptocodes,* Designs, Codes and Cryptography 1(1991),141-148.

[2] J.Bierbrauer and Tran van Trung: *Some highly symmetric authentication perpendicular arrays,* Designs, Codes and Cryptography 1(1992),307-319.

Jürgen Bierbrauer,
Department of Mathematics,
Michigan Technological University,
Houghton, MI 49931,USA.
Yves Edel,
Mathematisches Institut der Universität,
Im Neuenheimer Feld 288,
69120 Heidelberg,Germany.

Eingegangen am 16. Februar 1993