Flag-transitive 3-design from the action of $\mathrm{PSL}(2,q)$ on the projective line

Akihiro Munemasa

Tohoku University

G2C2, Hebei Normal University,
August 16, 2024

The action of $\mathrm{PSL}(2,q)$ on $\mathrm{PG}(1,q)$

The projective special linear group $\mathrm{PSL}(2,q)$ acts as linear fractional transformations:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : z \mapsto \frac{az+b}{cz+d} \quad (z \in \mathbb{F}_q \cup \{\infty\}),$$

where $ad - bc = 1$.

The purpose of this talk is to give a family of nice orbits consisting of $(q-1)/e$-element subset forming 3-designs.

More precisely,

- e is a positive integer with $e \geq 2$,
- q is a prime power with $q \equiv 1 \pmod{e}$,
- a representative for the orbit is the set of e-th powers in $\mathbb{F}_q^\times$.
- ... (additional conditions).

t-Designs

Let Ω be a finite set, and denote by $\binom{\Omega}{k}$ the family of k-element subsets of Ω.

Definition

A pair $(\Omega, \mathcal{B})$ is called a t-design if $\mathcal{B} \subseteq \binom{\Omega}{k}$ and, any t points of Ω is contained in a constant number of members of $\mathcal{B}$.

To avoid triviality, we assume $|\Omega| > k > t > 0$. Members of $\mathcal{B}$ are often called blocks.

The constant number in the definition is usually denoted by λ, and we say $\mathcal{B}$ is a t-(v, k, λ) design, where $v = |\Omega|$.

Definition

A permutation group G on a finite set Ω is said to be t-transitive if G acts transitively on the set of ordered t-tuples of distinct elements of Ω.

Definition

A permutation group G is said to be t-homogeneous if G acts transitively on $\binom{\Omega}{t}$ (of unordered t-tuples, i.e., t-element subsets).

Clearly, t-transitive $\implies$ t-homogeneous.

If G is a t-homogeneous permutation group on Ω, and $B \in \binom{\Omega}{k}$ with $|\Omega| > k > t$, then $(\Omega, G \cdot B)$ is a t-design, where $G \cdot B$ is the orbit of B under G,
If the set of blocks $\mathcal{B}$ is of the form $G \cdot B$, then the design $(\Omega, \mathcal{B})$ is called block-transitive, and a representative B is called a starter of the design $(\Omega, \mathcal{B})$ under G.

$\mathrm{PGL}(2,q)$ acting on $\mathbb{F}_q \cup \{\infty\}$

$\mathbf{PGL}(2,q)$ acts on $\mathbb{F}_q \cup \{\infty\}$ in terms of linear fractional transformation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : z \mapsto \frac{az+b}{cz+d} \quad (z \in \mathbb{F}_q \cup \{\infty\}).$$

This action is 3-transitive: $(\infty, 0, 1) \mapsto$ any triple of distinct elements of $\mathbb{F}_q \cup \{\infty\}$.

Any $B \in \binom{\mathbb{F}_q \cup \{\infty\}}{k}$, $k > 3$, is a starter of a block-transitive design under $\mathbf{PGL}(2,q)$.

How about $\mathbf{PSL}(2,q)$?

$\mathrm{PGL}(2,q) \supseteq \mathrm{PSL}(2,q)$

- $\mathrm{PGL}(2,q)$ is 3-transitive, hence 3-homogeneous on $\mathbb{F}_q \cup \{\infty\}$.
- If $q = 2^m$, then $\mathrm{PSL}(2,q) = \mathrm{PGL}(2,q)$ is 3-transitive and hence 3-homogeneous.

If q is odd, then $|\mathrm{PGL}(2,q) : \mathrm{PSL}(2,q)| = 2$.

- If $q \equiv -1 \pmod 4$, then $\mathrm{PSL}(2,q)$ is 3-homogeneous.
- If $q \equiv 1 \pmod 4$, then $\mathrm{PSL}(2,q)$ is not 3-homogeneous.

$q \equiv 1 \pmod 4$

Since $\mathbf{PGL}(2,q) \supsetneq \mathbf{PSL}(2,q)$,

$$\mathbf{PGL}(2,q)\cdot B \supseteq \mathbf{PSL}(2,q)\cdot B \quad \text{for } B \in \binom{\mathbb{F}_q \cup \{\infty\}}{k}.$$

It can happen that

$$\mathbf{PGL}(2,q)\cdot B = \mathbf{PSL}(2,q)\cdot B$$

for some B, and in this case, $\mathbf{PGL}(2,q)\cdot B = \mathbf{PSL}(2,q)\cdot B$ is a 3-design.

The converse, however,

$$\mathbf{PSL}(2,q)\cdot B \text{ is a } 3\text{-design} \implies \mathbf{PGL}(2,q)\cdot B = \mathbf{PSL}(2,q)\cdot B$$

is not true.

Bonnecaze and Solé (2021)

"The extended binary quadratic residue code of length 42 holds a 3-design." (Neither transitivity nor Assmus–Mattson theorem can provide a reason)

Consider $\chi\colon \mathbb{F}_q \to \{0, \pm 1\}$ defined by

$$\chi(a) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \in (\mathbb{F}_q^\times)^2, \\ -1 & \text{otherwise.} \end{cases}$$

(known as the Legendre symbol, quadratic residue character).

Let $q = 41$. The linear span over $\mathbb{F}_2$ of the rows of the $q \times q$ matrix

$$\frac{1}{2}((\chi(a-b)+1)_{a,b\in\mathbb{F}_q} - I)$$

is the binary quadratic residue code of length 41, denoted QR_{41}.

Bonnecaze and Solé (2021)

Then $QR_{41} \subseteq \mathbb{F}_2^{41}$, $\dim QR_{41} = 21$.

The extended binary quadratic residue code XQR_{42} of length 42 is obtained from QR_{41} by adding the "parity check coordinate."
Then $XQR_{42} \subseteq \mathbb{F}_2^{42}$, $\dim XQR_{42} = 21$.

For $x \in \mathbb{F}_2^n$,

$$\begin{aligned} \operatorname{supp}(x) &= \{i \mid 1 \le i \le n,\ x_i = 1\}, \\ \operatorname{wt}(x) &= |\operatorname{supp}(x)|. \end{aligned}$$

Let

$$\begin{aligned} \Omega &= \{1, 2, \dots, 42\}, \\ \mathcal{B} &= \{\operatorname{supp}(x) \mid x \in XQR_{42},\ \operatorname{wt}(x) = 10\}. \end{aligned}$$

Then $(\Omega, \mathcal{B})$ is a 3-$(42, 10, 18)$ design (verified by computer). WHY?

Awada, Miezaki, M., Nakasora (2024)

Let

$$\Omega = \{1, 2, \ldots, 42\},$$
$$\mathcal{B} = \{\mathrm{supp}(x) \mid x \in XQR_{42},\ \mathrm{wt}(x) = k\}.$$

Then $(\Omega, \mathcal{B})$ is a 3-design only if $k = 10, 32$ (verified by computer).

$\mathrm{Aut}\, XQR_{42} = \mathrm{PSL}(2, 41)$ acts block-transitively.

Let

$$\tilde{\mathcal{B}} = \{\mathrm{supp}(x) \mid x \in XQR_{42} \cup XQR_{42}^{\perp},\ \mathrm{wt}(x) = 10\}.$$

Then $(\Omega, \tilde{\mathcal{B}})$ is a 3-design (this fact can be theoretically generalized, but $|\tilde{\mathcal{B}}| = 2|\mathcal{B}|$. In fact, $\tilde{\mathcal{B}}$ is a $\mathrm{PGL}(2, 41)$-orbit.)

Let

$$\Omega = \{1, 2, \ldots, 42\},$$
$$\mathcal{B} = \{\text{supp}(x) \mid x \in XQR_{42},\ \text{wt}(x) = 10\}.$$

Then $(\Omega, \mathcal{B})$ is a 3-design (Bonnecaze and Solé, 2021).

$\text{Aut}\, XQR_{42} = \text{PSL}(2, 41)$ acts block-transitively.
$\mathcal{B} = \text{PSL}(2, 41) \cdot B \subsetneq \text{PGL}(2, 41) \cdot B$.

In fact, we may identify Ω with $\mathbb{F}_{41} \cup \{\infty\}$, and

$$B = \{1, \beta, \beta^2, \ldots, \beta^9\},$$

where β is a primitive 10-th root of 1 in $\mathbb{F}_{41}$. Equivalently, B is the set of quartic (4th power) residues in $\mathbb{F}_{41}$, i.e.,

$$B = \langle \beta \rangle, \quad \mathbb{F}_{41}^{\times} = \langle \alpha \rangle, \quad \beta = \alpha^4.$$

$G = \mathrm{PSL}(2, q)$, $q \equiv 1 \pmod 4$

For some choice of B, $(\mathbb{F}_q \cup \{\infty\}, G \cdot B)$ can happen to be a 3-design.

Theorem (Keranen–Kreher–Shiue, 2003)

Suppose $q \equiv 5$ or $13 \pmod{24}$. Let $B = \{\infty, 0, 1, -1\} \subseteq \mathbb{F}_q \cup \{\infty\}$. Then B is a starter of a block-transitive 3-$(q+1, 4, 3)$ design under G.

Theorem (Li–Deng–Zhang, 2018)

Suppose $q \equiv 1 \pmod{20}$. Let $B = \langle \alpha^{(q-1)/5} \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-$(q+1, 5, 3)$ design under G, if and only if there exists $\theta \in \mathbb{F}_q^\times$ such that $\chi(\theta) = -1$ and $\theta^2 - 4\theta - 1 = 0$.

No systematic work on $B \subseteq \mathbb{F}_q \cup \{\infty\}$ with $|B| > 5$.

Power residues in $\mathbb{F}_q^\times$

Let q be a prime power with $q \equiv 1 \pmod 4$, and let $e | q-1$. Let

$$\begin{aligned} \mathbb{F}_q^\times &= \langle \alpha \rangle, \\ B &= \langle \alpha^e \rangle, \\ G &= \mathrm{PSL}(2,q). \end{aligned}$$

Regarding $B \subseteq \mathbb{F}_q \cup \{\infty\}$, when is $(\mathbb{F}_q \cup \{\infty\}, G \cdot B)$ a 3-design?

- Bonnecaze–Solé, 2021: $q = 41$, $e = 4$.
- Li–Deng–Zhang, 2018: $q \equiv 1 \pmod{20}$, $e = (q-1)/5$, under some condition (which is satisfied for $q = 41$).

$\mathrm{PSL}(2,q)$ is not 3-homogeneous, but...

Assume $q \equiv 1 \pmod 4$.

There are only two orbits on $\binom{\mathbb{F}_q \cup \{\infty\}}{3}$ under $\mathrm{PSL}(2,q)$, with representatives

$$\{\infty, 0, 1\}, \{\infty, 0, \alpha\},$$

where $\mathbb{F}_q^\times = \langle \alpha \rangle$.

A $\mathrm{PSL}(2,q)$-orbit $\mathcal{B} \subseteq \binom{\mathbb{F}_q \cup \{\infty\}}{k}$ is the set of blocks of a 3-design if and only if

$$|\{B \in \mathcal{B} \mid \{\infty, 0, 1\} \subseteq B\}| = |\{B \in \mathcal{B} \mid \{\infty, 0, \alpha\} \subseteq B\}|.$$

Further simplification is as follows.

Let $q \equiv 1 \pmod 4$, $G = \mathrm{PSL}(2, q)$. Then

$$\binom{\mathbb{F}_q \cup \{\infty\}}{3} = \mathcal{O}_+ \cup \mathcal{O}_- \quad \text{(disjoint)},$$

where

$$\mathcal{O}_+ = G \cdot \{\infty, 0, 1\}, \qquad \mathcal{O}_- = G \cdot \{\infty, 0, \alpha\}.$$

Lemma (Tonchev, 1988)

Let $B \subseteq \mathbb{F}_q \cup \{\infty\}$ with $|B| > 3$. Then B is a starter of a block-transitive 3-design under G if and only if

$$\left|\binom{B}{3} \cap \mathcal{O}_+\right| = \left|\binom{B}{3} \cap \mathcal{O}_-\right|.$$

Moreover

$$\binom{\mathbb{F}_q^\times}{3} \cap \mathcal{O}_\pm = \{\{a, b, c\} \mid \chi((a-b)(b-c)(c-a)) = \pm 1\}.$$

Theorem (Bonnecaze–Solé, 2021, reformulated)

Let $q = 41$, $G = \mathrm{PSL}(2, q)$. Let $B = \langle \alpha^4 \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-design under G.

The proof amounts to showing

$$\left| \binom{B}{3} \cap \mathcal{O}_+ \right| = \left| \binom{B}{3} \cap \mathcal{O}_- \right|.$$

This can be verified directly (by hand, not by computer):

$$B = \langle 6^4 \rangle = \{1, 25, 10, 4, 18, 40, 16, 31, 37, 23\} \subseteq \mathbb{F}_{41}^\times = \langle 6 \rangle.$$

$\{1, 25, 10\} \in \mathcal{O}_+$ since $\chi((1-25)(25-10)(10-1)) = 1$,
$\{1, 25, 4\} \in \mathcal{O}_+$ since $\chi((1-25)(25-4)(4-1)) = 1$,
and so on: $\binom{10}{3} = 120$ times.

Theorem (Bonnecaze–Solé, 2021, reformulated)

Let $q = 41$, $G = \mathrm{PSL}(2, q)$. Let $B = \langle \alpha^4 \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-design under G.

Bonnecaze–Solé did not cite:

Theorem (Li–Deng–Zhang, 2018)

Suppose $q \equiv 1 \pmod{20}$. Let $B = \langle \alpha^{(q-1)/5} \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-$(q+1, 5, 3)$ design under $\mathrm{PSL}(2, q)$, if and only if there exists $\theta \in \mathbb{F}_q^\times$ such that $\chi(\theta) = -1$ and $\theta^2 - 4\theta - 1 = 0$.

For $q = 41$,

the former theorem says $B = \langle \alpha^4 \rangle$ is a starter of size $|B| = 10$,

the latter theorem says $B = \langle \alpha^8 \rangle$ is a starter of size $|B| = 5$.

Which prime power q satisfies the condition of Li–Deng–Zhang?

OEIS A325072

The sequence of primes

$$\mathbf{41, 61, 241, 281, 421, 601, 641, \ldots}$$

satisfying the condition of Li–Deng–Zhang:

$$\exists \theta \in \mathbb{F}_p^\times,\ \chi(\theta) = -1,\ \theta^2 - 4\theta - 1 = 0 \qquad \text{(LDZ)}$$

coincide with OEIS A325072: Prime numbers $p \equiv 1 \pmod{20}$ with

$$p \neq x^2 + 20y^2,\ x^2 + 100y^2.$$

Theorem

Let q be a prime power with $q \equiv 1 \pmod{20}$, let $\mathbb{F}_q^\times = \langle \alpha \rangle$ and $\beta = \alpha^{(q-1)/10}$. Let χ denote the quadratic residue character of $\mathbb{F}_q^\times$. Then the following are equivalent:

- (BS) $B = \langle \beta \rangle$ is a starter of a 3-design under $\mathrm{PSL}(2, q)$.
- (LDZ1) $B = \langle \beta^2 \rangle$ is a starter of a 3-design under $\mathrm{PSL}(2, q)$.
- (LDZ2) $\exists \theta \in \mathbb{F}_q^\times$ such that $\chi(\theta) = -1$ and $\theta^2 - 4\theta - 1 = 0$.
- (M) $\chi(\beta - 1) = -1$.
- (OEIS) q is an odd power of a prime which cannot be represented in the form $x^2 + 20y^2$ or $x^2 + 100y^2$, where x, y are positive integers.

Moreover, if one of the equivalent conditions is satisfied, then $B = \langle \beta \rangle$ is a starter of a flag-transitive 3-design under $\mathrm{PSL}(2, q)$.

flag-transitive $\iff$ block-transitive & block stabilizer is transitive on the set of points of the block.

OEIS A325072 : $41, 61, 241, 281, 421, \ldots$

This is the sequence of primes p with $p \equiv 1 \pmod{20}$ satisfying one of the following equivalent conditions:

- (LDZ2) $\exists \theta \in \mathbb{F}_p^\times$ such that $\chi(\theta) = -1$ and $\theta^2 - 4\theta - 1 = 0$.
- (M) $\chi(\beta - 1) = -1$, where $\beta \in \mathbb{F}_p$ is a primitive 10-th root of 1.
- (OEIS1) p cannot be represented in the form $x^2 + 20y^2$.
- (OEIS2) p cannot be represented in the form $x^2 + 100y^2$.
- (H) 5 is not a quartic residue in $\mathbb{F}_p$.

Brink (2009) showed (OEIS1) $\iff$ (OEIS2).

Hasse (1930) showed (OEIS2) $\iff$ (H).

Showing (LDZ2) $\iff$ (M) $\iff$ (H) is elementary.

Let q be a prime power with $q \equiv 1 \pmod{20}$, let $\mathbb{F}_q^\times = \langle \alpha \rangle$ and $\beta = \alpha^{(q-1)/10}$. Let χ denote the quadratic residue character of $\mathbb{F}_q^\times$.

(M) $\chi(\beta - 1) = -1$.

(BS) $B = \langle \beta \rangle$ is a starter of a 3-design under $\mathrm{PSL}(2, q)$.

Sketch of Proof (M) $\Longrightarrow$ (BS).

We need to show

$$\left| \binom{B}{3} \cap \mathcal{O}_+ \right| = 60 = \left| \binom{B}{3} \cap \mathcal{O}_- \right|,$$

where $B = \{1, \beta, \beta^2, \dots, \beta^9\}$. Recall

$$\binom{\mathbb{F}_q^\times}{3} \cap \mathcal{O}_\pm = \{\{a, b, c\} \mid \chi((a-b)(b-c)(c-a)) = \pm 1\}.$$

$B = \{1, \beta, \beta^2, \ldots, \beta^9\}$, where $\beta = \alpha^{(q-1)/10}$. We need to show

$$\left|\binom{B}{3} \cap \mathcal{O}_+\right| = 60 = \left|\binom{B}{3} \cap \mathcal{O}_-\right|.$$

Write

$$\chi(T) = \chi((a-b)(b-c)(c-a)) \quad (T = \{a, b, c\} \in \binom{B}{3}).$$

Then for $T \in \binom{B}{3}$,

$$T \in \mathcal{O}_+ \iff \chi(T) = +1.$$

Again $\binom{|B|}{3} = 120$ times? No, since $(q-1)/10$ is even, we have $\chi(\beta) = 1$. This means

$$\chi(\beta T) = \chi(\beta)^3 \chi(T) = \chi(T),$$

so $\chi(T)$ is constant on each orbit of $\langle \beta \rangle$.

Enough to do it for 12 times only.

$$\left|\binom{B}{3}\cap\mathcal{O}_+\right| = 60 = \left|\binom{B}{3}\cap\mathcal{O}_-\right|.$$

$\binom{B}{3}$ is decomposed into 12 orbits under $\langle\beta\rangle$:

$T_1 = \langle\beta\rangle\cdot\{1,\beta,\beta^2\}$	$T_7 = \langle\beta\rangle\cdot\{1,\beta,\beta^6\}$
$T_2 = \langle\beta\rangle\cdot\{1,\beta,\beta^3\}$	$T_8 = \langle\beta\rangle\cdot\{1,\beta^2,\beta^4\}$
$T_3 = \langle\beta\rangle\cdot\{1,\beta^2,\beta^3\}$	$T_9 = \langle\beta\rangle\cdot\{1,\beta^2,\beta^5\}$
$T_4 = \langle\beta\rangle\cdot\{1,\beta,\beta^4\}$	$T_{10} = \langle\beta\rangle\cdot\{1,\beta^3,\beta^5\}$
$T_5 = \langle\beta\rangle\cdot\{1,\beta^3,\beta^4\}$	$T_{11} = \langle\beta\rangle\cdot\{1,\beta^2,\beta^6\}$
$T_6 = \langle\beta\rangle\cdot\{1,\beta,\beta^5\}$	$T_{12} = \langle\beta\rangle\cdot\{1,\beta^3,\beta^6\}$

$$\chi(T_1) := \chi((1-\beta)(\beta-\beta^2)(\beta^2-1)) = ?$$
$$\chi(T_2) := \chi((1-\beta)(\beta-\beta^3)(\beta^3-1)) = ?$$

not computable each, but since $\beta^5 = -1$,

$$\frac{\chi(T_1)}{\chi(T_2)} = \frac{\chi((1-\beta)(\beta-\beta^2)(\beta^2-1))}{\chi((1-\beta)(\beta-\beta^3)(\beta^3-1))} = 1.$$

$T_1 = \langle\beta\rangle \cdot \{1, \beta, \beta^2\}$ $T_2 = \langle\beta\rangle \cdot \{1, \beta, \beta^3\}$ $\cdots$	$\cdots$ $\cdots$ $T_{12} = \langle\beta\rangle \cdot \{1, \beta^3, \beta^6\}$

Since $\chi(T_1) = \chi(T_2)$, we have $T_1 \subseteq \mathcal{O}_+ \iff T_2 \subseteq \mathcal{O}_+$.

In fact, using (M): $\chi(\beta - 1) = -1$, one of the following holds:

$$\bigcup_{i\in\{1,2,3,6,7,11\}} T_i \subseteq \mathcal{O}_\pm \quad \text{and} \quad \bigcup_{i\in\{4,5,8,9,10,12\}} T_i \subseteq \mathcal{O}_\mp, \quad \text{or}$$

$$\bigcup_{i\in\{1,2,3,9,10,11\}} T_i \subseteq \mathcal{O}_\pm \quad \text{and} \quad \bigcup_{i\in\{4,5,6,7,8,12\}} T_i \subseteq \mathcal{O}_\mp,$$

In both cases,

$$\left|\binom{B}{3} \cap \mathcal{O}_+\right| = 60 = \left|\binom{B}{3} \cap \mathcal{O}_-\right|.$$

This completes the proof of (M) $\Longrightarrow$ (BS).

Conclusion

Theorem (Bonnecaze–Solé, 2021, reformulated)

Let $q = 41$, $G = \mathrm{PSL}(2, q)$. Let $B = \langle \alpha^4 \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-design under G.

is generalized.

The prime power q can be an odd power of a prime in OEIS A325072 (and taking $B = \langle \alpha^{(q-1)/10} \rangle$).

Thank you very much for your attention!