Block-transitive 3-designs from $\mathrm{PSL}(2, q)$

宗政　昭弘
(MUNEMASA, Akihiro)
東北大学情報科学研究科
Graduate School of Information Sciences
Tohoku University

December 19, 2023

1 Introduction and preliminaries

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 $\mathbb{F}_q^\times$.
- $\ldots$ (additional conditions, to be stated later).

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

Definition 1. 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 $|\Omega| > k > t > 0$ in Definition 1. Members of $\mathcal{B}$ are often called **blocks**. The constant number in Definition 1 is usually denoted by λ, and we say $\mathcal{B}$ is a t-(v, k, λ) **design**, where $v = |\Omega|$.

Definition 2. A subgroup of the symmetric group on a finite set Ω is called a **permutation group** of degree $|\Omega|$. A permutation group G is said to be t-**transitive** if G acts transitively on the set of ordered t-tuples of distinct elements of Ω:

$$\{(x_1, \dots, x_t) \in \Omega^t \mid x_1, \dots, x_t : \text{ distinct}\}.$$

Examples follow:

- The symmetric group on Ω with $|\Omega| = n$ is n-transitive.
- The alternating group on Ω with $|\Omega| = n$ is $(n-2)$-transitive.
- The sporadic simple group M_{24} is a 5-transitive permutation group of degree 24.
- The projective general linear group $\mathrm{PGL}(2, q)$ is 3-transitive on the projective line $\mathbb{F}_q \cup \{\infty\} = \mathrm{PG}(1, q) = \mathbb{P}^1(\mathbb{F}_q)$, the 1-dimensional projective space.

Definition 3. A permutation group G is said to be t-**homogeneous** if G acts transitively on $\binom{\Omega}{t}$.

Recall that $\binom{\Omega}{t}$ is the set of unordered t-tuples, i.e., t-element subsets. Clearly, t-transitivity implies t-homogeneiety.

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.

The group $\mathrm{PGL}(2, q)$ acts on $\mathbb{F}_q \cup \{\infty\}$ in terms of linear fractional transformations

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

This action is 3-transitive: $(\infty, 0, 1) \mapsto$ any triple of distinct elements of $\mathbb{F}_q \cup \{\infty\}$. Thus, any $B \in \binom{\mathbb{F}_q \cup \{\infty\}}{k}$, $k > 3$, is a starter of a block-transitive design under $\mathrm{PGL}(2, q)$.

To what extent is this true for $\mathrm{PSL}(2, q)$? Recall

$$\begin{aligned} \mathrm{PGL}(n, q) &= \mathrm{GL}(n, q)/Z(\mathrm{GL}(n, q)), \\ \mathrm{PSL}(n, q) &= \mathrm{SL}(n, q)/(\mathrm{SL}(n, q) \cap Z(\mathrm{GL}(n, q)) \\ &\cong (\mathrm{SL}(n, q)Z(\mathrm{GL}(n, q)))/Z(\mathrm{GL}(n, q)), \\ \mathrm{PSL}(2, q) &= \mathrm{SL}(2, q)/\{\pm I\}. \end{aligned}$$

We already mentioned that $\mathrm{PGL}(2, q)$ 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 $|\mathrm{PGL}(2, q) : \mathrm{PSL}(2, q)| = 2$. The following fact is well known.

- 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.

If $G = \mathrm{PSL}(2,q)$ is 3-homogeneous on $\mathbb{F}_q \cup \{\infty\}$. then for $B \in \binom{\mathbb{F}_q \cup \{\infty\}}{k}$, $(\mathbb{F}_q \cup \{\infty\}, G \cdot B)$ is a 3-$(q+1, k, \lambda)$ design for some λ, where

$$\lambda = \frac{|G \cdot B| k(k-1)(k-2)}{(q+1)q(q-1)}.$$

can be computed from

$$|G \cdot B| = |G : \mathrm{Stab}_G(B)|.$$

Keranen and Kreher [9] investigated such designs for the case $q = 2^m$. For the case $q \equiv -1 \pmod 4$, see [15, 16, 18].

Since $\mathrm{PGL}(2,q) \supsetneqq \mathrm{PSL}(2,q)$, in general,

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

However, it can happen that $\mathrm{PGL}(2,q) \cdot B = \mathrm{PSL}(2,q) \cdot B$ for some B.

Since $|\mathrm{PGL}(2,q) : \mathrm{PSL}(2,q)| = 2$, we have the following.

Lemma 4. For $B \subseteq \mathbb{F}_q \cup \{\infty\}$, the following are equivalent:

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

(ii) $\exists \sigma \in \mathrm{PGL}(2,q)$ such that $\sigma(B) = B$ and $\sigma \notin \mathrm{PSL}(2,q)$.

Theorem 5. Suppose $q \equiv 1 \pmod{4e}$, e is odd. Let $B = \langle \alpha^e \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-design under $\mathrm{PSL}(2,q)$.

Proof. Let $\sigma =$ multiplication by α^e, and use Lemma 4 □

2 3-Designs not coming from Lemma 4 or Theorem 5

Lemma 4 and Theorem 5 give a sufficient condition for B to be a starter of a block-transitive 3-design under $\mathrm{PSL}(2,q)$. This condition is, however, not necessary.

Bonnecaze and Solé [2] found a block-transitive 3-design under $\mathrm{PSL}(2,41)$ which is not invariant under $\mathrm{PGL}(2,41)$. We give a description of this design. Let q be an odd prime power, and define $\chi\colon \mathbb{F}_q \to \{0, \pm 1\}$ by

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

This is known as the Legendre symbol, or 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}. 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?

Let

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

Then $(\Omega, \mathcal{B})$ is a 3-design only if $k = 10, 32$ (verified by computer, according to [2]). It is known that $\operatorname{Aut} XQR_{42} = \mathrm{PSL}(2, 41)$, and it acts transitively on $\mathcal{B}$ if $k = 10, 32$.

The design invariant under $\mathrm{PGL}(2, 41)$ is formed by taking the union of XQR_{42} and $XQR_{42}^{\perp}$ as follows:

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

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.)

In fact, we may identify Ω with $\mathbb{F}_{41} \cup \{\infty\}$. Let β be a primitive 10-th root of 1 in $\mathbb{F}_{41}$, and let

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

Equivalently, B is the set of quartic (4th power) residues in $\mathbb{F}_{41}$, i.e.,

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

Then $\mathcal{B} = \mathrm{PSL}(2, 41) \cdot B$.

3 Main results

In this section, we let q be a prime power with $q \equiv 1 \pmod 4$, and let $G = \mathrm{PSL}(2, q)$. For some particular choice of B, $(\mathbb{F}_q \cup \{\infty\}, G \cdot B)$ can happen to be a 3-design.

Theorem 6 (Keranen–Kreher–Shiue [10]). 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 7 (Li–Deng–Zhang [12])**.** 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 $\theta^2 - 4\theta - 1 = 0$.

For the remainder of this section, by a starter, we mean a starter $B \subseteq \mathbb{F}_q \cup \{\infty\}$ of a 3-design under $G = \mathrm{PSL}(2, q)$. Note that there has been no systematic work on finding a starter with $|B| > 5$. Earlier work include Keranen, Kreher and Shiue [10] for $|B| = 4$, Chen and Liu [5] for $|B| = 5$, Balachandran and Ray-Chaudhuri [1] for $|B| = 7$, and Li [11] for $|B| = 12$. Let q be a prime power with $q \equiv 1 \pmod 4$, and let $e | q - 1$. Let

$$\mathbb{F}_q^\times = \langle \alpha \rangle, \tag{1}$$
$$B = \langle \alpha^e \rangle, \tag{2}$$
$$G = \mathrm{PSL}(2, q). \tag{3}$$

Regarding $B \subseteq \mathbb{F}_q \cup \{\infty\}$, we are interested in the question when $(\mathbb{F}_q \cup \{\infty\}, G \cdot B)$ is a 3-design.

- Bonnecaze–Solé [2]: $q = 41$, $e = 4$.
- Li–Deng–Zhang [12]: $q \equiv 1 \pmod{20}$, $e = (q-1)/5$, under some condition.

Observe that $q = 41$ satisfies the condition $q \equiv 1 \pmod{20}$, but $e = 4$ does not satisfy $e = (q-1)/5$. Thus, the above two results look unrelated at the first glance. To connect these two, we need some preparation. There are only two orbits on $\binom{\mathbb{F}_q \cup \{\infty\}}{3}$ under G, namely,

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

where

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

In fact,

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

Thus, a G-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.

Lemma 8 (Tonchev [17, Theorem 1.6.1])**.** 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

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

Theorem 9 (Bonnecaze–Solé [2], reformulated)**.** Let $q = 41$, $G = \mathrm{PSL}(2, q)$. Let $e = 4$, $B = \langle \alpha^e \rangle \subseteq \mathbb{F}_q^\times = \langle \alpha \rangle$. Then B is a starter of a block-transitive 3-design under G.

The proof of Theorem 9 using Lemma 8 amounts to showing

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

which can be verified directly:

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

$\{1, 25, 10\} \in \mathcal{O}_+$ since $\chi((1-25)(25-10)(10-1)) = 1$,..., and so on.

For $q = 41$, Theorem 9 says $B = \langle \alpha^4 \rangle$ is a starter of size $|B| = 10$, while Theorem 7 says $B = \langle \alpha^8 \rangle$ is a starter of size $|B| = 5$. Since $\langle \alpha^4 \rangle$ is a union of two cosets of $\langle \alpha^8 \rangle$, it may not be too surprising that there is a connection.

Let us go back to the general setting (1)–(3). Let

$$B = \langle \alpha^{(q-1)/10} \rangle,$$
$$B' = \langle \alpha^{(q-1)/5} \rangle.$$

Then $|B| = 10$, $|B'| = 5$, and (by computer)

$$B \text{ is a starter of a 3-design under } \mathrm{PSL}(2, q)$$
$$\text{if } q = 41, 61, 241, 281, 421, 601, 641, \dots,$$
$$B' \text{ is a starter of a 3-design under } \mathrm{PSL}(2, q)$$
$$\text{if } q = 41, 61, 241, 281, 421, 601, 641, \dots,$$

The latter condition is, by [12]:

$$\exists \theta \in \mathbb{F}_q^\times,\ \chi(\theta) = -1,\ \theta^2 - 4\theta - 1 = 0. \tag{4}$$

The sequence of primes

$$41, 61, 241, 281, 421, 601, 641, \dots$$

satisfying (4) was found to be in coincidence with the sequence OEIS A325072 [14]: prime numbers $p \equiv 1 \pmod{20}$ with

$$p \neq x^2 + 20y^2,\ x^2 + 100y^2. \tag{5}$$

It turns out that various conditions mentioned above are all equivalent to each other.

Theorem 10. 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:

(LDZ1) There exists $\theta \in \mathbb{F}_q^\times$ such that $\chi(\theta) = -1$ and $\theta^2 - 4\theta - 1 = 0$.
(LDZ2) $B = \langle \beta^2 \rangle$ is a starter of a 3-design with block size 5 under $\mathrm{PSL}(2, q)$.
(BS) $B = \langle \beta \rangle$ is a starter of a 3-design with block size 10 under $\mathrm{PSL}(2, q)$.
(M) $\chi(\beta - 1) = -1$.
(OEIS) q is an odd power of a prime p with $p \equiv 1 \pmod{20}$ satisfying (5).

It is shown in [12] that (LDZ1) is equivalent to (LDZ2). So the new part is

$$\text{(LDZ1)} \iff \text{(BS)} \iff \text{(M)} \iff \text{(OEIS)}.$$

It is shown in [4] that, for a prime p with $p \equiv 1 \pmod{20}$, (5) is equivalent to

$$p \neq x^2 + 100y^2, \tag{6}$$

which is then equivalent to

$$5 \notin \langle \alpha^4 \rangle \tag{7}$$

by [8, p. 69]. The proof of Theorem 10 consists of establishing the equivalence of arithmetic conditions (LDZ1), (M) and (7), and of showing the equivalence of (BS) and (M) by using Lemma 8.

Acknowledgements

The author would like to thank Yoshinori Yamasaki for pointing out the sequence OEIS A325072 during the Ehime Algebra Seminar on October 20, 2023.

References

[1] Niranjan Balachandran and Dijen Ray-Chaudhuri. Simple 3-designs and $\mathrm{PSL}(2, q)$ with $q \equiv 1 \pmod 4$. *Des. Codes Cryptogr.*, 44(1-3):263–274, 2007.

[2] A. Bonnecaze and P. Sole, The extended binary quadratic residue code of length 42 holds a 3-design, *J. Combin. Des.* **29** (2021), no. 8, 528–532.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language, *J. Symb. Comp.* **24** (1997), 235–265.

[4] D. Brink, Five peculiar theorems on simultaneous representation of primes by quadratic forms, *J. Number Theory*, **129** (2009) 464–468.

[5] Jing Chen and Wei Jun Liu. 3-designs from $PSL(2, q)$ with $q \equiv 1 \pmod 4$. *Util. Math.*, 88:211–222, 2012.

[6] Shaojun Dai and Shangzhao Li. Flag-transitive 3-$(v, k, 3)$ designs and $\mathrm{PSL}(2, q)$ groups. *Algebra Colloq.*, 28(1):33–38, 2021.

[7] Cunsheng Ding, Chunming Tang, and Vladimir D. Tonchev. The projective general linear group $\mathrm{PGL}(2, 2^m)$ and linear codes of length $2^m + 1$. *Des. Codes Cryptogr.*, 89(7):1713–1734, 2021.

[8] Helmut Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II, 1930.

[9] M. S. Keranen and D. L. Kreher. 3-designs of $\mathrm{PSL}(2, 2^n)$ with block sizes 4 and 5. *J. Combin. Des.*, 12(2):103–111, 2004.

[10] M. S. Keranen, D. L. Kreher, and P. J.-S. Shiue. Quadruple systems of the projective special linear group $\mathrm{PSL}(2, q), q \equiv 1 \pmod 4$. *J. Combin. Des.*, 11(5):339–351, 2003.

[11] Weixia Li. On the existence of simple 3-$(30, 7, 15)$ and 3-$(26, 12, 55)$ designs. *Ars Combin.*, 95:531–536, 2010.

[12] Weixia Li, Dameng Deng, and Guangjun Zhang. Simple 3-$(q + 1, 5, 3)$ designs admitting an automorphism group $\mathrm{PSL}(2, q)$ with $q \equiv 1 \pmod 4$. *Ars Combin.*, 136:97–108, 2018.

[13] WeiJun Liu, JianXiong Tang, and YiXiang Wu. Some new 3-designs from $PSL(2, q)$ with $q \equiv 1 \pmod 4$. *Sci. China Math.*, 55(9):1901–1911, 2012.

[14] OEIS Foundation Inc, The Online Encyclopedia of Integer Sequences, `http://oeis.org`.

[15] Byeong-Kweon Oh, Jangheon Oh, and Hoseog Yu. New infinite families of 3-designs from algebraic curves over $\mathbb{F}_q$. *European J. Combin.*, 28(4):1262–1269, 2007.

[16] Byeong-Kweon Oh and Hoseog Yu. New infinite families of 3-designs from algebraic curves of higher genus over finite fields. *Electron. J. Combin.*, 14(1):Note 25, 7, 2007.

[17] Vladimir D. Tonchev. *Combinatorial configurations: designs, codes, graphs*, volume 40 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow; John Wiley & Sons, Inc., New York, 1988. Translated from the Bulgarian by Robert A. Melter.

[18] Hoseog Yu. 3-designs derived from plane algebraic curves. *Bull. Korean Math. Soc.*, 44(4):817–823, 2007.