Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-021-00997-y

Equidistant permutation group codes

Fatemeh Jafari[1] · **Alireza Abdollahi**[1,3] · **Javad Bagherian**[1] · **Maryam Khatami**[1] · **Reza Sobhani**[2]

Received: 11 August 2020 / Revised: 6 September 2021 / Accepted: 13 December 2021

Abstract
We study permutation codes which are groups and all of whose non-identity code elements have the same number of fixed points. It follows that over certain classes of groups such permutation codes exist.

Keywords Equidistant permutation codes · Positive type · Permutation groups

Mathematics Subject Classification 05A05 · 94B25 · 05E18

1 Introduction and results

Let n be a positive integer and let S_n denote the symmetric group on n letters, i.e. the set of all permutations of $[n] := \{1, \dots, n\}$. By a fixed point of $\alpha \in S_n$ we mean an element $i \in [n]$ such that $\alpha(i) = i$. We denote by $F(\alpha)$ the set $\{i \in [n] \mid \alpha(i) = i\}$ of all fixed points

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: On Coding Theory and Combinatorics: In Memory of Vera Pless".

✉ Fatemeh Jafari
math_fateme@yahoo.com

Alireza Abdollahi
a.abdollahi@math.ui.ac.ir

Javad Bagherian
bagherian@sci.ui.ac.ir

Maryam Khatami
m.khatami@sci.ui.ac.ir

Reza Sobhani
r.sobhani@sci.ui.ac.ir

1 Department of Pure Mathematics, Faculty of Mathematics and Statistics, University of Isfahan, 81746-73441 Isfahan, Iran

2 Department of Applied Mathematics and Computer Science, Faculty of Mathematics and Statistics, University of Isfahan, 81746-73441 Isfahan, Iran

3 School of Mathematics, Institute for Research in Fundamental Sciences (IPM), 19395-5746 Tehran, Iran

Published online: 05 January 2022

of α. For any two permutations $\sigma, \tau \in S_n$ the distance $d(\sigma, \tau)$ between σ and τ is defined by $n - |F(\sigma\tau^{-1})|$.

By a permutation code (PC) of length n we simply mean a non-empty subset $\mathcal{C}$ of S_n. A permutation code of length n is called equidistance (called EPC for short) whenever all two distinct permutations in $\mathcal{C}$ have the same distance $n-\lambda$ which we call the distance of $\mathcal{C}$, and λ is called the fixity of the code. The maximum size of an EPC of length n and the same distance $n-\lambda$ is denoted by $Me(n, \lambda)$. EPCs have been studied since the 1970s. Some techniques have been developed to derive lower and upper bounds on $Me(n, \lambda)$ [6,9,10,23–25,30,31]. An EPC is a special kind of equidistant frequency permutation codes (EFPCs) (introduced in [16]) which are an interesting kind of constant composition codes (CCC). CCCs have many applications, for example in powerline communications and balanced scheduling . The situation when CCCs are equidistant is of particular interest, since it is known that any CCC which is optimal must be equidistant (see [22]). We refer the reader to [3,4,7,8,15,22] for more details about CCCs and EFPCs.

By an equidistant permutation group code (EPGC) of length n we mean an EPC of length n which is a subgroup of S_n. So if $\mathcal{C}$ is an EPGC of the length n, the size M and the distance $n-\lambda$, then $\mathcal{C}$ is a subgroup of S_n of size M such that $|F(\alpha)| = \lambda$ for all non-trivial elements $\alpha \in \mathcal{C}$. Due to the advantages of restricting the permutation codes with a group structure in their construction and encoding (see [26, p. 2, lines 12–16] and [29, p. 1]), throughout this paper, we focus on EPGCs.

In this paper, we study EPG codes $\mathcal{C}$ whose distances are less than their lengths and such that there is no common fixed point for all elements of $\mathcal{C}$, i.e., $\mathcal{F}(\mathcal{C}) := \cap_{\sigma\in\mathcal{C}} F(\sigma)$ is empty. Note that if $\mathcal{F}(\mathcal{C}) \neq \varnothing$, then $\mathcal{C}$ can be considered as a permutation code on $[n] \setminus \mathcal{F}(\mathcal{C})$. Thus the restriction "having no common fixed point"can be easily put on any permutation code since all coding theoretic parameters of $\mathcal{C}$ is unchanged except its length. The former restriction "the same distance is less than the length"in our study of EPGC comes from the following discussion.

Let G be a permutation group code of length n, i.e. G is a subgroup of S_n. By definition the G-orbit containing $i \in [n]$, denoted by $\mathcal{O}(i)$, is the set $\{\sigma(i) \mid \sigma \in G\}$ and G is called transitive if it has exactly one orbit, that is, $\mathcal{O}(i) = [n]$ for all $i \in [n]$. As usual, G is called semiregular if $F(\alpha) = \varnothing$ for all non-trivial $\alpha \in G$. Thus G is semiregular if and only if G is equidistance whose distance is equal to its length. By definition G is called regular if it is both transitive and semiregular. By Burnside's lemma, the number of G-orbits is equal to $\frac{1}{|G|}\sum_{g\in G}|F(g)|$. So if G is transitive, then there exists $g_0 \in G$ such that $F(g_0) = \varnothing$. It follows that if G is also equidistance, $|F(g)| = 0$ for all $g \in G\setminus\{1\}$. Hence, G is regular and $|G| = n$ and so G is permutation isomorphic to the permutation group $G_R = \{\rho_g \mid g \in G\}$ is a subgroup of all permutations S_G on G, where for each $g \in G$, ρ_g is the map on G defined by right multiplication of g, i.e. $\rho(x) = xg$ for all $x \in G$. Hence, the permutation group G_R is the only transitive EPGC.

We summarize the above as follows.

Proposition 1 1 *A permutation group code is semiregular if and only if it is equidistance with the property that whose distance is equal to its length.*

2 *A permutation group code is equidistance and transitive if and only if it is regular. In particular, the distance is equal to its length.*

A semiregular permutation group code is acting on each of its orbits as a regular permutation group and so we focus our study to PGC which are non-semiregular.

Definition 2 We call a permutation group code $\mathcal{C}$ which is not semiregular with $\mathcal{F}(\mathcal{C}) = \varnothing$, a "non-trivial"permutation group code.

In the next section we shall see that the underlying group of a non-trivial equidistance permutation group code must be isomorphic to one of the following groups and each of the following groups can be isomorphic to a non-trivial EPGC.

(1) a p-group G with $H_p(G) := \langle x \in G \mid x^p \neq 1\rangle \neq G$ and $|G| > p$;
(2) a Frobenius group;
(3) a non p-group G such that $H_p(G) \neq G$ for some prime p;
(4) projective general linear group $PGL(2, p^h)$ of degree 2 over the field with p^h elements for some odd prime p and some integer $h > 0$;
(5) projective special linear group $PSL(2, p^h)$ of degree 2 over the field with p^h elements for some prime p and some integer $h > 0$;
(6) Suzuki group $Sz(2^{2h+1})$ for some integer $h > 0$.

Therefore what remains is to find all (if not possible at least some) of their non-trivial "equidistance"permutation representations of the above groups, that is, embeddings of these groups into symmetric groups such that their images will be EPGC. We shall do the latter for the classes (4), (5), (6) of above groups.

Our main result is the following.

Theorem 3 *Let $\mathcal{C}$ be a non-trivial EPGC with the fixity λ.*

(i) *If $\mathcal{C} \cong PSL(2, q)$, where $q \geq 4$ is a 2-power, then $\lambda \in \{\frac{q}{2}, \frac{q}{2} + 2, \ldots, q - 2, q, q + 1, q + 2, \ldots\}$.*
(ii) *If $\mathcal{C} \cong PSL(2, q)$, where $q = p^n > 4$ and p is an odd prime, then*

$$\lambda \in \{i \mid i \geq \frac{q(p-1)}{2p} \text{ and } i \text{ is an even integer}\}.$$

(iii) *If $\mathcal{C} \cong PGL(2, q)$, where $q = p^n > 4$ and p is an odd prime, then $\lambda \in \{\frac{q(p-1)}{p} + 2i \mid i \in \mathbb{N}\}$.*
(iv) *If $\mathcal{C} \cong Sz(q)$, where $q = 2^{2m+1} \geq 8$, then $\lambda \in \{q + 4i \mid i \in \mathbb{N}\}$.*

Moreover, if $\mathcal{C}$ is not isomorphic to any of groups (i)–(iv)*, then $\mathcal{C}$ satisfies one of the following conditions:*

(1) *$\mathcal{C}$ is a p-group with $H_p(\mathcal{C}) := \langle x \in \mathcal{C} \mid x^p \neq 1\rangle \neq \mathcal{C}$ and $|\mathcal{C}| > p$, for some prime p;*
(2) *$\mathcal{C}$ is a Frobenius group;*
(3) *$\mathcal{C}$ is not a p-group and $H_p(\mathcal{C}) \neq \mathcal{C}$, for some prime p.*

Remark 4 The proof of Theorem 3 gives a way of embedding into symmetric groups of the above groups for each given distance. We only mention "all" possible distances which can be occurred in the statement of the theorem.

The proof of Theorem 3 will be given in Sects. 2, 3, 4. In Sect. 5 non-trivial EPGCs of fixity 2 and minimum possible length are constructed where the underlying groups are isomorphic to the alternating groups of degree 4 and 5 and the symmetric group of degree 4. In Sect. 6 we study a combinatorial structure so-called generalized room squares related to equidistance permutation codes and we determine which generalized room squares are corresponding to EPGCs. We study the applications of EPGCs in Sect. 7, which is divided into two subsections. In Sect. 7.1, we discuss an approach to use EPGC to construct permutation codes whose set of distances between code words are small and in Sect. 7.2, we consider an important application of EPGCs in encoding process.

2 Preliminaries

Let G be a finite group. A set M is called a G-set if there is a map $\Phi : G \times M \to M$ (called an action), defined by $\Phi(g, m) \mapsto g \cdot m$, such that

(1) $1 \cdot m = m$ for all $m \in M$, where 1 denotes the unit element of G,
(2) $g_0 \cdot (g \cdot m) = (g_0 g) \cdot m$ for any $g, g_0 \in G$ and $m \in M$.

For each $g \in G$, we let $\mathrm{Fix}(g) := \{m \in M \mid g \cdot m = m\}$. Obviously, $[n]$ is a S_n-set and $\mathrm{Fix}(\sigma) = F(\sigma)$ for all $\sigma \in S_n$.

Definition 5 A group G is called of positive type in [17] if there exist a positive integer k and a G-set M with the following two properties:

(i) $|\mathrm{Fix}(g)| = k$ for all $g \in G \setminus \{1\}$,
(ii) $\cap_{g \in G} \mathrm{Fix}(g) = \varnothing$. (Such a G-set M is called to be of type k and also such a group G is called a group of type k on the G-set M.)

Definition 6 For any finite group G of positive type we denote by $\mathcal{K}(G)$ the set $\big\{k \in \mathbb{N} \,\big|\, G \text{ is of type } k\big\}$ and we let $t(G) := min\big(\mathcal{K}(G)\big)$.

Proposition 7 *If G is a group of positive type, then $\mathcal{K}(G)$ is closed under addition and multiplication.*

Proof If M_1 and M_2 are two G-sets of types k_1 and k_2, respectively, then it is easy to see that $M_1 \sqcup M_2$ (disjoint union of M_1 and M_2) and $M_1 \times M_2 := \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\}$ are G-sets of type $k_1 + k_2$ and $k_1 \cdot k_2$, respectively. This completes the proof. □

The following proposition shows the relation between a non-trivial EPGC and a group of positive type.

Proposition 8 *A finite group G is a group of positive type if and only if G is a non-trivial EPGC.*

Proof If G is a group of type k on G-set M, then it follows from properties (i) and (ii) of Definition 5 that G can be embedded to S_M by the map $\alpha : G \to S_M$, defined by $\alpha(g) : m \mapsto g \cdot m$ and so G is an EPGC of length $|M|$ such that $\mathcal{F}(G) = \varnothing$ and $|F(g)| = |\mathrm{Fix}(g)| = k$ for all non-trivial elements of G. Also if G is an EPGC of length n and distance $\lambda < n$ such that $\mathcal{F}(G) = \varnothing$, then clearly G is a group of type $n - \lambda$ on G-set $[n]$. This completes the proof. □

In view of Proposition 8, to study non-trivial EPGCs, it is sufficient to study groups of positive type. To study groups of positive type the concept of partition of a group appears.

Definition 9 A non-trivial partition of a group G is a set $\pi = \{H_1, \ldots, H_t\}$ of size $t > 1$ consisting of non-trivial subgroups H_i of G such that each non-trivial element of G belongs to exactly one subgroup H_i of π.

In [18], it is proved that a finite group G is of positive type if and only if G has a non-trivial partition. On the other hand, it follows from the series of the results of Baer [1], Kegel [19] and Suzuki [28] (see [32, p. 5]) that a group G has a non-trivial partition if and only if it satisfies one of the following conditions:

(1) G is a p-group with $H_p(G) := \langle x \in G \mid x^p \neq 1\rangle \neq G$ and $|G| > p$;

(2) G is a Frobenius group;
(3) G is not a p-group and $H_p(G) \neq G$ for some prime p;
(4) G is isomorphic with $PGL(2, p^h)$, p being an odd prime, $h > 0$;
(5) G is isomorphic with $PSL(2, p^h)$, p being a prime, $h > 0$;
(6) G is isomorphic with a Suzuki group $Sz(q)$; $q = 2^{2h+1}$, $h > 0$.

Therefore, if G is a non-trivial EPGC, then G must satisfy one of the above 6 conditions. In any of the above cases, by determining the set $\mathcal{K}(G)$, we can determine all possible positive values for λ such that G is an EPGC with $|F(\sigma)| = \lambda$ for all non-trivial $\sigma \in G$. In this paper, we determine $\mathcal{K}(G)$ when G satisfies the conditions (4), (5) and (6). To achieve the latter, we need some theorems and lemmas which are stated below.

In [17], Iwahori proved the following theorem:

Theorem 10 *A finite group G is of type k if and only if there exist subgroups $G_1, \ldots, G_r$ of G (not necessary distinct) such that*

(a) $G \neq G_i \neq \{1\}$ *for* $i = 1, \ldots, r$.
(b) $1^*_{G_1} + \cdots + 1^*_{G_r} = k \cdot 1^*_G + (r-k) \cdot 1^*_l$,

where $1^*_{G_i}$ means the character of G induced by the unit character 1_{G_i} of the subgroup G_i of G, i.e. $1^*_{G_i}(a) = \dfrac{|G|}{|G_i|} \cdot \dfrac{|a^G \cap G_i|}{|a^G|}$ where $a^G = \{g^{-1}ag \mid g \in G\}$, and also 1^*_l is the character of the regular representation of G, i.e. $1^*_l(a) = |G|$ if $a = 1$ and $1^*_l(a) = 0$ if $a \neq 1$.

Remark 11 By [18, Lemma 2], if H is a subgroup of a finite group G such that $H \cap H^x = H$ or $\{1\}$ for all $x \in G$, then for each $g \in G$, $1^*_H(g) = |N_G(H)|/|H|$ if $g^G \cap H \neq \varnothing$ and $1^*_H(g) = 0$ if $g^G \cap H = \varnothing$ (note that $H^x = \{x^{-1}hx \mid h \in H\}$ and $N_G(H)$ is the normalizer of H in G, i.e $N_G(H) = \{g \in G \mid H^g = H\}$).

Definition 12 A subgroup H of a finite group G is called special if $H \neq \{1\}$, $H \neq G$ and 1^*_H is constant on $C \setminus \{1\}$ for any cyclic subgroup C of G.

Remark 13 Let G be a finite group and assume that there exist subgroups $G_1, \ldots, G_r$ of G satisfying the conditions (a) and (b) of Theorem 10. Then by [17, Proposition 2.5], every G_i is a special subgroup of G. Moreover, in view of the proof of [17, Theorem II], if we let M be the disjoint union of the G-sets $G/G_i = \{xG_i \mid x \in G\}$ $(i = 1, \ldots, r)$, then M is a G-set of type k.

Lemma 14 *Let G be a finite group and let $C = \langle c \rangle$ be a cyclic subgroup of G such that*

(i) *For any $i \in \{1, \ldots, |C|\}$ either $|(c^i)^G \cap C| = |c^G \cap C|$ or $(c^i)^G \cap C = \{c^i, c^{-i}\}$,*
(ii) *$C \cap C^x = \{1\}$ or C for all $x \in G$.*

Then if H is a special subgroup of G, then either $C^x \leq H$ or $C^x \cap H = \{1\}$ for all $x \in G$.

Proof Let $|c^G \cap C| = t$. Since H is a special subgroup of G, we must have $1^*_H(c) = 1^*_H(c^i)$ for all $1 \leq i \leq |C| - 1$. Suppose for a contradiction that there exist $s \in \{2, \ldots, |C|-1\}$ and $x \in G$ such that $c^x \notin H$ and $\langle c^s \rangle^x \leq H$. Suppose firstly that $|(c^s)^G \cap C| = t$. Then the part (ii) of the assumption implies $|(c^s)^G| = t \cdot |\{C^g \mid g \in G\}| = |c^G|$. It is clear that $|c^G \cap H| < |(c^s)^G \cap H|$ and therefore

$$1^*_H(c) = \frac{|G|}{|H|} \cdot \frac{|c^G \cap H|}{|c^G|} < \frac{|G|}{|H|} \cdot \frac{|(c^s)^G \cap H|}{|(c^s)^G|} = 1^*_H(c^s),$$

that is a contradiction. Now suppose that $(c^s)^G \cap C = \{c^s, c^{-s}\}$. Then

$$1_H^*(c) = \frac{|G|}{|H|} \cdot \frac{|c^G \cap C||\{C^x \mid x \in G, C^x \leq H\}|}{|c^G \cap C||\{C^x \mid x \in G\}|}$$
$$< \frac{|G|}{|H|} \cdot \frac{|\{c^i, c^{-i}\}||\{\langle c^s \rangle^x \mid x \in G, \langle c^s \rangle^x \leq H\}|}{|\{c^i, c^{-i}\}||\{C^x \mid x \in G\}|} = 1_H^*(c^s),$$

that is a contradiction. This completes the proof. □

3 Equidistance actions of *PGL*(2, *q*) and *PSL*(2, *q*)

Let q be a prime power and let $X = GF(q) \cup \{\infty\}$. Then, the set of all mappings

$$\gamma : x \mapsto \frac{ax+b}{cx+d},$$

on X such that $a, b, c, d \in GF(q)$, $ad - bc \neq 0$ and $\gamma(\infty) = a/c$, $\gamma(-d/c) = \infty$ if $c \neq 0$, and $\gamma(\infty) = \infty$ if $c = 0$, is a group under composition of mappings called the projective general linear group of degree 2 over $GF(q)$ and is denoted by $PGL(2, q)$. We denote by $\left(\frac{a, \; b}{c, \; d}\right)$ such element $\gamma \in PGL(2, q)$. If we consider the mappings γ with $ad - bc = 1$, then we find another group called the projective special linear group of degree 2 over $GF(q)$ which is denoted by $PSL(2, q)$. It is well known that $|PGL(2, q)| = q(q^2 - 1)$, $|PSL(2, q)| = q(q^2 - 1)/d$, where $d = gcd(q - 1, 2)$, and $PGL(2, q) \cong PSL(2, q)$ if q is even. Hereafter, we let p be a prime, $q = p^n$ and $d = gcd(q - 1, 2)$.

Proposition 15 *Let $G = PGL(2, q)$ (resp. $PSL(2, q)$), where $q \geq 4$. Then*

- (i) *G possesses a cyclic subgroup A of order $q - 1$ (resp. $(q - 1)/d$) such that $N_G(A)$ is a dihedral group of order $2(q - 1)$ (resp. $2(q - 1)/d$).*
- (ii) *G possesses a cyclic subgroup B of order $q + 1$ (resp. $(q + 1)/d$) such that $N_G(B)$ is a dihedral group of order $2(q + 1)$ (resp. $2(q + 1)/d$).*
- (iii) *G possesses an elementary abelian p-group P of order q such that $N_G(P)$ is a Frobenius group with kernel P and complement A.*
- (iv) *The set $\{A^g, B^g, P^g \mid g \in G\}$ is a partition of G.*

Proof See [13, pp. 185–187 and pp. 191–193]. □

Theorem 16 *Let $G = PSL(2, q)$, where $q = 2^n$ and $n \geq 2$. Then*

$$\mathcal{K}(G) = \{\frac{q}{2}, \frac{q}{2} + 2, \ldots, q - 2, q, q + 1, q + 2, \ldots\}.$$

Proof Let $A = \langle a \rangle$, $B = \langle b \rangle$ and P be the subgroups of G introduced in Proposition 15 and let $D_1 = N_G(A)$, $D_2 = N_G(B)$ and $H = N_G(P)$. There are $q + 1$ conjugacy classes of G represented by the elements:

$$1, t, a, a^2, a^3, \ldots, a^{\frac{q-2}{2}}, b, b^2, b^3, \ldots, b^{\frac{q}{2}},$$

where $(a^i)^G \cap A = \{a^i, a^{-i}\}$, $(b^j)^G \cap B = \{b^j, b^{-j}\}$ for all $i \in \{1, \ldots, (q - 2)/2\}$ and $j \in \{1, \ldots, q/2\}$ and t is an element of order 2 of G. So by Lemma 14, if K is a special subgroup of G, then for all $x \in G$, either $K \cap T^x = \{1\}$ or T^x, where $T \in \{A, B\}$. Hence in view of the structure of subgroups of G (see [20, Theorem 1.2]), it can be seen that the special subgroups of G are as follows: A and its conjugates; B and its conjugates; D_1 and its conjugates; D_2 and its conjugates; H and its conjugates; elementrary abelian 2-groups P^i of order 2^i and their conjugates, where $1 \leq i \leq n$ and $P^n = P$. It follows from Remark 11 that $1_T^*(g) = |N_G(T)|/|T|$ if $g^G \cap T \neq \varnothing$ and $1_T^*(g) = 0$ if $g^G \cap T = \varnothing$ for any $g \in G \setminus \{1\}$ and $T \in \{A, B, P\}$. Before going on, let us state two points. First, since $|y^G \cap K| = |y^G \cap K^x|$ for any subgroup K of G and $x, y \in G$, $1_K^*(y) = 1_{K^x}^*(y)$. Second, recall that if R is a subgroup of a finite group G, then $|\{R^g \mid g \in G\}| = \frac{|G|}{|N_G(R)|}$. Since H is a Frobenius group with kernel P and complement A, H is of the order $q(q-1)$ and H is the union of subgroup P and exactly q conjugates of A. Hence $H \cap B^x = \{1\}$, for all $x \in G$, implies $1_H^*(b^j) = 0$ for all $j \in \{1, \ldots, q/2\}$, $|(a^j)^G \cap H| = 2q$ implies $1_H^*(a^j) = 2$ for all $j \in \{1, \ldots, (q-2)/2\}$ and $|t^G \cap H| = q - 1$ implies $1_H^*(t) = 1$. Since $D_1 = N_G(A)$ (resp. $D_2 = N_G(B)$) is a dihedral group of order $2(q-1)$ (resp. $2(q+1)$), D_1 (resp. D_2) is the union of A (resp. B) and $q - 1$ (resp. $q + 1$) elements of order 2 and therefore $1_{D_1}^*(b^j) = 0$ for all $j \in \{1, \ldots, q/2\}$ (resp. $1_{D_2}^*(a^i) = 0$ for all $i \in \{1, \ldots, (q-2)/2\}$), $1_{D_1}^*(a^j) = 1$ for all $j \in \{1, \ldots, (q-2)/2\}$ (resp. $1_{D_2}^*(b^j) = 1$ for all $j \in \{1, \ldots, q/2\}$) and $1_{D_1}^*(t) = q/2$ (resp. $1_{D_2}^*(t) = q/2$). It is clear that since P^i, $1 \leq i \leq n$, contains only $2^i - 1$ elements of order 2, $1_{P^i}^*(t) = \dfrac{q(2^i-1)}{2^i}$ and $1_{P^i}^*(t') = 0$ for any element t' of order greater than 2 of G. Obviously, $1_T^*(1) = |G|/|T|$ for all subgroups T of G. Table 1 depicts the characters of G induced by the unit characters of special subgroups of G, where $1 \leq r \leq (q-2)/2$, $1 \leq s \leq q/2$ and $1 \leq i \leq n$.

From Table 1 we get immediately that

$$(\frac{q}{4} - \frac{j}{2})1_A^* + (\frac{q}{4} + \frac{j}{2})1_B^* + j1_H^* + 1_{P^1}^* = (\frac{q}{2} + j)1_G^* + 1_l^*, \tag{3.1}$$

where $j \leq q/2$ is an even number and

$$(\frac{q-j-1}{2})1_A^* + (\frac{q+j-1}{2})1_B^* + 1_{D_1}^* + 1_{D_2}^* + j1_H^* = (q+j)1_G^* + 1_l^*, \tag{3.2}$$

where $j \leq q - 1$ is an odd number. Now, Theorem 10 and Proposition 7 imply that

$$\{\frac{q}{2}, \frac{q}{2} + 2, \ldots, q-2, q, q+1, q+2, \ldots\} \subseteq \mathcal{K}(G).$$

It follows from Theorem 10 that if $k \in \mathcal{K}(G)$, then there exist

$$x_1, x_2, \ldots, x_5, x_{6,1}, \ldots, x_{6,n} \in \mathbb{Z}^+$$

such that

$$\begin{cases} 2x_2 + x_3 = k \\ 2x_1 + x_4 + 2x_5 = k \\ \frac{q}{2}x_3 + \frac{q}{2}x_4 + x_5 + \sum_{i=1}^{n}(q - 2^{n-i})x_{6,i} = k \end{cases}. \tag{3.3}$$

So $k < \dfrac{q}{2}$ implies $x_3 = x_4 = x_{6,1} = \cdots = x_{6,n} = 0$ and $x_5 = k$. Then $2x_1 + 2k = k$ which leads to a contradiction. Also, if k is odd, then it follows from system of relations 3.3 that $x_3 \neq 0$ and $x_4 \neq 0$ and therefore $k \geq q+1$. So $\mathcal{K}(G) \subseteq \{\frac{q}{2}, \frac{q}{2}+2, \ldots, q-2, q, q+1, q+2, \ldots\}$ and this completes the proof. □

Theorem 17 *Let $G = PSL(2, q)$, where $q = p^n > 4$ and $p \neq 2$. Then*

$$\mathcal{K}(G) = \{i \geq \frac{q(p-1)}{2p} \mid i \text{ is an even number}\}.$$

Table 1 Characters of $G = PSL(2, q)$, where q is even, induced by the unit characters of special subgroups of G

	1	t	a^r	b^s
1_A^*	$q(q+1)$	0	2	0
1_B^*	$q(q-1)$	0	0	2
$1_{D_1}^*$	$\frac{q(q+1)}{2}$	$\frac{q}{2}$	1	0
$1_{D_2}^*$	$\frac{q(q-1)}{2}$	$\frac{q}{2}$	0	1
1_H^*	$q+1$	1	2	0
$1_{P^i}^*$	$\frac{q(q^2-1)}{2^i}$	$\frac{q(2^i-1)}{2^i}$	0	0

Proof Let $A = \langle a \rangle$, $B = \langle b \rangle$ and P be the subgroups of G introduced in Proposition 15 and let $D_1 = N_G(A)$, $D_2 = N_G(B)$ and $H = N_G(P)$. Also, let $t' = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}$ and $\tilde{t} = \begin{pmatrix} 1, & \mu \\ 0, & 1 \end{pmatrix}$ be two elements of order p in G, where μ is a generator of the multiplicative group $GF(q)^\times$. If $q \equiv 1(\bmod 4)$, then there are $\dfrac{q+5}{2}$ conjugacy classes of G represented by the elements:

$$1, \tilde{t}, t', a, a^2, a^3, \ldots, a^{\frac{q-1}{4}}, b, b^2, b^3, \ldots, b^{\frac{q-1}{4}},$$

and if $q \equiv 3(\bmod 4)$, then there are $\dfrac{q+5}{2}$ conjugacy classes of G represented by the elements:

$$1, \tilde{t}, t', a, a^2, a^3, \ldots, a^{\frac{q-3}{4}}, b, b^2, b^3, \ldots, b^{\frac{q+1}{4}},$$

where $(a^i)^G \cap A = \{a^i, a^{-i}\}$, $(b^j)^G \cap B = \{b^j, b^{-j}\}$, $|(t')^G \cap P| = |(\tilde{t})^G \cap P| = (q-1)/2$ for all $i \in \{1, \ldots, (q-1)/4\}$ and $j \in \{1, \ldots, (q-1)/4\}$ if $q \equiv 1(\bmod 4)$ and for all $i \in \{1, \ldots, (q-3)/4\}$ and $j \in \{1, \ldots, (q+1)/4\}$ if $q \equiv 3(\bmod 4)$. Note that if $q \equiv 1(\bmod 4)$ (resp. $q \equiv 3(\bmod 4)$), then $\{g \in G \mid g^2 = 1\} = (a^{\frac{q-1}{4}})^G$ (resp. $= (b^{\frac{q+1}{4}})^G$). Therefore, since in both of the cases $q \equiv 1(\bmod 4)$ and $q \equiv 3(\bmod 4)$ the cyclic subgroups A and B satisfy Lemma 14, dihedral groups $N_G(A)$ and $N_G(B)$ can not be the special subgroups of G. By the same argument as in the proof of Theorem 16 and by the structure of the subgroups of G (see [20, Theorem 1.2]) we determine all of the special subgroups of G and the characters of G induced by the unit character of all of them. The special subgroups of G are as follows: A and its conjugates; B and its conjugates; H and its conjugates; elementrary abelian p-groups P^i of order p^i and their conjugates, where $1 \leq i \leq n$ and $P^n = P$. Suppose first that n is an odd number. In view of [28, p. 263], if n is an odd number, then $p-1$ non-trivial elements of a cyclic subgroup of order p of G belong half to one and half to the other set of conjugacy classes of G represented by the elements $\tilde{t}$ and t'. So $|(t')^G \cap P^i| = |(\tilde{t})^G \cap P^i| = \dfrac{p^i - 1}{2}$ for all $1 \leq i \leq n$. Table 2 shows the characters of G induced by the unit characters of special subgroups of G, where n is an odd number, $1 \leq i \leq n$, $s \in \{1, \ldots, (q-1)/4\}$, $j \in \{1, \ldots, (q-1)/4\}$ and $s \in \{1, \ldots, (q+1)/4\}$, $j \in \{1, \ldots, (q-3)/4\}$ if $q \equiv 1(\bmod 4)$ and $q \equiv 3(\bmod 4)$, respectively.

From Table 2 we get immediately that

$$(\frac{m}{2} - r)1_A^* + \frac{m}{2}1_B^* + r1_H^* + 1_{P^1}^* = m1_G^* + 1_I^*, \tag{3.4}$$

Table 2 Characters of $G = PSL(2, q)$, where $q > 4$ is odd, induced by the unit characters of special subgroups of G

	1	t'	$\tilde{t}$	a^j	b^s
1_A^*	$q(q+1)$	0	0	2	0
1_B^*	$q(q-1)$	0	0	0	2
1_H^*	$q+1$	1	1	2	0
$1_{P^i}^*$	$\frac{q(q^2-1)}{2p^i}$	$\frac{q(p^i-1)}{2p^i}$	$\frac{q(p^i-1)}{2p^i}$	0	0

where $m = \dfrac{q(p-1)}{2p} + r$, $r \in \mathbb{Z}^+$ and m is even. So $\{i \geq \dfrac{q(p-1)}{2p} \mid i$ is an even number$\}$ $\subseteq \mathcal{K}(G)$. On the other hand, Theorem 10 implies that if $k \in \mathcal{K}(G)$, then there exist $x_1, x_2, x_3, x_{4,1}, \ldots, x_{4,n} \in \mathbb{Z}^+$ such that

$$\begin{cases} 2x_2 = k \\ 2x_1 + 2x_3 = k \\ x_3 + \sum_{i=1}^{n} \dfrac{q(p^i-1)}{2p^i} x_{4,i} = k \end{cases}. \tag{3.5}$$

Therefore k is an even number and also if $k < \dfrac{q(p-1)}{2p}$, then $x_{4,i} = 0$ for all $i \in \{1, \ldots, n\}$ and so $2x_1 + 2k = k$ which leads to a contradiction. So $t(G) = \dfrac{q(p-1)}{2p}$ and $\mathcal{K}(G) = \{i \geq \dfrac{q(p-1)}{2p} \mid i$ is even $\}$. Now suppose that n is even. In this case 1_A^*, 1_B^* and 1_H^* have the same values as the case n is odd. In view of [28, p. 263], in this case all $p-1$ non-trivial elements of a cyclic subgroup of order p of G belong to the same set of the conjugacy classes of G represented by the elements $\tilde{t}$ or t'. Therefore by the same argument as the case n is odd and since in this case $min\{1_{P^i}^*(t'), 1_{P^i}^*(\tilde{t}) \mid 1 \leq i \leq n\} \geq \dfrac{q(p^2-1)}{2p^2}$, it can be seen that $t(G) \geq \dfrac{q(p^2-1)}{2p^2}$ and if $k \in \mathcal{K}(G)$, then k is an even number. Hence $\mathcal{K}(G) \subseteq \{i \geq \dfrac{q(p-1)}{2p} \mid i$ is even$\}$ and this completes the proof. □

Theorem 18 *Let $G = PGL(2, q)$, where $q = p^n > 4$ and $p \neq 2$. Then $\mathcal{K}(G) = \{\dfrac{q(p-1)}{p} + 2i \mid i \in \mathbb{Z}^+\}$.*

Proof Let $A = \langle a \rangle$, $B = \langle b \rangle$ and P be the subgroups of G introduced in Proposition 15 and let $H = N_G(P)$. There are $q+2$ conjugacy classes of G represented by the elements:

$$1, t, a, a^2, a^3, \ldots, a^{\frac{q-1}{2}}, b, b^2, b^3, \ldots, b^{\frac{q+1}{2}},$$

where t is an element of order 2 of G, $|t^G \cap P| = q-1$, $(a^i)^G \cap A = \{a^i, a^{-i}\}$, $(b^j)^G \cap B = \{b^j, b^{-j}\}$ for all $i \in \{1, \ldots, (q-1)/2\}$ and $j \in \{1, \ldots, (q+1)/2\}$. So, the cyclic subgroups A and B satisfy Lemma 14 and therefore in view of the structure of the subgroups of G (see [2, Theorem 2]), it can be seen that the special subgroups of G are as follows: A and its conjugates; B and its conjugates; H and its conjugates; elementrary abelian p-groups P^i of order p^i and their conjugates, where $1 \leq i \leq n$ and $P^n = P$. Table 3 depicts the

Table 3 Characters of $G = PGL(2, q)$, where $q > 4$ is odd, induced by the unit characters of special subgroups of G

	1	t	a^j	b^s
1_A^*	$q(q+1)$	0	2	0
1_B^*	$q(q-1)$	0	0	2
1_H^*	$q+1$	1	2	0
$1_{P^i}^*$	$\frac{q(q^2-1)}{p^i}$	$\frac{q(p^i-1)}{p^i}$	0	0

characters of G induced by the unit characters of the special subgroups of G, where q is odd, $s \in \{1, \ldots, (q-1)/2\}$ and $j \in \{1, \ldots, (q+1)/2\}$.

It follows from Table 3 that

$$(\frac{m}{2} - i)1_A^* + \frac{m}{2}1_B^* + i1_H^* + 1_{P^1}^* = m1_G^* + 1_l^*, \tag{3.6}$$

where $m = \dfrac{q(p-1)}{p} + i$ and i is an even positive integer. Hence $\{\dfrac{q(p-1)}{p} + 2i \mid i \in \mathbb{Z}^+\} \subseteq \mathcal{K}(G)$. On the other hand by the same argument as in the proof of Theorem 17, it can be seen that if $k \in \mathcal{K}(G)$, then k is an even number and $k \geq \dfrac{q(p-1)}{p}$ and therefore $\mathcal{K}(G) = \{\dfrac{q(p-1)}{p} + 2i \mid i \in \mathbb{Z}^+\}$. This completes the proof. □

4 Equidistance actions of Suzuki groups

Let $q = 2^{2m+1} \geq 8$ and let π be the unique automorphism of the field $GF(q)$ with $\pi^2 x = x^2$ for all $x \in GF(q)$. Then Suzuki groups $Sz(q) := \left\langle S(a, b), M(\lambda), T \mid a, b \in GF(q), \lambda \in GF(q)^\times \right\rangle$, where

$$S(a,b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi a & 1 & 0 \\ a^2(\pi a) + ab + \pi b & a(\pi a) + b & a & 1 \end{pmatrix},$$

$$M(\lambda) := \begin{pmatrix} \lambda^{1+2^m} & 0 & 0 & 0 \\ 0 & \lambda^{2^m} & 0 & 0 \\ 0 & 0 & \lambda^{-2^m} & 0 \\ 0 & 0 & 0 & \lambda^{-(1+2^m)} \end{pmatrix}$$

and $T := \begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \end{pmatrix}$ (see [11, p. 3]). It is well known that $|Sz(q)| = q^2(q^2+1)(q-1)$.

Proposition 19 *Let $q = 2^{2m+1} \geq 8$ and $G = Sz(q)$. Then*

(i) *$K := \{M(\lambda) \mid \lambda \in GF(q)^\times\}$ is a cyclic subgroup of order $q-1$ of G. Moreover, $N_G(K)$ is a dihedral group of order $2(q-1)$.*

(ii) $Q := \{S(a,b) \mid a, b \in GF(q)\}$ *is a* 2*-subgroup of order* q^2 *and exponent* 4 *of* G. *Moreover,* $N_G(Q)$ *is a Frobenius group with kernel* Q *and complement* K. *We note that* Q *is a suzuki* 2*-group (see* [12]*) and the center of* Q *(denoted* $Z(Q)$*) is an elementary abelian* 2*-group of order* q.

(iii) G *possesses cyclic subgroups* U_1 *and* U_2 *of orders* $q+\sqrt{2q}+1$ *and* $q-\sqrt{2q}+1$*, respectively. Moreover,* $N_G(U_i)$*, for* $i \in \{1,2\}$*, is a Frobenius group with kernel* U_i *and complement* $\langle t_i \rangle$*, where* t_i *is an element of order* 4 *such that* $u^{t_i} = u^q$ *for all* $u \in U_i$*, and if* $u_i \in U_i$*, then* $C_G(u_i) = U_i$.

(iv) *The set* $\{U_1^x, U_2^x, K^x, Q^x \mid x \in G\}$ *is a partition of* G.

(v) *The maximal subgroups of* G *are as follows:* $N_G(Q)$*,* $N_G(K)$*,* $N_G(U_1)$*,* $N_G(U_2)$ *and* $Sz(s)$ *for maximal* s *such that* $s^t = q$ *for some positive integer* $t > 1$*, and their conjugates.*

Proof See [11, Theorem 4.1], [14, Lemma 3.1 and Theorem 3.10] and [21, Theorem 4.12]. □

Theorem 20 *Let* $q = 2^{2m+1} \geq 8$ *and* $G = Sz(q)$. *Then* $\mathcal{K}(G) = \{q+4i \mid i \in \mathbb{Z}^+\}$.

Proof Let $K = \langle k \rangle$, $U_1 = \langle u_1 \rangle$, $U_2 = \langle u_2 \rangle$ and Q be the introduced subgroups in Proposition 20. Let $\rho = S(1,0)$, $\rho^{-1} = S(1,1)$ and $\sigma = S(0,1)$ be three elements of G of orders 4, 4 and 2, respectively. There exist $\{i_2, \ldots, i_{t_1}\} \subset \{2, \ldots, q+\sqrt{2q}\}$ and $\{j_2, \ldots, j_{t_2}\} \subset \{2, \ldots, q-\sqrt{2q}\}$, where $t_1 = \dfrac{q+\sqrt{2q}}{4}$ and $t_2 = \dfrac{q-\sqrt{2q}}{4}$, such that the $q+3$ conjugacy classes of G represented by the elements:

$$1, \rho, \sigma, \rho^{-1}, u_1, {u_1}^{i_2}, \ldots, {u_1}^{i_{t_1}}, u_2, {u_2}^{j_2}, \ldots, {u_2}^{j_{t_2}}, k, k^2, k^3, \ldots, k^{\frac{q-2}{2}},$$

where $|({u_1}^t)^G \cap U_1| = |({u_2}^{t'})^G \cap U_2| = 4$, $(k^s)^G \cap K = \{k^s, k^{-s}\}$, $|\sigma^G \cap Q| = q-1$ and $|\rho^G \cap Q| = |(\rho^{-1})^G \cap Q| = \dfrac{q^2-q}{2}$ for all $t \in \{1, \ldots, q+\sqrt{2q}\}$, $t' \in \{1, \ldots, q-\sqrt{2q}\}$ and $s \in \{1, \ldots, q-2\}$. So by Lemma 14, if H is a special subgroup of G and $T \in \{U_1, U_2, K\}$, then $H \cap T^x = \{1\}$ or T^x for all $x \in G$. We note that since $\langle \rho \rangle$ is a cyclic subgroup of order 4 of G, if H is a special subgroup of G, then we must have $1_H^*(\rho) = 1_H^*(\rho^{-1}) = 1_H^*(\sigma)$. According to Remark 11 and part (iv) of Proposition 19, the subgroups U_1, U_2, K, Q and their conjugates are the special subgroups of G. It follows from the part (ii) of Proposition 19 that $Q' = N_G(Q)$ is the union of Q and exactly q^2 conjugates of K. Hence $1_{Q'}^*(a) = 0$, where $a \in U_1$ or U_2, and also $1_{Q'}^*(k^i) = \dfrac{q^2(q^2+1)(q-1)}{q^2(q-1)} \cdot \dfrac{2q^2}{q^2(q^2+1)} = 2$ for all $i \in \{1, \ldots, q-2\}$, $1_{Q'}^*(\sigma) = \dfrac{q^2(q^2+1)(q-1)}{q^2(q-1)} \cdot \dfrac{q-1}{(q-1)(q^2+1)} = 1$ and

$$1_{Q'}^*(\rho) = 1_{Q'}^*(\rho^{-1}) = \frac{q^2(q^2+1)(q-1)}{q^2(q-1)} \cdot \frac{\frac{q^2-q}{2}}{\frac{q^2-q}{2}(q^2+1)} = 1.$$

Therefore Q' is a special subgroup of G. Table 4 depicts the characters of G induced by the unit characters of the special subgroups of G introduced above, where $t \in \{1, \ldots, \dfrac{q+\sqrt{2q}}{4}\}$, $s \in \{1, \ldots, \dfrac{q-\sqrt{2q}}{4}\}$, $i_1 = j_1 = 1$ and $l \in \{1, \ldots, (q-2)/2\}$.

From Table 4 we get immediately that

$$\left(\frac{q-1+i}{4}\right)1_{U_1}^* + \left(\frac{q-1+i}{4}\right)1_{U_2}^* + 1_Q^* + \left(\frac{q-1-i}{2}\right)1_K^* + i\,1_{Q'}^* = (q-1+i)1_G^* + 1_I^*, \quad (4.1)$$

Table 4 Characters of $G = Sz(q)$, where $q = 2^{2m+1} \geq 8$, induced by the unit characters of special subgroups of G

	1	ρ	σ	ρ^{-1}	$u_1^{i_t}$	$u_2^{j_s}$	k^l
$1_{U_1}^*$	$q^2(q-1)(q-\sqrt{2q}+1)$	0	0	0	4	0	0
$1_{U_2}^*$	$q^2(q-1)(q+\sqrt{2q}+1)$	0	0	0	0	4	0
1_{Q}^*	$(q^2+1)(q-1)$	$q-1$	$q-1$	$q-1$	0	0	0
1_{K}^*	$q^2(q^2+1)$	0	0	0	0	0	2
$1_{Q'}^*$	q^2+1	1	1	1	0	0	2

where $i \in \mathbb{N}$. Hence $\{q+4i \mid i \in \mathbb{Z}^+\} \subseteq \mathcal{K}(G)$. To prove the latter inclusion is an equality, it is sufficient to prove that $t(G) = q$ and any element of $\mathcal{K}(G)$ is a multiple of 4. Let us show that if H is a special subgroup of G such that $H \cap \{U_1^x \mid x \in G\} \neq \varnothing$, then $H \in \{U_1^x \mid x \in G\}$. Suppose for a contradiction that $H \notin \{U_1^x \mid x \in G\}$ and U_1 and some conjugates of it are contained in H. The fact that every subgroup of a finite group is contained in a maximal subgroup implies there exists maximal subgroup M such that $H \leq M$. Since $|U_1|\big||M|$, it follows from part (v) of Proposition 19 that $M = N_G(U_1)$. Hence either $|H| = 2(q+\sqrt{2q}+1)$ or $H = M$. If $|H| = 2(q+\sqrt{2q}+1)$, then since $2\big||H|$ and $4 \nmid |H|$, it follows that $1_H^*(\sigma) \neq 0$ and $1_H^*(\rho) = 0$ that is a contradiction. Suppose that $H = N_G(U_1)$. So in view of the part (iii) of Proposition 19, H is the union of U_1 and exactly $q+\sqrt{2q}+1$ conjugates of $\langle t_1 \rangle$ such that the intersection of any two of such conjugates is equal to $\{1\}$. Therefore $1_H^*(\sigma) = \dfrac{q^2(q^2+1)(q-1)}{4(q+\sqrt{2q}+1)} \cdot \dfrac{q+\sqrt{2q}+1}{(q-1)(q^2+1)} = \dfrac{q^2}{4}$ and $1_H^*(\rho) = \dfrac{q^2(q^2+1)(q-1)}{4(q+\sqrt{2q}+1)} \cdot \dfrac{q+\sqrt{2q}+1}{\frac{(q^2-q)}{2}(q^2+1)} = \dfrac{q}{2}$ and so $1_H^*(\rho) \neq 1_H^*(\sigma)$ that is a contradiction. Hence, if $k_0 \in \mathcal{K}(G)$, then it follows from Table 4, Theorem 10 and above discussion that $4x_{U_1} = k_0$, where x_{U_1} is the number of existence of the subgroup U_1 and its conjugates belong to special subgroups $G_1, \ldots, G_r$ of Theorem 10. Therefore k_0 is a multiple of 4. Now suppose that H is a special subgroup of G such that $H \subset \cup_{x \in G} Q^x$ and $H \notin \{Q^x \mid x \in G\}$. It is clear that all non-trivial elements of H are of orders 2 and 4 and so $|H|\big|q^2$. Let $|H| = 2^i$ and let x and y be the number of elements of orders 2 and 4 in H, respectively. Hence $x + y + 1 = 2^i$. Obviously y elements of order 4 in H belong half to the conjugacy class represented by ρ and half to the conjugacy class represented by ρ^{-1}. So $1_H^*(\sigma) = \dfrac{|G|}{|H|} \cdot \dfrac{x}{(q-1)(q^2+1)}$ and $1_H^*(\rho) = \dfrac{|G|}{|H|} \cdot \dfrac{\frac{y}{2}}{\frac{q^2-q}{2}(q^2+1)}$. Since H is a special subgroup, we must have $1_H^*(\rho) = 1_H^*(\sigma)$ and therefore $qx = y$. Hence $x(1+q) = 2^i - 1$ and so $q^2 > 2^i > q$. Note that if $2^i = q^2$ then $x = q-1$ and $y = q^2 - q$ and $1_H^*(g) = 1_Q^*(g)$ for all $g \in G$. Let $2^i/q = 2^j$. So $q(2^j - x) = x+1$ which leads to a contradiction. Therefore if H is a special subgroup of G such that $H \subset \cup_{x \in G} Q^x$, then $H \in \{Q^x \mid x \in G\}$. Now suppose that H is a special subgroup of G containing Q and some conjugates of it. Let M be the maximal subgroup of G containing H. Since $q^2\big||M|$, it follows from the part (v) of Proposition 19 that $M = N_G(Q)$. So the part (ii) of Proposition 19 implies M is the union of Q and exactly q^2 conjugates of K. By the same argument as above, it can be seen that $Q \cap H = \{1\}$ or Q. If $Q \cap H = \{1\}$, then clearly $1_H^*(\sigma) = 1_H^*(\rho) = 1_H^*(\rho^{-1}) = 0$ and if $Q \cap H = Q$ and $H \neq Q$, then we must have $H = M$. Hence, if $k_0 \in \mathcal{K}(G)$, then it follows from Table 4, Theorem

10 and above discussion that $(q-1)x_Q + x_{Q'} = k_0$, where x_Q (resp. $x_{Q'}$) is the number of existence of the subgroup Q (resp. Q') and its conjugates belong to $G_1, \ldots, G_r$ of Theorem 10. Now if $x_Q = 0$, then $x_{Q'} = k_0$. Hence if $\mathcal{H} = \{H < G \mid H \text{ is a special subgroup of } G\}$ and $\mathcal{H}' = \mathcal{H} \setminus \{Q'\}$, then Table 4 and Theorem 10 imply $\sum_{H' \in \mathcal{H}'} x_{H'} 1^*_{H'}(k) = -k_0$, where $x_{H'}$ is the number of existence of the subgroup H' and its conjugates belong to the special subgroups $G_1, \ldots, G_r$ of Theorem 10, that is a contradiction. Therefore $x_Q \neq 0$ and so $k_0 \geq q-1$. Now since k_0 must be a multiple of 4 and $q \in \mathcal{K}(G)$, $t(G) = q$ and this completes the proof. □

Proof of Theorem 3 The result follows from the series of the results of Baer [1], Kegel [19] and Suzuki [28] (see page 3) and Theorems 16, 17, 18 and 20. □

5 Non-trivial equidistance actions of some groups of fixity 2

It is proved in [17, Theorem III] the only non-trivial EPGC with fixity 2 must be isomorphic to one the following groups:

1 alternating group A_4 of degree 4;
2 symmetric group S_4;
3 alternating group $A_5 \cong PSL(2,5)$ of degree 5;
4 a finite group G having a normal abelian subgroup A and an element $x \notin A$ such that the Sylow 2-subgroup of A is cyclic, $x^{-1}ax = a^{-1}$ for all $a \in A$, the order of x is 2 and $G = A\langle x \rangle$.

In the following, using Remark 13, we exhibit some equidistance permutation representations of groups A_4, S_4 and A_5 of fixity 2 with the minimum possible length 14, 26 and 62 respectively.

(1)

$$A_4 \cong \langle (2,10,4)(3,6,7)(5,11,13)(8,12,9), (1,5)(2,4)(6,9)(7,8)(10,14)(11,13) \rangle \leq S_{14}$$

(2)

$$\begin{aligned} S_4 \cong \langle &(1,18,20,3)(2,10,19,12)(4,21,23,6)(5,13,22,14)(7,24,26,9)(8,15,25,17), \\ &(1,26)(2,23)(3,20)(4,25)(5,22)(6,19)(7,24)(8,21)(9,18)(10,17)(11,14)(13,16) \rangle \leq S_{26} \end{aligned}$$

(3)

$$\begin{aligned} A_5 \cong \langle &(1,44,36,33,45)(2,38,52,27,18)(3,21,28,51,37)(4,16,29,53,39)(5,42,56,30,12), \\ &(6,14,22,50,46)(7,59,15,35,23)(8,24,34,10,58)(9,43,47,25,13)(11,40,62,32,54), \\ &(17,55,31,61,41)(26,49,57,60,48), (1,48,9,8,47)(2,21,20,3,52)(4,16,41,42,17), \\ &(5,56,61,62,55)(6,35,57,24,13), (7,14,25,58,36)(10,34,49,50,33)(11,30,12,54,53), \\ &(15,59,44,43,60), (18,19,27,37,28)(22,23,46,26,45)(29,39,32,31,40) \rangle \leq S_{62} \end{aligned}$$

6 Generalized room squares corresponding to EPGCs

One of the interesting classes of combinatorial designs which plays an important role in the study of EPCs is Generalized Room square.

Let X be a set of cardinality υ. A generalized Room square (GRS) of side r and index λ defined on X is an $r \times r$ array F having the following properties:

1. every cell of F contains a subset (possibly empty) of X,

2. each symbol of X occurs once in each row and column of F, and
3. any two distinct symbols of X occur together in exactly λ cells of F.

Denote such a GRS by $S(r, \lambda; \upsilon)$.

In [5], it is proved that the existence of any one of $S(r, \lambda; \upsilon)$ or EP (r, υ, λ) code implies the existence of the other. The following remark explains how to construct the GRS corresponding to an EPC.

Remark 21 Suppose that $\mathcal{C}$ is an EP (r, υ, λ) code and $\mathcal{C} = \{c_1, \ldots, c_\upsilon\}$. Let $X := \{x_1, \ldots, x_\upsilon\}$ and $I_{i,j} := \{h \in \{1, \ldots, \upsilon\} \mid c_h(i) = j\}$ for all $(i, j) \in \{1, \ldots r\} \times \{1, \ldots, r\}$. Let F be an $r \times r$ array such that for each $(i, j) \in \{1, \ldots r\} \times \{1, \ldots, r\}$, the (i, j)th cell of F contains the subset $X_{i,j} := \{x_h \mid h \in I_{i,j}\}$ of X. Then it is easy to see that F is an $S(r, \lambda; \upsilon)$.

In the sequel, we consider the properties of the GRS F introduced in Remark 21, where $\mathcal{C}$ is an EPGC.

Proposition 22 *Let $\mathcal{C}$ be an EPGC of length r and let F be the GRS corresponding to $\mathcal{C}$. Then for all $i, j \in \{1, \ldots r\}$*

(i) *if $j \notin \mathcal{O}(i)$, then the (i, j)th cell of F is entry.*
(ii) *if $j \in \mathcal{O}(i)$, then the (i, j)th cell of F contains a subset of size $|\mathcal{C}_i|$ (where $\mathcal{C}_i$ is the stabilizer of i, i.e. $\mathcal{C}_i := \{\alpha \in \mathcal{C} \mid \alpha(i) = i\}$).*

Proof Let $\mathcal{C}$ be an EPG (r, υ, λ) code. We follow the defnitions and notations as in Remark 21. If $j \notin \mathcal{O}(i)$, then clearly $I_{i,j} = \varnothing$ and therefore the (i, j)th cell of F is entry. Suppose that $j \in \mathcal{O}(i)$ and $\mathcal{C}_i = \{c_{e_1} = 1, c_{e_2}, \ldots, c_{e_n}\}$. Since $j \in \mathcal{O}(i)$, there exists $\alpha \in \mathcal{C}$ such that $\alpha(i) = j$. So $\alpha c_{e_t}(i) = j$ for all $t \in \{1, \ldots, n\}$. Now suppose that there is $\beta \in \mathcal{C} \setminus \{\alpha\}$ such that $\beta(i) = j$. Hence $\alpha^{-1}\beta(i) = i$ and therefore $\alpha^{-1}\beta \in \mathcal{C}_i$ which implies $\beta \in \alpha\mathcal{C}_i$. Hence if $\alpha\mathcal{C}_i = \{c_{s_1}, \ldots, c_{s_n}\}$, then $I_{i,j} = \{s_1, \ldots, s_n\}$ and so the (i, j)th cell of F contains a subset of size $|\mathcal{C}_i|$. This completes the proof. □

Remark 23 Let $\mathcal{C}$ be an EPG (r, υ, λ) code and let F be the introduced GRS in Remark 21.

(i) If $\mathcal{C}$ is transitive, then we must have $\lambda = 0$ and therefore $\mathcal{C}_i = \{1\}$ for all $i \in \{1, \ldots, r\}$. So Proposition 22 implies that F is a Latin square of order r (i.e. is an $r \times r$ array defined on the set X with every element of X occurring precisely once in each row and column) such that the main diagonal cells of F contain the same element of X.
(ii) Proposition 22 implies that all of the non-empty cells of a row of F contain subsets of X with the same size.
(iii) According to this fact that the stabilizers of elements in the same $\mathcal{C}$-orbit are conjugate and in view of Proposition 22, if $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_s$ are all $\mathcal{C}$-orbits, then by swapping the rows and columns of F, F can be convert to the following GRS, where $A_i, i \in \{1, \ldots, s\}$, is an $|\mathcal{O}_i| \times |\mathcal{O}_i|$ array such that all its cells contain subsets with the same size $\frac{|\mathcal{C}|}{|\mathcal{O}_i|}$ (note that by Orbit-Stabilizer Theorem, $|\mathcal{O}(j)| \cdot |\mathcal{C}_j| = |\mathcal{C}|$ for all $j \in \{1, \ldots, r\}$) and for each $i \neq j$, the $(\mathcal{O}_i, \mathcal{O}_j)$th cell of F is an $|\mathcal{O}_i| \times |\mathcal{O}_j|$ array such that all its cells are empty. Table 5 shows GRS corresponding to an EPGC.

7 Applications for EPGCs

We divide this section into two subsections. In the first one, we explore some potential applications of EPGCs in the construction of permutation codes of larger sizes. In the next

Table 5 GRS corresponding to an EPGC

	$\mathcal{O}_1$	$\mathcal{O}_2$	$\cdots$	$\mathcal{O}_{s-1}$	$\mathcal{O}_s$
$\mathcal{O}_1$	A_1		$\cdots$		
$\mathcal{O}_2$		A_2	$\vdots$		
$\vdots$	$\vdots$	$\cdots$	$\ddots$	$\vdots$	$\vdots$
$\mathcal{O}_{s-1}$				A_{s-1}	
$\mathcal{O}_s$					A_s

subsection, we will discuss the advantage of EPGCs in encoding process which comes from the fact that they are subgroups instead of subsets.

7.1 Potential applications in code construction

As we saw in the previous section, the existence of an EPC with parameters (r, υ, λ) is equivalent to the existence of $S(r, \lambda; \upsilon)$. On the other hand, when we restrict ourselves to EPGCs, the structure of corresponding GRSs were obtained and observed that the resulting GRSs have poor parameters. To fix this issue and construct better GRSs from EPGCs, we may proceed with the following method. Let $C \leq S_r$ be an EPGC of distance $r - \lambda$ and T be a set of right coset representatives of C in S_n. Clearly, for any x in T, the right coset Cx is also an EPC since for any c, d in C we have $d(cx, dx) = d(c, d)$. Now we want to add some right cosets of C to C such that the union is also an EPC. At the first step, we set $C^{(1)} := C$, and want to add one coset. If $C \cup Cx_1$ is an EPC then we need only to check that all distances $d(c, x_1)$ is equal to $r - \lambda$, for all $c \in C^{(1)}$. If we find one such x_1 in T then we set $C^{(2)} := C \cup Cx_1$. Now we look for the element x_2 in T for which all distances $d(c, x_2)$ is equal to $r - \lambda$, for all $c \in C^{(2)}$. If we proceed with this method and find elements $x_1, x_2, \ldots, x_l$ then $C^{(l+1)} := C \cup Cx_1 \cup \cdots \cup Cx_l$ is an EPC with parameters $(r, l\upsilon, \lambda)$. This improves the the parameters of the EPC and the corresponding GRS as well.

For example we have considered the permutation representation of the alternating group A_4 in the symmetric group S_{14} which gives us an EPGC with parameters (14, 12, 12). The number of right cosets of A_4 in S_{14} is 7264857600 which is a large number. We started searching among these cosets to improve our EPC or its corresponding GRS. We only found one of such cosets and hence we obtained a (14, 24, 12) EPC or an $S(14, 12, 24)$. Note that we have not completed the search in all cosets due to lack of time. Also, note that the best known EPC of length 14 and distance 12 has 40 codewords. It seems interesting to find a faster algorithm that can be run over all cosets of A_4 and find the best EPC that can be found from this method.

7.2 Application in encoding process

An important application of permutation group codes appears in encoding process. Like classical codes in which when a code is linear, we use a generator matrix (whose rows form a basis of the space) for the encoding process, here when the permutation code is a subgroup of the symmetric group, we can find a representation of the code that enables us to encode the data by using some generators of the code. Let us start with an example in our case. Consider the group $PSL(2, 4)$. By Remark 13 and theorem 16, we can embed this group into the symmetric group S_{62} which yield an EPGC. Let us denote this code by H. Set

$$\begin{aligned} a :=&(1,44,36,33,45)(2,38,52,27,18)(3,21,28,51,37)(4,16,29,53,39)\\ &(5,42,56,30,12)(6,14,22,50,46)\\ &(7,59,15,35,23)(8,24,34,10,58)(9,43,47,25,13)(11,40,62,32,54)\\ &(17,55,31,61,41)(26,49,57,60,48), \end{aligned}$$

and

$$\begin{aligned} b :=&(1,48,9,8,47)(2,21,20,3,52)(4,16,41,42,17)(5,56,61,62,55)\\ &(6,35,57,24,13)(7,14,25,58,36)\\ &(10,34,49,50,33)(11,30,12,54,53)(15,59,44,43,60)(18,19,27,37,28)\\ &(22,23,46,26,45)(29,39,32,31,40). \end{aligned}$$

Then we see that $PSL(2,4) \cong H = \langle a, b\rangle \leq S_{62}$. Now, if we set

$$\begin{aligned} p_1 :=&(1,26)(2,28)(3,27)(4,29)(5,30)(6,23)(7,22)(8,25)(9,24)(11,12)(13,14)\\ &(16,17)(18,19)(20,21)(31,62)\\ &(32,61)(33,58)(34,57)(35,60)(36,59)(37,51)(38,52)(39,54)(40,53)(41,56)\\ &(42,55)(43,48)(44,47)(45,50)(46,49), \end{aligned}$$

$$\begin{aligned} p_2 :=&(2,3)(4,5)(6,9)(7,8)(10,15)(11,17)(12,16)(13,14)(18,21)(19,20)(22,25)\\ &(23,24)(27,28)(29,30)(31,32)\\ &(33,36)(34,35)(37,38)(39,42)(40,41)(43,46)(44,45)(47,50)(48,49)(51,52)\\ &(53,56)(54,55)(57,60)(58,59)(61,62), \end{aligned}$$

$$\begin{aligned} \mu_1 :=&(1,13,10)(2,18,37)(3,20,51)(4,31,11)(5,61,12)(6,43,33)(7,45,57)(8,47,34)\\ &(9,49,58)(14,15,26)\\ &(16,29,32)(17,30,62)(19,38,27)(21,52,28)(22,44,35)(23,46,59)(24,48,36)\\ &(25,50,60)(40,41,53)(42,55,54), \end{aligned}$$

$$\begin{aligned} \mu_2 :=&(1,7,59,57,9)(3,18,38,37,20)(4,39,41,5,61)(6,23,44,10,47)\\ &(8,49,15,46,25)(11,55,62,53,16)\\ &(12,17,40,31,42)(13,60,45,43,58)(14,33,48,50,35)(19,27,21,51,52)\\ &(22,26,24,34,36)(29,32,30,56,54), \end{aligned}$$

$P := \langle p_1, p_2\rangle$, $Q_1 := \langle \mu_1\rangle$, $Q_2 := \langle \mu_2\rangle$, then P is an elementary abelian 2-group of order 4 and Q_1,Q_2 are cyclic subgroups of C of orders 3, 5, respectively. In fact, P is a 2-sylow, Q_1 is a 3-sylow and Q_2 is a 5-sylow subgroup of H. Moreover we have $N_H(P) = P \rtimes Q_1$, $N_H(P) \cap Q_2 = \{1\}$ and $|H| = |N_H(P)||Q_2|$. Therefor $H = PQ_1Q_2$, and if $g \in G$, then there exists unique

$$(\delta_1, \delta_2, \delta_3, \delta_4) \in \{0,1\} \times \{0,1\} \times \{0,1,2\} \times \{0,1,2,3,4\},$$

such that

$$g = p_1^{\delta_1} p_2^{\delta_2} \mu_1^{\delta_3} \mu_2^{\delta_4}. \tag{7.1}$$

Since this representation for g is unique, by considering the data as elements in

$$\{0, 1\} \times \{0, 1\} \times \{0, 1, 2\} \times \{0, 1, 2, 3, 4\},$$

and saving the generators p_1, p_2, μ_1, μ_2 in memory, we can do the encoding process easily.

We have the same discussion for the group $Sz(8)$. By Remark 13 and Theorem 16, we find a representation of $Sz(8)$ in S_{29128} which is an EPGC of fixity 8. Indeed, we find two elements a and b of orders 2 and 4, respectively, in S_{29128} such that $Sz(8) \cong H = \langle a, b\rangle \leq S_{29128}$. Also we find elements $g_1, g_2, g_3, h_1, h_2, h_3$ and k of orders 4,4,4,2,2,2 and 7, respectively, in H such that $Q = \langle g_1, g_2, g_3\rangle$ is a 2-sylow subgroup of G of order 64, $Z(Q) = \langle h_1, h_2, h_3\rangle$ is an elementary abelian 2-group of size 8, k belongs to the normalizer of Q in S_{29128} and any element $g \in H$ can be written uniquely in one of the following forms (see Proposition 26, below)

$$g = g_1^{\delta_1} g_2^{\delta_2} g_3^{\delta_3} h_1^{\delta_4} h_2^{\delta_5} h_3^{\delta_6}, \qquad g = g_1^{\delta_1} g_2^{\delta_2} g_3^{\delta_3} h_1^{\delta_4} h_2^{\delta_5} h_3^{\delta_6} k^{\delta_7} a g_1^{\delta_8} g_2^{\delta_9} g_3^{\delta_{10}} h_1^{\delta_{11}} h_2^{\delta_{12}} h_3^{\delta_{13}}, \tag{7.2}$$

where $\delta_i \in \{0, 1\}$, $i \in \{1, \ldots, 6, 8, \ldots, 13\}$, and $\delta_7 \in \{0, 1, \ldots, 6\}$. So, the uniqueness of the representation for g implies that by considering the data as elements in

$$\left\{\{0, 1\}^6 \times \{0, 1, \ldots, 6\} \times \{0\}^7, \{0, 1\}^6 \times \{0, 1, \ldots, 6\} \times \{1\} \times \{0, 1\}^6\right\},$$

and saving the generators $g_1, g_2, g_3, h_1, h_2, h_3, k, a, g_1, g_2, g_3, h_1, h_2, h_3$ in memory, we can do the encoding process easily.

In general, we need to find a decomposition like 7.1 or 7.2, for all of the groups elements prescribed in previous sections. In what follows, we introduce such a decomposition for the elements of $PGL(2, q)$, $PSL(2, q)$ and Suzuki groups.

Proposition 24 *let $G := PGL(2, p^n)$. Then G has a generating set $\{\mu_1, \ldots, \mu_n, a, b\}$ such that for each $x \in G$, there exists unique*

$$(\delta_1, \delta_2, \ldots, \delta_{n+2}) \in \{0, 1\} \times \cdots \times \{0, 1\} \times \{0, 1, \ldots, p^n - 2\} \times \{0, 1, \ldots, p^n\},$$

such that $x = \mu_1^{\delta_1} \mu_2^{\delta_2} \cdots \mu_n^{\delta_n} a^{\delta_{n+1}} b^{\delta_{n+2}}$.

Proof Let $A = \langle a\rangle$, $B = \langle b\rangle$ and P be the subgroups of G introduced in Proposition 15 and let $H = N_G(P)$. At first, we show that $G = HB$. In view of the parts iii and iv of Proposition 15, $B \cap H = \{1\}$. So $|HB| = \frac{|H||B|}{|H \cap B|} = q(q - 1)(q + 1) = |G|$. Hence $G = HB$. Therefore, if $x \in G$, then there exist $h \in H$ and $i \in \{0, 1, \ldots, p^n\}$ such that $x = hb^i$. On the other hand, since H is a Frobenius group with kernel P and complement A, $h = \lambda a^j$, where $j \in \{0, 1, \ldots, p^n - 2\}$ and $\lambda \in P$. So the result follows from this fact that since P is an elementary abelian p-group, there are $\mu_1, \ldots, \mu_n$ of order p in P such that $\lambda = \mu_1^{\delta_1} \mu_2^{\delta_2} \cdots \mu_n^{\delta_n}$, where $0 \leq \delta_1, \delta_2, \ldots, \delta_n \leq 1$. This completes the proof. □

Proposition 25 *let $G := PSL(2, q)$, $q = p^n$ and $p \neq 2$. Then G has a generating set $\{\mu_1, \ldots, \mu_n, a, t, b\}$ such that for each $x \in G$, there exists unique*

$$(\delta_1, \delta_2, \ldots, \delta_{n+3}) \in \{0, \ldots, p - 1\}^n \times \{0, 1, \ldots, \frac{q - 3}{2}\} \times \{0, 1\} \times \{0, 1, \ldots, \frac{q - 1}{2}\},$$

such that $x = \mu_1^{\delta_1} \mu_2^{\delta_2} \cdots \mu_n^{\delta_n} a^{\delta_{n+1}} t^{\delta_{n+2}} b^{\delta_{n+3}}$.

Proof Let $A = \langle a \rangle$, $B = \langle b \rangle$ and P be the subgroups of G introduced in Proposition 15 and let $H = N_G(P)$ and $D = N_G(B)$. Since there exists $t \in G$ of order 2 such that $D = \{t^i b^j \mid 0 \leq i \leq 1, 0 \leq j \leq \frac{q-1}{2}\}$, if we prove $H \cap D^y = \{1\}$ for some $y \in G$, then $G = HD^y$ and thus using the same argument as in the proof of Lemma 24, the result is obtained. Suppose first that $q \equiv 3 (\mathrm{mod}\, 4)$. In this case $\{x \in G \mid x^2 = 1\} = \{(b^{\frac{q+1}{4}})^g \mid g \in G\}$. So $H \cap D = \{1\}$. Now suppose that $q \equiv 1 (\mathrm{mod}\, 4)$. In this case $\{x \in G \mid x^2 = 1\} = \{(a^{\frac{q-1}{4}})^g \mid g \in G\}$. Since $N_G(D) = D$, $|\{D^g \mid g \in G\}| = \frac{q(q^2-1)}{2(q+1)} = \frac{q(q-1)}{2}$. Each of the D^g's contains $\frac{q+1}{2}$ elements of order 2. It is clear that all elements of order 2 in G are conjugate and there are $q(q+1)$ of them. So each one is in the same number of D^g's. Hence by the counts so far, each element of order 2 is in $\frac{q(q^2-1)}{4q(q+1)} = \frac{q-1}{4}$ of the D^g's. Then since H contains q elements of order 2, the intersection of H with at most $\frac{q(q-1)}{4}$ of D^g's is non-trivial. Therefore, there exists $y \in G$ such that $H \cap D^y = \{1\}$ and this completes the proof. □

In the following, we follow the notations in Sect. 4.

Proposition 26 *let $G := Sz(2^n)$, where $n \geq 3$ is an odd number. If $Q = \langle g_1, \ldots, g_m \rangle$, $Z(Q) = \langle h_1, \ldots, h_n \rangle$ and $K = \langle k \rangle$, then $\{g_1, \ldots, g_m, h_1, \ldots, h_n, k, T\}$ is a generating set of G such that for each $x \in G$, there exists unique*

$$(\delta_1, \delta_2, \ldots, \delta_{2m+2n+2}) \in \Big\{\{0,1\}^{m+n} \times \{0, \ldots, 2^n - 2\} \times \{1\} \times \{0,1\}^{m+n}, \{0,1\}^{m+n} \times \{0, \ldots, 2^n - 2\} \times \{0\}^{m+n+1}\Big\},$$

such that

$$x = g_1^{\delta_1} \cdots g_m^{\delta_m} h_1^{\delta_{m+1}} \cdots h_n^{\delta_{m+n}} k^{\delta_{m+n+1}} T^{\delta_{m+n+2}} g_1^{\delta_{m+n+3}} \cdots g_m^{\delta_{2m+n+2}} h_1^{\delta_{2m+n+3}} \cdots h_n^{\delta_{2m+2n+2}}.$$

Proof In view of [27, p. 3, lines 11–13], every element $g \in G$ can be uniquely decomposed into one of the following two products:

$$g = S(a,b)k^i T S(a',b'), \qquad g = S(a,b)k^i,$$

where $a, a', b, b' \in GF(2^n)$ and $0 \leq i \leq 2^n - 2$. Also, in view of [12, p. 2, lines 32–35], an element of Q can be written uniquely in the form $g_1^{\alpha_1} \cdots g_m^{\alpha_m} h_1^{\beta_1} \cdots h_n^{\beta_n}$, where the α_i and β_j are 0 or 1. This completes the proof. □

References

1. Baer R.: Partitionen endlicher Gruppen. Math. Z. **75**, 333–372 (1961).
2. Cameron P.J., Omidi G.R., Tayfeh-Rezaie B.: 3-Designs from $PGL(2, q)$. Electron. J. Comb. **13**, R50 (2006).
3. Chu W., Colbourn C., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**, 51–64 (2004).
4. Chu W., Colbourn C.J., Dukes P.: On constant composition codes. Discret. Appl. Math. **154**, 912–929 (2006).
5. Deza M., Mullin R.C., Vanstone S.A.: Room squares and equidistant permutation arrays. Ars Comb. **2**, 235–244 (1976).
6. Deza M., Vanstone S.A.: Bounds for permutation arrays. J. Stat. Plan. Inference **2**, 197–209 (1978).
7. Ding C., Yin J.: Combinatorial constructions of constant composition codes. IEEE Trans. Inf. Theory **51**, 3671–3674 (2005).
8. Ding C., Yin J.: A construction of optimal constant composition codes. Des. Codes Cryptogr. **40**, 157–165 (2006).

9. Heinrich K., van Rees G.H.J.: Some constructions for equidistant permutation arrays of index one. Util. Math. **13**, 193–200 (1978).
10. Heinrich K., van Rees G.H.J., Wallis W.D.: A general construction for equidistant permutation arrays. In: Bondy J.A., Murty U.S.R. (eds.) Graph Theory and Related Topics, pp. 247–252. Academic Press, New York (1979).
11. Héthelyi L., Horváth E., Petényi F.: The depth of subgroups of Suzuki groups. Commun. Algebra **43**(10), 4553–4569 (2015).
12. Higman G.: Suzuki 2-groups. Ill. J. Math. **7**, 79–96 (1963).
13. Huppert B.: Endliche Gruppen I. Springer, Berlin (1967).
14. Huppert B., Blackburn N.: Finite Groups III. Springer, Berlin (1982).
15. Huczynska S., Mullen G.: Frequency permutation arrays. J. Comb. Des. **14**, 463–478 (2006).
16. Huczynska S.: Equidistant frequency permutation arrays and related constant composition codes. Des. Codes Cryptogr. **54**, 109–120 (2010).
17. Iwahori N.: On a property of a finite group. J. Fac. Sci. Univ. Tokyo **11**, 113–144 (1964).
18. Iwahori N., Kondo T.: A criterion for the existence of a non-trivial partition of a finite group with applications to finite reflection groups. J. Math. Soc. Jpn. **17**, 207–215 (1965).
19. Kegel O.H.: Die Nilpotenz der Hp-Gruppen. Math. Z. **71**, 373–376 (1961).
20. King O.H.: The subgroup structure of finite classical groups in terms of geometric configuration. In: Webb B.S. (ed.) Survey in Combinatorics, vol. 327. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge (2005).
21. Lüneburg H.: Die Suzuki gruppen und ihre Geometrien, vol. 10. Lecture Notes in Mathematik. Springer, Berlin (1965).
22. Luo Y., Fu F.-W., Han Vinck A.J., Chen W.: On constant-composition codes over Z_q. IEEE Trans. Inf. Theory **49**, 3010–3016 (2003).
23. Mahmoodi A., Mathon R.: Enumeration and analysis of small equidistant permutation arrays. Congr. Numer. **87**, 5–25 (1992).
24. Mathon R.: Bounds for equidistant permutation arrays of index one. In: Combinatorial Mathematics: Proceedings of the Third International Conference, pp. 303–309. New York Academy of Sciences, New York (1989).
25. Mathon R., Vanstone S.A.: On the existence of doubly resolvable Kirkman systems and equidistant permutation arrays. Discret. Math. **30**, 157–172 (1980).
26. Peng L., Chen S., Guo S.: The construction of permutation group codes for communication systems: prime or prime power? IEEE Access **8**, 69953–69966 (2020).
27. Smolensky A.: Products of Sylow subgroups in Suzuki and Ree groups. Commun. Algebra **44**(10), 4422–4429 (2016).
28. Suzuki M.: On a finite group with a partition. Arch. Math. **12**, 241–274 (1961).
29. Tamo I., Schwartz M.: On the labeling problem of permutation group codes under the infinity metric. IEEE Trans. Inf. Theory **58**(10), 6595–6604 (2012).
30. Van Rees G.H.J., Vanstone S.A.: Equidistant permutation arrays: a bound. J. Austral. Math. Soc. Ser. A **33**, 262–274 (1982).
31. Vanstone S.A.: The asymptotic behaviour of equidistant permutation arrays. Can. J. Math. **21**, 45–48 (1979).
32. Zappa G.: Partitions and other covering of finite groups. Ill. J. Math. **47**, 571–580 (2003).