J. Group Theory **18** (2015), 407–433
DOI 10.1515/jgth-2014-0049

Twisted permutation codes

Neil I. Gillespie, Cheryl E. Praeger and Pablo Spiga

Communicated by Christopher W. Parker

Abstract. We introduce *twisted permutation codes*, which are frequency permutation arrays analogous to repetition permutation codes, namely, codes obtained from the repetition construction applied to a permutation code. In particular, we show that a lower bound for the minimum distance of a twisted permutation code is the minimum distance of a repetition permutation code. We give examples where this bound is tight, but more importantly, we give examples of twisted permutation codes with minimum distance strictly greater than this lower bound.

1 Introduction

Transmitting digital information using existing electrical infrastructure, known as *powerline communication*, has been proposed as a possible solution to the "last mile problem" in telecommunications [19, 24]. Constant composition codes are coding schemes that are particularly well suited to deal with the extra noise present in powerline communication, while at the same time maintaining a necessary constant power output [8, 9, 11, 23]. Moreover, it is suggested in [8] that *frequency permutation arrays*, a class of constant composition codes, are particularly well suited for powerline communication. A frequency permutation array of length $m = rq$ over an alphabet Q of size q is a code with the property that in each codeword, every letter from Q appears exactly r times. They have been studied in [20, 21]. In [17], the first two authors characterised a family of *neighbour transitive codes* (see Section 5) in which frequency permutation arrays play a central role. In the same paper, the *permutation codes* generated by groups in this family were classified, and by applying a repetition construction to these codes, infinite families of non-trivial neighbour transitive frequency permutation arrays were constructed. In this setting, repeating codewords improves the minimum distance of the code only by a factor of the number of repetitions. In this paper we introduce *twisted permutation codes*, which are frequency permutation arrays that are generated by groups and are analogous to repeated permutation codes. We give

For the first author, this research was supported by the Australian Research Council Federation Fellowship of the second author.

examples where the minimum distance is improved by a greater amount than that achieved by the repetition construction.

Let T be an abstract group and, as $|Q| = q$, identify the symmetric group on Q with S_q, the symmetric group on $\{1, \ldots, q\}$. We call a group homomorphism ρ from T to S_q a *representation* of T of *degree* q. Given such a representation we define the permutation code $C(T, \rho)$ (see Section 3). If α is a codeword in $C(T, \rho)$, we let $\mathrm{rep}_r(\alpha) = (\alpha, \ldots, \alpha)$ denote the r-tuple with constant entry α, and we let

$$\mathrm{Rep}_r(C(T, \rho)) = \{\mathrm{rep}_r(\alpha) : \alpha \in C(T, \rho)\}. \tag{1.1}$$

The code $\mathrm{Rep}_r(C(T, \rho))$ is a frequency permutation array of length rq where every letter appears r times in each codeword. (This is the repetition construction mentioned above.) A twisted permutation code is a frequency permutation array generated by a group T and several (not necessarily distinct) representations of T of the same degree. (See also Table 9.) Specifically, we consider an ordered r-tuple $\mathcal{I}$ of representations of T to S_q and construct the twisted permutation code $C(T, \mathcal{I})$ (see Section 3), a frequency permutation array of length rq over Q. By letting δ_{tw} be the minimum distance of $C(T, \mathcal{I})$ and δ_{rep} be the minimum of the minimum distances of $\mathrm{Rep}_r(C(T, \rho))$ as ρ varies over $\mathcal{I}$, we prove the following.

Theorem 1.1. *Let q be a positive integer, T be an abstract group, and $\mathcal{I}$ be an ordered r-tuple of (not necessarily distinct) permutation representations of T into S_q. Then $C(T, \mathcal{I})$ as defined in Section* 3 *is a frequency permutation array of length rq with minimum distance $\delta_{\mathrm{tw}} \geqslant \delta_{\mathrm{rep}}$. Moreover, the twisted permutation codes described in Table* 1 *have a minimum distance that is strictly greater than this lower bound.*

T	r	q	δ_{rep}	δ_{tw}	Reference
S_6	2	6	4	8	Section 4.1
A_6	2	6	6	8	Section 4.2
ASL(3, 2)	2	8	8	12	Section 7.1
S_6	4	60	176–192	$\leqslant 224$	Section 7.2

Table 1. Examples of twisted permutation codes with improved minimum distance.

Remark 1.2. The codes in the fourth line of Table 1 are described in Section 7.2. There are several different repetition permutation codes and also several different twisted permutation codes, with minimum distances, which can be obtained explicitly from Table 8 in Section 7.2, ranging from 176 to 192, and from 176 to 224, respectively.

In some cases, two representations of a group T to S_q can be identified with each other if there exists a relabelling of the point set Q that maps one to the other. However, this is not always possible, in which case the representations are distinct. For example, S_6 has two distinct representations of degree 6, which are interchanged by an outer automorphism of order 2. Each finite 2-transitive almost simple group has at most two distinct representations of the same degree, with one infinite family and six exceptional cases that have exactly two distinct representations [5, Table 7.4]. (This fact is a consequence of the Classification of Finite Simple Groups.) Additionally, these groups share the property of S_6 that the two actions are interchanged by an outer automorphism of order 2. For T being one of these groups and ρ_1, ρ_2 the distinct representations of T of the same degree, we consider the codes $C(T, (\rho_1, \rho_2))$ in Section 4 where we determine their minimum distance with respect to the lower bound δ_{rep}. We also prove in Theorem 5.1 that these codes are neighbour transitive.

Cameron [5] also states that the 2-transitive affine group $\mathrm{ASL}(2, r)$ with $r = 2^f$ for some positive integer $f \geqslant 2$ has r distinct representations of the same degree. In Section 6 we give an explicit construction of these distinct representations, and by letting $\mathcal{I}$ be an r-tuple of these actions, we determine the minimum distance of $C(\mathrm{ASL}(2, r), \mathcal{I})$ with respect to the lower bound δ_{rep}. Finally, in Section 7, we use the computer software program GAP to construct some further examples of twisted permutation codes. This allows us to prove Theorem 1.1 in Section 7.3.

2 Definitions

2.1 Codes

A code of length m over an alphabet Q of size q can be embedded as a subset of the vertex set of the Hamming graph $\Gamma = H(m, q)$, which has a vertex set $V(\Gamma)$ that consists of m-tuples with entries from Q, and an edge exists between two vertices if and only if they differ in precisely one entry. Throughout this paper we identify the alphabet Q with the set $\{1, \ldots, q\}$ and $\mathrm{Sym}(Q)$ with S_q. The automorphism group of $H(m, q)$, which we denote by $\mathrm{Aut}(\Gamma)$, is a semi-direct product $B \rtimes L$ where $B \cong S_q^m$ and $L \cong S_m$ ([4, Theorem 9.2.1]). Let $g = (g_1, \ldots, g_m) \in B$, $\sigma \in L$ and $\alpha = (\alpha_1, \ldots, \alpha_m) \in V(\Gamma)$. Then $g\sigma$ acts on α in the following way:

$$\alpha^{g\sigma} = (\alpha_{1\sigma^{-1}}^{g_{1\sigma^{-1}}}, \ldots, \alpha_{m\sigma^{-1}}^{g_{m\sigma^{-1}}}).$$

For all pairs of vertices $\alpha, \beta \in V(\Gamma)$, the *Hamming distance* between α and β, denoted by $d(\alpha, \beta)$, is defined to be the number of entries in which the two vertices differ. It is the distance between α and β in Γ. We let $\Gamma_k(\alpha)$ denote the set of vertices in Γ that are at distance k from α.

The *minimum distance*, $\delta(C)$, of a code C is the smallest distance between distinct codewords of C. If C consists of exactly one codeword, then we let $\delta(C) = 0$. Another code C' in $H(m, q)$ is *equivalent* to C if there exists an $x \in \mathrm{Aut}(\Gamma)$ such that $C^x = C'$, and if $C = C'$, we call x an *automorphism of* C. The *automorphism group of* C is the setwise stabiliser of C in $\mathrm{Aut}(\Gamma)$, which we denote by $\mathrm{Aut}(C)$. The *inner distance distribution of* C is the $(m+1)$-tuple

$$\kappa(C) = (a_0, \ldots, a_m)$$

where

$$a_i = \frac{|\{(\alpha, \beta) \in C^2 : d(\alpha, \beta) = i\}|}{|C|}. \tag{2.1}$$

We observe that $a_i \geqslant 0$ for all i and $a_0 = 1$. Moreover, $a_i = 0$ for $1 \leqslant i \leqslant \delta - 1$ and $|C| = \sum_{i=0}^{m} a_i$. For a codeword α, the *distance distribution from* α is the $(m+1)$-tuple

$$\kappa(\alpha) = (a_0(\alpha), \ldots, a_m(\alpha))$$

where $a_k(\alpha) = |\Gamma_k(\alpha) \cap C|$.

We say a code C is *distance invariant* if the number of codewords at distance i from a codeword is independent of the choice of codeword. That is $\kappa(C) = \kappa(\alpha)$ for each codeword α. It is straightforward to deduce that if a group of automorphisms of a code acts transitively, then the code is necessarily distance invariant.

2.2 Permutation groups

Let Ω be a nonempty set. We denote the group of permutations of Ω by $\mathrm{Sym}(\Omega)$. A *permutation group* on Ω is a subgroup of $\mathrm{Sym}(\Omega)$. Suppose G is a permutation group on Ω and $t \in G$. We define the *support of* t as the set

$$\mathrm{supp}(t) = \{\alpha \in \Omega : \alpha^t \neq \alpha\}$$

and the set of *fixed points of* t as

$$\mathrm{fix}(t) = \{\alpha \in \Omega : \alpha^t = \alpha\}.$$

It follows that $\Omega = \mathrm{supp}(t) \cup \mathrm{fix}(t)$ for all $t \in G$. We say G acts *regularly* on Ω if G acts transitively on Ω and $G_\alpha = 1$ for all $\alpha \in \Omega$.

Let G be an abstract group now. An *action* of G on Ω is a homomorphism ρ from G to $\mathrm{Sym}(\Omega)$, in which case we say G *acts on* Ω or ρ *defines an action of* G *on* Ω. We also call ρ a (*permutation*) *representation* of G on Ω. The *degree of the action* is the cardinality of Ω. In this paper, all actions have finite degree. Let $\rho_1 : G \to \mathrm{Sym}(\Omega)$ and $\rho_2 : H \to \mathrm{Sym}(\Omega')$ be actions of the groups G, H on Ω and Ω'. We say these actions are *permutationally isomorphic* if there exists

a bijection $\lambda : \Omega \to \Omega'$ and an isomorphism $\varphi : \rho_1(G) \to \rho_2(H)$ such that

$$\lambda(\alpha^{\rho_1(g)}) = \lambda(\alpha)^{\varphi(\rho_1(g))} \quad \text{for all } \alpha \in \Omega \text{ and } g \in G, \tag{2.2}$$

and we call (λ, φ) a *permutational isomorphism*. If $G = H$ and φ is the identity map, then we say the two actions of G are *equivalent*. However, if there does not exist a bijection $\lambda : \Omega \to \Omega'$ such that (2.2) holds with $G = H$ and φ equal to the identity map, then we say the two actions are *inequivalent.*

3 Constructions

Let $Q = \{1, \ldots, q\}$ and $H(q, q)$ be the Hamming graph of length q over Q. We denote the symmetric group on Q by S_q. Let T be an abstract group and $\rho : T \to S_q$ be an action of T on Q denoted by $t \mapsto t\rho$. For $t \in T$, we identify the permutation $t\rho$ with the vertex in $H(q, q)$ that represents its passive form, that is, with $\alpha(t, \rho) = (1^{t\rho}, \ldots, q^{t\rho}) \in H(q, q)$. We naturally define

$$C(T, \rho) = \{\alpha(t, \rho) : t \in T\}. \tag{3.1}$$

The code $C(T, \rho)$ is an example of a *permutation code*. Permutation codes were introduced in the 1970s [2, 3, 15], where *sets* of permutations in their passive form were considered rather than groups. Due to applications in *powerline communication*, Chu, Colbourn and Dukes [8] renewed the interest in permutation codes, giving new constructions of such codes. Other interesting results on permutation codes include a beautiful decoding algorithm by Bailey [1] for permutation codes of groups; Cameron and Wanless' [7] examination of the covering radius of a permutation code; and Cameron and Gadouleau's [6] introduction of the *remoteness of a code* and their examination of this parameter with respect to permutation codes.

As discussed in Section 2, the automorphism group of $\Gamma = H(q, q)$ is equal to $B \rtimes L$ where $B \cong S_q^q$ and $L \cong S_q$. To distinguish between automorphisms of Γ and permutations in S_q, we introduce the following notation. For $t \in T$ and $\rho : T \to S_q$, we let $x_{t\rho} = (t\rho, \ldots, t\rho) \in B$, and we let $\sigma(t\rho)$ denote the automorphism induced by $t\rho$ in L. Since ρ is a homomorphism, it holds for $t \in T$ and $\alpha(s, \rho) \in V(\Gamma)$ that

$$\begin{aligned} \alpha(s, \rho)^{x_{t\rho}} &= (1^{s\rho}, \ldots, q^{s\rho})^{(t\rho, \ldots, t\rho)} \\ &= (1^{s\rho t\rho}, \ldots, q^{s\rho t\rho}) \\ &= (1^{(st)\rho}, \ldots, q^{(st)\rho}) \\ &= \alpha(st, \rho). \end{aligned}$$

Now, suppose that $i^{t\rho} = j$ for $i, j \in Q$. Then, by considering $\alpha(s, \rho)$ as the q-tuple $(\alpha_1, \ldots, \alpha_q)$, it holds that

$$\alpha(s, \rho)^{\sigma(t\rho)}|_j = \alpha_i = i^{s\rho} = j^{t^{-1}\rho s\rho} = j^{(t^{-1}s)\rho}.$$

Thus $\alpha(s, \rho)^{\sigma(t\rho)} = \alpha(t^{-1}s, \rho)$, and we have proved the following.

Lemma 3.1. *Let $\alpha(s, \rho) \in C(T, \rho)$ and $t \in T$. Then*

$$\alpha(s, \rho)^{x_{t\rho}} = \alpha(st, \rho) \quad \textit{and} \quad \alpha(s, \rho)^{\sigma(t\rho)} = \alpha(t^{-1}s, \rho).$$

As any group has a regular action on itself by right multiplication, it is a consequence of Lemma 3.1 that $\mathrm{Diag}(T, \rho) = \{x_{t\rho} : t \in T\}$ acts regularly on $C(T, \rho)$. This, in particular, implies that $C(T, \rho)$ is distance invariant.

Lemma 3.2. *For $t \in T$ we have*

$$d(\alpha(1, \rho), \alpha(t, \rho)) = |\mathrm{supp}(t\rho)|.$$

Moreover, $C(T, \rho)$ has minimum distance

$$\delta(C(T, \rho)) = \min\{|\mathrm{supp}(t\rho)| : 1 \neq t \in T\},$$

the minimal degree of $T\rho$.

Proof. For $1 \neq t \in T$ it follows that $\alpha(1, \rho)|_i \neq \alpha(t, \rho)|_i$ if and only if $i \neq i^{t\rho}$, which holds if and only if $i \in \mathrm{supp}(t\rho)$, from which the first statement follows. Now, as $C = C(T, \rho)$ is distance invariant, it has minimum distance

$$\delta(C) = \min\{d(\alpha(1, \rho), \alpha(t, \rho)) : 1 \neq t \in T\}.$$

Thus $\delta(C) = \min\{|\mathrm{supp}(t\rho)| : 1 \neq t \in T\}$. □

We now consider a more general construction. Let $\mathcal{I} = (\rho_1, \ldots, \rho_r)$ be an ordered list of r (not necessarily distinct) representations from T to S_q and define

$$\alpha(t, \mathcal{I}) = (\alpha(t, \rho_1), \ldots, \alpha(t, \rho_r)) \in H(rq, q),$$

which is an r-tuple of codewords of the form given in (3.1). Hence, we naturally define

$$C(T, \mathcal{I}) = \{\alpha(t, \mathcal{I}) : t \in T\}.$$

We call $C(T, \mathcal{I})$ a *twisted permutation code*. Note that if $r = 1$, this is just the construction given in (3.1), and if $\rho_1 = \cdots = \rho_r$, then $C(T, \mathcal{I}) = \mathrm{Rep}_r(C(T, \rho_1))$ as in (1.1).

Proposition 3.3. *Consider the code $C(T, \mathcal{I})$, with notation as above. Then $C(T, \mathcal{I})$ is a frequency permutation array of length rq. Moreover:*

(i) *There exists a group of automorphisms acting regularly on $C(T, \mathcal{I})$. In particular $C(T, \mathcal{I})$ is distance invariant.*

(ii) *The size of $C(T, \mathcal{I})$ is equal to the order of the factor group T/K, where $K = \bigcap_{\rho \in \mathcal{I}} \ker \rho$.*

(iii) *One has*

$$\delta(C(T, \mathcal{I})) = \min_{t \in T^{\#}} \sum_{\rho \in \mathcal{I}} |\mathrm{supp}(t\rho)| \geqslant \min_{\rho \in \mathcal{I}} \{\delta(\mathrm{Rep}_r(C(T, \rho)))\},$$

where $T^{\#} = T \setminus \{1\}$.

Proof. Each codeword in $C(T, \mathcal{I})$ is an r-tuple of permutation codewords, so it is clear that $C(T, \mathcal{I})$ is a frequency permutation array of length rq.

(i) For $t \in T$ let $x(t, \mathcal{I}) = (x_{t\rho_1}, \ldots, x_{t\rho_r}) \in \mathrm{Diag}(T, \rho_1) \times \cdots \times \mathrm{Diag}(T, \rho_r)$, and let $\mathrm{Diag}(T, \mathcal{I}) = \{x(t, \mathcal{I}) : t \in T\}$. Then $x(t, \mathcal{I})$ acts naturally on $\alpha(s, \mathcal{I})$ in the following way:

$$\begin{aligned}
\alpha(s, \mathcal{I})^{x(t,\mathcal{I})} &= (\alpha(s, \rho_1), \ldots, \alpha(s, \rho_r))^{(x_{t\rho_1}, \ldots, x_{t\rho_r})} \\
&= (\alpha(s, \rho_1)^{x_{t\rho_1}}, \ldots, \alpha(s, \rho_r)^{x_{t\rho_r}}) \\
&= (\alpha(st, \rho_1), \ldots, \alpha(st, \rho_r)) \qquad \text{(by Lemma 3.1)} \\
&= \alpha(st, \mathcal{I}).
\end{aligned}$$

Since T has a regular action on itself by right multiplication, we deduce that $\mathrm{Diag}(T, \mathcal{I})$ acts regularly on $C(T, \mathcal{I})$. Hence $C(T, \mathcal{I})$ is distance invariant.

(ii) From the proof of statement (i) it follows that $\alpha(s, \mathcal{I}) = \alpha(t, \mathcal{I})$ if and only if $\alpha(st^{-1}, \mathcal{I}) = \alpha(1, \mathcal{I})$, which holds if and only if $st^{-1} \in K$. Hence the size of $C(T, \mathcal{I})$ is equal to the order of the factor group T/K.

(iii) For an element $t \in T^{\#}$ it is clear that the distance between $\alpha(1, \mathcal{I})$ and $\alpha(t, \mathcal{I})$ in $H(rq, q)$ is equal to the sum of the distances between $\alpha(1, \rho)$ and $\alpha(t, \rho)$ in $H(q, q)$ as ρ varies over $\mathcal{I}$. That is,

$$d(\alpha(1, \mathcal{I}), \alpha(t, \mathcal{I})) = \sum_{\rho \in \mathcal{I}} d(\alpha(1, \rho), \alpha(t, \rho)) = \sum_{\rho \in \mathcal{I}} |\mathrm{supp}(t\rho)|, \tag{3.2}$$

where the last equality follows from Lemma 3.2. Thus the distance between $\alpha(1, \mathcal{I})$ and any codeword in $C(T, \mathcal{I})$ is minimised when this expression is minimised. Consequently, as $C(T, \mathcal{I})$ is distance invariant, it follows that

$$\delta(C(T, \mathcal{I})) = \min_{t \in T^{\#}} \sum_{\rho \in \mathcal{I}} |\mathrm{supp}(t\rho)|.$$

To prove the inequality in the statement, we make the following observation:

$$\begin{aligned}\min_{t\in T^{\#}}\sum_{\rho\in\mathcal{J}}|\mathrm{supp}(t\rho)| &\geqslant \min_{t\in T^{\#}}\{r\cdot\min_{\rho\in\mathcal{J}}\{|\mathrm{supp}(t\rho)|\}\}\\ &= \min_{\rho\in\mathcal{J}}\{r\cdot\min_{t\in T^{\#}}\{|\mathrm{supp}(t\rho)|\}\}\\ &= \min_{\rho\in\mathcal{J}}\{r\cdot\delta(C(T,\rho))\} \qquad \text{(by Lemma 3.2)}\\ &= \min_{\rho\in\mathcal{J}}\{\delta(\mathrm{Rep}_r(C(T,\rho)))\}. \qquad \square\end{aligned}$$

Remark 3.4. (a) Consider the code $C(T,\mathcal{J})$ and let K be as in Proposition 3.3 (ii). Also let $\tilde{T}=T/K$, and for $\rho\in\mathcal{J}$ define $\tilde{\rho}:\tilde{T}\to S_q$ given by $Kt\mapsto t\rho$. It is straightforward to check that $\tilde{\rho}$ is well defined and that $\ker\tilde{\rho}=\ker\rho/K$. By defining $\tilde{\mathcal{J}}=(\tilde{\rho}_1,\ldots,\tilde{\rho}_r)$, it follows that $C(T,\mathcal{J})=C(\tilde{T},\tilde{\mathcal{J}})$. Moreover,

$$\tilde{K}=\bigcap_{\tilde{\rho}\in\tilde{\mathcal{J}}}\ker\tilde{\rho}=\bigcap_{\rho\in\mathcal{J}}(\ker\rho/K)=\Big(\bigcap_{\rho\in\mathcal{J}}\ker\rho\Big)/K=1.$$

Thus, for any twisted permutation code, by replacing T with T/K we can assume that $K=1$ and that $|C(T,\mathcal{J})|=|T|$.

(b) The lower bound in Proposition 3.3 (iii) can be equal to zero. For example, if for some representation $\rho'\in\mathcal{J}$ it holds that $\ker\rho'=T$, then

$$\min_{\rho\in\mathcal{J}}\{\delta(\mathrm{Rep}_r(C(T,\rho)))\}=0.$$

This is because $\mathrm{Rep}_r(C(T,\rho'))$ consists of just one codeword.

In Sections 4 and 7, we give examples of twisted permutation codes with minimum distance strictly greater than the lower bound in Proposition 3.3 (iii). However, this lower bound can be attained by letting $\mathcal{J}=(\rho,\ldots,\rho)$ for some representation $\rho:T\to S_q$, because as we said above, in this case

$$C(T,\mathcal{J})=\mathrm{Rep}_r(C(T,\rho)).$$

The following result shows that this lower bound can also be attained in a slightly more general setting.

Lemma 3.5. *Let $\mathcal{J}=(\rho_1,\ldots,\rho_r)$ be an r-tuple of actions of T of degree q. Suppose that $|\mathrm{supp}(t\rho_i)|=|\mathrm{supp}(t\rho_j)|$ for all i,j and for all $t\in T$. Then $C(T,\mathcal{J})$ has the same inner distance distribution as $\mathrm{Rep}_r(C(T,\rho_i))$ for $i=1,\ldots,r$. In particular $\delta(C(T,\mathcal{J}))$ achieves the lower bound in Proposition* 3.3 (iii).

Proof. Let $C = C(T, \mathcal{I})$. By Proposition 3.3, C is distance invariant. Thus the inner distance distribution of C is equal to the distance distribution from $\alpha(1, \mathcal{I})$. That is, the kth entry of $\kappa(C)$ is equal to $|\Gamma_k(\alpha(1, \mathcal{I})) \cap C|$. It follows from (3.2) that

$$\alpha(t, \mathcal{I}) \in \Gamma_k(\alpha(1, \mathcal{I})) \cap C \iff \sum_{\rho \in \mathcal{I}} |\mathrm{supp}(t\rho)| = k. \tag{3.3}$$

As $|\mathrm{supp}(t\rho_i)| = |\mathrm{supp}(t\rho_j)|$ for all i, j, the expression on the right of (3.3) is equal to $r|\mathrm{supp}(t\rho_i)|$ for each $i = 1, \ldots, r$. Thus the kth entry of $\kappa(C)$ is equal to $|\{t \in T : |\mathrm{supp}(t\rho_i)| = k/r\}|$ for each $i = 1, \ldots, r$.

Now, for $i \in \{1, \ldots, r\}$ let $\mathcal{I}_{\rho_i} = (\rho_i, \ldots, \rho_i)$, and let

$$C' = C(T, \mathcal{I}_{\rho_i}) = \mathrm{Rep}_r(C(T, \rho_i)).$$

Again, because the code C' is distance invariant, the kth entry of $\kappa(C')$ is equal to $|\Gamma_k(\alpha(1, \mathcal{I}_{\rho_i})) \cap C'|$ and

$$\alpha(t, \mathcal{I}_{\rho_i}) \in \Gamma_k(\alpha(1, \mathcal{I}_{\rho_i})) \cap C' \iff \sum_{j=1}^{r} |\mathrm{supp}(t\rho_i)| = r|\mathrm{supp}(t\rho_i)| = k.$$

It follows that the kth entry of $\kappa(C')$ is equal to $|\{t \in T : |\mathrm{supp}(t\rho_i)| = k/r\}|$, as above. □

In Section 6 we give an example of an infinite family of twisted permutation codes, each generated by a set $\mathcal{I}$ of r representations that are pairwise distinct, and whose minimum distance achieves the lower bound in Proposition 3.3 (iii).

4 Examples from almost simple 2-transitive groups

The first examples of twisted permutation codes that we introduce are constructed from finite 2-transitive groups of almost simple type. It is well known that a finite 2-transitive group of almost simple type has at most two inequivalent actions, and the groups with precisely two actions are listed in Table 2, which is taken from [5, Table 7.4]. We consider each group T from Table 2 as a permutation group in its natural action, so q is equal to the degree of T. For each line in Table 2 it holds that the normaliser in S_q of T is an index 2 subgroup of $\mathrm{Aut}(T)$. Thus, we let $\mathcal{I} = (\rho_1, \rho_2)$ where ρ_1 is the identity map and ρ_2 is an outer automorphism of T such that $\rho_2^2 = \rho_1$ (see Remark 4.1), and we consider the code $C(T, \mathcal{I})$.

Remark 4.1. For each T in Table 2, there exists an outer automorphism of T that is an involution. For T in the last line of Table 2, the automorphism induced by the

Degree	T	Conditions
6	S_6, A_6	–
11	$\mathrm{PSL}(2,11)$	–
12	M_{12}	–
15	A_7	–
176	HS	–
$(\ell^n-1)/(\ell-1)$	$\mathrm{PSL}(n,\ell) \leqslant T \leqslant \mathrm{P\Gamma L}(n,\ell)$	$n > 2$

Table 2. 2-transitive almost simple groups with two inequivalent actions.

inverse transpose map is the required outer automorphism. For each of the other groups in Table 2, we consult the character table of T in the ATLAS [12]. For each T we find a conjugacy class of elements in $\mathrm{Aut}(T)\backslash\overline{N_{S_q}(T)}$ which has elements of order 2. (Here $\overline{N_{S_q}(T)}$ denotes the subgroup of $\mathrm{Aut}(T)$ induced by $N_{S_q}(T)$.)

4.1 The symmetric group $T = S_6$

By referring to the character table of S_6 in the ATLAS, we can determine the number of fixed points in each action for each conjugacy class of S_6. By subtracting this from the degree of S_6, we determine, again for each action, the size of the support for the elements in each conjugacy class of S_6. We give this information in Table 3. By summing the sizes of the supports for each conjugacy class, it follows from Proposition 3.3 that $C(S_6, \mathcal{J})$ has minimum distance 8. The minimal degree of S_6 is 2 in both actions, and so $\mathrm{Rep}_2(C(S_6, \rho_i))$ has minimum distance 4 for $i = 1, 2$. Thus, $C(S_6, \mathcal{J})$ has the same size and length as $\mathrm{Rep}_2(C(S_6, \rho_i))$ (for $i = 1, 2$), but has double the minimum distance. In particular, $\delta(C(S_6, \mathcal{J}))$ is greater than the lower bound in Proposition 3.3 (iii).

Conjugacy class	1A	2A	2B	2C	3A	3B	4A	4B	5AB	6A	6B
$\lvert\mathrm{supp}(t\rho_1)\rvert$	0	4	2	6	3	6	6	4	5	5	6
$\lvert\mathrm{supp}(t\rho_2)\rvert$	0	4	6	2	6	3	6	4	5	6	5
Sum of supports	0	8	8	8	9	9	12	8	10	11	11

Table 3. The symmetric group S_6.

4.2 The alternating group $T = A_6$

Again, by referring to the ATLAS, we determine, for each action, the size of the support for the elements in each conjugacy class of A_6. We present this information in Table 4. It follows from Proposition 3.3 that we can read off the minimum distance of $C(A_6, \mathcal{I})$ from Table 4, which is 8. The minimal degree of A_6 in both actions is 3, so $\mathrm{Rep}_2(C(A_6, \rho_i))$ has minimum distance 6 for $i = 1, 2$. Thus $C(A_6, \mathcal{I})$ is strictly greater than the lower bound in Proposition 3.3 (iii).

Conjugacy class	1A	2A	3A	3B	4A	5A	5B
$\lvert\mathrm{supp}(t\rho_1)\rvert$	0	4	3	6	6	5	5
$\lvert\mathrm{supp}(t\rho_2)\rvert$	0	4	6	3	6	5	5
Sum of supports	0	8	9	9	12	10	10

Table 4. The alternating group A_6.

4.3 The Mathieu group $T = M_{12}$

In Table 5 we give the size of the support, for each action, of the elements in each conjugacy class of M_{12} (see [12]). By Proposition 3.3, we deduce that

$$\delta(C(M_{12}, \mathcal{I})) = 16.$$

This is equal to the minimum distance of $\mathrm{Rep}_2(C(M_{12}, \rho_i))$ for $i = 1, 2$ as the outer automorphism ρ_2 does not change the cycle structure of the elements in the conjugacy class 2B, for which the size of the support is equal to the minimal degree of M_{12}. However, the codes $C(M_{12}, \mathcal{I})$ and $\mathrm{Rep}_2(C(M_{12}, \rho_i))$ for $i = 1$ or 2 are inequivalent. This can be seen by considering the distance distribution of each code. By Proposition 3.3, both codes $C(M_{12}, \mathcal{I})$ and $\mathrm{Rep}_2(C(M_{12}, \rho_i))$ are distance invariant. Therefore, the respective inner distance distribution is equal to the distance distribution from any codeword. In the code $C(M_{12}, \mathcal{I})$, the codewords that are at distance 16 from $\alpha(1, \mathcal{I})$ are the codewords associated with elements from the conjugacy class 2B. Hence, in the inner distance distribution of $C(M_{12}, \mathcal{I})$, one has $a_{16} = 495$, the size of the conjugacy class 2B in M_{12}. However, in the code $\mathrm{Rep}_2(C(M_{12}, \rho_i))$, the codewords that are at distance 16 from $(\alpha(1, \rho_i), \alpha(1, \rho_i))$ are precisely the elements from the conjugacy classes 2B and 4B or 4A respectively for $i = 1$ or 2. Hence, in this case a_{16} is equal to the sum of the sizes of the conjugacy classes 2B and 4B or 4A respectively, which is equal to 3465 (note classes 4B and 4A contain the same number of elements).

Conjugacy class	1A	2A	2B	3A	3B	4A	4B	5A
$\lvert\mathrm{supp}(t\rho_1)\rvert$	0	12	8	9	12	12	8	10
$\lvert\mathrm{supp}(t\rho_2)\rvert$	0	12	8	9	12	8	12	10
Sum of supports	0	24	16	18	24	20	20	20

Conjugacy class	6A	6B	8A	8B	10A	11A	11B
$\lvert\mathrm{supp}(t\rho_1)\rvert$	12	11	12	10	12	11	11
$\lvert\mathrm{supp}(t\rho_2)\rvert$	12	11	10	12	12	11	11
Sum of supports	24	22	22	22	24	22	22

Table 5. The Mathieu group M_{12}.

The inner distribution for each code can be calculated in this way and is given in Table 6. Note that we only give the non-zero terms of the inner distribution.

$\kappa(C)$	a_0	a_{16}	a_{18}	a_{20}	a_{22}	a_{24}
$C(M_{12}, \mathcal{I})$	1	495	1760	15444	56880	20460
$\mathrm{Rep}_2(C(M_{12}, \rho_i))$	1	3465	1760	21384	33120	35310

Table 6. Inner distance distributions.

In the remaining cases from Table 2, we claim that $|\mathrm{supp}(t\rho_1)| = |\mathrm{supp}(t\rho_2)|$ for each $t \in T$. Consequently by Lemma 3.5, $C(T, \mathcal{I})$ has the same inner distance distribution as $\mathrm{Rep}_2(C(T, \rho_i))$ for $i = 1, 2$, and therefore the same minimum distance. Hence, in these cases the code $C(T, \mathcal{I})$ has a minimum distance that is equal to the lower bound in Proposition 3.3 (iii) even though $\rho_1 \neq \rho_2$.

4.4 The groups $T = \mathrm{PSL}(2, 11)$, A_7, HS

By referring to the ATLAS, we see that in each case the permutation character of the action generated by ρ_1 is the same as the permutation character of the action generated by ρ_2. In particular, for $T = \mathrm{PSL}(2, 11)$, A_7 or HS, the permutation character for both actions is equal to 1A + 10B, 1A + 14B, or 1A + 175A respectively [12, pp. 7, 10, 80]. Hence $|\mathrm{fix}(t\rho_1)| = |\mathrm{fix}(t\rho_2)|$ for all $t \in T$ and so $|\mathrm{supp}(t\rho_1)| = |\mathrm{supp}(t\rho_2)|$ for all $t \in T$.

4.5 The projective linear groups $\mathrm{PSL}(n,\ell) \trianglelefteq T \leq \mathrm{P\Gamma L}(n,\ell)$

In its natural action T is acting 2-transitively on $\mathcal{P}$, the set of $(\ell^n-1)/(\ell-1)$ one-dimensional subspaces of $V=\mathbb{F}_\ell^n$. Moreover, under ρ_2, the action of T is permutationally isomorphic to the action of T on $\mathcal{B}$, the set of $(\ell^n-1)/(\ell-1)$ hyperplanes of V. It holds that each hyperplane is uniquely determined by the set of one-dimensional subspaces it contains. Consequently $\mathcal{D}=(\mathcal{P},\mathcal{B})$ forms a symmetric 2-design, and in particular, T is a group of automorphisms of $\mathcal{D}$. Consequently, the cycle structure of $t\rho_1$ is the same as that for $t\rho_2$, for all $t\in T$, see [22, Corollary 3.2]. Hence, $|\mathrm{supp}(t\rho_1)|=|\mathrm{supp}(t\rho_2)|$ for all $t\in T$.

An open question for the cases in Sections 4.4 and 4.5 is whether $C(T,\mathcal{I})$ is equivalent to $\mathrm{Rep}_r(C(T,\rho_i))$, for $i=1$ or 2, under the automorphisms of the Hamming graph.

5 Neighbour transitivity

Let C be a code in $H(m,q)$. For any vertex v in $H(m,q)$ we let

$$d(v,C)=\min\{d(v,\beta):\beta\in C\}$$

and

$$C_i=\{v:d(v,C)=i\}.$$

We call C_1 the *set of neighbours of* C, and if there exists a group of automorphisms G such that both C and C_1 are G-orbits, then we say that C is *G-neighbour transitive*, or simply *neighbour transitive*.

Throughout this section T is one of the groups from Table 2, and $C(T,\mathcal{I})$ is the code generated by $\mathcal{I}=(\rho_1,\rho_2)$ where ρ_1 is the identity map and ρ_2 is an outer automorphism of T such that $\rho_2^2=\rho_1$. As we mentioned in the introduction, one of the motivations for considering twisted permutation codes comes from the family of neighbour transitive permutation codes classified in [17] and their subsequent neighbour transitive repetition constructions. In this section we prove the following for the codes presented above.

Theorem 5.1. *For each T in Table 2, the code $C(T,\mathcal{I})$ is neighbour transitive.*

Before we prove Theorem 5.1, we first show that any automorphism of T defines an automorphism of $N_{S_q}(T)$. We define the following homomorphism:

$$\begin{aligned}\vartheta : N_{S_q}(T) &\to \mathrm{Aut}(T),\\ y &\mapsto \overline{y},\end{aligned} \tag{5.1}$$

where $t^{\overline{y}}=y^{-1}ty$ for all $t\in T$, and we denote the image of $N_{S_q}(T)$ by $\overline{N_{S_q}(T)}$.

Since T is acting 2-transitively, and therefore primitively, it follows that

$$\ker(\vartheta) = C_{S_q}(T) = 1,$$

see [14, Theorem 4.2A]. Hence $N_{S_q}(T) \cong \overline{N_{S_q}(T)}$. For each group in Table 2 it is known that $\overline{N_{S_q}(T)}$ is a subgroup of index 2 in $\mathrm{Aut}(T)$, and therefore is normal in $\mathrm{Aut}(T)$. Thus for $\rho \in \mathrm{Aut}(T)$ and $y \in N_{S_q}(T)$ one has $\rho^{-1}\overline{y}\rho \in \overline{N_{S_q}(T)}$. Moreover, because $N_{S_q}(T) \cong \overline{N_{S_q}(T)}$, there exists a unique $y' \in N_{S_q}(T)$ such that $\rho^{-1}\overline{y}\rho = \overline{y'}$. Thus, for $\rho \in \mathrm{Aut}(T)$, $\hat{\rho} : N_{S_q}(T) \mapsto N_{S_q}(T)$ given by

$$y\hat{\rho} = \vartheta^{-1}(\rho^{-1}\overline{y}\rho) = y' \tag{5.2}$$

is a well-defined automorphism of $N_{S_q}(T)$. We note that (5.2) implies

$$\overline{y\hat{\rho}} = \rho^{-1}\overline{y}\rho.$$

To simplify the notation, for $y \in N_{S_q}(T)$ we write $y\rho$ for $y\hat{\rho}$, and regard ρ as a representation of $N_{S_q}(T)$.

The code $C(T, \mathcal{I})$ is contained in the vertex set of $\Gamma^2 = H(2q, q)$, which we can identify with the set of arbitrary 2-tuples of vertices from $\Gamma = H(q, q)$. Thus, given arbitrary automorphisms $x, y \in \mathrm{Aut}(\Gamma)$, we let $(x, y) \in \mathrm{Aut}(\Gamma) \times \mathrm{Aut}(\Gamma)$ act on the vertices of Γ^2 in the following way:

$$(\alpha_1, \alpha_2)^{(x,y)} = (\alpha_1^x, \alpha_2^y), \tag{5.3}$$

where $\alpha_1, \alpha_2 \in V(\Gamma)$. We now construct a group of automorphisms of $C(T, \mathcal{I})$ that stabilises $\alpha(1, \mathcal{I})$. To do this we first construct an automorphism of $C(T, \rho)$, for any $\rho \in \mathrm{Aut}(T)$, in $\Gamma = H(q, q)$. Now ρ defines an automorphism of $N_{S_q}(T)$, so $y\rho \in N_{S_q}(T)$ for $y \in N_{S_q}(T)$, and we let

$$\begin{aligned} x_{y\rho} = (y\rho, \ldots, y\rho) &\in B \cong S_q^q, \\ \sigma(y\rho) &\in L \cong S_q, \\ a(y, \rho) = x_{y\rho}\sigma(y\rho) &\in \mathrm{Aut}(\Gamma). \end{aligned}$$

Suppose that $i^{y\rho} = j$. Then it follows that

$$\alpha(t, \rho)^{a(y,\rho)}|_j = i^{t\rho y\rho} = j^{(y\rho)^{-1}t\rho y\rho} = j^{(y^{-1}ty)\rho},$$

and hence

$$\alpha(t, \rho)^{a(y,\rho)} = \alpha(y^{-1}ty, \rho). \tag{5.4}$$

We now define

$$A(T, \mathcal{I}) = \{a(y, \mathcal{I}) = (a(y, \rho_1), a(y, \rho_2)) : y \in N_{S_q}(T)\},$$

where we regard ρ_1, ρ_2 as representations of $N_{S_q}(T)$. Allowing $A(T, \mathcal{I})$ to act on vertices of Γ^2 as in (5.3), it follows from (5.4) that

$$\alpha(t, \mathcal{I})^{a(y,\mathcal{I})} = \alpha(y^{-1}ty, \mathcal{I})$$

for all $t \in T$. As $y \in N_{S_q}(T)$, we deduce that $A(T, \mathcal{I})$ is a group of automorphisms $C(T, \mathcal{I})$ that stabilises $\alpha(1, \mathcal{I})$.

Let σ be the automorphism of Γ^2 that maps (α_1, α_2) to (α_2, α_1) for all vertices $\alpha_1, \alpha_2 \in V(\Gamma)$. We observe that $\alpha(t, \rho) = \alpha(t\rho, \rho_1)$ for any $\rho \in \mathrm{Aut}(T)$ and any $t \in T$ (recall ρ_1 is the identity automorphism). Hence, recalling that $\rho_2^2 = \rho_1$, it follows that

$$\alpha(t, \mathcal{I})^{\sigma} = (\alpha(t, \rho_2), \alpha(t, \rho_1)) = (\alpha(t\rho_2, \rho_1), \alpha(t\rho_2, \rho_2)) = \alpha(t\rho_2, \mathcal{I}).$$

Thus σ is also an automorphism of $C(T, \mathcal{I})$ that stabilises $\alpha(1, \mathcal{I})$.

Lemma 5.2. *Let $H = \langle A(T, \mathcal{I}), \sigma \rangle$. Then H acts transitively on $\Gamma_1^2(\alpha(1, \mathcal{I}))$.*

Proof. We first describe the neighbours of the codeword $\alpha(1, \rho)$ for $\rho \in \mathrm{Aut}(T)$ in $\Gamma = H(q, q)$. Following the notation of [17], for $1 \leqslant i, j, k \leqslant q$ we let

$$\nu(\alpha(1, \rho), i, j)|_k = \begin{cases} k & \text{if } k \neq i, \\ j & \text{if } k = i, \end{cases}$$

so

$$\Gamma_1(\alpha(1, \rho)) = \{\nu(\alpha(1, \rho), i, j) : i \neq j\}.$$

It follows from [17, Lemma 1] and (5.4) that

$$\nu(\alpha(1, \rho), i, j)^{a(y,\rho)} = \nu(\alpha(1, \rho)^{a(y,\rho)}, i^{y\rho}, j^{y\rho}) = \nu(\alpha(1, \rho), i^{y\rho}, j^{y\rho}).$$

Thus, because $N_{S_q}(T)$ is acting 2-transitively, we deduce that

$$A(T, \rho) = \{a(y, \rho) : y \in N_{S_q}(T)\}$$

acts transitively on $\Gamma_1(\alpha(1, \rho))$ in Γ. Hence $A(T, \mathcal{I})$ has two orbits on $\Gamma_1^2(\alpha(1, \mathcal{I}))$ in Γ^2, which are

$$\mathcal{O}_1 = \{(\nu, \alpha(1, \rho_2)) : \nu \in \Gamma_1(\alpha(1, \rho_1))\},$$
$$\mathcal{O}_2 = \{(\alpha(1, \rho_1), \nu) : \nu \in \Gamma_1(\alpha(1, \rho_2))\}.$$

Because $1\rho_2 = 1$, it follows that $\alpha(1, \rho_2) = \alpha(1\rho_2, \rho_1) = \alpha(1, \rho_1)$, and so

$$\Gamma_1(\alpha(1, \rho_1)) = \Gamma_1(\alpha(1, \rho_2)).$$

Thus σ interchanges $\mathcal{O}_1$ and $\mathcal{O}_2$. □

We prove Theorem 5.1 by considering the group $G = \langle \mathrm{Diag}(T, \mathcal{I}), A(T, \mathcal{I}), \sigma \rangle$. It follows from Lemma 3.3 that $\mathrm{Diag}(T, \mathcal{I})$ acts regularly on $C(T, \mathcal{I})$. Adding to this the result of Lemma 5.2, we deduce that G is a group of automorphisms of $C(T, \mathcal{I})$ that acts transitively on $C(T, \mathcal{I})$. It also follows from Lemma 5.2 that the stabiliser of $\alpha(1, \mathcal{I})$ in G is equal to H. By allowing G to translate any two neighbours of $C(T, \mathcal{I})$ to two neighbours of $\alpha(1, \mathcal{I})$, and then allowing an element of H to map one of these neighbours to the other, we deduce that G acts transitively on the set of neighbours of $C(T, \mathcal{I})$, which proves Theorem 5.1.

6 The affine special linear group ASL(2, r)

Let $V = \mathbb{F}_r^2$ be the two-dimensional vector space of row vectors over the finite field $\mathbb{F}_r$ of size $r = 2^f$ for some positive integer $f \geqslant 2$. The group $\mathrm{ASL}(2, r)$ is equal to the split extension of N, the translations of V, by $\mathrm{SL}(2, r)$, the group of invertible 2×2 matrices over $\mathbb{F}_r$ with determinant 1, and $\mathrm{ASL}(2, r)$ has a natural 2-transitive action on V. It is known that there are r conjugacy classes of complements of N in $\mathrm{ASL}(2, r)$ (see [10]). By embedding $\mathrm{ASL}(2, r)$ into $\mathrm{SL}(3, r)$, in this section we construct a representative for each of these conjugacy classes. Then, by considering the coset action on each representative, we give an explicit construction of the r inequivalent 2-transitive actions of $\mathrm{ASL}(2, r)$ of degree r^2. We let $\mathcal{I} = (\rho_1, \ldots, \rho_r)$, where the ρ_i are the representations for these inequivalent actions, and we prove the following.

Theorem 6.1. *Let $\mathcal{I}$ be as above. Then the code $C(\mathrm{ASL}(2, r), \mathcal{I})$ has the same inner distance distribution, and therefore also the same minimum distance, as the code $\mathrm{Rep}_r(C(\mathrm{ASL}(2, r), \rho_i))$ for $i = 1, \ldots, r$.*

Remark 6.2. The code in Theorem 6.1 shows us that given any even prime power r, we can construct a twisted permutation code with r pairwise distinct representations such that the code has a minimum distance equal to the lower bound of Proposition 3.3 (iii).

To embed $\mathrm{ASL}(2, r)$ into $\mathrm{SL}(3, r)$ we begin by taking an element a of order $r - 1$ in $\mathbb{F}_r^*$ and letting $b = (1 + a^2)^{-1}$. As $f \geqslant 2$, we see that b is well defined. Consider the matrices

$$x = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad z = \begin{pmatrix} b & b^2 + b + 1 \\ 1 & b + 1 \end{pmatrix}. \tag{6.1}$$

For every $w \in \mathbb{F}_r$ we define

$$u = wa + wb + w \quad \text{and} \quad v = w + wa,$$

and

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a^{-1} \end{pmatrix}, \qquad Y_w = \begin{pmatrix} 1 & 0 & v \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

$$Z_w = \begin{pmatrix} 1 & w & u \\ 0 & b & b^2+b+1 \\ 0 & 1 & b+1 \end{pmatrix}, \quad S_w = \langle X, Y_w, Z_w \rangle.$$

Lemma 6.3. *We have* $\mathrm{SL}(2,r) = \langle x, y, z \rangle$ *and* $\mathrm{SL}(2,r) \cong S_w$.

Proof. As the field element a has order $r-1$, we have

$$x^{r-1} = 1 \quad \text{and} \quad X^{r-1} = 1. \tag{6.2}$$

Also, a direct computation shows that

$$y^2 = 1 \quad \text{and} \quad Y_w^2 = 1. \tag{6.3}$$

The characteristic polynomial of z is

$$(\Lambda - b)(\Lambda - (b+1)) + b^2 + b + 1 = \Lambda^2 + \Lambda + 1$$

and hence $z^2 + z + 1 = 0$. From this it follows with an easy computation that

$$z^3 = 1 \quad \text{and} \quad Z_w^3 = 1. \tag{6.4}$$

Using the definition of a, b, X, Y_w and Z_w, we see with a rather long (but simple and direct) computation that

$$\begin{aligned} (xz)^2 = (yz)^2 = [x^i, y]^2 = 1, \\ (XZ_w)^2 = (Y_w Z_w)^2 = [X^i, Y_w]^2 = 1, \end{aligned} \tag{6.5}$$

for every $i \in \{0, \ldots, r-1\}$.

Since r is even, we see that a^2 is also a generator of the multiplicative group of the field $\mathbb{F}_r$. So, let

$$p(\Lambda) = c_f \Lambda^f + c_{f-1}\Lambda^{f-1} + c_{f-2}\Lambda^{f-2} + \cdots + c_1\Lambda + c_0$$

be the minimal polynomial of a^2 over the ground field $\mathbb{F}_2$, that is, $c_i \in \{0,1\}$ and $p(a^2) = 0$. Now a computation shows that

$$y^{c_0} x y^{c_1} x y^{c_2} x \cdots x y^{c_f} = \begin{pmatrix} a^f & \zeta \\ 0 & a^{-f} \end{pmatrix}$$

with

$$\zeta = c_f a^f + c_{f-1}a^{f-2} + c_{f-2}a^{f-4} + \cdots + c_1 a^{-f+2} + c_0 a^{-f}.$$

In particular, $a^f \zeta = p(a^2) = 0$ and hence $\zeta = 0$. This gives that

$$x^f = y^{c_0} x y^{c_1} x y^{c_2} x \cdots x y^{c_f}. \tag{6.6}$$

Similarly, we have

$$Y_w^{c_0} X Y_w^{c_1} X Y_w^{c_2} X \cdots X Y_w^{c_f} = \begin{pmatrix} 1 & 0 & v\zeta \\ 0 & a^f & \zeta \\ 0 & 0 & a^{-f} \end{pmatrix} = X^f. \tag{6.7}$$

As x, y and z have determinant 1, we have $\langle x, y, z\rangle \leqslant \mathrm{SL}(2, r)$. Also, we see from [13, Section 7.6, lines 9–10] that $\mathrm{SL}(2, r)$ has presentation with three generators R, S and U and with relators

$$\begin{aligned} &R^{r-1} = S^2 = U^3 = (RU)^2 = (SU)^2 = 1, \\ &[R^i, S]^2 = 1 \quad \text{for every } i \in \{1, \ldots, r-1\}, \\ &R^f = S^{c_0} R S^{c_1} R S^{c_2} R \cdots S^{c_{f-1}} R S^{c_f}. \end{aligned}$$

In particular, from (6.2)–(6.7) we obtain that $\langle x, y, z\rangle$ and S_w both satisfy the defining relations of $\mathrm{SL}(2, r)$ and hence are isomorphic to a quotient of $\mathrm{SL}(2, r)$. Since $f \geqslant 2$, the group $\mathrm{SL}(2, r)$ is simple and the lemma follows. □

For $\mathbf{v} \in V$ let $\varphi_{\mathbf{v}}$ denote the translation of V by $\mathbf{v}$. By letting $\varphi_{\mathbf{v}}$, x, y and z act on an arbitrary vector of V, we determine the following relations:

$$x^{-1}\varphi_{\mathbf{v}} x \varphi_{\mathbf{v}x} = y^{-1}\varphi_{\mathbf{v}} y \varphi_{\mathbf{v}y} = z^{-1}\varphi_{\mathbf{v}} z \varphi_{\mathbf{v}z} = 1 \quad \text{for all } \mathbf{v} \in V. \tag{6.8}$$

If $\mathbf{v} = (v_1, v_2) \in V$, we let

$$e(\mathbf{v}) = \begin{pmatrix} 1 & v_1 & v_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$E = \{e(\mathbf{v}) : \mathbf{v} \in V\}.$$

Direct calculation shows that, for $\mathbf{v} \in V$ and $w \in \mathbb{F}_r$, the following relations hold:

$$X^{-1} e(\mathbf{v}) X e(\mathbf{v}\,x) = Y_w^{-1} e(\mathbf{v}) Y_w e(\mathbf{v}\,y) = Z_w^{-1} e(\mathbf{v}) Z_w e(\mathbf{v}\,z) = 1. \tag{6.9}$$

It is a consequence of (6.9) that S_w normalises E for each w. Furthermore, by Lemma 6.3, $S_w \cong \mathrm{SL}(2,r)$, which is simple as $f \geqslant 2$, and so $E \cap S_w = 1$ for each w. Thus we can define

$$G = ES_0,$$

the split extension of E by S_0. Since $Y_w = e(\mathbf{v_1})Y_0$ and $Z_w = e(\mathbf{v_2})Z_0$ where $\mathbf{v_1} = (0,v)$, $\mathbf{v_2} = (w,u) \in V$, we conclude that S_w is a subgroup of G for each w. Hence G is also equal to the split extension of E by S_w for each w. Thus another consequence of Lemma 6.3 is that

$$\mathrm{ASL}(2,r) = \langle \varphi_{\mathbf{v}}, x, y, z : \mathbf{v} \in V \rangle,$$

and

$$G = \langle e(\mathbf{v}), X, Y_w, Z_w : \mathbf{v} \in V \rangle \quad \text{for each } w \in \mathbb{F}_r.$$

For $w \in \mathbb{F}_r$ let $\tau_w : \mathrm{ASL}(2,r) \to G$ be the group homomorphism that takes

$$x \mapsto X, \quad y \mapsto Y_w, \quad z \mapsto Z_w, \quad \text{and} \quad \varphi_{\mathbf{v}} \mapsto e(\mathbf{v}) \quad \text{for each } \mathbf{v} \in V.$$

We observe, from (6.2)–(6.9), that τ_w is well defined. Furthermore, because E and S_w are both subgroups of $\tau_w(\mathrm{ASL}(2,r))$, we deduce the following.

Lemma 6.4. *The map τ_w is an isomorphism from* $\mathrm{ASL}(2,r)$ *to G for each $w \in \mathbb{F}_r$.*

Note that since $H^1(\mathrm{SL}(2,r), N) \cong \mathbb{F}_r$ by [10, Table 4.3, type A_1], we have that the group $\mathrm{ASL}(2,r)$ contains exactly r conjugacy classes of complements of N in $\mathrm{ASL}(2,r)$. We now show that in this embedding of $\mathrm{ASL}(2,r)$ in $\mathrm{SL}(3,r)$, each conjugacy class of complements of N contains a unique group S_w for some $w \in \mathbb{F}_r$.

Lemma 6.5. *For each w and w' in $\mathbb{F}_r$ with $w \neq w'$, the groups S_w and $S_{w'}$ are not conjugate in G.*

Proof. Let w and w' be in $\mathbb{F}_r$ and suppose that S_w and $S_{w'}$ are conjugate in G. As $G = ES_w = ES_{w'}$ and $E \cap S_w = E \cap S_{w'} = 1$, it follows that S_w and $S_{w'}$ are conjugate via an element $e(\mathbf{v}) \in E$ for some $\mathbf{v} = (v_1, v_2) \in V$. Furthermore, as $X \in S_w \cap S_{w'}$, we have $X^{-1}, X^{e(\mathbf{v})} \in S_{w'}$ and hence $X^{-1}X^{e(\mathbf{v})} \in S_{w'}$. Now

$$X^{-1}X^{e(\mathbf{v})} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & a \end{pmatrix} \begin{pmatrix} 1 & v_1 & v_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & v_1 & v_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & v_1 + v_1 a & v_2 + v_2 a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

As $E \cap S_{w'} = 1$, we must have $v_1 + v_1 a = 0$ and $v_2 + v_2 a = 0$, that is, $v_1 a = v_1$ and $v_2 a = v_2$. Since $f \geqslant 2$, we have $a \neq 1$ and hence $v_1 = v_2 = 0$. This gives $e(\mathbf{v}) = 1$ and hence $S_w = S_{w'}$.

From the previous paragraph we have $Y_w, Y_{w'} \in S_w$ and hence $Y_w Y_{w'} \in S_w$. Now,

$$Y_w Y_{w'} = \begin{pmatrix} 1 & 0 & w + wa \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & w' + w'a \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & (w + w') + (w + w')a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $E \cap S_w = 1$, we must have $(w + w')a = w + w'$ and hence $w + w' = 0$. This gives $w = w'$ and the lemma follows. □

Let Ω_w be the set of right cosets of S_w in G. As S_w normalises E, and because $G = E S_w$, it follows that every right coset of S_w in Ω_w has a coset representative in E. Moreover, because $E \cap S_w = 1$, each $e(\mathbf{v}) \in E$ uniquely determines the right coset it belongs to. Hence the map $\iota_w : V \to \Omega_w$ given by $\mathbf{v} \mapsto S_w e(\mathbf{v})$ is a well-defined bijection.

Proposition 6.6. *Under (ι_w, τ_w), the action of G on Ω_w is permutationally isomorphic to the action of* $\mathrm{ASL}(2, r)$ *on V.*

Proof. Let $\mathbf{v} \in V$ and consider the generator y of $\mathrm{ASL}(2, r)$. From the definition of ι_w it follows that $\iota_w(\mathbf{v}y) = S_w e(\mathbf{v}y)$. Now, it follows from (6.8) that

$$\iota_w(\mathbf{v})\tau_w(y) = S_w e(\mathbf{v}) Y_w = S_w Y_w e(\mathbf{v}y) = S_w e(\mathbf{v}y).$$

Thus $\iota_w(\mathbf{v}y) = \iota_w(\mathbf{v})\tau_w(y)$. By applying similar arguments to the other generators of $\mathrm{ASL}(2, r)$, we conclude that (ι_w, τ_w) is a permutational isomorphism. □

It is a consequence of Proposition 6.6 that G acts 2-transitively on Ω_w for each $w \in \mathbb{F}_r$. Moreover, it follows from Lemma 6.5 and [5, Theorem 1.3] that for $w' \neq w$ the action of G on $\Omega_{w'}$ is inequivalent to the action of G on Ω_w. Hence these actions of G on Ω_w, for w in $\mathbb{F}_r$, are r pairwise inequivalent 2-transitive actions of degree r^2. Thus, by considering the action of $\mathrm{ASL}(2, r)$ on the right cosets of $\tau_0^{-1}(S_w)$ for each $w \in S_w$, it follows that $\mathrm{ASL}(2, r)$ has r inequivalent 2-transitive actions of degree r^2. To prove Theorem 6.1, we look at the number of fixed points of an element of $\mathrm{ASL}(2, r)$ in each of these actions.

Lemma 6.7. *Let* $1 \neq t \in \mathrm{ASL}(2, r)$ *be an element that has at least two fixed points in some* 2*-transitive representation of degree* r^2*. Then* t *fixes* r *points in every* 2*-transitive representation. Moreover,* $|t| = 2$*.*

Proof. By Proposition 6.6, each 2-transitive action of $\mathrm{ASL}(2, r)$ of degree r^2 is permutationally isomorphic to its natural action on V. Thus without loss of generality, we can assume that t fixes at least two points in the natural action of $\mathrm{ASL}(2, r)$. As $\mathrm{ASL}(2, r)$ acts 2-transitively on V, it follows that t is conjugate to an element that fixes $\mathbf{0} = (0, 0)$ and $\mathbf{e_2} = (0, 1)$. It holds that

$$\mathrm{SL}(2, r)_{\mathbf{e_2}} = \left\{ M_c = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbb{F}_r \right\}, \tag{6.10}$$

so t is conjugate to $M_{c'}$ for some $c' \in \mathbb{F}_r^*$. It is straightforward to show that $\mathrm{fix}(M_{c'}) = \{(0, c) : c \in \mathbb{F}_r\}$ and $|M_{c'}| = 2$. So t fixes r points in this action and has order 2. Now, as r is an even prime power, $c' = \ell^2$ for some $\ell \in \mathbb{F}_r$. Conjugating $M_{c'}$ by the diagonal matrix $\mathsf{Diag}(\ell, \ell^{-1})$ gives the group element y in (6.1). Moreover, for $0 \neq w$, it holds that

$$\tau_0^{-1} \tau_w(y) = \tau_0^{-1}(Y_w) = \varphi_{\mathbf{v}} y,$$

where $\mathbf{v} = (0, v)$ with $v = w + wa$, and $\mathrm{fix}(\varphi_{\mathbf{v}} y) = \{(v, c) : c \in \mathbb{F}_r\}$. It follows that $\tau_0^{-1} \tau_w(t)$ fixes r points. In particular, t fixes r points in every 2-transitive representation. □

Corollary 6.8. *Let* $t \in \mathrm{ASL}(2, r)$*. Then* t *fixes* 0*,* 1 *or* r *points in each* 2*-transitive representation of* $\mathrm{ASL}(2, r)$ *of degree* r^2*.*

Lemma 6.9. *Let* $t \in \mathrm{ASL}(2, r)$ *be a non-trivial element of odd order. Then* t *fixes exactly one point in each* 2*-transitive representation of* $\mathrm{ASL}(2, r)$*.*

Proof. Suppose in some 2-transitive representation of $\mathrm{ASL}(2, r)$ that t has no fixed points. Then in that representation t has a cycle of minimal length $b > 1$. As the order of t is equal to the least common multiple of the disjoint cycle lengths of t, it follows that b is odd as $|t|$ is odd. If all the disjoint cycles have length b, then b divides r^2 (because t has no fixed points), which is a contradiction as $r = 2^f$. Thus there exists a cycle of length $c > b$. Hence $t^b \neq 1$, and t^b fixes at least $b > 1$ points. By Lemma 6.7, it follows that t^b fixes r points and $|t^b| = 2$. Hence $t^{2b} = 1$. Now, because $t^b \neq 1$ and $|t|$ is a multiple of b, it follows that $|t| = 2b$, contradicting the fact that $|t|$ is odd. Thus t fixes at least one point in every representation. If t fixes more than one point in some representation, then by Lemma 6.7, $|t| = 2$, which is a contradiction. □

Lemma 6.10. *Let $t \in \mathrm{ASL}(2,r)$ be an element of even order. Then t fixes the same number of points in each 2-transitive representation of* $\mathrm{ASL}(2,r)$.

Proof. Suppose $|t| = 2$. Then, in any 2-transitive representation of $\mathrm{ASL}(2,r)$, t can be written as the disjoint union of transpositions. Thus t cannot fix exactly one point, otherwise 2 would divide $r^2 - 1$, which is a contradiction. Hence, by Corollary 6.8, t either fixes r points or 0 points. By Lemma 6.7, if t fixes r points, then t fixes r points in each 2-transitive representation of $\mathrm{ASL}(2,r)$. Hence if t has no fixed points, then t has no fixed points in every 2-transitive representation of $\mathrm{ASL}(2,r)$.

Now assume that $|t| > 2$. Because $|t| > 2$, it follows from Lemma 6.7 that t cannot fix r points. So, in every 2-transitive representation, t fixes either 0 or 1 point. Suppose t fixes one point in some 2-transitive representation, and let b be the minimal non-trivial cycle length of t in that representation. Further suppose that $t^b = 1$, so $|t| = b$. Then the disjoint union of the points in the b-cycles of t is equal to support of t, which has size $r^2 - 1$. Hence b divides $r^2 - 1$. Thus b is odd, contradicting the fact that $|t|$ is even. Hence $t^b \neq 1$. Now, t^b fixes at least $1 + b$ points, so by Lemma 6.7, t^b fixes r points and $|t^b| = 2$. Hence $|t| = 2b$. Moreover, the set of $r - 1$ fixed points of t^b points that are not fixed by t is equal the disjoint union of the points that form the b-cycles of t. Hence b divides $r - 1$, and so b is odd. However, as t fixes one point, it follows that t is conjugate to some $h \in \mathrm{SL}(2,r)$, and so t^b is conjugate to $h^b \in \mathrm{SL}(2,r)$. Now, $\mathrm{SL}(2,r)$ has only one conjugacy class of involutions (see for example [18, p. 95]), so h^b is conjugate the element y in (6.1). It is straightforward to show that the subgroup $\mathrm{SL}(2,r)_{\mathbf{e}_2}$ from (6.10) is the centraliser in $\mathrm{SL}(2,r)$ of y, and has order r. Hence, because h centralises h^b it follows that $|h|$ divides r, and so $|t|$ divides r, contradicting the fact that $|t| = 2b$ with b odd. So t has no fixed points in each 2-transitive representation of $\mathrm{ASL}(2,r)$. □

To prove Theorem 6.1, we let $\mathcal{I} = (\rho_1, \ldots, \rho_r)$, where the ρ_i are the representations of the r inequivalent 2-transitive actions of $\mathrm{ASL}(2,r)$ of degree r^2. It is a consequence of Lemmas 6.9 and 6.10 that

$$|\mathrm{fix}(t\rho_i)| = |\mathrm{fix}(t\rho_j)|$$

for all i, j and for all $t \in \mathrm{ASL}(2,r)$. Hence

$$|\mathrm{supp}(t\rho_i)| = |\mathrm{supp}(t\rho_j)|$$

for all i, j and for all $t \in \mathrm{ASL}(2,r)$. Thus Theorem 6.1 is now a consequence of Lemma 3.5.

7 Coset actions on the computer

In this final section we use the algebraic computer software GAP [16] to analyse two further groups acting on sets of cosets of certain subgroups.

7.1 The affine group ASL(3, 2)

We first consider the 2-transitive action of the affine group AGL(3, 2) on $\mathbb{F}_2^3$. It is well known that the number of distinct actions of a 2-transitive group G of affine type is equal to the order of the cohomology group $H^1(G_0, N)$ ([5, Section 7.3]), where G_0 is the stabiliser of a point in the natural action of G and N is the unique minimal normal subgroup of G. This in turn is equal to the number of G-conjugacy classes of the complements of N in G. For the group AGL(3, 2), there are two distinct actions [5, Table 7.3]. To generate these actions, we use the "Complementclasses" function in GAP to find two representatives H_1, H_2 of these conjugacy classes. If Ω_i is the set of right cosets of H_i in ASL(3, 2), we can construct in GAP the representation $\rho_i : \mathrm{ASL}(3,2) \to \mathrm{Sym}(\Omega_i)$ that describes the action of ASL(3, 2) on Ω_i, for $i = 1, 2$. The group AGL(3, 2) has eleven conjugacy classes $\mathcal{C}_j$, and for each one, we calculate $|\mathrm{supp}(t\rho_i)|$ for some $t \in \mathcal{C}_j$ for $i = 1, 2$ and $j = 1, \ldots, 11$. We give this information in Table 7. The minimal degree of both actions is 4, so $\mathrm{Rep}_2(\mathrm{AGL}(3,2), \rho_i)$ has minimum distance 8 for $i = 1$ or 2. However, it follows from Proposition 3.3 that $C(\mathrm{AGL}(3,2), \mathcal{I})$ has minimum distance 12, where $\mathcal{I} = (\rho_1, \rho_2)$.

Conjugacy class	1	2	3	4	5	6	7	8	9	10	11
$\lvert\mathrm{supp}(t\rho_1)\rvert$	0	8	4	8	8	6	8	6	8	7	7
$\lvert\mathrm{supp}(t\rho_2)\rvert$	0	8	8	4	8	8	6	6	8	7	7
Sum of supports	0	16	12	12	16	14	14	12	16	14	14

Table 7. The affine group ASL(3, 2).

7.2 The symmetric group S_6

The second action we consider is S_6 acting on the right cosets of subgroups of order 12. Using GAP, we determine that S_6 has four conjugacy classes of subgroups of order 12. Let H_i be a representative for each conjugacy class, Ω_i be the set of right cosets of H_i in S_6, and ρ_i be the representation that describes the action. We calculate in GAP the size of the supports for an element from each

Conjugacy class	1A	2A	2B	2C	3A	3B	4A	4B
$\lvert\mathrm{supp}(t\rho_1)\rvert$	0	56	60	60	60	48	60	60
$\lvert\mathrm{supp}(t\rho_2)\rvert$	0	56	60	60	48	60	60	60
$\lvert\mathrm{supp}(t\rho_3)\rvert$	0	56	44	60	57	60	60	60
$\lvert\mathrm{supp}(t\rho_4)\rvert$	0	56	60	44	60	57	60	60
Sum of supports	0	224	224	224	225	225	240	240

Conjugacy class	5AB	6A	6B
$\lvert\mathrm{supp}(t\rho_1)\rvert$	60	60	60
$\lvert\mathrm{supp}(t\rho_2)\rvert$	60	60	60
$\lvert\mathrm{supp}(t\rho_3)\rvert$	60	59	60
$\lvert\mathrm{supp}(t\rho_4)\rvert$	60	60	59
Sum of supports	240	239	239

Table 8. The symmetric group S_6 acting on subgroups of order 12, one from each of the four conjugacy classes.

conjugacy class for each representation, which we present in Table 8. From this table we see that S_6 under ρ_3 has the smallest minimal degree, which is 44. Thus, by letting $\mathcal{I} = (\rho_1, \ldots, \rho_4)$, it follows that

$$\min_{\rho\in\mathcal{I}}\{\delta(\mathrm{Rep}_4(C(T,\rho))\} = 4 \cdot 44 = 176.$$

However, Proposition 3.3 implies that $C(S_6, \mathcal{I})$ has minimum distance 224, the minimum of the sums of the supports over the four actions, as is shown in Table 8.

The minimum distance of $C(S_6, \mathcal{I})$ is actually maximal from an alternative perspective. Consider the set of representations $\mathcal{S} = \{\rho_1, \rho_2, \rho_3, \rho_4\}$. Let $\mathcal{I}$ be formed by taking any four elements from $\mathcal{S}$ but allowing repeats of representations. Note that the order in which the representations appear in $\mathcal{I}$ does not affect the minimum distance of the code it generates. Using GAP, we calculate the minimum distance $\delta(C)$ of $C = C(S_6, \mathcal{I})$ for each possible $\mathcal{I}$ and give this in Table 9. We see that this minimum distance is maximised when each representation appears exactly once in $\mathcal{I}$, as above. In Table 9 we label $\mathcal{I} = (\rho_{i_1}, \rho_{i_2}, \rho_{i_3}, \rho_{i_4})$ by $\{i_1, i_2, i_3, i_4\}$.

$\mathcal{J}$	$\delta(C)$	$\mathcal{J}$	$\delta(C)$	$\mathcal{J}$	$\delta(C)$
$\{1,1,1,1\}$	192	$\{2,2,2,1\}$	204	$\{4,4,4,2\}$	192
$\{2,2,2,2\}$	192	$\{2,2,2,3\}$	201	$\{4,4,4,3\}$	192
$\{3,3,3,3\}$	176	$\{2,2,2,4\}$	204	$\{1,1,2,2\}$	216
$\{4,4,4,4\}$	176	$\{3,3,3,1\}$	192	$\{1,1,3,3\}$	208
$\{1,1,1,2\}$	204	$\{3,3,3,2\}$	192	$\{1,1,4,4\}$	208
$\{1,1,1,3\}$	204	$\{3,3,3,4\}$	192	$\{2,2,3,3\}$	208
$\{1,1,1,4\}$	201	$\{4,4,4,1\}$	192	$\{2,2,4,4\}$	208

$\mathcal{J}$	$\delta(C)$	$\mathcal{J}$	$\delta(C)$
$\{3,3,4,4\}$	208	$\{3,3,1,2\}$	208
$\{1,1,2,3\}$	216	$\{3,3,1,4\}$	208
$\{1,1,2,4\}$	213	$\{3,3,2,4\}$	208
$\{1,1,3,4\}$	214	$\{4,4,1,2\}$	208
$\{2,2,1,3\}$	213	$\{4,4,1,3\}$	208
$\{2,2,1,4\}$	216	$\{4,4,2,3\}$	208
$\{2,2,3,4\}$	213	$\{1,2,3,4\}$	224

Table 9. The symmetric group S_6 acting on subgroups of order 12, one from each of the four conjugacy classes.

7.3 Proof of Theorem 1.1

Let T be an abstract group, $\mathcal{J}$ be an ordered r-tuple of (not necessarily distinct) permutation representations of T into S_q for some q. By letting $\delta_{\mathrm{tw}} = \delta(C(T,\mathcal{J}))$ and $\delta_{\mathrm{rep}} = \min_{\rho\in\mathcal{J}}\{\delta(\mathrm{Rep}_r(C(T,\rho))\}$, the first assertions of Theorem 1.1 follow from Proposition 3.3. The final assertions follow from Sections 4.1, 4.2, 7.1 and 7.2.

Bibliography

[1] R. F. Bailey, Error-correcting codes from permutation groups, *Discrete Math.* **309** (2009), no. 13, 4253–4265.

[2] I. Blake, Permutation codes for discrete channels, *IEEE Trans. Inform. Theory* **20** (1974), no. 1, 138–140.

[3] I. F. Blake, G. Cohen and M. Deza, Coding with permutations, *Inf. Control* **43** (1979), no. 1, 1–19.

[4] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Ergeb. Math. Grenzgeb. (3) 18, Springer-Verlag, Berlin, 1989.

[5] P. J. Cameron, *Permutation Groups*, London Math. Soc. Stud. Texts 45, Cambridge University Press, Cambridge, 1999.

[6] P. J. Cameron and M. Gadouleau, Remoteness of permutation codes, *European J. Combin.* **33** (2012), no. 6, 1273–1285.

[7] P. J. Cameron and I. M. Wanless, Covering radius for sets of permutations, *Discrete Math.* **293** (2005), no.1–3, 91–109.

[8] W. Chu, C. J. Colbourn and P. Dukes, Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.* **32** (2004), no. 1–3, 51–64.

[9] W. Chu, C. J. Colbourn and P. Dukes, On constant composition codes, *Discrete Appl. Math.* **154** (2006), no. 6, 912–929.

[10] E. Cline, B. Parshall and L. Scott, Cohomology of finite groups of Lie type. I, *Publ. Math. Inst. Hautes Études Sci.* **45** (1975), 169–191.

[11] C. J. Colbourn, T. Kløve and A. C. H. Ling, Permutation arrays for powerline communication and mutually orthogonal Latin squares, *IEEE Trans. Inform. Theory* **50** (2004), no. 6, 1289–1291

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Eynsham, 1985.

[13] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 3rd ed., Springer-Verlag, New York, 1972.

[14] J. D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. 163, Springer-Verlag, New York, 1996.

[15] P. Frankl and M. Deza, On the maximum number of permutations with given maximal or minimal distance, *J. Combin. Theory Ser. A* **22** (1977), no. 3, 352–360.

[16] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.3, 2013, `http://www.gap-system.org`.

[17] N. Gillespie and C. Praeger, Diagonally neighbour transitive codes and frequency permutation arrays, *J. Algebraic Combin.* **39** (2014), no. 3, 733–747.

[18] L. C. Grove, *Groups and Characters*, John Wiley & Sons, New York, 1997.

[19] A. J. Han Vinck, Coded modulation for power line communications, *AEÜ Int. J. Electron. Comm.* **54** (2000), 45–49.

[20] S. Huczynska, Equidistant frequency permutation arrays and related constant composition codes, *Des. Codes Cryptogr.* **54** (2010), no. 2, 109–120.

[21] S. Huczynska and G. L. Mullen, Frequency permutation arrays, *J. Combin. Des.* **14** (2006), no. 6, 463–478.

[22] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc. Lecture Note Ser. 74, Cambridge University Press, Cambridge, 1983.

[23] Y. Luo, F. W. Fu, A. J. H. Vinck and W. Chen, On constant-composition codes over Z_q, *IEEE Trans. Inform. Theory* **49** (2003), no. 11, 3010–3016.

[24] N. Pavlidou, A. Han Vinck, J. Yazdani and B. Honary, Power line communications: State of the art and future trends, *IEEE Commun. Mag.* **41** (2003), no. 4, 34–40.

Received April 3, 2014.

Author information

Neil I. Gillespie, Heilbronn Institute for Mathematical Research,
School of Mathematics, Howard House, University of Bristol, United Kingdom.
E-mail: neil.gillespie@bristol.ac.uk

Cheryl E. Praeger, Centre for Mathematics of Symmetry and Computation,
School of Mathematics and Statistics, The University of Western Australia,
35 Stirling Highway, Crawley, Western Australia 6009, Australia;
and King Abdulaziz University, Jeddah, Saudi Arabia.
E-mail: cheryl.praeger@uwa.edu.au

Pablo Spiga, Dipartimento di Matematica e Applicazioni,
University of Milano–Bicocca, Via Cozzi 55, 20125 Milano, Italy.
E-mail: pablo.spiga@unimib.it