Increasing the minimum distance of codes by twisting

Marzieh Akbari
Faculty of Mathematics
K. N. Toosi University of Technology
Tehran, Iran
m.akbari@dena.kntu.ac.ir

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

Cheryl E. Praeger
Centre for the Mathematics of Symmetry and Computation
Department of Mathematics and Statistics
The University of Western Australia
Australia
cheryl.praeger@uwa.edu.au

Submitted: Jan 8, 2016; Accepted: Jul 28, 2018; Published: Aug 24, 2018

Abstract

Twisted permutation codes, introduced recently by the second and third authors, belong to the family of frequency permutation arrays. Like some other codes in this family, such as the repetition permutation codes, they are obtained by a repetition construction applied to a smaller code (but with a "twist" allowed). The minimum distance of a twisted permutation code is known to be at least the minimum distance of a corresponding repetition permutation code, but in some instances can be larger. We construct two new infinite families of twisted permutation codes with minimum distances strictly greater than those for the corresponding repetition permutation codes. These constructions are based on two infinite families of finite groups and their representations. The first is a family of p-groups, for an odd prime p, while the second family consists of the 4-dimensional symplectic groups over a finite field of even order. In the latter construction, properties of the graph automorphism of these symplectic groups play an important role.

Mathematics Subject Classifications: 11T71, 20G40

1 Introduction

When considering the delivery of services to customers, the "last mile" refers to the often problematic last leg of the journey. In the case of infrastructure providers in the telecommunications industry, the "last mile" is the piece of infrastructure connecting the customer

to the main infrastructure. It has been proposed that this "last mile" could involve communication via powerlines as an effective means of delivering reliable telecommunications at low cost [11, 15]. Such a solution requires new kinds of encoding techniques for robust communication of information, and for this purpose constant composition codes, in particular the subclass of frequency permutation arrays, have been suggested as suitable coding schemes to solve the narrow band and impulse noise problems associated with powerline communication [4, 5].

Frequency permutation arrays (FPA) are also used with multilevel flash memories. Flash memory is an electronic non-volatile memory that uses floating-gate cells to store information: namely, cells are organized into blocks, where each block has a large number ($\approx 10^5$) of cells [6]. Given a set of n cells with distinct charge levels, the rank of a cell indicates the relative position of its own charge level, and so the ranks of the n cells induce a permutation of $\{1, 2, \ldots, n\}$. Schwartz et al. [14, 17] studied error-correcting codes for such permutations under the infinity norm, motivated by a novel storage scheme for flash memories called rank modulation (which uses these permutations). As for other applications of flash memory: Shieh and Tasi applied FPAs to provide multilevel flash memory with error correcting capabilities, and because of their efficient encoding and decoding algorithms, FPAs can be used in flash memory systems to represent information and correct errors caused by charge level fluctuation [16].

Our aim is to exploit an idea introduced in [10] to construct two new infinite families of FPAs with better error-correcting properties than those obtained by using a standard construction. Most of the examples given in [10] are related to specific 2-transitive permutation groups, and our motivation was to show that the technique could be successful in a broader setting. We now introduce the concepts.

A *constant composition code* of length m over an alphabet Q of size q is a subset of Q^m such that there are positive integers $p_1, \ldots, p_q$ with $\sum p_i = m$ and in each codeword the i^{th} letter of Q occurs p_i times. If the constants p_i are all equal, hence equal to $p = m/q$, such a code is called a *frequency permutation array* (FPA). FPAs have been studied, for example, in [4, 12, 13]. They also play an important role in the study of *neighbour transitive codes*, introduced by the second and third authors [7]. In particular they arise naturally in certain classifications of these codes [8, 9]. In the even more special case of FPAs with $m = q$, each codeword is a permutation on m letters; such an FPA is called an (m, d) *permutation array*, usually denoted by $PA(m, d)$, if the Hamming distance between any two distinct permutations in the set is at least d.

The codes we study are called *twisted permutation codes*. They are FPAs with potentially good error-correcting properties (see [10]). The construction method is based on using groups and their representations, and is a generalisation of the construction of repetition permutation codes. In [10], the second and third authors, with Spiga, proved that the error-correcting capability of a twisted permutation code is at least as good as that of a corresponding repetition permutation code for the group, and gave examples for which it was better (see [10, Table 1]). In this paper, we give two new infinite families of twisted permutation codes with improved error correcting capability. We hope that the ideas behind these constructions might suggest further new constructions with equal or

better improvements. *We would be interested to know how much improvement in error correction is possible: can this be quantified?*

For a finite group T, a homomorphism $\rho : T \to \mathrm{Sym}(\Omega)$ from T into the symmetric group of all permutations of a set Ω is called a *permutation representation* of T on Ω. Our construction involves typically several different permutation representations of T on the same set. One way in which such multiple permutation representations arise is by composing a given permutation representation ρ with an automorphism φ of T, since the map $\varphi \circ \rho$ (where we apply φ first and then ρ) is again a homomorphism from T to $\mathrm{Sym}(\Omega)$. See Section 2 for a discussion of the relevant concepts.

Let T be an abstract group, let $\mathcal{I}$ be an ordered r-tuple of permutation representations of T on the set $\{1, \ldots, q\}$ (with repeats allowed), and let ρ be (any) one of these representations. In Section 2.3 we define the twisted permutation code $C(T, \mathcal{I})$. A special case, the repetition permutation code, is $C(T, \rho^r)$ for the constant r-tuple $\rho^r = (\rho, \ldots, \rho)$. Twisted permutation codes are frequency permutation arrays of length rq over the alphabet $\{1, \ldots, q\}$ with each letter occurring r times in each codeword. Let δ_{tw} denote the minimum distance of $C(T, \mathcal{I})$, and let δ_{rep} be the minimum of the minimum distance of $C(T, \rho^r)$, over all ρ. We prove the following (noting that $|T| = p^{k+1}$ if $T = G_k$, and $|\mathrm{Sp}(4, 2^n)| = 2^{4n}(2^{4n} - 1)(2^{2n} - 1)$).

Theorem 1. *The twisted permutation codes described in Table* 1 *have size* $|T|$ *and minimum distance* δ_{tw} *strictly greater than* δ_{rep}.

T	r	q (permutation degree)	δ_{tw}	$\delta_{tw} - \delta_{\mathrm{rep}}$	Ref.
G_k	p	p^k	$p^{k+1} - p$	$p^2 - p$	Sec. 3 (Prop. 9)
$\mathrm{Sp}(4, 2^n)$	2	$2^{3n} + 2^{2n} + 2^n + 1$	$2^{3n+1} + 2^{2n}$	2^{2n}	Sec. 4 (Prop. 4.6)

Table 1: Twisted Permutation Codes with $\delta_{tw} > \delta_{\mathrm{rep}}$.

2 Definitions and Preliminaries

2.1 Codes in Hamming Graphs.

For positive integers m, q, each at least 2, the Hamming graph $\Gamma = H(m, q)$ is the graph whose vertex set $V(\Gamma)$ is the set of m-tuples with entries from an alphabet Q of size q, such that two vertices form an edge if and only if they differ in precisely one entry. A code C of length m over Q is a subset of $V(\Gamma)$.

The automorphism group of Γ, which we denote by $\mathrm{Aut}(\Gamma)$, is the semi-direct product $B \rtimes L$ where $B \cong S_q^m$ and $L \cong S_m$, see [2, Theorem 9.2.1]. Its action is described as follows: for $g = (g_1, \ldots, g_m) \in B$, $\sigma \in L$ and $\alpha = (\alpha_1, \ldots, \alpha_m) \in V(\Gamma)$,

$$\alpha^g = (\alpha_1^{g_1}, \ldots, \alpha_m^{g_m}), \quad \alpha^\sigma = (\alpha_{1^{\sigma^{-1}}}, \ldots, \alpha_{m^{\sigma^{-1}}}).$$

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, and so we usually refer simply to distance, rather than Hamming distance. The *minimum distance,* $\delta(C)$*,* defined only for codes C with at least two codewords, is the smallest distance between distinct codewords of C, that is,

$$\delta(C) := \min\{d(\alpha, \beta) | \alpha, \beta \in C, \alpha \neq \beta\}.$$

A code C is called *distance invariant* if, for all positive integers i, the number of codewords at distance i from a codeword $\alpha \in C$ is independent of the choice of α.

2.2 Permutation Groups

Let Ω be an arbitrary non-empty set. We denote by $\mathrm{Sym}(\Omega)$ the group of all permutations of Ω, called the symmetric group on Ω. A *permutation group* on Ω is a subgroup of $\mathrm{Sym}(\Omega)$. For $t \in \mathrm{Sym}(\Omega)$ and $\alpha \in \Omega$, we denote by α^t the image of α under t. Suppose that G is a permutation group on Ω and $t \in G$. We define the *support of* t by

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

and the set of *fixed points of* t by

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

Then $\Omega = \mathrm{supp}(t) \cup \mathrm{fix}(t)$ for all $t \in G$. For a group G of order at least 2, the minimum value $\min\{|\,\mathrm{supp}(t)| \,:\, 1 \neq t \in G\}$ is called the *minimal degree* of G.

Let G_1 and G_2 be two groups acting on the sets Ω_1 and Ω_2, respectively. Then the two actions are said to be *permutationally isomorphic* if there exists a bijection $\lambda : \Omega_1 \to \Omega_2$ and an isomorphism $\varphi : G_1 \to G_2$ such that

$$\lambda(\alpha^g) = \lambda(\alpha)^{g^\varphi} \quad \text{for all } \alpha \in \Omega_1 \text{ and } g \in G_1. \tag{1}$$

The pair (λ, φ) is called a *permutational isomorphism*.

2.3 Construction

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

$$C(T, \rho) := \{\alpha(t, \rho) \,:\, t \in T\} \tag{2}$$

as a code in $H(q, q)$. Then $C(T, \rho)$ is a (q, d)-permutation array, where d is the minimal degree of $\rho(T)$:

Lemma 2. *[10, Lemma 3.2] For $t \in T$, the distance $d(\alpha(1_T, \rho), \alpha(t, \rho)) = |\,\mathrm{supp}(\rho(t))|$, and $C(T, \rho)$ has minimum distance $\delta(C(T, \rho))$ equal to the minimal degree*

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

of $\rho(T)$.

Now we consider a general construction. Let $\mathcal{I} = (\rho_1, \ldots, \rho_r)$ be an ordered list of representations from T to S_q (with repetitions allowed) and define

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

an r-tuple of codewords of the form given in (2). Set

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

Then $C(T, \mathcal{I})$ is a code in $H(rq, q)$, and is called a *twisted permutation code*. In particular, if $r = 1$ then $C(T, \mathcal{I})$ is the permutation code $C(T, \rho_1)$ given in (2), and if $\rho_1 = \cdots = \rho_r$ then $C(T, \mathcal{I}) = C(T, \rho_1^r)$ is called the *r-fold repetition permutation code* for $T\rho_1$.

Proposition 3. *[10, Proposition 3.3 and equation (3.2)] With the notation as above, consider the code $C = C(T, \mathcal{I})$. Then,*

(i) $\mathrm{Aut}(C)$ *has a subgroup acting regularly on C; in particular, C is distance invariant;*

(ii) $|C| = |T/K|$, *where* $K = \cap_{\rho \in \mathcal{I}} \ker \rho$;

(iii) $\delta(C) = \min_{t \in T^\#}\{\sum_{\rho \in \mathcal{I}} |\operatorname{supp}(\rho(t))|\} \geqslant \min_{\rho \in \mathcal{I}}\{\delta(C(T, \rho^r)\}$, *where* $T^\# = T \backslash \{1\}$. *In particular, for* $\rho \in \mathcal{I}$, $\delta(C(T, \rho^r) = rd$, *where d is the minimal degree of* $\rho(T)$.

The lower bound for $\delta(C(T, \mathcal{I}))$ given in Proposition 3 (iii) is the bound we wish to improve on!

3 The affine group

In this section we use affine groups to construct a family of twisted permutation codes with minimum distance greater than the lower bound of Proposition 3. Let k be an integer and p an odd prime such that $p > k \geqslant 2$, and let $V = \mathbb{F}_p^k$ be the vector space of k-dimensional row vectors over the finite field $\mathbb{F}_p$, and let e_i denote the ith standard basis (row) vector of V, for $i = 1, \ldots, k$.

3.1 The matrix group $\overline{G}_k$ and the affine group G_k

We define a subgroup $\overline{G}_k$ of $\mathrm{GL}(k+1, p)$ which turns out to be isomorphic to a subgroup G_k of order p^{k+1} of the affine group $\mathrm{AGL}(k, p)$ (Lemmas 5(d) and 6). The representation in terms of $(k+1) \times (k+1)$ matrices is computationally convenient. We define a matrix $B_k := I_k + A_k \in \mathrm{GL}(k, p)$ where I_k is the $k \times k$ identity matrix and, writing X^T for the transpose of a matrix X, A_k is given by

$$A_k = \begin{pmatrix} \mathbf{0} \\ e_1 \\ \vdots \\ e_{k-1} \end{pmatrix} = \begin{pmatrix} e_2^T & \ldots & e_k^T & \mathbf{0} \end{pmatrix}. \tag{3}$$

Thus B_k is a lower unitriangular matrix, and in particular B_k is nonsingular. We write $B_k^i = (B_k)^i$ for any integer i, so in particular $B_k^0 = I_k$. For $\mathbf{v} \in V$ and $i \geqslant 1$, we set

$$g_{\mathbf{v},i} = \begin{pmatrix} 1 & \mathbf{v} \\ \mathbf{0} & B_k^i \end{pmatrix} \tag{4}$$

and we define $\overline{G}_k$ as the subset

$$\overline{G}_k := \{g_{\mathbf{v},i} : \ \mathbf{v} \in V, \ 0 \leqslant i \leqslant p-1\} \tag{5}$$

of $\mathrm{GL}(k+1,p)$. We prove in Lemma 5 that $\overline{G}_k$ is a group with the operation of matrix multiplication. For a vector $\mathbf{v} \in V$, we denote by $\varphi_{\mathbf{v}}$ the translation by $\mathbf{v}$, and for a matrix $B \in \mathrm{GL}(k,p)$ we denote by Φ_B the linear transformation $V \to V$ given by $\mathbf{v} \mapsto \mathbf{v}\,B$. Then we define the subset

$$G_k := \{\varphi_{\mathbf{v}}\Phi_{B_k^i} : \ \mathbf{v} \in V, \ i \geqslant 1\} \tag{6}$$

of the affine group $\mathrm{AGL}(k,p)$. We prove in Lemma 5 that G_k is a subgroup of $\mathrm{AGL}(k,p)$, and in Lemma 6 that G_k is isomorphic to $\overline{G}_k$. As preparation we define $\Omega(k,0) := \mathbf{0}_k$, $\Omega(k,1) := I_k$ and, for $i \geqslant 2$, we set $\Omega(k,i) := I + B_k + B_k^2 + \cdots + B_k^{i-1}$.

Lemma 4. *For $2 \leqslant k < p$ and any positive integer i, we have*

$$B_k^i = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ i & 1 & 0 & \cdots & 0 \\ \binom{i}{2} & i & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{i}{k-1} & \binom{i}{k-2} & \binom{i}{k-3} & \cdots & 1 \end{pmatrix} \text{ and } \Omega(k,i) = \begin{pmatrix} i & 0 & 0 & \cdots & 0 \\ \binom{i}{2} & i & 0 & \cdots & 0 \\ \binom{i}{3} & \binom{i}{2} & i & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{i}{k} & \binom{i}{k-1} & \binom{i}{k-2} & \cdots & i \end{pmatrix} \tag{7}$$

where for $1 \leqslant j \leqslant k-1$, the matrix entry $\binom{i}{j}$ denotes $\underbrace{1+\ldots+1}_{\binom{i}{j}}$ in $\mathbb{F}_p$. In particular, $B_k^p = I_k$, B_k has multiplicative order p, and $\Omega(k,p) = \mathbf{0_k}$.

Proof. First we deal with B_k^i. Multiplying together the two expressions for A_k in (3) we find that

$$A_k^2 = \begin{pmatrix} e_3^T & \ldots & e_k^T & \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

Then observe that, by induction, for $1 \leqslant s \leqslant k-1$,

$$A_k^s = \begin{pmatrix} e_{s+1}^T & \ldots & e_k^T & \mathbf{0} & \ldots & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ I_{k-s} & \mathbf{0} \end{pmatrix}.$$

Thus $A_k^k = \mathbf{0}$. Now for any positive integer i we evaluate

$$B_k^i = (I_k + A_k)^i = I_k + \binom{i}{1}A_k + \binom{i}{2}A_k^2 + \ldots + \binom{i}{i-1}A_k^{i-1} + A_k^i.$$

Using the expression for A_k^s above and the fact that $A_k^k = \mathbf{0}$, we obtain the expression for B_k^i in the statement. Since $k < p$, it follows that $B_k^p = I_k$. Since $B_k \neq I_k$ it follows that B_k has multiplicative order p.

Now we consider $\Omega(k,i)$. We will use the following binomial identity (see, for example, [3, (4.3.9)][1]): for $0 \leqslant \ell \leqslant i-1$,

$$\sum_{j=0}^{i-1} \binom{j}{\ell} = \sum_{j=\ell}^{i-1} \binom{j}{\ell} = \binom{i}{\ell+1}.$$

Using this, and Lemma 4, it follows that the (s,t) entry of $\Omega(k,i)$, $a_{s,t}$, satisfies

$$a_{s,t} = \begin{cases} 0 & \text{if } t > s \\ \sum_{j=0}^{i-1} \binom{j}{s-t} = \binom{i}{s-t+1} & \text{if } t \leqslant s, \end{cases}$$

giving us the required expression for $\Omega(k,i)$. Since $k < p$, we deduce that $\Omega(k,p) = \mathbf{0}$. □

Lemma 5. *Let $2 \leqslant k < p$ and, for $\mathbf{v} \in V$ and $i \geqslant 0$, let $g_{\mathbf{v},i}, \varphi_{\mathbf{v}}\Phi_{B_k^i}$ and $\Omega(k,i)$ be as above. Let $\mathbf{v}, \mathbf{w} \in V$ and $i, j \geqslant 0$. Then*

(a) $i \equiv j \pmod p \iff g_{\mathbf{v},i} = g_{\mathbf{v},j} \iff \Phi_{B_k^i} = \Phi_{B_k^j} \iff \Omega(k,i) = \Omega(k,j)$;

(b) $(\mathbf{v} = \mathbf{w}$ and $i \equiv j \pmod p) \iff g_{\mathbf{v},i} = g_{\mathbf{w},j} \iff \varphi_{\mathbf{v}}\Phi_{B_k^i} = \varphi_{\mathbf{w}}\Phi_{B_k^j}$;

(c) $g_{\mathbf{v},i}g_{\mathbf{w},j} = g_{\mathbf{v}\,B_k^j + \mathbf{w}, i+j}$; $\varphi_{\mathbf{v}}\Phi_{B_k^i} \circ \varphi_{\mathbf{w}}\Phi_{B_k^j} = \varphi_{\mathbf{v}+\mathbf{w}B_k^{-i}}\Phi_{B_k^{i+j}}$; and $\Omega(k,i+j) = \Omega(k,i) + B_k^i\Omega(k,j)$;

(d) both $\overline{G}_k$ and G_k are groups of order p^{k+1}.

Proof. First we deal with all assertions about $\Omega(k,i)$. The equality $\Omega(k,i) = \Omega(k,j)$ holds by Lemma 4 if and only if $i \equiv j \pmod p$, as required for part (a). The assertion in (c) follows from the definition, namely that $\Omega(k,0) := \mathbf{0}_k$, $\Omega(k,1) := I_k$, and for $i \geqslant 2$, $\Omega(k,i) := I + B_k + B_k^2 + \cdots + B_k^{i-1}$.

The remaining assertions of part (a) follow from part (b), which we now proceed to prove. It follows from (4) that $g_{\mathbf{v},i} = g_{\mathbf{v},j}$ if and only if $\mathbf{v} = \mathbf{w}$ and $B_k^i = B_k^j$, and the latter equality holds if and only if $i \equiv j \pmod p$ by Lemma 4. Now we consider the affine maps. If $\mathbf{v} = \mathbf{w}$ and $i \equiv j \pmod p$ then $B_k^i = B_k^j$ by Lemma 4, so $\varphi_{\mathbf{v}}\Phi_{B_k^i} = \varphi_{\mathbf{w}}\Phi_{B_k^j}$. Suppose conversely that $\varphi_{\mathbf{v}}\Phi_{B_k^i} = \varphi_{\mathbf{w}}\Phi_{B_k^j} = \psi$, say. Then, for all $\mathbf{x} \in V$, $\mathbf{x}\psi = (\mathbf{x}+\mathbf{v})B_k^i = (\mathbf{x}+\mathbf{w})B_k^j$. Taking $\mathbf{x} = \mathbf{0}$ this implies that $\mathbf{v}\,B_k^i = \mathbf{w}B_k^j$, and so, for all $\mathbf{x}$, $\mathbf{x}B_k^i = \mathbf{x}B_k^j$. This, in turn, implies that $B_k^i = B_k^j$ and hence, by Lemma 4, that $i \equiv j \pmod p$. Since B_k^i is invertible, $\mathbf{v}\,B_k^i = \mathbf{w}B_k^j$ now implies that $\mathbf{v} = \mathbf{w}$. Thus (b), and hence also (a), are proved.

[1] It is sometimes called the Hockey-stick identity, see https://en.wikipedia.org/wiki/Hockey-stick_identity

Now we prove part (c). The equality $g_{\mathbf{v},i}g_{\mathbf{w},j} = g_{\mathbf{v}\,B_k^j+\mathbf{w},i+j}$ follows from matrix multiplication using (4). Let $\psi = \varphi_{\mathbf{v}}\Phi_{B_k^i} \circ \varphi_{\mathbf{w}}\Phi_{B_k^j}$. Then, for $\mathbf{x} \in V$, $\mathbf{x}\psi = ((\mathbf{x}+\mathbf{v})B_k^i+\mathbf{w})B_k^j = (\mathbf{x}+\mathbf{v}+\mathbf{w}B_k^{-i})B_k^{i+j}$, and hence $\psi = \varphi_{\mathbf{v}+\mathbf{w}B_k^{-i}}\Phi_{B_k^{i+j}}$. Thus part (c) is proved.

It follows from parts (a) and (c) that $\overline{G}_k$ and G_k are closed under the relevant multiplication, and hence both are groups. The groups have order p^{k+1}, by part (b). □

Now we study several maps from G_k to $\overline{G}_k$, all of which turn out to be isomorphisms.

Lemma 6. *For each $\mathbf{w} \in V$, the map $\tau_{\mathbf{w}} : G_k \to \overline{G}_k$ defined by*

$$\tau_{\mathbf{w}} : \varphi_{\mathbf{v}}\Phi_{B_k^i} \longmapsto g_{\mathbf{v}\,B_k^i+\mathbf{w}\Omega(k,i),i} \quad \text{for each } \mathbf{v} \in V \text{ and for } 0 \leqslant i \leqslant p-1,$$

is an isomorphism.

Proof. Since B_k is invertible, it follows from Lemma 5 (b) that $\tau_{\mathbf{w}}$ is injective, and then the fact that $\tau_{\mathbf{w}}$ is a bijection follows from Lemma 5 (d). It remains to prove that $\tau_{\mathbf{w}}$ is a homomorphism, and for this we use all of the equalities in Lemma 5(c): for each $\mathbf{v}_1, \mathbf{v}_2 \in V$ and for each i, j,

$$\begin{aligned}
\tau_{\mathbf{w}}(\varphi_{\mathbf{v}_1}\Phi_{B_k^i})\tau_{\mathbf{w}}(\varphi_{\mathbf{v}_2}\Phi_{B_k^j}) &= g_{\mathbf{v}_1\,B_k^i+\mathbf{w}\Omega(k,i),i} \cdot g_{\mathbf{v}_2\,B_k^j+\mathbf{w}\Omega(k,j),j} \\
&= g_{(\mathbf{v}_1\,B_k^i+\mathbf{w}\Omega(k,i))B_k^j+\mathbf{v}_2\,B_k^j+\mathbf{w}\Omega(k,j),i+j} \\
&= g_{(\mathbf{v}_1+\mathbf{v}_2\,B_k^{-i})B_k^{i+j}+\mathbf{w}\Omega(k,i+j),i+j} \\
&= \tau_{\mathbf{w}}(\varphi_{\mathbf{v}_1+\mathbf{v}_2\,B_k^{-i}}\Phi_{B_k^{i+j}}) \\
&= \tau_{\mathbf{w}}(\varphi_{\mathbf{v}_1}\Phi_{B_k^i} \cdot \varphi_{\mathbf{v}_2}\Phi_{B_k^j}).
\end{aligned}$$

□

3.2 Viewing $\overline{G}_k$ as a permutation group

In the usual action of $\overline{G}_k$ on the row space $\mathbb{F}_p^{k+1}$ we show that $\overline{G}_k$ is faithful and transitive on the subset $\Omega := \{(1, \mathbf{v}) | \, \mathbf{v} \in V\}$ of $\mathbb{F}_p^{k+1}$, and we will regard $\overline{G}_k$ as a permutation group on Ω.

Lemma 7. *Let $2 \leqslant k < p$, let $\Omega = \{(1, \mathbf{v}) | \, \mathbf{v} \in V = \mathbb{F}_p^k\}$, and let $\overline{G}_k$ be as in (5).*

(a) Then Ω is $\overline{G}_k$-invariant, and $\overline{G}_k$ is faithful and transitive on Ω.

(b) For $\mathbf{v} = (v_1, v_2, \ldots, v_k) \in V$ and $0 \leqslant i \leqslant p-1$,

(i) $g_{\mathbf{v},i}$ fixes p points of $\Omega \iff 1 \leqslant i \leqslant p-1$ and $v_k = 0$;

(ii) $g_{\mathbf{v},i}$ fixes no points of $\Omega \iff$ either $1 \leqslant i \leqslant p-1$ and $v_k \neq 0$, or $i = 0$ and $\mathbf{v} \neq \mathbf{0}$.

(iii) $g_{\mathbf{v},i}$ fixes all p^k points of $\Omega \iff i = 0$ and $\mathbf{v} = \mathbf{0}$.

Proof. Consider $g_{\mathbf{v},i} \in \overline{G}_k$, where $\mathbf{v} = (v_1, v_2, \ldots, v_k)$ and $0 \leqslant i \leqslant p-1$, and $(1, \mathbf{x}) \in \Omega$, where $\mathbf{x} = (x_1, x_2, \ldots, x_k)$. Then by Lemma 4 and some easy calculations,

$$\begin{aligned}(1,\mathbf{x})g_{\mathbf{v},i} &= (1, x_1, x_2, \ldots, x_k)\begin{pmatrix} 1 & v_1 & v_2 & \cdots & v_k \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & i & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \binom{i}{k-1} & \binom{i}{k-2} & \cdots & 1 \end{pmatrix} \\ &= \left(1, v_1 + \sum_{t=0}^{k-1}\tbinom{i}{t}x_{t+1}, v_2 + \sum_{t=0}^{k-2}\tbinom{i}{t}x_{t+2}, \ldots, v_k + x_k\right) \in \Omega.\end{aligned}$$

Thus Ω is invariant under the action of $\overline{G}_k$. In particular, taking $\mathbf{x} = \mathbf{0}$, we see that $(1,\mathbf{0})g_{\mathbf{v},i}$ is equal to $(1, v_1, v_2, \ldots, v_k) = (1, \mathbf{v})$. Letting $\mathbf{v}$ vary through V this shows that $\overline{G}_k$ is transitive on Ω. Also, it shows that the only group elements fixing $(1,\mathbf{0})$ are those of the form $g_{\mathbf{0},i}$. Finally, taking $\mathbf{x} = (0, \ldots, 0, 1)$, we find that the only value of i such that $g_{\mathbf{0},i}$ fixes $(1, \mathbf{x})$ is $i = 0$. Thus $\overline{G}_k$ is faithful on Ω, proving part (a) and also part (b)(iii).

Suppose in the above display that $g_{\mathbf{v},i} \neq g_{\mathbf{0},0}$ and that $(1,\mathbf{x})g_{\mathbf{v},i} = (1,\mathbf{x})$. Comparing the entries in both sides of the equation, we see that

$$x_j = v_j + \sum_{t=0}^{k-j}\binom{i}{t}x_{t+j}. \quad \text{for } j = 1, \ldots, k. \tag{8}$$

In particular, (8) with $j = k$ implies that $v_k = 0$. If $i = 0$ then (8) implies that $x_j = v_j + x_j$ for all j, so $\mathbf{v} = \mathbf{0}$. Thus, $g_{\mathbf{v},i} = g_{\mathbf{0},0}$, which is a contradiction. Hence, if $g_{\mathbf{v},i} \neq g_{\mathbf{0},0}$ and $g_{\mathbf{v},i}$ fixes a point of Ω, then $1 \leqslant i \leqslant p-1$ and $v_k = 0$.

Conversely suppose that $1 \leqslant i \leqslant p-1$ and $v_k = 0$. Then $(1,\mathbf{x})$ is fixed by $g_{\mathbf{v},i}$ if and only if the equations (8) hold. Now there exists i' such that $1 \leqslant i' \leqslant p-1$ and $ii' \equiv 1 \pmod p$. We solve the equations (8) for $j = k, k-1, \ldots, 1$ to determine recursively $x_{k-1}, \ldots, x_2$. The equation with $j = k$ yields the tautology $x_k = x_k$, while the equation for $j = k-1$ implies $0 = v_{k-1} + ix_k$, that is, $x_k = -i'v_{k-1}$. Continuing to solve the equations for $j = k-2, \ldots, 1$ yields

$$x_{j+1} = \begin{cases} -i'\,v_{k-1} & \text{if } j = k-1 \\ -i'\big(v_j + \sum_{t=2}^{k-j}\binom{i}{t}x_{t+j}\big) & \text{if } j = 1, \ldots, k-2. \end{cases} \tag{9}$$

Thus $x_2, \ldots, x_k$ are determined by $\mathbf{v} = (v_1, v_2, \ldots, v_k)$, while x_1 is unrestricted; so $g_{\mathbf{v},i}$ fixes exactly p points of Ω, namely $(1,\ a,\ x_2,\ \ldots,\ x_k)$ for $a \in \mathbb{F}_p$. This completes the proof of part (b). □

3.3 Multiple permutation representations of G_k on Ω

Now that we regard $\overline{G}_k$ as a permutation group on Ω (as described in Subsection 3.2), we may view the $\tau_{\mathbf{w}}$ in Lemma 6 as faithful permutation representations of G_k into $\mathrm{Sym}(\Omega)$.

We study p of these permutation representations, and from them build a family of twisted permutation codes.

Lemma 8. *For $r \in \mathbb{F}_p$, let $\mathbf{w}_r := (0, 0, \ldots, 0, r) \in V$, and $\rho_r := \tau_{\mathbf{w}_r}$, as defined in Lemma 6. Then ρ_r is a faithful, transitive permutation representation of G_k on Ω. Further let $\mathbf{v} \in V$ and let i be an integer such that $0 \leqslant i \leqslant p-1$, and $(\mathbf{v}, i) \neq (\mathbf{0}, 0)$.*

(i) If $i = 0$ then, for each $r \in \mathbb{F}_p$, $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i})$ has no fixed points in Ω.

(ii) If $i \neq 0$, then there exists a unique $r \in \mathbb{F}_p$ such that $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i})$ fixes p points of Ω, and for each $s \neq r$, $\rho_s(\varphi_{\mathbf{v}}\Phi_{B_k^i})$ has no fixed points in Ω.

Proof. Since $\rho_r := \tau_{\mathbf{w}_r}$ is a homomorphism, and since we regard $\overline{G}_k$ as a permutation group of Ω, it follows that ρ_r is a permutation representation of G_k on Ω. It is faithful and transitive, by Lemmas 6 and 7.

From the definition in Lemma 6, $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i}) = g_{\mathbf{v}',i}$, where $\mathbf{v}' = \mathbf{v}\, B_k^i + \mathbf{w_r}\Omega(k,i)$. Suppose first that $i = 0$. Then $\mathbf{v} \neq \mathbf{0}$, by assumption, and $\Omega(k,i) = \mathbf{0}_k$ by Lemmas 4 and 5(a). As B_k is invertible, it follows that $\mathbf{v}' \neq \mathbf{0}$, and hence, by Lemma 7 that $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i})$ has no fixed points in Ω, proving (i).

Suppose then that $1 \leqslant i \leqslant p-1$. Then by Lemma 4, $\mathbf{w}_r\Omega(k,i)$ has k^{th} entry ri. As r ranges over $\mathbb{F}_p$, we find exactly one value of r for which the k^{th} entry of $\mathbf{v}'$ is zero, and hence, by Lemma 7, for this unique value of r, $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i}) = g_{\mathbf{v}',i}$ has p fixed points in Ω, and for all other values, $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i})$ has no fixed points in Ω. □

Table 2 summarises the information about the support sizes of $\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i})$ derived in the proof of Lemma 8.

i and r	$i = 0$, any r	$1 \leqslant i < p$, $ri = -v_k$	$1 \leqslant i < p$, $ri \neq -v_k$
$\lvert\operatorname{supp}(\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i}))\rvert$	p^k	$p^k - p$	p^k

Table 2: $\lvert\operatorname{supp}(\rho_r(\varphi_{\mathbf{v}}\Phi_{B_k^i}))\rvert$ for $r \in \mathbb{F}_p, \mathbf{v} \in V$, $0 \leqslant i < p$, with $\mathbf{v}B_k^i = (v_1, \ldots, v_k)$ and $(\mathbf{v}, i) \neq (\mathbf{0}, 0)$.

3.4 Twisted permutation codes for G_k

We now define a family of twisted permutation codes using these permutation representations of G_k on Ω. Let $q = p^k$, and choose an ordering $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_q)$ for the q vectors of V. For each $g_{\mathbf{v},i} \in \overline{G}_k$, define a vertex in the Hamming graph of length q over Ω by writing the passive form for $g_{\mathbf{v},i}$

$$\alpha_0(g_{\mathbf{v},i}) = ((1, \mathbf{v}_1)g_{\mathbf{v},i}, \ldots, (1, \mathbf{v}_q)g_{\mathbf{v},i}), \tag{10}$$

that is, the ith entry of $\alpha_0(g_{\mathbf{v},i})$ is the image of $(1, \mathbf{v}_i)$ under $g_{\mathbf{v},i}$. We denote the sequence of permutation representations of G_k in Lemma 8 by $\mathcal{I} := (\rho_0, \rho_1, \ldots, \rho_{p-1})$. We associate with g the following vertex of the Hamming graph of length qp over Ω:

$$\alpha(\varphi_{\mathbf{v}}\Phi_{B_k^i}, \mathcal{I}) := (\alpha_0(\rho_0(\varphi_{\mathbf{v}}\Phi_{B_k^i})), \alpha_0(\rho_1(\varphi_{\mathbf{v}}\Phi_{B_k^i})), \ldots, \alpha_0(\rho_{p-1}(\varphi_{\mathbf{v}}\Phi_{B_k^i})))$$

that is, $\alpha(\varphi_{\mathbf{v}}\Phi_{B_k^i}, \mathcal{I})$ is a p-tuple of vertices of the form (10). We define the corresponding twisted permutation code relative to $\mathcal{I}$ as

$$C(G_k, \mathcal{I}) = \{\alpha(g, \mathcal{I}) | g \in G_k\}.$$

For the untwisted versions we choose any $s \in \mathbb{F}_p$, and we first define the permutation code as in (2)

$$C(G_k, \rho_s) = \{\alpha(g, \rho_s) | g \in G_k\}, \text{ where } \alpha(g, \rho_s) = \alpha_0(\rho_s(g)) \text{ for } g \in G_k.$$

As noted in Subsection 2.3 (see Lemma 2), $C(G_k, \rho_s)$ is a (q, d)-permutation array, where d is the minimal degree of $\rho_s(G_k) = \overline{G}_k$, and by Lemma 7, $d = q - p = p^k - p$. Note also that $C(G_k, \rho_s)$ is independent of the choice of s. Thus, the p-fold repetition permutation code $C(G_k, \rho_s^p)$ generated by $C(G_k, \rho_s)$ is also independent of s.

Proposition 9. *For $s \in \mathbb{F}_p$ and with the notation above, the codes $C(G_k, \mathcal{I})$ and $C(G_k, \rho_s^p)$ each have size $|G_k| = p^{k+1}$, and have minimum distance $p^{k+1} - p$ and $p^{k+1} - p^2$, respectively. The lower bound given by Proposition 3 for the minimum distance of $C(G_k, \mathcal{I})$ is $p^{k+1} - p^2$.*

We note that $\delta(C(G_k, \mathcal{I})) = p^{k+1} - p$ is strictly greater than the lower bound $p^{k+1} - p^2$ given by Proposition 3 (iii).

Proof. Since each ρ_s is faithful, the codes all have size $|G_k| = p^{k+1}$. As noted above, the minimum distance of $C(G_k, \rho_s^p)$ is $p^k - p$. Hence the lower bound on the minimum distance of $C(G_k, \mathcal{I})$ given by Proposition 3(iii), namely the minimum distance of $C(G_k, \rho_s^p)$, is $p^{k+1} - p^2$. On the other hand, by Proposition 3(iii), the minimum distance of $C(G_k, \mathcal{I})$ is the minimum, over all non-identity $g \in G_k$, of $\sum_{\rho_s \in \mathcal{I}} |\operatorname{supp}(\rho_s(g))|$. By Lemma 8 and Table 2, for $g = \varphi_{\mathbf{v}}\Phi_{B_k^i} \in G_k$ with $0 \leqslant i < p$, $\mathbf{v} \in V$ and $(\mathbf{v}, i) \neq (\mathbf{0}, 0)$, this sum is $p^{k+1} - p$ if $i \neq 0$, and p^{k+1} if $i = 0$. Thus $\delta(C(G_k, \mathcal{I})) = p^{k+1} - p$. □

4 The symplectic group

In this section, we consider the symplectic group $T = \mathrm{Sp}(4, q)$ over a field of order $q = 2^n \geqslant 4$. We exploit the fact that G has an outer automorphism τ which does not map transvections to transvections (see Section 4.2). We preserve this notation throughout. Set $\mathcal{I} = \{\iota, \tau\}$ where ι denotes the identity map. We show that the twisted permutation code $C(T, \mathcal{I})$ has minimum distance strictly greater than the lower bound in Proposition 3.

4.1 The group Sp(4, q)

Let $V = \mathbb{F}^4$, the space of 4-dimensional row vectors over a field $\mathbb{F}$ of order $q = 2^n$. Then V admits a non-degenerate symplectic form β with isometry group $T = \mathrm{Sp}(4, q)$. Let e_1, e_2, f_1, f_2 be a symplectic basis for V such that $\{e_1, f_1\}$ and $\{e_2, f_2\}$ are hyperbolic pairs, and

$$V = \langle e_1, f_1 \rangle \perp \langle e_2, f_2 \rangle,$$

that is, $\beta(e_i, f_i) = 0$ for $i = 1, 2$, and if $\{i, j\} = \{1, 2\}$ then $\beta(e_i, e_j) = \beta(f_i, f_j) = \beta(e_i, f_j) = 0$. Then $M := \langle e_1, e_2 \rangle$ is a maximal totally isotropic subspace with $\dim M = 2 = (\dim V)/2$. We use "Witt's Lemma", stated below, versions of which go back to Witt's work in [20] – a proof may be found in the book of Artin [1, p.121].

Lemma 10. *Let U be a subspace of a non-degenerate symplectic space V, and let $f : U \to V$ be a linear isometry. Then f can be extended to a linear isometry of V, that is, there is a linear isometry $h : V \to V$ such that $f(u) = h(u)$ for all $u \in U$.*

Lemma 11. *Let $g \in T = \mathrm{Sp}(4, q)$ such that there are (at least) three 1-dimensional subspaces, each fixed setwise by g, which span a 3-dimensional subspace. Then g is conjugate in T to an element whose matrix, with respect to the ordered basis (e_1, f_1, e_2, f_2), has the following form, for some $a, b, d \in \mathbb{F}$,*

$$\begin{pmatrix} a & 0 & 0 & 0 \\ d & a^{-1} & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b^{-1} \end{pmatrix}. \tag{11}$$

Proof. By assumption V contains three linearly independent vectors v_1, v_2, v_3 such that g fixes each $\langle v_i \rangle$ setwise, and thus g fixes setwise $W := \langle v_1, v_2, v_3 \rangle$. Since W is of odd dimension, its radical $R := W \cap W^\perp$ (where $W^\perp = \{w \in W \mid (w, u) = 0 \text{ for all } u \in W\}$) must be non-zero, and also $R < W$, because the maximum dimension of the totally isotropic subspaces of V is equal to 2. Thus W/R is nontrivial and non-degenerate, and hence $\dim(W/R) = 2$ and $\dim R = 1$. Further, since $R \subseteq W^\perp$, and since V is non-degenerate, we have $W = R^\perp$. Now there is a linear isometry $R \to V$ which maps R to $\langle e_1 \rangle$, and by Lemma 10 this extends to an element of T mapping R to $\langle e_1 \rangle$. Replacing g, if necessary, by its conjugate under this element, we may assume that $R = \langle e_1 \rangle$ and hence that $W = R^\perp = \langle e_1, e_2, f_2 \rangle$.

We claim that the setwise stabiliser $\mathrm{Stab}_T(W)$ is transitive on the 1-spaces contained in $W \setminus R$. To see this, let w_1 and w_2 be linearly independent vectors in $W \setminus R$. Then $U_i := \langle e_1, w_i \rangle$ is totally isotropic for $i = 1, 2$. There is a unique linear map $f : U_1 \to V$ such that $f : e_1 \to e_1, \quad w_1 \to w_2$, and this map f is a linear isometry, because U_i is totally isotropic for $i = 1, 2$. Therefore, by Lemma 10, there exists y in T such that $y : e_1 \to e_1, \quad w_1 \to w_2$. Now y fixes $\langle e_1 \rangle$, and hence also $\langle e_1 \rangle^\perp = W$, so $y \in \mathrm{Stab}_T(W)$ and the claim is established.

In what follows, we may assume without loss that $v_1 \in W \setminus R$. By the previous paragraph, there exists an element $x \in \mathrm{Stab}_T(W)$ such that x sends $v_1 \to e_2$ and $e_1 \to e_1$.

So $g^x = x^{-1}gx$ fixes $\langle e_2\rangle$ setwise. Hence g^x fixes $\langle e_1\rangle$, $\langle e_2\rangle$, and W. Since g^x is a conjugate of our original element g, there exists a vector $w \in W \setminus \langle e_1, e_2\rangle$ such that $\langle w\rangle$ is fixed by g^x. Replacing w by a scalar multiple if necessary, we may assume that $w = ce_1 + de_2 + f_2$, for some $c, d \in \mathbb{F}$. Now $W = \langle e_1, e_2, f_2\rangle = \langle e_1, e_2, w\rangle$ and it is straightforward to check that the map $\phi : W \to V$ such that $\phi : e_1 \to e_1,\ \ e_2 \to e_2,\ \ f_2 \to w$, defines a linear isometry. Hence by Lemma 10, there exists an element say $y \in T$ such that $y : e_1 \to e_1,\ \ e_2 \to e_2,\ \ f_2 \to w$. Then $g^{xy^{-1}} = yg^xy^{-1}$ fixes $\langle e_1\rangle$, $\langle e_2\rangle$, and $\langle f_2\rangle$. Now we replace g by its conjugate $g^{xy^{-1}}$. Then g fixes W, $\langle e_1\rangle$, $\langle e_2\rangle$, and $\langle f_2\rangle$, and so, for some a, b, c' and d_i,

$$g : e_1 \to ae_1,\ \ e_2 \to be_2,\ \ f_2 \to c'f_2,\ \ f_1 \to d_1e_1 + d_2f_1 + d_3e_2 + d_4f_2.$$

Since g preserves the form and $(e_2, f_2) = 1$, $(e_1, f_1) = 1$, $(e_2, f_1) = 0$, and $(f_1, f_2) = 0$, we obtain $c' = b^{-1}$, $d_2 = a^{-1}$, $d_4 = 0$, and $d_3 = 0$. This shows that the matrix for g with respect to the ordered basis (e_1, f_1, e_2, f_2) is as in (11) with $d = d_1$. □

4.2 Viewing Sp(4, q) as a permutation group.

The group $T = \mathrm{Sp}(4, q)$ has a faithful, transitive permutation representation on the set

$$\Omega = \mathrm{PG}(V) = \{\langle v\rangle \mid v \in V\},$$

of 1-dimensional subspaces (1-spaces) of V, and we henceforth regard T as a permutation group of Ω. For any $g \in \mathrm{GL}(4, q)$, we write the subset of 1-spaces fixed setwise by g as

$$\mathrm{Fix}_\Omega(g) = \{\langle v\rangle \mid \langle v\rangle^g = \langle v\rangle, \langle v\rangle \in \Omega\}.$$

Transvections play a pivotal role in our construction. As in [18, page 71], for $u \in V$ and $d \in \mathbb{F}$, the *symplectic transvection* $t_{d,u}$ relative to the symplectic form β is defined as the map

$$t_{d,u}(v) = v + d\beta(v, u)u \quad \text{for } v \in V.$$

Each $t_{d,u} \in \mathrm{Sp}(4, q)$ and, for example, the matrix in (11) with $a = b = 1$ is the transvection t_{d,e_1}. More generally, transvections may be defined on any vector space U over a field $\mathbb{K}$ by replacing $d\beta(v, u)$ in the displayed formula above with $\varphi(v)$, for any linear functional $\varphi : U \to \mathbb{K}$ ([18, page 20]). In particular if $\dim U$ is odd and U is an orthogonal geometry defined by a quadratic form Q such that the polar form β' of Q is non-degenerate, then the corresponding orthogonal group $\mathrm{O}(U)$ (the isometry group of Q) contains transvections if and only if $\mathbb{K}$ has characteristic 2. Moreover, when $\mathbb{K}$ has characteristic 2, the radical $U^\perp$ of U with respect to β' is 1-dimensional, β' induces a symplectic form on $U/U^\perp$, and there is a one-to-one correspondence between the transvections in $\mathrm{O}(U)$ and the symplectic transvections on $U/U^\perp$ relative to this symplectic form [18, page 144]. These comments are the basis (in the 4-dimensional case) of Lemma 13(ii) in the next subsection.

Lemma 12. *Let $g \in T$ with $g \neq 1$. If g is a symplectic transvection, then $|\mathrm{Fix}_\Omega(g)| = q^2 + q + 1$, and otherwise $|\mathrm{Fix}_\Omega(g)| \leqslant 2q + 2$.*

Proof. If a non-scalar element $g \in \mathrm{GL}(4,q)$ fixes a 2-dimensional subspace $\langle v_1, v_2\rangle$ setwise and g fixes $\langle v_1\rangle$ and $\langle v_2\rangle$, then the number of 1-spaces in $\langle v_1, v_2\rangle$ fixed setwise by g is 2 or $q+1$. Thus there is nothing to prove if all the 1-spaces fixed setwise by g lie in a 2-space. So we assume that g fixes setwise three 1-spaces $\langle v_1\rangle$, $\langle v_2\rangle$, and $\langle v_3\rangle$ such that v_1, v_2, v_3 are linearly independent. Then by Lemma 11, conjugating g by an element of T if necessary, we may assume that the matrix for g with respect to the ordered basis (e_1, f_1, e_2, f_2) is as in (11), we write $W = \langle e_1, e_2, f_2\rangle$, and g fixes $\langle e_1\rangle$, $\langle e_2\rangle$, and $\langle f_2\rangle$.

Let $S = \{a, a^{-1}, b, b^{-1}\}$. Let $v = xe_1 + yf_1 + ze_2 + wf_2 \in W \setminus \{0\}$, and suppose that g fixes $\langle v\rangle$ setwise, so $vg = tv$ for some $t \in \mathbb{F} \setminus \{0\}$. Then

$$\begin{aligned} ax + yd &= tx,\\ a^{-1}y &= ty,\\ bz &= tz,\\ b^{-1}w &= tw. \end{aligned}$$

We find $\mathrm{Fix}_\Omega(g)$ and its size according to the possibilities for $|S|$ and d (as in (11)). Assume first that $d = 0$. In this case $|S| \geqslant 2$ since $g \neq 1$ and the only scalar matrix in $\mathrm{Sp}(4,q)$ is the identity.

(1) If $|S| = 4$ (i.e., a, a^{-1}, b, b^{-1} are all distinct), then $\mathrm{Fix}_\Omega(g) = \{\langle e_1\rangle, \langle f_1\rangle, \langle e_2\rangle, \langle f_2\rangle\}$, and so $|\mathrm{Fix}_\Omega(g)| = 4 < 2q+2$ (and g is not a transvection).

(2) If $|S| = 3$, then either $a = a^{-1}$ or $b = b^{-1}$ and we find

$$\mathrm{Fix}_\Omega(g) = \begin{cases} \left\{\langle xe_1 + yf_1\rangle, \langle e_2\rangle, \langle f_2\rangle \mid x, y \in \mathbb{F}, (x,y) \neq (0,0)\right\} & \text{if} \quad a = a^{-1},\\ \left\{\langle e_1\rangle, \langle f_1\rangle, \langle ze_2 + wf_2\rangle | z, w \in \mathbb{F}, (z,w) \neq (0,0)\right\} & \text{if} \quad b = b^{-1}. \end{cases}$$

Thus $|\mathrm{Fix}_\Omega(g)| = q + 3 \leqslant 2q + 2$ (and g is not a transvection).

(3) If $|S| = 2$, then

$$\mathrm{Fix}_\Omega(g) = \begin{cases} \left\{\langle xe_1 + yf_1\rangle, \langle ze_2 + wf_2\rangle | x, y, z, w \in \mathbb{F}, (x,y), (z,w) \neq (0,0)\right\}\\ \text{if} \quad a = a^{-1}, b = b^{-1},\\ \left\{\langle xe_1 + ze_2\rangle, \langle yf_1 + wf_2\rangle | x, y, z, w \in \mathbb{F}, (x,z), (y,w) \neq (0,0)\right\}\\ \text{if} \quad a^{-1} \neq a = b,\\ \left\{\langle xe_1 + wf_2\rangle, \langle yf_1 + ze_2\rangle | x, y, z, w \in \mathbb{F}, (x,w), (y,z) \neq (0,0)\right\}\\ \text{if} \quad a^{-1} \neq a = b^{-1}. \end{cases}$$

Thus $|\mathrm{Fix}_\Omega(g)| = 2q + 2 < 1 + q + q^2$ (and g is not a transvection).

Now we assume that $d \neq 0$. Let $h := (a^{-1} - a)^{-1}$.

(1) If $|S| = 4$ (i.e., a, a^{-1}, b, b^{-1} are all distinct), then

$$\mathrm{Fix}_\Omega(g) = \Big\{\langle e_1\rangle, \langle d_1 h e_1 + f_1\rangle, \langle e_2\rangle, \langle f_2\rangle\Big\},$$

and $|\mathrm{Fix}_\Omega(g)| = 4 < 2q + 2$ (and g is not a transvection).

(2) If $|S| = 3$, then exactly one of $a = a^{-1}$ or $b = b^{-1}$, and we find

$$\mathrm{Fix}_\Omega(g) = \begin{cases} \{\langle e_1\rangle, \langle e_2\rangle, \langle f_2\rangle\} & \text{if} \quad a = a^{-1} \\ \Big\{\langle e_1\rangle, \langle d_1 h e_1 + f_1\rangle, \langle z e_2 + w f_2\rangle | z, w \in \mathbb{F}, (z, w) \neq (0, 0)\Big\} & \text{if} \quad b = b^{-1} \end{cases}$$

and $|\mathrm{Fix}_\Omega(g)| = 3$ or $q + 3$ respectively, so is less that $2q + 2$ (and g is not a transvection).

(3) If $|S| = 2$, then

$$\mathrm{Fix}_\Omega(g) = \Big\{\langle e_1\rangle, \langle z e_2 + w f_2\rangle | z, w \in \mathbb{F}, (z, w) \neq (0, 0)\Big\},$$

if $a = a^{-1}$ and $b = b^{-1}$, and hence in this case $|\mathrm{Fix}_\Omega(g)| = q + 2$. Similarly, we obtain

$$\mathrm{Fix}_\Omega(g) = \begin{cases} \Big\{\langle x e_1 + z e_2\rangle, \langle d_1 h y e_1 + y f_1 + w f_2\rangle | x, y, z, w \in \mathbb{F}, (x, z), (y, w) \neq (0, 0)\Big\} \\ \text{if} \quad a = b, \\ \Big\{\langle x e_1 + w f_2\rangle, \langle d_1 h y e_1 + y f_1 + z e_2\rangle | x, y, z, w \in \mathbb{F}, (x, w), (y, z) \neq (0, 0)\Big\} \\ \text{if} \quad a = b^{-1}. \end{cases}$$

and in these two cases $|\mathrm{Fix}_\Omega(g)| = 2q + 2$ (and g is not a transvection).

(4) If $|S| = 1$, then $a = b = a^{-1}$ and g has determinant $a^4 = 1$, so $a = 1$ (since q is even). As noted above, in ths case g is the symplectic transvection t_{d,e_1}. Then

$$\mathrm{Fix}_\Omega(g) = \Big\{\langle x e_1 + z e_2 + w f_2\rangle | x, z, w \in \mathbb{F}, (x, z, w) \neq (0, 0, 0)\Big\},$$

and its size is equal to $q^2 + q + 1$. This is the only case in which the number of 1-spaces fixed setwise by g is more that $2q + 2$. □

4.3 A second permutation representation of $\mathbf{Sp}(4, q)$ on Ω

We construct another permutation representation making use of an outer automorphism τ of $T = \mathrm{Sp}(4, q)$. Such an automorphism arises only when q is even, as it is here. We need information about the action of τ, especially on the involutions in T. The following lemma is taken from [18] (see also the discussion preceding Lemma 12).

Lemma 13. *The following conditions hold, for all $m \geqslant 2$ and even q:*

(*i*) $O(2m+1,q)$ *is isomorphic to* $\mathrm{Sp}(2m,q)$ (see [18, Theorem 11.9]).

(*ii*) *Every transvection in* $O(2m+1,q)$ *corresponds to a symplectic transvection in* $\mathrm{Sp}(2m,q)$ (see [18, p. 144]).

(*iii*) $\mathrm{PSp}(4,q) \simeq P\Omega(5,q)$, *for both even and odd* q (see [18, Corollary 12.32]).

As pointed out by Todd [19], using Lemma 13 one can obtain some isomorphisms between $T = \mathrm{Sp}(4,2^n)$ and $O(5,2^n)$. However the geometric reasons for these isomorphisms are quite different. Taylor [18, p. 201] observes that a certain 4-dimensional T-invariant section $\overline{W}$ of the (6-dimensional) exterior square $\Lambda_2 V$ of $V = \mathbb{F}^4$ admits a nondegenerate alternating form which is invariant under T. Moreover each element $g \in T$ induces a linear map of $\Lambda_2 V$, which we denote by $\Lambda_2 g$, and $\Lambda_2 g$ induces a linear map $\overline{\Lambda_2 g} \in \mathrm{Sp}(\overline{W})$, giving an isomorphism $T \to \mathrm{Sp}(\overline{W})$ defined by $g \mapsto \overline{\Lambda_2 g}$. Further, Taylor [18, pp. 201-202] constructs an explicit linear isomorphism $\overline{p} : \overline{W} \to V$ such that the map $\tau : T \to T$ defined by

$$\tau(g) = \overline{p}\ \overline{\Lambda_2 g}\ \overline{p}^{-1}$$

is an automorphism of T. Let t be a symplectic transvection in T. Then Taylor shows [18, p. 202] that $\tau(t)$ has a 2-dimensional fixed point space in V, and hence that $\tau(t)$ is not a symplectic transvection. Thus τ is not induced by conjugation by any element of T, that is, τ is an outer automorphism of T. Taylor [18, p.202] also shows that τ^2 is the automorphism of T induced by the field automorphism $x \mapsto x^2$ of $\mathbb{F}$, so τ has order $2n$. In particular, τ^2 is a semilinear map, thus leaving the class of transvections invariant. He also notes that, if n is odd, the field automorphism τ^2 can be expressed as the square of another field automorphism, say σ, and in this case the related outer automorphism $\sigma^{-1}\tau$ has order 2.

A computation for the specific transvection $t = t_{1,e_1}$ shows that in this case $\overline{\Lambda_2 t}$ fixes exactly $q+1$ of the 1-spaces of $\overline{W}$, and hence that $\tau(t)$ fixes exactly $q+1$ of the 1-spaces of V. As all symplectic transvections are conjugate in T, this is true for all symplectic transvections t, that is, $|\mathrm{Fix}_\Omega(\tau(t))| = q+1$.

Lemma 14. *The image of a symplectic transvection of* $\mathrm{Sp}(4,q)$ *under the (outer) automorphism τ is an element with exactly $q+1$ fixed 1-spaces.*

As above, we may regard the outer automorphism from Lemma 14 as a second (faithful, transitive) permutation representation of T on Ω. We let $\mathcal{I} = (\iota, \tau)$,with ι the identity automorphism of T, and construct the twisted permutation code $C(T,\mathcal{I})$ for $T = \mathrm{Sp}(4,q)$ relative to $\mathcal{I}$. Set $m := |\Omega| = (q^4-1)/(q-1)$, and choose an ordering $(\langle v_1\rangle, \langle v_2\rangle, \ldots, \langle v_m\rangle)$ for Ω. Each $g \in T$ then corresponds to the vertex

$$\alpha(g,\iota) = (\langle v_1\rangle^g, \langle v_2\rangle^g, \ldots, \langle v_m\rangle^g)$$

of the Hamming graph of length m over Ω. We define the permutation code as

$$C(T,\iota) = \{\alpha(g,\iota) | g \in T\}$$

and the twisted permutation code $C(T,\mathcal{I})$ relative to $\mathcal{I}=(\iota,\tau)$ as the code in the Hamming graph of length $2m=2q^3+2q^2+2q+2$ over Ω consisting of the vertices

$$\alpha(g,\mathcal{I})=(\alpha(g,\iota),\alpha(g,\tau)) \quad \text{for } g\in T.$$

Proposition 15. *Let $T=\mathrm{Sp}(4,q)$ ($q=2^n\geqslant 4$) and $\mathcal{I}=(\iota,\tau)$ be as above. Then the twisted permutation code $C(T,\mathcal{I})$ has size $|T|$, and minimum distance $2q^3+q^2$, while the 2-fold repetition permutation codes $C(T,\iota^2)$ and $C(T,\tau^2)$ have minimum distance $2q^3$. The difference between the minimum distance of $C(T,\mathcal{I})$ and the lower bound given by Proposition 3 is q^2.*

Proof. By Proposition 3, the minimum distance $\delta(C(T,\mathcal{I}))$ is equal to the minimum of $|\operatorname{supp}(g)|+|\operatorname{supp}(\tau(g))|$, for $g\neq 1$ in T, where $\operatorname{supp}(g)$ denotes the subset of Ω consisting of the 1-spaces which are moved by g (not fixed setwise). It follows from Lemmas 12 and 14 that, if g is a transvection, then $|\operatorname{supp}(g)|+|\operatorname{supp}(\tau(g))|=(m-q^2-q-1)+(m-q-1)=2q^3+q^2$. Similarly, if $\tau(g)$ is a transvection then, by Lemma 14, $\tau^2(g)$ and (since τ^2 is a semilinear map) also g fixes exactly $q+1$ of the 1-spaces, and again we obtain $|\operatorname{supp}(g)|+|\operatorname{supp}(\tau(g))|=2q^3+q^2$. For all other non-identity elements g, it follows from Lemma 12 that $|\operatorname{supp}(g)|+|\operatorname{supp}(\tau(g))|\geqslant 2(m-2q-2)$, which is strictly greater than $2q^3+q^2$ for $q\geqslant 4$. Therefore, $\delta(C(T,\mathcal{I}))=2q^3+q^2$.

Finally, we have from Proposition 3 and Lemma 12 that the lower bound in Proposition 3, and also the minimum distances of the repetition permutation codes, are all equal to the minimum of $2|\operatorname{supp}(g)|$ for nontrivial $g\in T$, and that this is attained when g is a transvection and is $2(m-q^2-q-1)=2q^3$. The difference between $\delta(C(T,\mathcal{I}))$ and this lower bound is q^2. □

4.4 Proof of Theorem 1.

By considering $\delta_{tw}:=\delta(C(T,\mathcal{I}))$ and $\delta_{\mathrm{rep}}:=\min_{\rho\in\mathcal{I}}\{\delta(C(T,\rho^r))\}$, Theorem 1 follows from Propositions 9 and 15.

Acknowledgements

The first author would like to thank the School of Mathematics and Statistics of the University of Western Australia for their hospitality during the preparation of this paper. She also would like to express her deep gratitude to the second and third authors for numerous mathematical discussions.

The second author acknowledges the support of a grant from the University of Western Australia associated with the Australian Research Council Federation Fellowship FF0776186 of the third author.

All authors gratefully acknowledge insightful comments from an anonymous referee which led to significant improvements in the exposition of the paper.

References

[1] Artin, E. Geometric algebra. *Interscience Publishers, Inc., New York-London*, 1957. x+214 pp.

[2] Brouwer, A. E., Cohen, A. M., Neumaier, A. Distance-regular graphs. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 18. *Springer-Verlag*, Berlin, 1989.

[3] Brualdi, Richard A. Introductory combinatorics. *North-Holland, New York-Oxford-Amsterdam*, 1977.

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

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

[6] Cappelletti, P., Golla, C., Olivo, P., Zanoni, E. Flash Memories. *Kluwer Academic Press*, 1999.

[7] Gillespie, N. I. and Praeger, C. E. Neighbour transitivity on codes in Hamming graphs. *Des. Codes Cryptogr.*, 67, (2013), no. 3, 385–393.

[8] Gillespie, N. I. and Praeger, C. E. Diagonally neighbour transitive codes. *J. Algebraic Combinatorics*, Vol 39, Issue 3, (2014), 733–747.

[9] Gillespie, N. I. and Praeger, C. E. Classification of a family of neighbour transitive codes. arXiv:1405.5427.

[10] Gillespie, N. I., Praeger, C. E., Spiga, P. Twisted permutation codes. *J. Group Theory*, 18 (2015), no. 3, 407–433.

[11] Han Vinck, A. J. Coded modulation for power line communications. *AEÜ Journal*, 45–49 (Jan 2000).

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

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

[14] Jiang, A., Schwartz, M., Bruck, J. Error-Correcting Codes for Rank Modulation. *International Symposium on Information Theory (ISIT)*, pp. 1736–1740, July 2008.

[15] Pavlidou, N., Han Vinck, A., Yazdani, J., Honary, B. Power line communications: state of the art and future trends. *Communications Magazine, IEEE* 41(4), 34–40 (2003).

[16] Shieh, M., Tasi, S. Decoding frequency permutation arrays under Chebyshev distance. *IEEE Trans. Inform. Theory* 56 (2010), no. 11, 5730–5737.

[17] Tamo, I., Schwartz, M. Correcting limited-magnitude errors in the rank-modulation scheme. *IEEE Trans. Inform. Theory* 56 (2010), no. 6, 2551–2560.

[18] Taylor, D. E. The geometry of the classical groups. Sigma Series in Pure Mathematics, 9. *Heldermann Verlag, Berlin*, 1992. xii+229 pp.

[19] Todd, J.A. As it might have been. *Bull. London Math Soc.*, 2 (1970), Issue 1, 1–4.

[20] Witt, E. Theorie der quadratischen Formen in beliebigen Körpern, *J. Reine Angew. Math.*, 176 (1937), 31–44.