View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Explore Bristol Research

Gillespie, N. I., & Praeger, C. E. (2014). Diagonally neighbour transitive codes and frequency permutation arrays. Journal of Algebraic Combinatorics, 39(3), 733-747. DOI: 10.1007/s10801-013-0465-6

Peer reviewed version

License (if available):
Unspecified

Link to published version (if available):
10.1007/s10801-013-0465-6

Link to publication record in Explore Bristol Research
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via Springer at http://link.springer.com/article/10.1007%2Fs10801-013-0465-6. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/pure/about/ebr-terms.html arXiv:1204.2900v2 [math.CO] 2 Apr 2014

DIAGONALLY NEIGHBOUR TRANSITIVE CODES AND FREQUENCY PERMUTATION ARRAYS

NEIL I. GILLESPIE AND CHERYL E. PRAEGER

Abstract. Constant composition codes have been proposed as suitable coding schemes to solve the narrow band and impulse noise problems associated with powerline communication. In particular, a certain class of constant composition codes called frequency permutation arrays have been suggested as ideal, in some sense, for these purposes. In this paper we characterise a family of neighbour transitive codes in Hamming graphs in which frequency permutation arrays play a central rode. We also classify all the permutation codes generated by groups in this family.

1. Introduction

Powerline communication has been proposed as a solution to the "last mile problem" in the delivery of fast and reliable telecommunications at the lowest cost [13, 17]. Any coding scheme designed for powerline communication must maintain a constant power output, while at the same time combat both *permanent narrow band noise* and *impulse noise*, as well as the usual white Gaussian/background noise [5, 13, 17]. Addressing the last of these, the authors introduced *neighbour transitive codes* (see below) as a group theoretic analogue to the assumption that white Gaussian noise affects symbols in codewords independently at random [9] - an assumption often made in the theory of error-correcting codes [18, p.5]. To deal with the other noise considerations in powerline communication, *constant composition codes* (CCC) have been proposed as suitable coding schemes [5, 6] - these codes are of length m over an alphabet of size q and have the property that each codeword has p_i occurrences of the ith letter of the alphabet, where the p_i are positive integers such that $\sum p_i = m$. It is also suggested in [5] that constant composition codes where the p_i are all roughly m/q are particularly well suited for powerline communication. Constant composition codes where each letter occurs m/q times in each codeword are called *frequency permutation arrays*, and were introduced in [14]. In this paper we characterise a family of neighbour transitive codes in which frequency permutation arrays play a central role, and we classify the subfamily consisting of *permutation codes* generated by groups (each of which is associated with a 2-transitive permutation group).

We consider a code of length m over an alphabet Q of size q to be a subset of the vertex set of the Hamming graph $\Gamma = H(m,q)$, which has automorphism group $\mathrm{Aut}(\Gamma) \cong S_q^m \rtimes S_m$. We define the

Date: draft typeset October 17, 2016

2000 Mathematics Subject Classification: 05E20, 20B25, 94B60.

Key words and phrases: powerline communication, constant composition codes, frequency permutation arrays, neighbour transitive codes, permutation codes, automorphism groups .

automorphism group of a code C to be the setwise stabiliser of C in $\mathrm{Aut}(\Gamma)$, and we denote it by $\mathrm{Aut}(C)$ (and note that this is a more general notion than is sometimes used in the literature). We define the *the set of neighbours of* C to be the set C_1 of vertices in Γ that are not codewords, but are adjacent to at least one codeword in C. We say C is X*-neighbour transitive*, or simply *neighbour transitive*, if there exists a group X of automorphisms such that both C and C_1 are X-orbits.

Let α be a vertex in $H(m,q)$, and suppose $\{a_1,\ldots,a_k\}$ is the set of letters that occur in α. The *composition of* α is the set

$$Q(\alpha)=\{(a_1,p_1),\ldots,(a_k,p_k)\}, \tag{1.1}$$

where the p_i are positive integers and there are exactly p_i occurrences of the letter a_i in the codeword α. Also let $\mathcal{I}(\alpha)=\{p_1,\ldots,p_k\}$, which can be a multi-set. It follows from the definition that, for a constant composition code, $k=q$ and $Q(\alpha)=Q(\beta)$ for all codewords α,β. As such, we can talk of the *composition of a constant composition code*, which is equal to $Q(\alpha)$ for each codeword α. Now, for a set $\mathcal{I}$ of k positive integers that sum to m, with $k\leqslant q$, let $\Pi(\mathcal{I})$ be the set of vertices α in $H(m,q)$ with $\mathcal{I}(\alpha)=\mathcal{I}$. Then, for any constant composition code C, there exists a set $\mathcal{I}$ of q positive integers such that $C\subseteq\Pi(\mathcal{I})$.

As automorphisms of a CCC must leave its composition invariant, it is natural to ask what types of automorphisms might do this, particularly as we are interested in neighbour transitive CCC's. The group S_q (which we identify with the Symmetric group of Q) induces a faithful action on the vertices of Γ in which elements of S_q act naturally on each of the m entries of a vertex. We denote the image of S_q under this action by $\mathrm{Diag}_m(S_q)$ (since it is a diagonal subgroup of the base group S_q^m of $\mathrm{Aut}(\Gamma)$, see (2.1)). It follows (from Lemma 2.6) that $\Pi(\mathcal{I})$ is left invariant under $\mathrm{Diag}_m(S_q)$. Similarly, the group L of all permutations of entries fixes $\Pi(\mathcal{I})$ setwise. (This holds because any permutation of the entries of a vertex α is a rearrangement of the letters occurring in α, leaving the composition $Q(\alpha)$ unchanged.) Moreover, the group $\langle\mathrm{Diag}_m(S_q),L\rangle=\mathrm{Diag}_m(S_q)\rtimes L$ is the largest subgroup of $\mathrm{Aut}(\Gamma)$ that leaves invariant $\Pi(\mathcal{I})$ for all $\mathcal{I}$ (for example no other element of $\mathrm{Aut}(\Gamma)$ fixes $\Pi(\{m\})$). Hence it is natural to ask which CCC's are fixed setwise by the group $\mathrm{Diag}_m(S_q)\rtimes L$, or more specifically, which are X-neighbour transitive with $X\leqslant\mathrm{Diag}_m(S_q)\rtimes L$. This leads to the following definition.

Definition 1.1. A code C in $H(m,q)$ is *diagonally* X*-neighbour transitive*, or simply *diagonally neighbour transitive*, if it is X-neighbour transitive for some $X\leqslant\mathrm{Diag}_m(S_q)\rtimes L$.

Our first major result characterises diagonally neighbour transitive codes, and shows that diagonally neighbour transitive CCC's are necessarily frequency permutation arrays.

Theorem 1.2. *Let C be a diagonally neighbour transitive code in $H(m,q)$. Then either C is a frequency permutation array; $C=\{(a,\ldots,a)\}$ for some letter a; or C is one of the codes described in Definition 3.1 (i), (ii) or (iii), none of which is a constant composition code.*

Theorem 1.2 gives us a nice characterisation of diagonally neighbour transitive codes, but it does not provide us with any examples of neighbour transitive frequency permutation arrays. We consider *permutation codes* to find examples of such codes. By identifying the alphabet Q with the set $\{1,\ldots,q\}$, any permutation $t \in S_q$ can be associated with the q-tuple $\alpha(t)$ in $H(q,q)$, which has ith entry equal to the image of i under t. For example, if $q=3$ and $t=(1,2,3)$, then $\alpha(t)=(2,3,1)$. For a subset T of S_q, we define $C(T)=\{\alpha(t)\,:\,t\in T\}$, called the *permutation code generated by* T, and $N_{S_q}(T)=\{x\in S_q\,:\,T^x=T\}$.

Theorem 1.3. *Let T be a subgroup of S_q. Then the permutation code $C(T)$ is diagonally neighbour transitive in $H(q,q)$ if and only if $N_{S_q}(T)$ is 2-transitive. Moreover, for any positive integer p and diagonally neighbour transitive code $C(T)$, the code $\mathrm{Rep}_p(C(T))$, given in (2.2), is a diagonally neighbour transitive frequency permutation array in $H(pq,q)$.*

In Section 2 we introduce the required definitions and some preliminary results. Then, in Section 3, we give some examples of diagonally neighbour transitive codes in $H(m,q)$. Finally, we prove Theorems 1.2 and 1.3 in Sections 4 and 5 respectively.

2. Definitions and Preliminaries

Any code of length m over an alphabet Q of size q can be embedded in the vertex set of the *Hamming graph*. The Hamming graph $\Gamma=H(m,q)$ has vertex set $V(\Gamma)$, the set 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 we assume that $m,q\geqslant 2$. 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 [4, Theorem 9.2.1]. Let $g=(g_1,\dots,g_m)\in B$, $\sigma\in L$ and $\alpha=(\alpha_1,\dots,\alpha_m)\in V(\Gamma)$. Then g and σ act on α in the following way:

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

For any subgroup T of S_q, we define the following subgroup of B:

$$\mathrm{Diag}_m(T)=\{(h,\dots,h)\in B\,:\,h\in T\}. \tag{2.1}$$

Let $M=\{1,\dots,m\}$, and view M as the set of vertex entries of $H(m,q)$. Let 0 denote a distinguished element of the alphabet Q. For $\alpha\in V(\Gamma)$, the *support of* α is the set $\mathrm{supp}(\alpha)=\{i\in M\,:\,\alpha_i\neq 0\}$. The *weight of* α is defined as $\mathrm{wt}(\alpha)=|\mathrm{supp}(\alpha)|$. 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. We let $\Gamma_k(\alpha)$ denote the set of vertices in $H(m,q)$ that are at distance k from α. For $a_1,\dots,a_k\in Q$ and positive integers $p_1,\dots,p_k$ such that $\sum p_i=m$, we let $(a_1^{p_1},a_2^{p_2},\dots,a_k^{p_k})$ denote the vertex

$$(\underbrace{a_1,\dots,a_1}_{p_1},\underbrace{a_2,\dots,a_2}_{p_2},\dots,\underbrace{a_k,\dots,a_k}_{p_k})\in V(\Gamma)$$

Let $\alpha=(\alpha_1,\dots,\alpha_m)\in V(\Gamma)$. For $a\in Q$ we let $\nu(\alpha,i,a)\in V(\Gamma)$ denote the vertex with jth entry

$$\nu(\alpha,i,a)|_j=\begin{cases}\alpha_j & \text{if } j\neq i\\ a & \text{if } j=i.\end{cases}$$

We note that if $\alpha_i=a$ then $\nu(\alpha,i,a)=\alpha$, otherwise $\nu(\alpha,i,a)\in\Gamma_1(\alpha)$. Throughout this paper whenever we refer to $\nu(\alpha,i,a)$ as a *neighbour of* α, or being adjacent to α, we mean that $a\in Q\backslash\{\alpha_i\}$. The following straight forward result describes the action of automorphisms of Γ on vertices of this form.

Lemma 2.1. *Let* $\alpha = (\alpha_1, \dots, \alpha_m) \in V(\Gamma)$*,* $a \in Q$*, and* $x = (h_1, \dots, h_m)\sigma \in \mathrm{Aut}(\Gamma)$*. Then* $\nu(\alpha, i, a)^x = \nu(\alpha^x, i^\sigma, a^{h_i})$*, and is adjacent to* α^x *if and only if* $\nu(\alpha, i, a)$ *is adjacent to* α*.*

For a code C in $H(m, q)$, the *minimum distance,* δ*, of* C is the smallest distance between distinct codewords of C. For any $\gamma \in V(\Gamma)$, we define

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

to be the *distance of* γ *from* C. The *covering radius of* C, which we denote by ρ, is the maximum distance that any vertex in $H(m, q)$ is from C. We let C_i denote the set of vertices that are distance i from C, and deduce, for $i \leqslant \lfloor (\delta - 1)/2 \rfloor$, that C_i is the disjoint union of $\Gamma_i(\alpha)$ as α varies over C. Furthermore, $C_0 = C$ and $\{C, C_1, \dots, C_\rho\}$ forms a partition of $V(\Gamma)$ called the *distance partition of* C. In particular, the *complete code* $C = V(\Gamma)$ has covering radius 0 and trivial distance partition $\{C\}$; and if C is not the complete code, we call the non-empty subset C_1 the *set of neighbours of* C. Let C and C' be codes in $H(m, q)$. We say C and C' are *equivalent* if there exists $x \in \mathrm{Aut}(\Gamma)$ such that $C^x = C'$, and if $C' = C$ we call x an automorphism of C. Recall, the automorphism group of C, denoted by $\mathrm{Aut}(C)$, is the setwise stabiliser of C in $\mathrm{Aut}(\Gamma)$.

Let C be a code in $H(m, q)$ with distance partition $\{C, C_1, \dots, C_\rho\}$. As we defined in the introduction, we say C is X-neighbour transitive if there exists $X \leqslant \mathrm{Aut}(\Gamma)$ such that C_i is an X-orbit for $i = 0, 1$. If there exists $X \leqslant \mathrm{Aut}(\Gamma)$ such that C_i is an X-orbit for $i = 0, \dots, \rho$, we say C is X*-completely transitive*, or simply *completely transitive.*

Remark 2.2. The reader should note that the definition of neighbour transitivity given in [9] is more general than the one given here in that it only requires C_1 to be an X-orbit. However, it is not unreasonable to use the definition given here because if $\delta \geqslant 3$ and C_1 is an X-orbit with $X \leqslant \mathrm{Aut}(C)$, then X necessarily acts transitively on C, and furthermore, it is shown in [9] that an automorphism group that fixes C_1 setwise often has to also fix C setwise. Note also that completely transitive codes are necessarily neighbour transitive.

Lemma 2.3. *Let* C *be a code with distance partition* $\mathcal{C} = \{C, C_1, \dots, C_\rho\}$ *and* $y \in \mathrm{Aut}(\Gamma)$*. Then* $C_i^y := (C_i)^y = (C^y)_i$ *for each* i*. In particular, the code* C^y *has distance partition* $\{C^y, C_1^y, \dots, C_\rho^y\}$*, and* $\mathcal{C}$ *is* $\mathrm{Aut}(C)$*-invariant. Moreover,* C *is* X*-neighbour (completely) transitive if and only if* C^y *is* X^y*-neighbour (completely) transitive.*

Proof. Let $\beta \in C_i$. Then there exists $\alpha \in C$ such that $d(\beta, \alpha) = i$. Since automorphisms preserve adjacency it follows that $d(\beta^y, \alpha^y) = i$. Thus $d(\beta^y, C^y) \leqslant i$. The same argument shows that if $j = d(\beta^y, C^y)$ then $i = d(\beta, C) = d((\beta^y)^{y^{-1}}, (C^y)^{y^{-1}}) \leqslant j$, and hence $d(\beta^y, C^y) = i$. Thus $(C_i)^y \subseteq (C^y)_i$. A similar argument shows that $(C^y)_i \subseteq (C_i)^y$. Hence $(C_i)^y = (C^y)_i$. Therefore, without ambiguity, we can denote this set by C_i^y. Thus the distance partition of C^y is $\{C^y, C_1^y \dots, C_\rho^y\}$. In particular, if $y \in \mathrm{Aut}(C)$, it follows that $(C_i)^y = (C^y)_i = C_i$ for each i. That is $\mathcal{C}$ is $\mathrm{Aut}(C)$-invariant. Finally, C is X-neighbour (completely) transitive if and only if C_i is an X-orbit for $i = 0, 1$ $(i = 0, \dots, \rho)$, which holds if and only if C_i^y is an X^y-orbit for $i = 0, 1$ $(i = 0, \dots, \rho)$. $\square$

Let C be a code with covering radius ρ and let $s \in \{0, \dots, \rho\}$. As in [4, p. 346], we say C is *s-regular* if for each vertex $\gamma \in C_i$, with $i = 0, \dots, s$, and integer $k = 0, \dots, m$, the number of codewords at distance k from γ depends only on i and k, and is independent of the choice of $\gamma \in C_i$. If $s = \rho$ we say C is *completely regular.*

Remark 2.4. It is known that completely transitive codes are necessarily completely regular [11, Lemma 2.1]. Similarly, because automorphisms preserve adjacency, it is straight forward to show that any neighbour transitive code is necessarily 1-regular.

Lemma 2.5. *Let C be a completely regular code in $H(m, q)$ with distance partition $\{C, C_1, \dots, C_\rho\}$. Then C_ρ is completely regular with distance partition $\{C_\rho, C_{\rho-1}, \dots, C_1, C\}$; and $\mathrm{Aut}(C) = \mathrm{Aut}(C_\rho)$. Furthermore, C is X-completely transitive if and only if C_ρ is X-completely transitive.*

Proof. The fact that C_ρ is completely regular with distance partition $\{C_\rho, C_{\rho-1}, \dots, C\}$ is given in [16]. It then follows from Lemma 2.3 that $\mathrm{Aut}(C) = \mathrm{Aut}(C_\rho)$. By definition, C is X-completely transitive if and only if each C_i is an X-orbit, which therefore holds if and only if C_ρ is X-completely transitive. $\square$

For $\alpha \in V(\Gamma)$, recall $Q(\alpha)$, the composition of α defined in (1.1). For each distinct p_i that appears in $Q(\alpha)$ we want to register the number of distinct letters that appear p_i times. We let

$$\mathrm{Num}(\alpha) = \{(p_1, s_1), \dots, (p_j, s_j)\}$$

where (p_i, s_i) means that s_i distinct letters appear p_i times in α. We note that $\sum s_i = k$, the number of distinct letters that occur in α.

Lemma 2.6. *Let $\alpha \in V(\Gamma)$ with $Q(\alpha) = \{(a_1, p_1), \dots, (a_k, p_k)\}$ and $x = (h, \dots, h)\sigma \in \mathrm{Diag}_m(S_q) \rtimes L$. Then $Q(\alpha^x) = \{(a_1^h, p_1), \dots, (a_k^h, p_k)\}$ and $\mathrm{Num}(\alpha^x) = \mathrm{Num}(\alpha)$.*

Proof. Let $\alpha = (\alpha_1, \dots, \alpha_m)$ and $a \in Q$. Note that $\alpha_i = a$ if and only if $\alpha_i^h = a^h$, and that $\alpha_i^h = \alpha^x|_{i^\sigma}$. Therefore for every occurrence of a in α there is a corresponding occurrence of a^h in α^x. Thus $Q(\alpha^x) = \{(a_1^h, p_1), \dots, (a_k^h, p_k)\}$. We note that $\{p_1, \dots, p_k\}$ is left invariant by the action of x on α. Therefore $\mathrm{Num}(\alpha) = \mathrm{Num}(\alpha^x)$. $\square$

Corollary 2.7. *Let C be a diagonally X-neighbour transitive code, and let $\nu \in C_i$ for $i = 0, 1$. Then $\mathrm{Num}(\nu') = \mathrm{Num}(\nu)$ for all $\nu' \in C_i$. If in addition $X \leqslant L$, then $Q(\nu') = Q(\nu)$ for all $\nu' \in C_i$.*

For a positive integer p, we can identify the vertex set of the Hamming graph $\Gamma^{(p)} = H(mp, q)$ with the set of arbitrary p-tuples of vertices from $\Gamma = H(m, q)$. For a group $X \leqslant \mathrm{Aut}(\Gamma)$, we let $(x, \sigma) \in X \times S_p$ act on the vertices of $\Gamma^{(p)}$ in the following way:

$$(\alpha_1, \dots, \alpha_p)^{(x,\sigma)} = (\alpha^x_{1\sigma^{-1}}, \dots, \alpha^x_{p\sigma^{-1}}),$$

where $\alpha_1, \dots, \alpha_p \in V(\Gamma)$. For $\alpha \in V(\Gamma)$, we let $\mathrm{rep}_p(\alpha) = (\alpha, \dots, \alpha) \in V(\Gamma^{(p)})$, and for a code C in Γ with minimum distance δ we let

$$\mathrm{Rep}_p(C) = \{\mathrm{rep}_p(\alpha) \,:\, \alpha \in C\}, \tag{2.2}$$

which is a code in $\Gamma^{(p)}$ with minimum distance $p\delta$. It follows that $\mathrm{rep}_p(\alpha)^{(x,\sigma)} = \mathrm{rep}_p(\alpha^x)$, and so C is an X-orbit if and only if $\mathrm{Rep}_p(C)$ is an $(X \times S_p)$-orbit. For $\alpha, \nu \in V(\Gamma)$ we let $\mu(\mathrm{rep}_p(\alpha), i, \nu)$ denote the vertex constructed by changing the ith vertex entry of $\mathrm{rep}_p(\alpha)$ from α to ν. It follows that $\nu \in \Gamma_1(\alpha)$ if and only if $\mu(\mathrm{rep}_p(\alpha), i, \nu) \in \Gamma_1(\mathrm{rep}_p(\alpha))$, and that $\mu(\mathrm{rep}_p(\alpha), i, \nu)^{(x,\sigma)} = \mu(\mathrm{rep}_p(\alpha^x), i^\sigma, \nu^x)$.

Lemma 2.8. *Let C be an X-neighbour transitive code in $\Gamma = H(m,q)$ with $\delta \geqslant 2$ such that a stabiliser X_α acts transitively on $\Gamma_1(\alpha)$ for some $\alpha \in C$. Then $\mathrm{Rep}_p(C)$ is $(X \times S_p)$-neighbour transitive in $H(mp,q)$.*

Proof. It follows from the comments above and Lemma 2.3 that we only need to prove the transitivity on the neighbours of $\mathrm{Rep}_p(C)$. Let $\nu_1, \nu_2 \in \mathrm{Rep}_p(C)_1$. Then there exist i, j and $\beta, \gamma \in C$ such that $\nu_1 = \mu(\mathrm{rep}_p(\beta), i, \nu_\beta)$ and $\nu_2 = \mu(\mathrm{rep}_p(\gamma), j, \nu_\gamma)$ for some adjacent vertices ν_β, ν_γ of β, γ in Γ respectively. There exists $x \in X$ such that $\beta^x = \gamma$, so $\nu_1^{(x,1)} = \mu(\mathrm{rep}_p(\gamma), i, \nu_\beta^x)$, and $\nu_\beta^x \in \Gamma_1(\gamma)$ since adjacency is preserved by x in Γ. As X acts transitively on C, and because X_α acts transitively on $\Gamma_1(\alpha)$, there exists $y \in X_\gamma$ such that $\nu_\beta^{xy} = \nu_\gamma$. By choosing $\sigma \in S_p$ such that $i^\sigma = j$, we deduce that $\nu_1^{(xy,\sigma)} = \nu_2$. □

Let C be a neighbour transitive code in $H(m,q)$ with $\delta = 1$. Let $\alpha, \beta \in C$ such that $d(\alpha, \beta) = 1$, and $\nu \in \Gamma_1(\alpha) \cap C_1$ (such a vertex exists by the transitivity on C). It follows that $\nu_1 = \mu(\mathrm{rep}_p(\alpha), 1, \nu)$, $\nu_2 = \mu(\mathrm{rep}_p(\alpha), 1, \beta) \in \mathrm{Rep}_p(C)_1$ in $H(pq,q)$. However, there does not exist $x \in \mathrm{Aut}(C)$ such that $\beta^x = \nu$ because $\mathrm{Aut}(C)$ fixes C setwise, and so ν_1 and ν_2 are not contained in the same $(\mathrm{Aut}(C) \times S_p)$-orbit. Thus the condition that $\delta \geqslant 2$ in Lemma 2.8 is essential.

3. Examples of Neighbour Transitive Codes

In this section we define four infinite families of codes and prove that all codes in these families are neighbour transitive. In Section 4, we use these codes to classify diagonally neighbour transitive codes in $\Gamma = H(m,q)$. In all cases $m > 1$.

Definition 3.1. (i) The *repetition code in* $H(m,q)$ is

$$\mathrm{Rep}(m,q) = \{(a^m) : a \in Q\} = \{\alpha \in V(\Gamma) : \mathrm{Num}(\alpha) = \{(m,1)\}\}.$$

(ii) Let $m < q$, and define

$$\begin{aligned}\mathrm{Inj}(m,q) &= \{(\alpha_1, \ldots, \alpha_m) \in V(\Gamma) : \alpha_i \neq \alpha_j \text{ for } i \neq j\} \\ &= \{\alpha \in V(\Gamma) : \mathrm{Num}(\alpha) = \{(1,m)\}\}.\end{aligned}$$

(iii) Let m be odd with $m \geqslant 3$ and $q = 2$, and define, in $\Gamma = H(m,2)$,

$$\begin{aligned}W([m/2],2) &= \{\alpha \in V(\Gamma) : \mathrm{wt}(\alpha) = (m \pm 1)/2\} \\ &= \{\alpha \in V(\Gamma) : \mathrm{Num}(\alpha) = \{((m+1)/2, 1), ((m-1)/2, 1)\}\}.\end{aligned}$$

(iv) Let p be any positive integer, and let $m = pq$, and define

$$\mathrm{All}(pq,q) = \{\alpha \in V(\Gamma) : \mathrm{Num}(\alpha) = \{(p,q)\}\}$$

Remark 3.2. The codes $\mathrm{Inj}(m,q)$ are examples of *injection codes*, which were recently introduced by Dukes [7]. Note also that $\mathrm{All}(pq,q)$ is the largest possible frequency permutation array of length pq over an alphabet of size q.

Theorem 3.3. *Let C be one of the codes in Definition 3.1. Then C is neighbour transitive with $\mathrm{Aut}(C)=\mathrm{Diag}_m(S_q)\rtimes L$. Moreover, C has minimum distance $\delta=m$, 1, 1 and 2 respectively in (i), (ii), (iii), (iv) of Definition 3.1.*

Proof. It follows from Lemma 2.6 that, in all cases, $\mathrm{Aut}(C)$ contains $H=\mathrm{Diag}_m(S_q)\rtimes L$, and it is clear that the minimum distance of C is as stated. Moreover, it is easy to check that the group H acts transitively on C (again in all four cases). Now, the set C_1 of neighbours is

$$C_1=\begin{cases}\{\nu\in V(\Gamma)\,:\,\mathrm{Num}(\nu)=\{(m-1,1),(1,1)\}\,\} & \text{in case (i)}\\ \{\nu\in V(\Gamma)\,:\,\mathrm{Num}(\nu)=\{(2,1),(1,m-2)\}\,\} & \text{in case (ii)}\\ \{\nu\in V(\Gamma)\,:\,\mathrm{Num}(\nu)=\{((m+3)/2,1),((m-3)/2,1)\}\,\} & \text{in case (iii)}\\ \{\alpha\in V(\Gamma)\,:\,\mathrm{Num}(\alpha)=\{(p+1,1),(p,q-2),(p-1,1)\}\,\} & \text{in case (iv)}\end{cases}$$

(noting that in case (iv) we may have $q=2$), and again in all cases it is straight forward to check that H is transitive on C_1. Thus C is H-neighbour transitive. It remains to prove that $\mathrm{Aut}(C)=H$. Suppose to the contrary that $\mathrm{Aut}(C)$ contains $y=(h_1,\dots,h_m)\sigma$ such that $h_i\neq h_j$ for some $i\neq j$. Since $L\leqslant H\leqslant\mathrm{Aut}(C)$, we may assume that $\sigma=1$ and that $h_1\neq h_2$. Moreover, since $\mathrm{Diag}_m(S_q)\leqslant\mathrm{Aut}(C)$, we may further assume that $h_2=1$, so $h_1\neq 1$. Let $a,b\in Q$ such that $a^{h_1}=b\neq a$. We consider the cases above separately, and in the first two cases arrive at a contradiction by exhibiting a codeword $\alpha\in C$ such that $\alpha^y\notin C$.

(i) If $C=\mathrm{Rep}(m,q)$ then $(a^m)^y|_1=b$ and $(a^m)^y|_2=a$, so $(a^m)^y\notin C$.

(ii) If $C=\mathrm{Inj}(m,q)$, then C contains a codeword α with $\alpha_1=a$ and $\alpha_2=b$. However, α^y has $\alpha^y|_1=\alpha^y|_2=b$, so $\alpha^y\notin C$.

(iii) Let $q=2$, $C=W([m/2],2)$ with $m\geqslant 3$ and m odd, and consider

$$C'=\mathrm{Rep}(m,2)=\{\mathbf{0}=(0,\dots,0),\mathbf{1}=(1,\dots,1)\}.$$

Let $\alpha\in V(\Gamma)$ such that $\mathrm{wt}(\alpha)=k$ for $1\leqslant k\leqslant m-1$. Then $d(\alpha,\mathbf{0})=k$ and $d(\alpha,\mathbf{1})=m-k$. If $k\leqslant(m-1)/2$, then $k\leqslant m-1-k<m-k$, and so $d(\alpha,C')=k$. If $k\geqslant(m+1)/2$, then $k\geqslant m+1-k>m-k$, and so $d(\alpha,C')=m-k$. It follows that $d(\alpha,C')$ is maximised when $k=(m-1)/2$ or $k=(m+1)/2$, and in both cases $d(\alpha,C')=(m-1)/2$. Thus C' has covering radius $\rho=(m-1)/2$. It also follows that

$$C'_\rho=W([m/2],2)=C.$$

It is known that C' is completely transitive and hence completely regular [10, Sec. 2]. Moreover, we have just proved that $\mathrm{Aut}(C')=H$. Therefore, by Lemma 2.5, $\mathrm{Aut}(C)=\mathrm{Aut}(C')=H$.

(iv) Let $\nu\in V(\Gamma)$ and suppose $Q(\nu)=\{(a_1,p_1),\dots,(a_k,p_k)\}$ with $p_1\geqslant p_2\geqslant\dots\geqslant p_k$. Then $k\leqslant q$ and $p_1+\dots+p_k=m=pq$, and in particular $p_1\geqslant p$. There exists $\sigma\in L\leqslant\mathrm{Aut}(C)$ such that $\nu^\sigma=(a_1^{p_1},a_2^{p_2},\dots,a_k^{p_k})$. Consider the codeword $\alpha=(a_1^p,a_2^p,\dots,a_q^p)\in C$. Then ν^σ and α agree in at least the first p entries. Therefore $d(\nu^\sigma, \alpha) \leqslant p(q-1)$ and so $d(\nu, C) = d(\nu^\sigma, C) \leqslant p(q-1)$. Therefore $\rho \leqslant p(q-1)$. Now consider $\nu = (a, \dots, a)$ for some $a \in Q$. It follows from the definition of C that $d(\nu, \alpha) = p(q-1)$ for all $\alpha \in C$. Therefore $d(\nu, C) = p(q-1)$ and so $\rho = p(q-1)$. Moreover, $\mathrm{Rep}(m,q) \subseteq C_\rho$. Now suppose $\nu \in C_\rho$ and $Q(\nu) = \{(a_1, p_1), \dots, (a_k, p_k)\}$ with $k \geqslant 2$ and $p_1 \geqslant p$. There exists $\sigma \in L \leqslant \mathrm{Aut}(C)$ such that $\nu^\sigma = (a_1^p, a_2^{p_2}, a_1^{p_1-p}, a_3^{p_3}, \dots, a_k^{p_k})$. Since $\sigma \in \mathrm{Aut}(C)$, Lemma 2.3 implies that $\nu^\sigma \in C_\rho$ also. Consider the codeword $\alpha = (a_1^p, a_2^p, \dots, a_q^p)$. Then ν^σ and α agree in the first $p + p_2 > p$, therefore $d(\nu^\sigma, \alpha) \leqslant pq - (p+1) < p(q-1)$, which is a contradiction as $\nu^\sigma \in C_\rho$. It follows that $C_\rho = \mathrm{Rep}(m,q)$. In particular, by Lemma 2.3, $\mathrm{Aut}(C)$ leaves $\mathrm{Rep}(m,q)$ invariant and so $\mathrm{Aut}(C)$ is contained in $\mathrm{Aut}(\mathrm{Rep}(m,q))$, which we have just proved is equal to H. □

The proof of Theorem 3.3 yields the following immediate corollary.

Corollary 3.4. *(i) If $q = 2$ and $m \geqslant 3$ is odd, then $C = W([m/2], 2)$ has covering radius $\rho = (m-1)/2$ and $C_\rho = \mathrm{Rep}(m,2)$. Furthermore, C and C_ρ are completely transitive.*

(ii) If $m = pq$ for some p, then $C = \mathrm{All}(pq, q)$ has covering radius $\rho = p(q-1)$ and $C_\rho = \mathrm{Rep}(m,q)$.

4. Characterising Diagonally Neighbour Transitive Codes.

In this section we characterise diagonally neighbour transitive codes in $\Gamma = H(m,q)$. However, before we consider such codes, we first prove some interesting results about connected subsets Δ of $V(\Gamma)$ (that is to say, the subgraph of Γ induced on Δ is connected).

Lemma 4.1. *Let Δ be a connected subset of $V(\Gamma)$. Let C be a code that is a proper subset of Δ. Then $C_1 \cap \Delta \neq \emptyset$.*

Proof. Let $\alpha \in C$ and $\beta \in \Delta \backslash C$. Since Δ is a connected subset, there exists a path

$$\alpha = \alpha^0, \alpha^1, \dots, \alpha^\ell = \beta$$

such that each $\alpha^i \in \Delta$. Because $\alpha \in C$ and $\beta \notin C$, there is a least $i < \ell$ such that $\alpha^i \in C$ and $\alpha^{i+1} \notin C$. Since $d(\alpha^i, \alpha^{i+1}) = 1$, it follows that $\alpha^{i+1} \in C_1$. □

Lemma 4.2. *The codes $\mathrm{Inj}(m,q)$ (with $1 < m < q$) and $W([m/2], 2)$ (with m odd and $m \geqslant 3$) are connected subsets of $V(\Gamma)$.*

Proof. Firstly we consider $\Delta_1 = \mathrm{Inj}(m,q)$. Let $\alpha, \beta \in \Delta_1$. We shall prove that α, β are connected by a path in Δ_1 using induction on the distance $d(\alpha, \beta)$ in Γ. This is true if $d(\alpha,\beta) = 1$, so assume that $d(\alpha, \beta) = w > 1$, and the property holds for distances less than w. Let $S = \{k : \alpha_k = \beta_k\}$, $i \in M \backslash S$ and $\alpha^* = \nu(\alpha, i, \beta_i)$. Then α^* is adjacent to α in Γ. If $\beta_i \neq \alpha_k$ for all $k \in M \backslash (S \cup \{i\})$, then $\alpha^* \in \Delta_1$ and $d(\alpha^*, \beta) = w - 1$. Therefore, by the inductive hypothesis, α^* and β are connected by a path in Δ_1 and hence so are α and β. Thus we may assume that $\beta_i = \alpha_j$ for some $j \in M \backslash (S \cup \{i\})$. We note that j is unique since $\alpha \in \Delta_1$. Also $\alpha_j^* = \alpha_i^*$ and so $\alpha^* \notin \Delta_1$. Since $m < q$, there exists $a \in Q \backslash \{\alpha_1, \dots, \alpha_m\}$. Let $\alpha^\diamondsuit = \nu(\alpha, j, a)$. Then $\alpha^\diamondsuit \in \Delta_1 \cap \Gamma_1(\alpha)$. If $a = \beta_j$ then $d(\alpha^\diamondsuit, \beta) = w - 1$. Therefore, by the inductive hypothesis, $\alpha^\diamondsuit$ and β are connected by a path in Δ_1 and hence so are α and

β. If $a \neq \beta_j$ then $d(\alpha^{\diamondsuit}, \beta) = w$. In this case let $\alpha^{\heartsuit} = \nu(\alpha^{\diamondsuit}, i, \beta_i)$. It follows that $\alpha^{\heartsuit} \in \Delta_1 \cap \Gamma_1(\alpha^{\diamondsuit})$ and $d(\alpha^{\heartsuit}, \beta) = w - 1$. Therefore by the inductive hypothesis, $\alpha^{\heartsuit}$ and β are connected by a path in Δ_1 and hence so are α and β. Thus Δ_1 is connected by induction.

We now consider the set $\Delta_2 = W([m/2], 2)$. Let $\alpha, \beta \in \Delta_2$ such that $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta) = (m+1)/2$. Furthermore let $\mathcal{S} = \mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta)$, $\mathcal{J} = \mathrm{supp}(\alpha) \backslash \mathcal{S} = \{j_1, \ldots, j_\ell\}$ and $\mathcal{K} = \mathrm{supp}(\beta) \backslash \mathcal{S} = \{k_1, \ldots, k_\ell\}$. Let $\alpha^0 = \alpha$ and for $i = 1, \ldots, 2\ell$ let α^i be the vertex in $V(\Gamma)$ with

$$\mathrm{supp}(\alpha^i) = \begin{cases} \mathrm{supp}(\alpha^{i-1}) \backslash \{j_{(i+1)/2}\} & \text{if } i \text{ is odd} \\ \mathrm{supp}(\alpha^{i-1}) \cup \{k_{i/2}\} & \text{if } i \text{ is even.} \end{cases}$$

It follows that $\mathrm{wt}(\alpha^i) = (m-1)/2$ or $(m+1)/2$ if i is odd or even respectively. Moreover, $d(\alpha^i, \alpha^{i-1}) = 1$ for $i = 1, \ldots, 2\ell$. Thus

$$\alpha = \alpha^0, \alpha^1, \ldots, \alpha^{2\ell} = \beta$$

is a path in Δ_2 from α to β. A similar argument shows that there exists a path in Δ_2 between two vertices of weight $(m-1)/2$. Now suppose $\alpha, \beta \in \Delta_2$ are such that they have different weights with, say, α having weight $(m-1)/2$. Let $k \in \mathrm{supp}(\beta) \backslash \mathrm{supp}(\alpha)$ and α^1 be such that $\mathrm{supp}(\alpha^1) = \mathrm{supp}(\alpha) \cup \{k\}$. Then α^1 is adjacent to α and has weight $(m+1)/2$, and as we have just shown, there exists a path in Δ_2 from α^1 to β. □

Theorem 4.3. *Let C be a diagonally X-neighbour transitive code in $\Gamma = H(m, q)$. Then one of the following holds:*

(i) $C = \{(a, \ldots, a)\}$ *for some* $a \in Q$*;*
(ii) $C = \mathrm{Rep}(m, q)$*;*
(iii) $C = \mathrm{Inj}(m, q)$ *where* $m < q$*;*
(iv) $C = W([m/2], 2)$ *where* $m \geqslant 3$ *and odd;*
(v) *there exists a positive integer* p *such that* $m = pq$ *and* C *is contained in* $\mathrm{All}(pq, q)$.

Proof. Let $\alpha \in C$ and suppose that α has composition

$$Q(\alpha) = \{(a_1, p_1), \ldots, (a_k, p_k)\}$$

with $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_k$ and $k \leqslant q$. Let $H = \mathrm{Diag}_m(S_q) \rtimes L$. We break our analysis up into the cases $k = 1$ and $k \geqslant 2$.

<u>Case $k = 1$:</u> In this case $\alpha = (a_1, \ldots, a_1)$ and

$$C = \alpha^X \subseteq \alpha^H = \mathrm{Rep}(m, q).$$

If $|C| = 1$, then $X \leqslant H_\alpha = \mathrm{Diag}_m(S_{q-1}) \rtimes L$ and $C_1 = \{\nu(\alpha, i, b) : 1 \leqslant i \leqslant m, b \in Q \backslash \{a_1\}\}$. As H_α fixes setwise C and C_1, and is transitive on both, it follows that C is H_α-neighbour transitive. By the above reduction we only find $C = \{(a_1, \ldots, a_1)\}$, but of course the examples here are $\{(a, \ldots, a)\}$ for all $a \in Q$, as in (i). Suppose now that $|C| \geqslant 2$. Since $C \subseteq \mathrm{Rep}(m, q)$ it follows that $\delta = m$. By Remark 2.4, C is 1-regular, and because $\delta = m$, C is equivalent to $\mathrm{Rep}(m, q)$ by [10, Sec. 2]. Thus $|C| = q$ and $C = \mathrm{Rep}(m, q)$, as in (ii).

Case $k \geqslant 2$: Suppose first that $p_1 = 1$. Then $k = m$ and

$$\alpha \in \hat{C} = \begin{cases} \mathrm{All}(q,q) & \text{if } m = q \\ \mathrm{Inj}(m,q) & \text{if } m < q. \end{cases}$$

Since H fixes $\hat{C}$ and $X \leqslant H$, we have that $C = \alpha^X \subseteq \alpha^H = \hat{C}$. If $m = q$ then (v) holds. Thus assume that $m < q$ and $\hat{C} = \mathrm{Inj}(m,q)$. In this case C_1 contains $\nu = \nu(\alpha, m, \alpha_1)$ and $\mathrm{Num}(\nu) = \{(2,1),(1,m-2)\}$. By Corollary 2.7, $\mathrm{Num}(\nu') = \mathrm{Num}(\nu)$ for all $\nu' \in C_1$, and in particular, $C_1 \cap \hat{C} = \emptyset$. If C is a proper subset of $\hat{C}$ then, by Lemmas 4.1 and 4.2, we have that $C_1 \cap \hat{C} \neq \emptyset$, which is a contradiction. Thus $C = \mathrm{Inj}(m,q)$ and (iii) holds.

We can now assume that $p_1 \geqslant 2$. As S_m acts m-transitively, there exists $\sigma \in L$ such that $\alpha^\sigma = (a_1^{p_1}, \ldots, a_k^{p_k}) \in C^\sigma$. By Lemma 2.3, C^σ is X^σ-neighbour transitive, and as $\mathrm{Diag}_m(S_q)$ is centralised by L, it follows that $X^\sigma \leqslant H$. Let $\bar{X} = X^\sigma$, $\bar{\alpha} = \alpha^\sigma$ and $\bar{C} = C^\sigma$. Suppose that $k < q$. Then $q \geqslant 3$ and there exists $a \in Q$ that does not occur in $\bar{\alpha}$. Consider $\nu_1 = (a, a_1^{(p_1-1)}, a_2^{p_2}, \ldots, a_k^{p_k})$ and $\nu_2 = (a_1^{(p_1+1)}, a_2^{(p_2-1)}, \ldots, a_k^{p_k})$, which are both adjacent to $\bar{\alpha}$. Then $\mathrm{Num}(\nu_1)$, $\mathrm{Num}(\nu_2)$ and $\mathrm{Num}(\bar{\alpha})$ are pairwise distinct, which is a contradiction to Corollary 2.7. Thus $k = q$. If $p_j = p_1$ for all j, then $m = pq$ (where $p = p_1$) and $\mathrm{Num}(\bar{\alpha}) = \{(p,q)\}$. Thus $\bar{\alpha} \in \mathrm{All}(pq,q)$ and

$$\bar{C} = \bar{\alpha}^{\bar{X}} \subseteq \bar{\alpha}^H = \mathrm{All}(pq,q).$$

As $\sigma \in \mathrm{Aut}(\mathrm{All}(pq,q))$, it follows that $C = \bar{C}^{\sigma^{-1}} \subseteq \mathrm{All}(pq,q)$ and (v) holds. Thus we now assume that $p_1 > p_k$. Let t be minimal such that $p_1 > p_t$, that is, $p = p_1 = p_2 = \ldots = p_{t-1} > p_t$, and note that $t \geqslant 2$. Define $\nu_1 \in \Gamma_1(\bar{\alpha})$ by

$$\nu_1 = \begin{cases} (a_1^p, \ldots, a_{t-2}^p, a_{t-1}^{p+1}, a_t^{p_t-1}, \ldots, a_q^{p_q}) & \text{if } t \geqslant 3 \\ (a_1^{p+1}, a_t^{p_t-1}, a_{t+1}^{p_{t+1}}, \ldots, a_q^{p_q}) & \text{if } t = 2 \end{cases}$$

and note that $(p+1,1) \in \mathrm{Num}(\nu_1)$ for all t, and $(p,t-2) \in \mathrm{Num}(\nu_1)$ if $t \geqslant 3$, while no element of $\mathrm{Num}(\nu_1)$ has first entry p if $t = 2$. As $(p,t-1) \in \mathrm{Num}(\bar{\alpha})$ it follows that $\mathrm{Num}(\nu_1) \neq \mathrm{Num}(\bar{\alpha})$, and so Corollary 2.7 implies that $\nu_1 \in \bar{C}_1$. We claim that $t = 2$, $p_t = p_2 = p-1$ and $q = 2$.

Assume to the contrary that the claim is false. Then t, p_2, q satisfy the conditions in column 2 of Table 1 for exactly one of the lines. For each line of Table 1, let ν_2 be the vertex in column 3. In each case $\nu_2 \in \Gamma_1(\bar{\alpha})$ and $\mathrm{Num}(\nu_2) \neq \mathrm{Num}(\bar{\alpha})$. We also have that $\mathrm{Num}(\nu_1) \neq \mathrm{Num}(\nu_2)$: this is clear in lines 2 and 3 since then no element of $\mathrm{Num}(\nu_2)$ has first entry $p+1$, while in line 1, $(p,t-3) \in \mathrm{Num}(\nu_2)$ if $t > 3$ and no entry of $\mathrm{Num}(\nu_2)$ has first entry p if $t = 3$. Since $\mathrm{Num}(\nu_2) \neq \mathrm{Num}(\bar{\alpha})$, it follows from Corollary 2.7 that $\nu_2 \in C_1$. However, Corollary 2.7 then implies that $\mathrm{Num}(\nu_2) = \mathrm{Num}(\nu_1)$, which is a contradiction. Thus the claim is proved. As $t = 2$, $p_2 = p-1$ and $q = 2$, it follows that $m = 2p-1 \geqslant 3$ and $\bar{\alpha} = (a_1^p, a_2^{p-1})$. By identifying Q with $\{0,1\}$, it follows that $\bar{\alpha}$ has weight $p = (m+1)/2$ or $p-1 = (m-1)/2$, and therefore so does $\alpha = \bar{\alpha}^{\sigma^{-1}}$, since $\sigma \in L$. Thus $\alpha \in W([m/2],2)$ and

$$C = \alpha^X \subseteq \alpha^H = W([m/2],2).$$

Let $\nu \in \Gamma_1(\alpha)$. Then ν has weight $(m+3)/2$ or $(m-3)/2$ and $\mathrm{Num}(\nu) = \{((m+3)/2,1),((m-3)/2,1)\}$. Thus $\mathrm{Num}(\nu) \neq \mathrm{Num}(\alpha)$ and Corollary 2.7 implies that $\nu \in C_1$. Hence Corollary 2.7 implies that $\mathrm{Num}(\nu') = \mathrm{Num}(\nu)$ for all $\nu' \in C_1$, in particular $C_1 \cap W([m/2],2) = \emptyset$. If C is a proper subset

Table 1. Neighbours of $\bar{\alpha}$

Line	Case	$\nu_2 \in \Gamma_1(\bar{\alpha})$
1	$t > 2$	$(a_1^{p+1}, a_2^{p-1}, a_3^p, \ldots, a_{t-1}^p, a_t^{p_t}, \ldots, a_q^{p_q})$
2	$t = 2$, $p_2 \leqslant p - 2$	$(a_1^{p-1}, a_2^{p_2+1}, a_3^{p_3}, \ldots, a_q^{p_q})$
3	$t = 2$, $p_2 = p - 1$, $q \geqslant 3$	$(a_1^p, a_2^p, a_3^{p_3-1}, \ldots, a_q^{p_q})$

of $W([m/2], 2)$ then, by Lemmas 4.1 and 4.2, $C_1 \cap W([m/2], 2) \neq \emptyset$, which is a contradiction. Thus $C = W([m/2], 2)$ and (iv) holds. □

Remark 4.4. Theorem 4.3 gives us a proof of Theorem 1.2. None of the codes in cases (i)–(iv) of Theorem 4.3 are constant composition codes, and any subset of $\mathrm{All}(pq, q)$ is necessarily a frequency permutation array.

5. Neighbour transitive frequency permutation arrays

We first consider frequency permutation arrays for which each letter from the alphabet Q appears exactly once in each codeword. Such codes are known as *permutation codes*. Permutation codes were first examined in the mid 1960s and 1970s [2, 3, 8, 19], but there has been renewed interest due to the possible applications in powerline communication, see [1, 5, 15, 20] for example.

In order to describe permutation codes, we identify the alphabet Q with the set $\{1, \ldots, q\}$ and consider codes in the Hamming graph $\Gamma = H(q, q)$. For $g \in S_q$ we define the vertex

$$\alpha(g) = (1^g, \ldots, q^g) \in V(\Gamma).$$

Recall that for a subset $T \subseteq S_q$, we define the *permutation code generated by* T to be the code

$$C(T) = \{\alpha(g) \in V(\Gamma) \,:\, g \in T\}.$$

For a permutation $g \in S_q$, the *fixed point set of* g is the set $\mathrm{fix}(g) = \{a \in Q \,:\, a^g = a\}$, and the *degree of* g is equal to $\deg(g) = q - |\,\mathrm{fix}(g)|$. For $g, h \in S_q$, it is known that $d(\alpha(g), \alpha(h)) = \deg(g^{-1}h)$ [1]. Thus, for $T \subseteq S_q$, it holds that $C(T)$ has minimum distance $\delta = \min\{\deg(g^{-1}h) \,:\, g, h \in T,\, g \neq h\}$, and if T is a group, this is called the *minimal degree of* T [3].

Recall that the Hamming graph Γ has automorphism group $\mathrm{Aut}(\Gamma) = B \rtimes L$ 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 $y \in S_q$ we let $x_y = (y, \ldots, y) \in B$, and we let $\sigma(y)$ denote the automorphism induced by y in L. For $\alpha(g) \in V(\Gamma)$,

$$\alpha(g)^{x_y} = (1^g, \ldots, q^g)^{(y, \ldots, y)} = (1^{gy}, \ldots, q^{gy}) = \alpha(gy).$$

Now, suppose that $i^y = j$ for $i, j \in Q$. Then, by considering $\alpha(g)$ as the q-tuple $(\alpha_1, \ldots, \alpha_q)$, it holds that $\alpha(g)^{\sigma(y)}|_j = \alpha_i = i^g = j^{y^{-1}g}$. Thus $\alpha(g)^{\sigma(y)} = \alpha(y^{-1}g)$, proving Lemma 5.1.

Lemma 5.1. *Let $\alpha(g) \in V(\Gamma)$ and $y \in S_q$. Then $\alpha(g)^{x_y} = \alpha(gy)$ and $\alpha(g)^{\sigma(y)} = \alpha(y^{-1}g)$.*

Recall from Remark 2.4 that neighbour transitive codes are 1-regular. It turns out that there exists exactly one 1-regular permutation code with minimum distance $\delta = 2$. Before we prove this we introduce the following concepts. We regard $1 \in Q$ as the analogue of zero from linear codes, and define the *weight* of a vertex $\beta \in V(\Gamma)$ to be $d(\alpha, \beta)$, where $\alpha = (1, \ldots, 1) \in V(\Gamma)$. For $\beta = (\beta_i), \gamma = (\gamma_i) \in V(\Gamma)$, we say β is *covered* by γ if $\beta_i = \gamma_i$ for each i such that $\beta_i \neq 1$. Furthermore, we say that a non-empty set $\mathcal{D}$ of vertices of weight k in $H(q,q)$ is a *q-ary $t-(q,k,\lambda)$ design* if for every vertex ν of weight t, there exist exactly λ vertices in $\mathcal{D}$ that cover ν.

Lemma 5.2. *Let T be a subset of S_q. Then $C(T)$ is 1-regular with $\delta = 2$ if and only if $T = S_q$.*

Proof. The reverse direction follows from Theorem 3.3 and observing that $\mathrm{All}(q,q) = C(S_q)$. To prove the converse, we first claim that there exists a positive integer λ such that $|\Gamma_2(\alpha(t)) \cap C(T)| = q(q-1)\lambda/2$ for all $\alpha(t) \in C(T)$. The code $C(T)$ is equivalent to a 1-regular code C with minimum distance 2 that contains $\alpha = (1, \ldots, 1)$. By interpreting a result of Goethals and van Tilborg [12, Thm. 9], it follows that $\Gamma_2(\alpha) \cap C$ forms a q-ary $1-(q,2,\lambda)$ design for some positive integer λ. By counting the pairs $(\nu, \beta) \in \Gamma_1(\alpha) \times (\Gamma_2(\alpha) \cap C)$ such that β covers ν, we deduce that $|\Gamma_2(\alpha) \cap C| = q(q-1)\lambda/2$. As C is 1-regular, this holds for all codewords $\beta \in C$. Furthermore, this property is also preserved by equivalence, so the claim holds.

Let $\alpha(g_1) \in C(T)$ and $S = \Gamma_2(\alpha(g_1)) \cap C(T)$. As $C(T)$ is 1-regular with $\delta = 2$, it follows that $S \neq \emptyset$. Let $\alpha(g_2) \in S$. Then $d(\alpha(g_2 g_1^{-1}), \alpha(1)) = 2$, and so $g_2 g_1^{-1} = t'$ is a transposition. Consequently, for each $\alpha(g) \in S$ there exists a transposition $t \in S_q$ such that $g = t g_1$. There are exactly $q(q-1)/2$ transpositions in S_q, so $|S| \leqslant q(q-1)/2$. However, by the above claim, $|S| \geqslant q(q-1)/2$. Thus $S = \{\alpha(t g_1) : t \text{ is a transposition in } S_q\}$. Any permutation can be written as a product of transpositions, so for $g \in T$ we have that $g = t_1 t_2 \ldots t_\ell$ for some transpositions $t_1, \ldots, t_\ell \in S_q$. We have just shown that $t_1 g = t_1 t_1 t_2 \ldots t_\ell = t_2 \ldots t_\ell \in T$. Repeating this argument, we first deduce that $1 \in T$, and then that every permutation is in T. □

Let T be a subgroup of S_q. As any group has a regular action on itself by right multiplication, it follows from Lemma 5.1 that $\mathrm{Diag}_q(T) = \{x_y : y \in T\}$ acts regularly on $C(T)$. We also define

$$A(T) = \{x_y \sigma(y) : y \in N_{S_q}(T)\},$$

where $N_{S_q}(T) = \{y \in S_q : T^y = T\}$. For $x_y \sigma(y) \in A(T)$, Lemma 5.1 implies that $\alpha(t)^{x_y \sigma(y)} = \alpha(y^{-1} t y)$ for all $\alpha(t) \in C(T)$. As $y \in N_{S_q}(T)$, we deduce that $A(T) \leqslant \mathrm{Aut}(C(T))_{\alpha(1)}$. We now prove Theorem 1.3.

Proof. Suppose that $C(T)$ is diagonally X-neighbour transitive in $H(q,q)$, and suppose first that $\delta = 2$. By Remark 2.4, $C(T)$ is 1-regular, and so Lemma 5.2 implies that $T = S_q$. In this case $N_{S_q}(S_q) = S_q$ is 2-transitive. Now suppose that $\delta \geqslant 3$, and consider the neighbours $\nu(\alpha(1), i_1, i_2)$, $\nu(\alpha(1), j_1, j_2)$ for $i_1 \neq i_2$ and $j_1 \neq j_2$. There exists $x = x_y \sigma(z) \in X$ such that $\nu(\alpha(1), i_1, i_2)^x = \nu(\alpha(1), j_1, j_2)$, and as $x \in \mathrm{Aut}(C(T))$, it follows that $\alpha(t)^x \in C(T)$ for all $\alpha(t) \in T$. By Lemma 5.1, $\alpha(t)^x = \alpha(z^{-1} t y)$, so $z^{-1} t y \in T$ for all $t \in T$. In particular, since T is a subgroup, $z^{-1} y \in T$, and so $y^{-1} z \in T$. Hence $y^{-1} z z^{-1} t y = y^{-1} t y \in T$ for all $t \in T$, that is, $y \in N_{S_q}(T)$. Since $y^{-1} z \in T$ it follows that $z \in N_{S_q}(T)$.

By Lemma 2.1, $\nu(\alpha(1), i_1, i_2)^x = \nu(\alpha(z^{-1}y), i_1^z, i_2^y)$, and because $\delta \geqslant 3$ it follows that $\alpha(z^{-1}y) = \alpha(1)$. Thus $z = y$, $i_1^z = j_1$ and $i_2^z = j_2$. In particular, $N_{S_q}(T)$ acts 2-transitively on Q.

Now assume that $N_{S_q}(T)$ is 2-transitive, and let $X = \langle A(T), \mathrm{Diag}_q(T)\rangle$. As $\mathrm{Diag}_q(T)$ acts regularly on $C(T)$, it follows that X acts transitively on $C(T)$. Consider $\nu(\alpha(1), i_1, i_2)$, $\nu(\alpha(1), j_1, j_2) \in \Gamma_1(\alpha(1))$. As $N_{S_q}(T)$ is 2-transitive, there exists $y \in N_{S_q}(T)$ such that $i_1^y = j_1$ and $i_2^y = j_2$. Let $x = x_y\sigma(y) \in A(T)$. By Lemma 2.1, $\nu(\alpha(1), i_1, i_2)^x = \nu(\alpha(y^{-1}y), i_1^y, i_2^y) = \nu(\alpha(1), j_1, j_2)$. Thus $A(T)$ acts transitively on $\Gamma_1(\alpha(1))$. Because X acts transitively on $C(T)$, we deduce that X acts transitively on the set of neighbours of $C(T)$. This proves the first statement in Theorem 1.3.

Finally suppose that $C(T)$ is a diagonally neighbour transitive code in $H(q,q)$ and let p be a positive integer. By the previous argument it follows that $N_{S_q}(T)$ is 2-transitive and $C(T)$ is X-neighbour transitive with $X = \langle A(T), \mathrm{Diag}_q(T)\rangle$. Moreover $X_{\alpha(1)} = A(T)$ acts transitively on $\Gamma_1(\alpha(1))$. Thus, by Proposition 2.8, $\mathrm{Rep}_p(C(T))$ is $(X \times S_p)$-neighbour transitive in $H(pq,q)$, and because $X \leqslant \mathrm{Diag}_q(S_q) \rtimes L$ it follows that $X \times S_p \leqslant \mathrm{Diag}_{pq}(S_q) \rtimes S_{pq}$. □

6. Acknowledgements

This research was supported by the Australian Research Council Federation Fellowship FF0776186 of the second author and also, for the first author, by an Australian Postgraduate Award.

References

[1] Bailey, R.F.: Error-correcting codes from permutation groups. Discrete Math. **309**(13), 4253–4265 (2009)
[2] Blake, I.: Permutation codes for discrete channels. Information Theory, IEEE Transactions on **20**(1), 138 – 140 (1974).
[3] Blake, I.F., Cohen, G., Deza, M.: Coding with permutations. Inform. and Control **43**(1), 1–19 (1979)
[4] 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)]*, vol. 18. Springer-Verlag, Berlin (1989)
[5] Chu, W., Colbourn, C.J., Dukes, P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**(1-3), 51–64 (2004)
[6] Chu, W., Colbourn, C.J., Dukes, P.: On constant composition codes. Discrete Appl. Math. **154**(6), 912–929 (2006)
[7] Dukes, P.: Coding with injections. Designs, Codes and Cryptography. Online first (2011). DOI 10.1007/s10623-011-9547-4
[8] Frankl, P., Deza, M.: On the maximum number of permutations with given maximal or minimal distance. J. Combinatorial Theory Ser. A **22**(3), 352–360 (1977)
[9] Gillespie, N., Praeger, C.: Neighbour transitivity on codes in Hamming graphs. Des. Codes Cryptogr. **67**(3), 385–393 (2013).
[10] Gillespie, N.I., Giudici, M., Praeger, C.E.: Classification of a family of completely transitive codes. arXiv:1208.0393 (2012)
[11] Giudici, M., Praeger, C.E.: Completely transitive codes in Hamming graphs. European J. Combin. **20**(7), 647–661 (1999).
[12] Goethals, J.M., van Tilborg, H.C.A.: Uniformly packed codes. Philips Res. Rep. **30**, 9–36 (1975)
[13] Han Vinck, A.J.: Coded modulation for power line communications. AEÜ Journal **Jan**, 45–49 (2000). arXiv:1104.4528v1
[14] Huczynska, S., Mullen, G.L.: Frequency permutation arrays. J. Combin. Des. **14**(6), 463–478 (2006).
[15] Keevash, P., Ku, C.Y.: A random construction for permutation codes and the covering radius. Des. Codes Cryptogr. **41**(1), 79–86 (2006)

[16] Neumaier, A.: Completely regular codes. Discrete Math. **106/107**, 353–360 (1992). A collection of contributions in honour of Jack van Lint

[17] 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).

[18] Pless, V.: Introduction to the theory of error-correcting codes, third edn. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York (1998). A Wiley-Interscience Publication

[19] Slepian, D.: Permutation modulation. Proc. IEEE **53**(3), 228–236 (1965)

[20] Smith, D., Montemanni, R.: Permutation codes with specified packing radius. Designs, Codes and Cryptography **69**(1), 95–106 (2013).

[Gillespie and Praeger] Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, Western Australia 6009, [Praeger] also affiliated with King Abdulaziz University, Jeddah, Saudi Arabia.

E-mail address: `neil.gillespie@graduate.uwa.edu.au, cheryl.praeger@uwa.edu.au`