

# 2-Neighbour-Transitive Codes with Small Blocks of Imprimitivity\*

Neil I. Gillespie

Heilbronn Institute for Mathematical Research  
School of Mathematics, Howard House  
University of Bristol, BS8 1SN, United Kingdom

neil.gillespie@bristol.ac.uk

Daniel R. Hawtin<sup>†</sup>

School of Science & Environment (Mathematics)  
Memorial University of Newfoundland, Grenfell Campus  
Corner Brook, NL, A2H 5G5, Canada

dan.hawtin@gmail.com

Cheryl E. Praeger

Centre for the Mathematics of Symmetry and Computation  
The University of Western Australia  
Crawley, WA, 6009, Australia

cheryl.praeger@uwa.edu.au

Submitted: Jul 30, 2018; Accepted: Dec 30, 2019; Published: Feb 7, 2020

© The authors. Released under the CC BY-ND license (International 4.0).

## Abstract

A code  $C$  in the Hamming graph  $\Gamma = H(m, q)$  is a subset of the vertex set  $V\Gamma$  of the Hamming graph; the elements of  $C$  are called *codewords*. Any such code  $C$  induces a partition  $\{C, C_1, \dots, C_\rho\}$  of  $V\Gamma$ , where  $\rho$  is the *covering radius* of the code, based on the distance each vertex is to its nearest codeword. For  $s \in \{1, \dots, \rho\}$  and  $X \leq \text{Aut}(C)$ , if  $X$  is transitive on each of  $C, C_1, \dots, C_s$ , then  $C$  is said to be  $(X, s)$ -neighbour-transitive. In particular,  $C$  is said to be  $X$ -completely transitive if  $C$

---

\*The second author is grateful for the support of an Australian Research Training Program Scholarship and a University of Western Australia Safety-Net Top-Up Scholarship. The research forms part of Australian Research Council Project FF0776186. We are most grateful for the anonymous referee's helpful and detailed comments.

<sup>†</sup>Current address: Department of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia.

is  $(X, \rho)$ -neighbour-transitive. It is known that for any  $(X, 2)$ -neighbour-transitive code with minimum distance at least 5, either i)  $X$  is faithful on the set of coordinate entries, ii)  $C$  is  $X$ -alphabet-almost-simple or iii)  $C$  is  $X$ -alphabet-affine. Classifications of  $(X, 2)$ -neighbour-transitive codes in the first two categories having minimum distance at least 5 and 3, respectively, have been achieved in previous papers. Hence this paper considers case iii).

Let  $q = p^{dm}$  and identify the vertex set of  $H(m, q)$  with  $\mathbb{F}_p^{dm}$ . The main result of this paper classifies  $(X, 2)$ -neighbour-transitive codes with minimum distance at least 5 that contain, as a block of imprimitivity for the action of  $X$  on  $C$ , an  $\mathbb{F}_p$ -subspace of  $\mathbb{F}_p^{dm}$  of dimension at most  $d$ . When considering codes with minimum distance at least 5,  $X$ -completely transitive codes are a proper subclass of  $(X, 2)$ -neighbour-transitive codes. This leads, as a corollary of the main result, to a solution of a problem posed by Giudici in 1998 on completely transitive codes.

**Mathematics Subject Classifications:** 05E18, 94B05, 05B05

## 1 Introduction

Classifying classes of codes is an important task in error correcting coding theory. The parameters of perfect codes over prime power alphabets have been classified; see [31] or [34]. In contrast, for the classes of *completely regular* and *s-regular* codes, introduced by Delsarte [11] as a generalisation of *perfect* codes, similar classification results have only been achieved for certain subclasses. Recent results include [3, 4, 5, 6]. For a survey of results on completely regular codes see [7]. Classifying families of *2-neighbour transitive* codes has been the subject of [15, 16].

A subset  $C$  of the vertex set  $V\Gamma$  of the Hamming graph  $\Gamma = H(m, q)$  is called a *code*, the elements of  $C$  are called *codewords*, and the subset  $C_i$  of  $V\Gamma$  consisting of all vertices of  $H(m, q)$  having nearest codeword at Hamming distance  $i$  is called the *set of  $i$ -neighbours* of  $C$ . The definition of a completely regular code  $C$  involves certain combinatorial regularity conditions on the *distance partition*  $\{C, C_1, \dots, C_\rho\}$  of  $C$ , where  $\rho$  is the *covering radius*. The current paper concerns the algebraic analogues, defined directly below, of the classes of completely regular and *s-regular* codes. Note that the group  $\text{Aut}(C)$  is the setwise stabiliser of  $C$  in the full automorphism group of  $H(m, q)$ ; precise definitions of notations are available in Section 2.

**Definition 1.** Let  $C$  be a code in  $H(m, q)$  with covering radius  $\rho$ , let  $s \in \{1, \dots, \rho\}$ , and  $X \leq \text{Aut}(C)$ . Then  $C$  is said to be

1.  $(X, s)$ -neighbour-transitive if  $X$  acts transitively on each of the sets  $C, C_1, \dots, C_s$ ,
2.  $X$ -neighbour-transitive if  $C$  is  $(X, 1)$ -neighbour-transitive,
3.  $X$ -completely transitive if  $C$  is  $(X, \rho)$ -neighbour-transitive, and,
4.  $s$ -neighbour-transitive, neighbour-transitive, or completely transitive, respectively, if  $C$  is  $(\text{Aut}(C), s)$ -neighbour-transitive,  $\text{Aut}(C)$ -neighbour-transitive, or  $\text{Aut}(C)$ -completely transitive, respectively.

A variant of the above concept of complete transitivity was introduced for linear codes by Solé [29], with the above definition first appearing in [23]. Note that non-linear completely transitive codes do indeed exist; see [21]. Completely transitive codes form a subfamily of completely regular codes, and  $s$ -neighbour-transitive codes are a sub-family of  $s$ -regular codes, for each  $s$ . It is hoped that studying 2-neighbour-transitive codes will lead to a better understanding of completely transitive and completely regular codes. Indeed a classification of 2-neighbour-transitive codes would have as a corollary a classification of completely transitive codes.

Completely transitive codes have been studied in [6, 13], for instance. Neighbour-transitive codes are investigated in [17, 19, 20]. The class of 2-neighbour-transitive codes is the subject of [15, 16], and the present work comprises part of the second author's PhD thesis [24]. Recently, codes with 2-transitive actions on the coordinate entries of vertices in the Hamming graph have been used to construct families of codes that achieve capacity on erasure channels [26], and many 2-neighbour-transitive codes indeed admit such an action; see Proposition 6.

Each vertex of  $H(m, q)$  is of the form  $\alpha = (\alpha_1, \dots, \alpha_m)$ , where the entries  $\alpha_i$  come from an *alphabet*  $Q$  of size  $q$ . A typical automorphism of  $H(m, q)$  is a composition of two automorphisms, each of a special type. An automorphism of the first type corresponds to an  $m$ -tuple  $(h_1, \dots, h_m)$  of permutations of  $Q$  and maps a vertex  $\alpha$  to  $(\alpha_1^{h_1}, \dots, \alpha_m^{h_m})$ . An automorphism of the second type corresponds to a permutation of the set  $M = \{1, \dots, m\}$  of subscripts and simply permutes the entries of vertices, for example the map corresponding to the permutation (123) of  $M$  maps  $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \dots, \alpha_m)$  to  $(\alpha_3, \alpha_1, \alpha_2, \alpha_4, \dots, \alpha_m)$ . (More details are given in Section 2.1.) It is sometimes helpful to distinguish between entries in the different positions, and we will refer to the set of entries occurring in position  $i$  as  $Q_i$ . Then maps of the second type may be viewed as permuting the subsets  $Q_1, \dots, Q_m$  between themselves in the same way that they permute  $M$ .

For a subgroup  $X$  of automorphisms of  $H(m, q)$ , the subgroup  $K$  of  $X$  consisting of all elements which fix each of the  $Q_i$  setwise is a normal subgroup of  $X$  and is the kernel of the action  $X$  induces on  $M$ . Also, for each  $i \in M$ , the set of elements of  $X$  which fix  $Q_i$  setwise forms a subgroup  $X_i$  of  $X$ , and  $X_i$  induces a subgroup of permutations of  $Q_i$ , which we denote by  $X_i^{Q_i}$ . (Again, more details are given in Section 2.1.)

It was shown in [15] that the family of  $(X, 2)$ -neighbour-transitive codes can be subdivided into three disjoint sub-families, according properties of the group  $X$  (see Proposition 7). We now introduce these sub-families in Definition 2.

**Definition 2.** Let  $C$  be a code in  $H(m, q)$  and let  $X \leq \text{Aut}(C)$ . Moreover, let  $Q_i$ ,  $X_i$  and  $K$  be as described above. Then  $C$  is

1. *X-entry-faithful* if  $X$  acts faithfully on  $M$ , that is,  $K = 1$ ,
2. *X-alphabet-almost-simple* if  $K \neq 1$ ,  $X$  acts transitively on  $M$ , and  $X_i^{Q_i}$  is a 2-transitive almost-simple group, and,
3. *X-alphabet-affine* if  $K \neq 1$ ,  $X$  acts transitively on  $M$ , and  $X_i^{Q_i}$  is a 2-transitive affine group.

Note that Propositions 6 and 7, and the fact that every 2-transitive group is either affine or almost-simple (see [9, Section 154] or [12, Theorem 4.1B]), ensure that every 2-neighbour-transitive code satisfies precisely one of the cases given in Definition 2.

Those  $(X, 2)$ -neighbour transitive codes that are also  $X$ -entry-faithful and have minimum distance at least 5 are classified in [15]; while those that are  $X$ -alphabet-almost-simple and have minimum distance at least 3 are classified in [16]. Hence, in this paper we study  $X$ -alphabet-affine codes. For such graphs  $q = p^d$  for some prime  $p$  and positive integer  $d$ , and we identify the vertex set of the Hamming graph  $H(m, q)$  with the  $(dm)$ -dimensional vector space  $V = \mathbb{F}_p^{dm}$ . For a nontrivial subspace  $W$  of  $V$  we denote by  $T_W$  the group of translations by elements of  $W$ ; recall for a subgroup  $X$  of  $\text{Aut}(H(m, q))$  (the automorphism group of  $H(m, q)$ ), we denote by  $K$  the kernel of the action of the group  $X$  on  $M$ ; and we note that  $K = X \cap B$  where  $B \cong S_q^m$  is the base group of  $\text{Aut}(H(m, q))$ ; see Section 2.

**Definition 3.** Let  $q = p^d$ ,  $V = \mathbb{F}_p^{dm}$  be as above and let  $W$  be a non-trivial  $\mathbb{F}_p$ -subspace of  $V$ . An  $(X, 2)$ -neighbour-transitive extension of  $W$  is an  $(X, 2)$ -neighbour-transitive code  $C$  containing  $\mathbf{0}$  such that  $T_W \leq X$ , where  $T_W$  is the group of translations by elements of  $W$ , and  $W$  is fixed setwise by  $K = X \cap B$ . Note that  $T_W \leq X$  and  $\mathbf{0} \in C$  means that  $W \subseteq C$ . If  $C \neq W$  then the extension is said to be *non-trivial*.

The main result of this paper, below, classifies all  $(X, 2)$ -neighbour-transitive extensions of  $W$ , supposing  $W$  is a  $k$ -dimensional  $\mathbb{F}_p$ -subspace of  $V$ , where  $k \leq d$ . Theorem 4 may be seen as a sequel of [15, Theorem 1.1] where, rather than assuming that the kernel  $K$  of the action of  $X$  on  $M$  is trivial, the condition  $k \leq d$  limits the size of  $W$ , implicitly restricting the possibilities for  $K$ . The motivation for assuming  $k \leq d$  comes largely from [22, Problem 6.5.4], which proposes investigating hypotheses similar to those of Theorem 4, but in the context of  $X$ -completely transitive codes in  $H(m, 2)$ ; see also Corollary 5.

**Theorem 4.** Let  $V = \mathbb{F}_p^{dm}$  be the vertex set of the Hamming graph  $H(m, p^d)$  and  $C$  be an  $(X, 2)$ -neighbour-transitive extension of a subspace  $W$  of  $V$  as in Definition 3, where  $C$  has minimum distance  $\delta \geq 5$  and  $W$  is a non-trivial  $\mathbb{F}_p$ -subspace of  $V$  with  $\mathbb{F}_p$ -dimension  $k \leq d$ . Then  $p = 2$ ,  $d = 1$ ,  $W$  is the binary repetition code in  $H(m, 2)$ , and one of the following holds:

1.  $C = W$  with  $\delta = m$ ;
2.  $C = \mathcal{H}$ , where  $\mathcal{H}$  is the Hadamard code of length 12, as in Definition 12, with  $\delta = 6$ ;  
or,
3.  $C = \mathcal{P}$ , where  $\mathcal{P}$  is the punctured code of the Hadamard code of length 12, as in Definition 12, with  $\delta = 5$ .

A corollary of Theorem 4 regarding completely transitive codes is stated below. This result was originally proved in [14, Theorem 10.2] using somewhat different methods, with the problem first being posed in [22, Problem 6.5.4]. The group  $\text{Diag}_m(G)$ , where  $G \leq \text{Sym}(Q)$ , is defined in Section 2.1.

**Corollary 5.** *Let  $C$  be an  $X$ -completely transitive code in  $H(m, 2)$  with minimum distance  $\delta \geq 5$  such that  $K = X \cap B = \text{Diag}_m(S_2)$ . Then  $C$  is equivalent to one of the codes appearing in Theorem 4, each of which is indeed completely transitive.*

Section 2 introduces the notation used throughout the paper and Section 3 proves the main results.

## 2 Notation and preliminaries

Let the set of coordinate entries  $M$  and the alphabet  $Q$  be sets of sizes  $m$  and  $q$ , respectively, both  $m$  and  $q$  integers at least 2. The vertex set  $V\Gamma$  of the Hamming graph  $\Gamma = H(m, q)$  consists of all functions from the set  $M$  to the set  $Q$ , usually expressed as  $m$ -tuples. Let  $Q_i \cong Q$  be the copy of the alphabet in the entry  $i \in M$  so that the vertex set of  $H(m, q)$  is identified with the Cartesian product

$$V\Gamma = \prod_{i \in M} Q_i.$$

An edge exists between two vertices if and only if they differ as  $m$ -tuples in exactly one entry. Note that  $S^\times$  will denote the set  $S \setminus \{0\}$  for any set  $S$  containing 0. In particular,  $Q$  will usually be a vector-space here, and hence contains the zero vector. A code  $C$  is a subset of  $V\Gamma$ . If  $\alpha$  is a vertex of  $H(m, q)$  and  $i \in M$  then  $\alpha_i$  refers to the value of  $\alpha$  in the  $i$ -th entry, that is,  $\alpha_i \in Q_i$ , so that  $\alpha = (\alpha_1, \dots, \alpha_m)$  when  $M = \{1, \dots, m\}$ . For more in depth background material on coding theory see [10] or [28].

Let  $\alpha, \beta$  be vertices and  $C$  be a code in a Hamming graph  $H(m, q)$  with  $0 \in Q$  a distinguished element of the alphabet. A summary of important notation regarding codes in Hamming graphs is contained in Table 1.

Note that if the minimum distance  $\delta$  of a code  $C$  satisfies  $\delta \geq 2s$ , then the set of  $s$ -neighbours  $C_s$  satisfies  $C_s = \cup_{\alpha \in C} \Gamma_s(\alpha)$  and if  $\delta \geq 2s + 1$  this is a disjoint union. This fact is crucial in many of the proofs below; it is often assumed that  $\delta \geq 5$ , in which case every element of  $C_2$  is distance 2 from a unique codeword.

A *linear* code is a code  $C$  in  $H(m, q)$  with alphabet  $Q = \mathbb{F}_q$  a finite field, so that the vertices of  $H(m, q)$  form a vector space  $V$ , such that  $C$  is an  $\mathbb{F}_q$ -subspace of  $V$ . Given  $\alpha, \beta \in V$ , the usual inner product is given by  $\langle \alpha, \beta \rangle = \sum_{i \in M} \alpha_i \beta_i$ . The *dual* code of  $C$  is  $C^\perp = \{\beta \in V \mid \forall \alpha \in C, \langle \alpha, \beta \rangle = 0\}$ .

The *Singleton bound* (see [11, 4.3.2]) is a well known bound for the size of a code  $C$  in  $H(m, q)$  with minimum distance  $\delta$ , stating that  $|C| \leq q^{m-\delta+1}$ . For a linear code  $C$  this may be stated as  $\delta^\perp - 1 \leq k \leq m - \delta + 1$ , where  $k$  is the dimension of  $C$ ,  $\delta$  is the minimum distance of  $C$  and  $\delta^\perp$  is the minimum distance of  $C^\perp$ .

A vertex or an entire code from a Hamming graph  $H(m, q)$  may be projected into a smaller Hamming graph  $H(k, q)$ . For a subset  $J = \{j_1, \dots, j_k\} \subseteq M$  the *projection of*  $\alpha$ , with respect to  $J$ , is  $\pi_J(\alpha) = (\alpha_{j_1}, \dots, \alpha_{j_k})$ . For a code  $C$  the *projection of*  $C$ , with respect to  $J$ , is  $\pi_J(C) = \{\pi_J(\alpha) \mid \alpha \in C\}$ .

Notation	Explanation
$\mathbf{0}$	vertex with 0 in each entry
$(a^k, 0^{m-k})$	vertex with $a \in Q$ first $k$ entries and 0 otherwise
$\text{diff}(\alpha, \beta) = \{i \in M \mid \alpha_i \neq \beta_i\}$	set of entries in which $\alpha$ and $\beta$ differ
$\text{supp}(\alpha) = \{i \in M \mid \alpha_i \neq 0\}$	support of $\alpha$
$\text{wt}(\alpha) =  \text{supp}(\alpha) $	weight of $\alpha$
$d(\alpha, \beta) =  \text{diff}(\alpha, \beta) $	Hamming distance
$\Gamma_s(\alpha) = \{\beta \in V\Gamma \mid d(\alpha, \beta) = s\}$	set of $s$ -neighbours of $\alpha$
$\delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$	minimum distance of $C$
$d(\alpha, C) = \min\{d(\alpha, \beta) \mid \beta \in C\}$	distance from $\alpha$ to $C$
$\rho = \max\{d(\alpha, C) \mid \alpha \in V\Gamma\}$	covering radius of $C$
$C_s = \{\alpha \in V\Gamma \mid d(\alpha, C) = s\}$	set of $s$ -neighbours of $C$
$\{C = C_0, C_1, \dots, C_\rho\}$	distance partition of $C$

Table 1: Hamming graph notation.

## 2.1 Automorphisms of a Hamming graph

The automorphism group  $\text{Aut}(\Gamma)$  of the Hamming graph is the semi-direct product  $B \rtimes L$ , where  $B \cong \text{Sym}(Q)^m$  and  $L \cong \text{Sym}(M)$  (see [8, Theorem 9.2.1]). Note that  $B$  and  $L$  are called the *base group* and the *top group*, respectively, of  $\text{Aut}(\Gamma)$ . Since we identify  $Q_i$  with  $Q$ , we also identify  $\text{Sym}(Q_i)$  with  $\text{Sym}(Q)$ . If  $h \in B$  and  $i \in M$  then  $h_i \in \text{Sym}(Q_i)$  is the image of the action of  $h$  in the entry  $i \in M$ . Let  $h \in B$ ,  $\sigma \in L$  and  $\alpha \in V\Gamma$ . Then  $h$  and  $\sigma$  act on  $\alpha$  explicitly via:

$$\alpha^h = (\alpha_1^{h_1}, \dots, \alpha_m^{h_m}) \quad \text{and} \quad \alpha^\sigma = (\alpha_{1\sigma^{-1}}, \dots, \alpha_{m\sigma^{-1}}).$$

For reasons of readability we often write the image  $\alpha^\sigma$  as  $(\alpha_{1\sigma^{-1}}, \dots, \alpha_{m\sigma^{-1}})$ . The automorphism group of a code  $C$  in  $\Gamma = H(m, q)$  is  $\text{Aut}(C) = \text{Aut}(\Gamma)_C$ , the setwise stabiliser of  $C$  in  $\text{Aut}(\Gamma)$ .

Let  $G$  be a group acting on a set  $\Omega$ ,  $\omega \in \Omega$  and  $S \subseteq \Omega$ . Then,

1.  $G_\omega$  denotes the subgroup of  $G$  stabilising  $\omega$ ,
2.  $G_S$  denotes the setwise stabiliser of  $S$  in  $G$ ,
3.  $G_{(S)}$  denotes the point-wise stabiliser of  $S$  in  $G$ , and,
4. if  $G$  fixes  $S$  setwise then  $G^S$  denotes the subgroup of  $\text{Sym}(S)$  induced by  $G$ .

(For more background and notation on permutation groups see, for instance, [12].) In particular, let  $X \leq \text{Aut}(\Gamma)$ . Then:

1. For  $x \in X$ , recall that  $x = h\sigma$  where  $h \in B$  and  $\sigma \in L$ . Then  $x^M = \sigma$  denotes the permutation of  $M$  induced by  $x$ , and we write  $X^M = \{x^M \mid x \in X\}$ ; we call  $X^M$

the *action of  $X$  on entries*. Note that a pre-image  $x$  of an element  $x^M$  of  $X^M$  need not fix any vertex of  $H(m, q)$ .

2.  $K = K \cap B$  is the kernel  $X_{(M)}$  of the action of  $X$  on entries and is precisely the subgroup of  $X$  fixing  $M$  point-wise.
3. If  $i \in M$ , then  $X_i$  denotes the stabiliser of the entry  $i$  and any  $x \in X_i$  is of the form  $h\sigma$  ( $h \in B$  and  $\sigma \in L$ ) where  $\sigma$  fixes  $i \in M$ . So  $x = h\sigma$  induces the permutation  $h_i \in \text{Sym}(Q_i)$  on the alphabet  $Q_i$ . This defines a homomorphism from  $X_i$  to  $\text{Sym}(Q_i)$  and we denote the image of this homomorphism by  $X_i^{Q_i}$ . We refer to  $X_i^{Q_i}$  as the *action on the alphabet*.
4. For any  $Y \leq X_i$  we write  $Y^{Q_i} = \{y^{Q_i} \mid y \in Y\}$  so that  $Y^{Q_i} \leq X^{Q_i} \leq \text{Sym}(Q_i)$ . In particular, for  $Y = K = X \cap B$ , we have  $K \leq \prod_{i \in M} K^{Q_i}$ , where here  $K$  projects onto each direct factor.

Given a group  $A \leq \text{Sym}(Q)$  an important subgroup of  $\text{Aut}(\Gamma)$  is the group  $\text{Diag}_m(A)$ , where an element of  $A$  acts the same in each entry. Formally, for each  $a \in \text{Sym}(Q)$ , let  $\text{diag}_m(a) = (a, a, \dots, a) \in B$  and for each  $A \leq \text{Sym}(Q)$ , define  $\text{Diag}_m(A) = \{\text{diag}_m(a) \mid a \in A\}$ .

It is worth mentioning that coding theorists often consider more restricted groups of automorphisms, such as the group  $\text{PermAut}(C) = \{\sigma \mid h\sigma \in \text{Aut}(C), h = 1 \in B, \sigma \in L\}$ . The elements of this group are called *pure permutations* on the entries of the code.

Two codes  $C$  and  $C'$  in  $H(m, q)$  are said to be *equivalent* if there exists some  $x \in \text{Aut}(\Gamma)$  such that  $C^x = \{\alpha^x \mid \alpha \in C\} = C'$ . Equivalence preserves many of the important properties in coding theory, such as minimum distance and covering radius, since  $\text{Aut}(\Gamma)$  preserves distances in  $H(m, q)$ .

## 2.2 s-Neighbour-transitive codes

This section presents preliminary results regarding  $(X, s)$ -neighbour-transitive codes, defined in Definition 1. The next results give certain 2-homogeneous and 2-transitive actions associated with an  $(X, 2)$ -neighbour-transitive code.

**Proposition 6.** [15, Proposition 2.5] *Let  $C$  be an  $(X, s)$ -neighbour-transitive code in  $H(m, q)$  with minimum distance  $\delta$ , where  $\delta \geq 3$  and  $s \geq 1$ . Then for  $\alpha \in C$  and  $i \leq \min\{s, \lfloor \frac{\delta-1}{2} \rfloor\}$ , the stabiliser  $X_\alpha$  fixes setwise and acts transitively on  $\Gamma_i(\alpha)$ . In particular, the action of  $X_\alpha$  on  $M$  is  $i$ -homogeneous.*

**Proposition 7.** [15, Proposition 2.7] *Let  $C$  be an  $(X, 1)$ -neighbour-transitive code in  $H(m, q)$  with minimum distance  $\delta \geq 3$  and  $|C| > 1$ . Then  $X_i^{Q_i}$  acts 2-transitively on  $Q_i$  for all  $i \in M$ .*

The next result gives information about the order of the stabiliser of a codeword in the automorphism group of a 2-neighbour-transitive code and is a strengthening of [15, Lemma 2.10].

**Lemma 8.** *Let  $C$  be an  $(X, 2)$ -neighbour-transitive code in  $H(m, q)$  with  $\delta \geq 5$  and  $\mathbf{0} \in C$ , and let  $i, j \in M$  be distinct. Then the following hold:*

1. *The stabiliser  $X_{\mathbf{0},i,j}$  acts transitively on each of the sets  $Q_i^\times$  and  $Q_j^\times$ .*
2. *Moreover,  $X_{\mathbf{0},i,j}$  has at most two orbits on  $Q_i^\times \times Q_j^\times$ , and if  $X_{\mathbf{0},i,j}$  has two orbits on  $Q_i^\times \times Q_j^\times$  then both orbits are the same size and  $X_{\mathbf{0}}$  acts 2-transitively on  $M$ .*
3. *The order of  $X_{\mathbf{0}}$ , and hence  $|X|$ , is divisible by  $\binom{m}{2}(q-1)^2$ .*
4. *If  $|X_{\mathbf{0}}| = \binom{m}{2}$  then  $q = 2$ .*

*Proof.* Now  $X_{\mathbf{0}}$  acts transitively on  $\Gamma_2(\mathbf{0})$ , by Proposition 6, since  $\delta \geq 5$ . Since  $|\Gamma_2(\mathbf{0})| = \binom{m}{2}(q-1)^2$ , parts 3 and 4 hold. Also, we have that the stabiliser  $X_{\mathbf{0},\{i,j\}}$  of the subset  $\{i, j\} \subseteq M$  is transitive on the set of weight 2 vertices with support  $\{i, j\}$ . Hence  $X_{\mathbf{0},i,j}$  has at most two orbits on  $Q_i^\times \times Q_j^\times$  and if there are two they have equal size. Note that if  $X_{\mathbf{0},i,j}$  has one orbit on  $Q_i^\times \times Q_j^\times$  then  $X_{\mathbf{0},i,j}$  acts transitively on each of  $Q_i^\times$  and  $Q_j^\times$ . Suppose that  $X_{\mathbf{0},i,j}$  has two orbits on  $Q_i^\times \times Q_j^\times$ , and hence that  $X_{\mathbf{0},i,j} \neq X_{\mathbf{0},\{i,j\}}$ . By Proposition 6,  $X_{\mathbf{0}}$  acts 2-homogeneously on  $M$ . Since  $X_{\mathbf{0},i,j} \neq X_{\mathbf{0},\{i,j\}}$ , we have that  $X_{\mathbf{0}}$  is in fact 2-transitive on  $M$ , proving part 2. Let  $k$  be the number of  $X_{\mathbf{0},i,j}$ -orbits on  $Q_i^\times$ . Since  $X_{\mathbf{0}}$  is 2-transitive on  $M$ , it follows that  $X_{\mathbf{0},i,j}^{Q_i^\times}$  is permutation isomorphic to  $X_{\mathbf{0},i,j}^{Q_j^\times}$  and hence  $X_{\mathbf{0},i,j}$  has the same number of orbits on each of  $Q_i^\times$  and  $Q_j^\times$ . Since each orbit of  $X_{\mathbf{0},i,j}$  on  $Q_i^\times \times Q_j^\times$  is contained in the Cartesian product of an orbit on  $Q_i^\times$  with an orbit on  $Q_j^\times$ , it follows that  $X_{\mathbf{0},i,j}$  has at least  $k^2$  orbits on  $Q_i^\times \times Q_j^\times$ . However,  $k \geq 2$  implies  $k^2 \geq 4$ , contradicting part 2, and hence part 1 holds.  $\square$

The concept of a design, introduced below, comes up frequently in coding theory. Let  $\alpha \in H(m, q)$  and  $0 \in Q$ . A vertex  $\nu$  of  $H(m, q)$  is said to be *covered* by  $\alpha$  if  $\nu_i = \alpha_i$  for every  $i \in M$  such that  $\nu_i \neq 0$ .

**Definition 9.** A  $q$ -ary  $s$ - $(m, k, \lambda)$  design in  $\Gamma = H(m, q)$  is a subset  $\mathcal{D}$  of vertices of  $\Gamma_k(\mathbf{0})$  (where  $k \geq s$ ) such that each vertex  $\nu \in \Gamma_s(\mathbf{0})$  is covered by exactly  $\lambda$  vertices of  $\mathcal{D}$ . The elements of  $\mathcal{D}$  are called *blocks*.

When  $q = 2$ , that is, in the case of a binary design, then each vertex of  $\mathcal{D}$  can be interpreted as the characteristic vector of a  $k$ -element subset of  $\{1, \dots, m\}$ . Thus the set  $\mathcal{D}$  can be thought of as a collection of  $k$ -element subsets of  $\{1, \dots, m\}$ , called blocks, and the ‘‘covering condition’’ becomes the condition that each  $s$ -element subset of  $\{1, \dots, m\}$  is contained in exactly  $\lambda$  blocks. With this interpretation, these structures are usually called *combinatorial designs*.

The following equations can be found, for instance, in [30]. Let  $\mathcal{D}$  be a combinatorial  $s$ - $(m, k, \lambda)$  design with  $|\mathcal{D}| = b$  blocks and let  $r$  be the number of blocks containing any given point. Then  $mr = bk$ ,  $r(k-1) = \lambda(m-1)$  and

$$b = \frac{m(m-1) \cdots (m-s+1)}{k(k-1) \cdots (k-s+1)} \lambda. \tag{1}$$



The definition below is required in order to state the remaining two results of this section.

**Definition 10.** Let  $C$  be a code in  $H(m, q)$  with covering radius  $\rho$ , and  $s$  be an integer with  $0 \leq s \leq \rho$ . Then,

1.  $C$  is  $s$ -regular if, for each  $i \in \{0, 1, \dots, s\}$ , each  $k \in \{0, 1, \dots, m\}$ , and every vertex  $\nu \in C_i$ , the number  $|\Gamma_k(\nu) \cap C|$  depends only on  $i$  and  $k$ , and,
2.  $C$  is completely regular if  $C$  is  $\rho$ -regular.

**Lemma 11.** [15, Lemma 2.16] Let  $C$  be an  $(X, s)$ -neighbour transitive code in  $H(m, q)$ . Then  $C$  is  $s$ -regular. Moreover, if  $C$  has minimum distance  $\delta \geq 2s$  and contains  $\mathbf{0}$ , then for each  $k \leq m$  the set of codewords of weight  $k$  forms a  $q$ -ary  $s$ -( $m, k, \lambda$ ) design, for some  $\lambda$ .

**Definition 12.** [15, Definition 4.1] Let  $\mathcal{P}$  be the punctured Hadamard 12 code, obtained as follows (see [28, Part 1, Section 2.3]). First, we construct a normalised Hadamard matrix  $H_{12}$  of order 12 using the Paley construction.

1. Let  $M = \mathbb{F}_{11} \cup \{*\}$  and let  $H_{12}$  be the  $12 \times 12$  matrix with first row  $v$ , where  $v_a = -1$  if  $a$  is a square in  $\mathbb{F}_{11}$  (including 0), and  $v_a = 1$  if  $a$  is a non-square in  $\mathbb{F}_{11}$  or  $a = * \in M$ , taking the orbit of  $v$  under the additive group of  $\mathbb{F}_{11}$  acting on  $M$  to form 10 more rows and adding a final row, the vector  $(-1, \dots, -1)$ .
2. The Hadamard code  $\mathcal{H}$  of length 12 in  $H(12, 2)$  then consists of the vertices  $\alpha$  such that there exists a row  $u$  in  $H_{12}$  or  $-H_{12}$  satisfying  $\alpha_a = 0$  when  $u_a = 1$  and  $\alpha_a = 1$  when  $u_a = -1$ .
3. The punctured code  $\mathcal{P}$  of  $\mathcal{H}$  is obtained by deleting the coordinate  $*$  from  $M$ . The weight 6 codewords of  $\mathcal{P}$  form a binary 2-(11, 6, 3) design, which we denote throughout by  $\mathcal{D}$ . The code  $\mathcal{P}$  consists of the following codewords: the zero codeword, the vector  $(1, \dots, 1)$ , the characteristic vectors of the 2-(11, 6, 3) design  $\mathcal{D}$ , and the characteristic vectors of the complement of that design, which forms a 2-(11, 5, 2) design. (Both  $\mathcal{D}$  and its complement are unique up to isomorphism [32].)
4. The even weight subcode  $\mathcal{E}$  of  $\mathcal{P}$  is the code consisting of the zero codeword and the 2-(11, 6, 3) design.

**Proposition 13.** [15, Proposition 4.3] Let  $C$  be a 2-regular code in  $H(11, 2)$  with  $\delta \geq 5$  and  $|C| \geq 2$ . Then one of the following holds:

1.  $\delta = 11$  and  $C$  is equivalent to the binary repetition code,
2.  $\delta = 5$  and  $C$  is equivalent to the punctured Hadamard code  $\mathcal{P}$ , or
3.  $\delta = 6$  and  $C$  is equivalent to the even weight subcode  $\mathcal{E}$  of  $\mathcal{P}$ .

### 3 Extensions of the binary repetition code

In this section it will be shown that the hypotheses of Theorem 4 imply that  $W$  is the binary repetition code in  $H(m, q)$ . From there, all  $(X, 2)$ -neighbour-transitive extensions of the binary repetition code are classified. First, a more general result regarding  $(X, 2)$ -neighbour-transitive codes. Note that a *system of imprimitivity* for the action of a group  $G$  on a set  $\Omega$  is a non-trivial partition of  $\Omega$  preserved by  $G$ , and a part of the partition is called a *block of imprimitivity*.

**Lemma 14.** *Suppose  $C$  is an  $(X, 2)$ -neighbour-transitive code with  $\delta \geq 5$  and that  $\Delta$  is a block of imprimitivity for the action of  $X$  on  $C$ . Then  $\Delta$  is an  $(X_\Delta, 2)$ -neighbour-transitive code with minimum distance  $\delta_\Delta \geq 5$ .*

*Proof.* Since  $\Delta$  is a block of imprimitivity for the action of  $X$  on  $C$ , it follows that  $X_\Delta$  is transitive on  $\Delta$ . Since  $\delta \geq 5$  and  $\Delta \subseteq C$  it follows that  $\delta_\Delta \geq 5$ . Since  $X_\Delta$  fixes  $\Delta$ , we have that  $X_\Delta$  fixes  $\Delta_1$  and  $\Delta_2$ . It remains to show that  $X_\Delta$  is transitive on  $\Delta_i$  for  $i = 1, 2$ . Let  $i \in \{1, 2\}$  and  $\mu, \nu \in \Delta_i$ . Then, since  $\delta_\Delta \geq 5$ , there exists  $\alpha, \beta \in \Delta$  such that  $\mu \in \Gamma_i(\alpha)$  and  $\nu \in \Gamma_i(\beta)$ . Moreover,  $\mu, \nu \in C_i$  since  $\delta \geq 5$ . Hence, there exists  $x \in X$  such that  $\mu^x = \nu$  and, since  $\delta \geq 5$ ,  $\alpha^x = \beta$  and so lies in  $\Delta \cap \Delta^x$ . Since  $\Delta$  is a block of imprimitivity, it follows that  $x$  fixes  $\Delta$  setwise, so that  $x \in X_\Delta$ . Thus  $X_\Delta$  is transitive on  $\Delta_i$  for  $i \in \{1, 2\}$ .  $\square$

**Corollary 15.** *Let  $C$  be an  $(X, 2)$ -neighbour-transitive extension of  $W$  such that  $C$  has minimum distance  $\delta \geq 5$ . Then  $W$  is a block of imprimitivity for the action of  $X$  on  $C$  and  $W$  is  $(X_W, 2)$ -neighbour-transitive with minimum distance  $\delta_W \geq 5$ .*

*Proof.* Now,  $K = K_W$  is normal in  $X$  and  $T_W \leq K_W$  is transitive on  $W$  from which it follows that  $W$  is an orbit of  $K$  on  $C$  and hence, by [12, Theorem 1.6A (i)], is a block of imprimitivity for the action of  $X$  on  $C$ . Thus, the result is implied by Lemma 14.  $\square$

The next result shows that the binary repetition code is the only 2-neighbour-transitive code which is a  $k$ -dimensional  $\mathbb{F}_p$ -subspace of  $V = \mathbb{F}_p^{dm}$ , identified with the vertex set of  $H(m, p^d)$ , such that  $1 \leq k \leq d$ .

**Lemma 16.** *Let  $q = p^d$  and  $V = \mathbb{F}_p^{dm}$  be the vertex set of the Hamming graph  $H(m, q)$  and let  $W$  be a  $k$ -dimensional  $\mathbb{F}_p$ -subspace of  $V$ , with  $1 \leq k \leq d$ , such that  $W$  is an  $(X, 2)$ -neighbour-transitive code with minimum distance  $\delta \geq 5$ . Then  $q = 2$  and  $W$  is the binary repetition code in  $H(m, 2)$ .*

*Proof.* We claim that  $\delta = m$ . As any  $(X, 2)$ -neighbour transitive code is also 2-regular, by Lemma 11, and  $\mathbf{0} \in W$ , proving the claim implies the result, by [15, Lemma 2.15]. Suppose for a contradiction that  $\delta < m$ . It follows that there exists a weight  $\delta$  codeword  $\alpha \in W$  and distinct  $i, j \in M$  such that  $\alpha_i = 0$  and  $\alpha_j \neq 0$ . Now,  $X_{\mathbf{0}, i, j}$  acts transitively on  $Q_j^\times$ , by Lemma 8, so that for all non-zero  $a \in \mathbb{F}_p^d$  there exists some  $x_a \in X_{\mathbf{0}, i, j}$  such that  $\alpha^{x_a} \in W$  with  $(\alpha^{x_a})_j = a$ . As  $a$  ranges over all non-zero  $a \in \mathbb{F}_p^d$  this gives  $p^d - 1$  distinct codewords. Since  $|W| = p^k \leq p^d$ , and  $\mathbf{0} \in W$ , it follows that  $|W| = p^d$  and  $k = d$ .

Note that since  $\alpha_i = 0$  and  $x_a \in X_{\mathbf{0},i,j}$  this implies that every element of  $W$  has  $i$ -th entry 0. By Proposition 6,  $X_{\mathbf{0}}$  is, in particular, transitive on  $M$ . Hence, there exists some  $y = h\sigma \in X_{\mathbf{0}}$ , with  $h \in B$  and  $\sigma \in L$ , such that  $j^\sigma = i$ . Thus  $\alpha^y \in W$  with  $(\alpha^y)_i \neq 0$ . This gives a contradiction, proving the claim that  $\delta = m$ .  $\square$

Lemma 16 implies part 1 of Theorem 4 and also that, given the hypotheses of Theorem 4, it can be assumed that  $q = 2$  and  $W$  is the repetition code in  $H(m, 2)$ .

**Lemma 17.** *Let  $C$  be an  $(X, 2)$ -neighbour-transitive extension of  $W$ , where  $W$  is the repetition code in  $H(m, 2)$ , with  $\delta \geq 5$ . Then  $X_{\mathbf{0}} \cong X_{\mathbf{0}}^M = X_W^M$ ,  $K = T_W$  and  $X_W = T_W \rtimes X_{\mathbf{0}}$ .*

*Proof.* Let  $W$  be the repetition code in  $H(m, 2)$ . If  $x = h\sigma \in X_{\mathbf{0}}$ , with  $h \in B$  and  $\sigma \in L$ , then  $q = 2$  implies  $h_i = 1$  for all  $i \in M$ . Thus  $X_{\mathbf{0}} \cong X_{\mathbf{0}}^M$ . By Corollary 15,  $W$  is a block of imprimitivity for the action of  $X$  on  $C$ , from which it follows that  $X_W = T_W \rtimes X_{\mathbf{0}}$ , since  $T_W$  acts transitively on  $W$ . Thus,  $X_{\mathbf{0}} \cong X_{\mathbf{0}}^M = X_W^M$  and  $K = T_W$ .  $\square$

**Lemma 18.** *Suppose  $C$  is a non-trivial  $(X, 2)$ -neighbour transitive extension of the repetition code  $W$  in  $H(m, 2)$ , where  $C$  has minimum distance  $\delta \geq 5$ . Then  $\delta \neq m$ ,  $X^M$  acts 2-transitively on  $M$  and  $X_W^M$  acts 2-homogeneously on  $M$ . Moreover, if  $X_W^M$  acts 2-transitively on  $M$  then  $X_{i,j}^M$  has a normal subgroup of index 2, where  $i, j \in M$  and  $i \neq j$ .*

*Proof.* First, note that  $\omega \in W$  if and only if  $\omega_i = \omega_j$  for all  $i, j \in M$ . Since  $C \neq W$  there exists a codeword  $\alpha \in C \setminus W$  and distinct  $i, j \in M$  such that  $\alpha_i = 0$  and  $\alpha_j = 1$ , since otherwise  $\alpha \in W$ . Note that this implies that  $\delta \neq m$ . Let  $J = \{i, j\} \subseteq M$  and consider the projection code  $P = \pi_J(C)$ . Now,  $\pi_J(W) = \{(0, 0), (1, 1)\} \subseteq P$  and  $\pi_J(\alpha) = (0, 1) \in P$ . Also,  $\beta = \alpha + (1, \dots, 1) \in C$ , since  $T_W \leq X$ , which implies  $\pi_J(\beta) = (1, 0) \in P$ . Thus,  $P$  is the complete code in the Hamming graph  $H(2, 2)$ . By [15, Corollary 2.6],  $X_{\{i,j\}}$  acts transitively on  $C$ , from which it follows that  $X_{\{i,j\}}^P$  acts transitively on  $P$ . Thus  $|P| = 4$  divides  $|X_{\{i,j\}}^P|$  and hence also divides  $|X|$ . By Lemma 17,  $K = T_W$  so that  $|K| = 2$ . Thus 2 divides  $|X/K|$ . Proposition 6 and [12, Exercise 2.1.11] then imply that  $X/K = X^M$  is 2-transitive.

By Corollary 15,  $W$  is  $(X_W, 2)$ -neighbour-transitive. Thus, by Proposition 6,  $X_W^M$  is 2-homogeneous on  $M$ . Suppose  $X_W^M$  is 2-transitive on  $M$ . Since  $X_{W,\{i,j\}}^P$  contains  $K$  and interchanges  $i$  and  $j$ ,  $|X_{W,\{i,j\}}^P|$  is divisible by 4. Now,  $|X_{\{i,j\}}^P| \leq 8$ , since  $\text{Aut}(H(2, 2)) = (S_2 \times S_2) \rtimes S_2$ . Furthermore,  $|X_{\{i,j\}}^P : X_{W,\{i,j\}}^P| = 2$ , since  $X_{\{i,j\}}^P$  acts transitively on  $P$ . Thus  $X_{\{i,j\}}^P = (S_2 \times S_2) \rtimes S_2$ , and so  $|X_{i,j}^P| = 4$ . Let  $H$  be the kernel of the action of  $X_{i,j}$  on  $P$ . Since the only non-identity element of  $K = T_W$  acts non-trivially on  $P$ , we deduce that  $|K^P| = 2$  and  $H \cap K = 1$ . Hence,

$$\frac{X_{i,j}^P}{K^P} \cong \frac{X_{i,j}/H}{HK/H} \cong \frac{X_{i,j}}{HK} \cong \frac{X_{i,j}/K}{HK/K} \cong \frac{X_{i,j}^M}{H^M}.$$

Therefore,  $X_{i,j}^M$  has a quotient of size 2, since  $|X_{i,j}^P/K^P| = 2$ , and thus  $H^M$  is a normal subgroup of  $X_{i,j}^M$  of index 2.  $\square$

The socle of a finite group is the product of all its minimal normal subgroups. If  $C$  is an  $(X, 2)$ -neighbour-transitive extension of the binary repetition code  $W$  in  $H(m, 2)$  then the next two results show that the socles of  $X^M$  and  $X_W^M$  cannot be equal and that the socle of  $X^M$  cannot be  $A_m$ .

**Lemma 19.** *Let  $W$  be the repetition code in  $H(m, 2)$  and  $C$  be a non-trivial  $(X, 2)$ -neighbour-transitive extension of  $W$  with  $\delta \geq 5$ . Then  $\text{soc}(X/K) \neq \text{soc}(X_W/K)$ .*

*Proof.* Let  $H \leq X$  such that  $K < H$  and  $H/K = \text{soc}(X/K)$ . Note that this implies that  $H \trianglelefteq X$ . By Lemma 17,  $X_W = K \rtimes X_0$ . Suppose  $H/K = \text{soc}(X_W/K)$ , and note that by Lemma 18,  $X_W^M = X_W/K$  acts 2-homogeneously on  $M$  and  $X^M \cong X/K$  acts 2-transitively on  $M$  with the same socle.

By considering vertices as characteristic vectors of subsets of  $M$ , we may identify the set of all subsets of  $M$  with the vertex set  $V \cong \mathbb{F}_2^m$  of  $H(m, 2)$ . By Lemma 17,  $K = T_W \cong \mathbb{Z}_2$ . Consider the quotient of  $H(m, 2)$  by the orbits of  $K$ , thereby identifying each subset  $J$  of  $M$  with its complement  $\bar{J}$ . In particular,  $W$  is identified with  $\{\emptyset, M\}$ . This gives induced actions of  $X$ ,  $X_W$  and  $X_0$  on the set:

$$\mathcal{O} = \{ \{J, \bar{J}\} \mid J \in C \}.$$

Note that  $\mathcal{O}$  is a set of partitions of  $M$ , and  $x \in X \setminus X_W$  does not necessarily fix  $\{|J|, |\bar{J}|\}$ . Since the single non-trivial element of  $K$  maps  $J \subseteq M$  to  $\bar{J}$ , for each  $J$ , it follows that  $K$  fixes every element of  $\mathcal{O}$ . Thus,  $K$  is in the kernel  $X_{(\mathcal{O})}$  of the action of  $X$  on  $\mathcal{O}$ . If  $x \in X \setminus X_W$ , then  $\{\emptyset, M\}^x \neq \{\emptyset, M\}$ , so that  $X_{(\mathcal{O})} \leq X_W$ . By Lemma 17,  $X_W = K \rtimes X_0$ . It follows that  $X_{(\mathcal{O})}/K \trianglelefteq X_W/K$ , and, since  $H/K = \text{soc}(X_W/K)$ , either  $X_{(\mathcal{O})}/K = 1$ , or  $H/K \trianglelefteq X_{(\mathcal{O})}/K$ .

Suppose that  $H/K \leq X_{(\mathcal{O})}/K$ . Note that, by assumption,  $C \neq W$ . As  $H/K$  fixes  $\mathcal{O}$  element-wise,  $H/K$  fixes the non-trivial partition  $\{J, \bar{J}\}$ , for each  $J \in C \setminus W$ . Since  $H/K = \text{soc}(X_W/K)$  acts transitively on  $M$ , we have that  $H/K$  acts imprimitively on  $M$  and  $|J| = |\bar{J}|$ , so that 2 divides  $m$  and  $\delta = m/2$ . By [25], a 2-homogeneous but not 2-transitive group has odd degree, and hence the fact that  $2 \mid m$  implies that  $X_0$  acts 2-transitively on  $M$ . By [9, Section 134 and Theorem IX, p. 192], a 2-transitive group with an imprimitive socle has a normal subgroup of prime power order. Thus, by [12, Section 7.7], we deduce that  $X_W^M$  is affine and, since  $2 \mid m$ , we have that  $X_W^M \leq \text{AGL}_d(2)$  and  $M \cong \mathbb{F}_2^d$ . Since  $X_W^M$  and  $X^M$  have the same socle,  $X^M$  is also an affine 2-transitive group. Now, if  $U = \{J, \bar{J}\}$  is fixed by the group of translations of  $\mathbb{F}_2^d$  acting on  $M$ , then either  $J$  or  $\bar{J}$  is a  $(d-1)$ -space of  $M$ . Let  $i = 0 \in M$ . Then  $X_{W,i}$  acts transitively on  $M \setminus \{i\}$ , that is, on the set of 1-spaces of  $M$ . Since each 1-space is orthogonal to a  $(d-1)$ -space, it follows that  $X_{W,i}$  also acts transitively on the set of  $(d-1)$ -spaces of  $M$ . This implies  $|\mathcal{O} \setminus \{\emptyset, M\}| = 2^d - 1$ , the number of  $(d-1)$ -spaces in  $M$ . Thus,  $|C| = 2^d |W|$ . Now  $K \leq X_W \leq X$  implies  $|C|/|W| = |X|/|X_W| = |X^M|/|X_W^M|$ , that is,  $|X^M| = 2^d |X_W^M|$ . This gives a contradiction, as there is no finite transitive linear group acting on  $2^d - 1$  points with an index  $2^d$  subgroup that remains transitive on  $2^d - 1$  points (see [27, Hering's Theorem]). Thus,  $X_{(\mathcal{O})}/K = 1$ .

$G$	$H$	degree
$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	$\text{PSL}_3(2)$	7
$\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$	$\text{PSL}_2(11)$ or $M_{11}$	11
$\mathbb{Z}_{23} \rtimes \mathbb{Z}_{11}$	$M_{23}$	23
$\text{PSL}_2(7)$	$\text{AGL}_3(2)$	8
$A_7$	$A_8$	15
$\text{PSL}_2(11)$	$M_{11}$	11
$\text{PSL}_2(11)$ or $M_{11}$	$M_{12}$	12
$\text{PSL}_2(23)$	$M_{24}$	24

Table 2: Groups  $G < H \leq S_m$  where  $H$  is 2-transitive,  $G$  is 2-homogeneous,  $\text{soc}(H) \neq A_m$  and  $\text{soc}(G) \neq \text{soc}(H)$ ; see [15, Proposition 4.4 and Table 3].

By Lemma 18,  $X^M$  acts 2-transitively on  $M$ . Since  $H/K = \text{soc}(X/K)$ , it follows that  $H/K$  acts transitively on  $M$ . As  $X$  acts transitively on  $\mathcal{O}$ , the stabiliser in  $X/K$  of any element of  $\mathcal{O}$  is conjugate in  $X/K$  to the stabiliser  $X_W/K$  of  $\{\emptyset, M\} \in \mathcal{O}$ . It follows from this that  $H/K$  fixes every element of  $\mathcal{O}$ , since  $H/K \trianglelefteq X/K$  and  $H \leq X_W/K$ . If  $H/K$  fixes each element of  $\mathcal{O}$  then  $H/K \leq X_{(\mathcal{O})}/K$ , giving a contradiction. Thus  $\text{soc}(X/K) \neq \text{soc}(X_W/K)$ .  $\square$

**Lemma 20.** *Let  $C$  be a non-trivial  $(X, 2)$ -neighbour-transitive extension of  $W$  with  $\delta \geq 5$ , where  $W$  is the repetition code in  $H(m, 2)$ . Then  $\text{soc}(X^M) \neq A_m$ .*

*Proof.* Suppose  $\text{soc}(X^M) = A_m$ . By Lemma 18,  $X_W/K \cong X_W^M$  is a 2-homogeneous group and thus primitive, and, by Lemma 19,  $\text{soc}(X_W/K) \neq \text{soc}(X/K)$ . By Lemma 17,  $|C| = |X : X_{\mathbf{0}}| = 2|X : X_W| = 2|X/K : X_W/K|$ . Now, [2] (see also [33, Theorem 14.2]) gives a lower bound on the index of a primitive non-trivial subgroup  $G$  of the symmetric group  $S_m$ , with  $G$  not containing the alternating group, of  $|S_m : G| \geq \lfloor (m+1)/2 \rfloor!$ . Since  $X_W^M$  is primitive and  $X/K \cong A_m$  or  $S_m$ , it follows that

$$|C| = 2|X/K : X_W/K| \geq t|X/K : X_W/K| = |S_m : X_W^M| \geq \lfloor (m+1)/2 \rfloor!,$$

where  $t = 1$  or  $2$ . However, by the Singleton bound we have  $|C| \leq 2^{m-\delta+1} \leq 2^{m-4}$ . Combining these two inequalities, we have  $\lfloor (m+1)/2 \rfloor! \leq 2^{m-4}$ , which does not hold when  $m \geq 5$ .  $\square$

The main theorem can now be proved.

*Proof of Theorem 4.* Suppose  $C$  is an  $(X, 2)$ -neighbour-transitive extension of  $W$  with  $\delta \geq 5$ , where  $W$  is a  $k$ -dimensional  $\mathbb{F}_p$ -subspace of  $V = \mathbb{F}_p^{dm}$  and  $1 \leq k \leq d$ . By Lemma 16,  $W$  is the binary repetition code (not just an equivalent copy of it, since  $\mathbf{0} \in W$ ) and thus  $q = 2$ . If  $C = W$  then  $C$  is a trivial extension of  $W$  and outcome 1 holds. Suppose the extension is non-trivial. Then, by Lemma 18,  $\delta \neq m$ ,  $X^M$  acts 2-transitively on  $M$  and either  $X_W^M$  is 2-transitive and  $X_{i,j}^M$  has an index 2 normal subgroup, or  $X_W^M$  acts 2-homogeneously, but not 2-transitively, on  $M$ . Also, by Lemma 19, the socles of  $X^M$  and

$X_W^M$  are not equal, and, by Lemma 20,  $\text{soc}(X^M) \neq A_m$ . Thus, by [15, Proposition 4.4], the possibilities for  $X^M$  and  $X_W^M$  are as in Table 2.

Now  $T_W \leq X$  implies that if there exists some weight  $k$  codeword in  $C$ , then there is also a weight  $m - k$  codeword. Thus  $\delta \leq m/2$  and  $\delta \geq 5$  implies  $m \geq 10$ . In particular,  $X^M \neq \text{PSL}_3(2)$  or  $\text{AGL}_3(2)$ . Suppose  $X^M \cong \text{PSL}_2(11)$  and  $m = 11$ . Then  $\delta = 5$  and, by Proposition 13,  $C$  is either the punctured Hadamard code  $\mathcal{P}$  or the even weight subcode  $\mathcal{E}$  of the punctured Hadamard code. The even weight subcode of the punctured Hadamard code is not invariant under  $T_W$ , so  $C \neq \mathcal{E}$ . Moreover, as in the proof of [15, Proposition 4.3], the only copy of  $\text{PSL}_2(11)$  in  $\text{Aut}(\mathcal{P})$  fixes  $\mathbf{0}$ , and hence  $X_{\mathbf{0}}^M \cong \text{PSL}_2(11)$ . This implies that  $X_W^M = \text{PSL}_2(11)$ , by Lemma 17, and thus  $X^M = X_W^M$ , a contradiction.

Suppose  $m = 23$ ,  $X^M \cong M_{23}$  and  $X_W^M \cong \mathbb{Z}_{23} \rtimes \mathbb{Z}_{11}$ . By Lemma 17,  $X_W = T_W \rtimes X_{\mathbf{0}}$  and  $K = T_W$ , so that  $|X_{\mathbf{0}}| = |X_W^M|$  which gives  $|C| = |X|/|X_{\mathbf{0}}| = 2|X^M|/|X_W^M|$ , and hence  $|C| = 80640$ . However, this contradicts the bound of  $|C| \leq 24106$  for a code of length 23 with  $\delta \leq 5$  from [1, Table I and Theorem 1].

Suppose  $m = 15$ ,  $X^M \cong A_8$  and  $X_W^M \cong A_7$ . Then  $X_{i,j}^M \cong A_6$  is simple, contradicting Lemma 18.

Suppose  $m = 11$ ,  $X^M \cong M_{11}$  and  $X_W^M \cong \text{PSL}_2(11)$ . Then, by Proposition 13,  $C$  is either the punctured Hadamard code  $\mathcal{P}$  or the even weight subcode of  $\mathcal{P}$ . The even weight subcode of  $\mathcal{P}$  is not invariant under  $T_W$ , so  $C = \mathcal{P}$ . The automorphism group of  $\mathcal{P}$  is  $X = \text{Aut}(\mathcal{P}) \cong 2 \times M_{11}$  with  $X_{\mathbf{0}} \cong \text{PSL}_2(11)$  and  $K = T_W$ . By [18, Theorem 1.1]  $\mathcal{P}$  is an  $(X, 2)$ -neighbour-transitive extension of  $W$ , as in outcome 3.

Suppose  $m = 12$ ,  $X^M \cong M_{12}$  and  $X_W^M \cong M_{11}$  or  $\text{PSL}_2(11)$ . If  $X_W^M \cong \text{PSL}_2(11)$  then, as the index of  $\text{PSL}_2(11)$  in  $M_{12}$  is 144, we have  $|C| = 288$ . However, since  $\delta \geq 5$ , the Singleton bound gives  $|C| \leq 2^{m-\delta+1} \leq 256$ . Thus  $X_W^M \cong M_{11}$  and  $|C| = 24$ . If weight 5 codewords exist then, by Lemma 11 and (2.1), there are

$$b = \frac{v(v-1)\lambda}{k(k-1)} = \frac{12 \cdot 11\lambda}{5 \cdot 4} = \frac{3 \cdot 11\lambda}{5}$$

of them, for some  $\lambda$  divisible by 5. Since  $\lambda \geq 5$  implies  $b \geq 33 > |C| = 24$ , it follows that  $\lambda = 0$ . Thus  $\delta \geq 6$ , and as  $\delta \leq m/2 = 6$ , it follows that  $\delta = 6$ . The Hadamard code  $\mathcal{H}$  of length 12 with  $X = \text{Aut}(\mathcal{H}) \cong 2 \cdot M_{12}$ ,  $X_{\mathbf{0}} \cong M_{12}$  and  $K = T_W$  is then the unique  $(X, 2)$ -neighbour-transitive extension of  $W$  with these parameters, by [18, Theorem 1.1], as in outcome 2.

Finally, suppose  $m = 24$ ,  $X^M \cong M_{24}$  and  $X_W^M \cong \text{PSL}_2(23)$ . Then  $X_{i,j}^M \cong M_{22}$  is simple, contradicting Lemma 18.  $\square$

Finally, the proof of Corollary 5 is given below.

*Proof of Corollary 5.* Suppose  $C$  is  $X$ -completely transitive with minimum distance  $\delta \geq 5$  such that  $K = \text{Diag}_m(S_2)$ , and assume that  $\mathbf{0} \in C$ . The fact that  $\delta \geq 5$  implies that  $C_2$  is non-empty and thus  $C$  is  $(X, 2)$ -neighbour-transitive. Since  $K \trianglelefteq X$  and  $X$  acts transitively on  $C$ , it follows from Lemma 14 that the orbit  $\Delta = \mathbf{0}^K$  of  $\mathbf{0}$  under  $K$  is an  $(X_{\Delta}, 2)$ -neighbour-transitive code. Since  $K = \text{Diag}_m(S_2)$  we have that  $|\Delta| = 2$  and  $\Delta$  has minimum distance  $m$ . Thus, since any 2-neighbour-transitive code is 2-regular, [15,

Lemma 2.15] implies that  $\Delta$  is the binary repetition code in  $H(m, 2)$ . Hence,  $q = 2$ ,  $Q \cong \mathbb{Z}_2$  and  $C$  satisfies the hypotheses of Theorem 4, and so is one of the codes listed there. The binary repetition code has automorphism group  $\text{Diag}_m(S_2) \rtimes \text{Sym}(M)$  and is seen to be completely transitive by identifying the vertices of  $H(m, 2)$  with the subsets of  $M$ . By [18, Theorem 1.1], the Hadamard code of length 12 and its punctured code are completely transitive. This completes the proof.  $\square$

## References

- [1] M. R. Best, A. E. Brouwer, F. J. Macwilliams, A. M. Odlyzko, and N. J. A. Sloane. Bounds for binary codes of length less than 25. *IEEE Trans. Information Theory*, 24(1):81–93, 1978.
- [2] A. Bochert. Ueber die zahl der verschiedenen werthe, die eine function gegebener buchstaben durch vertauschung derselben erlangen kann. *Mathematische Annalen*, 33(4):584–590, 1889.
- [3] J. Borges and J. Rifà. On the nonexistence of completely transitive codes. *IEEE Trans. Information Theory*, 46(1):279–280, 2000.
- [4] J. Borges, J. Rifà, and V. A. Zinoviev. On linear completely regular codes with covering radius  $\rho = 1$ , construction and classification. [arXiv:0906.0550](https://arxiv.org/abs/0906.0550), 2009.
- [5] J. Borges, J. Rifà, and V. A. Zinoviev. New families of completely regular codes and their corresponding distance regular coset graphs. *Designs, Codes and Cryptography*, 70(1–2):139–148, 2014.
- [6] J. Borges, J. Rifà, and V. A. Zinoviev. Families of completely transitive codes and distance transitive graphs. *Discrete Mathematics*, 324:68–71, 2014.
- [7] J. Borges, J. Rifà, and V. A. Zinoviev. On completely regular codes. *Problems of Information Transmission*, 55(1):1–45, 2019.
- [8] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.
- [9] W. Burnside. *Theory of groups of finite order*. Cambridge: Cambridge Univ. Press (reprinted: 1955 New York: Dover Publ.), 2nd edition, 1911.
- [10] P. J. Cameron and J. H. van Lint. *Designs, Graphs, Codes and Their Links*. London Mathematical Society Student Texts. Cambridge University Press, 1991.
- [11] P. Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory*. Philips research reports: Supplements. N. V. Philips’ Gloeilampenfabrieken, 1973.
- [12] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163. New York: Springer, 1996.
- [13] N. Gill, N. I. Gillespie, and J. Semeraro. Conway groupoids and completely transitive codes. *Combinatorica*, 38(2):1–44, 2018.
- [14] N. I. Gillespie. *Neighbour transitivity on codes in Hamming graphs*. PhD thesis, The University of Western Australia, Perth, Australia, 2011.

- [15] N. I. Gillespie, M. Giudici, D. R. Hawtin, and C. E. Praeger. Entry-faithful 2-neighbour transitive codes. *Designs, Codes and Cryptography*, 79(3):549–564, 2016.
- [16] N. I. Gillespie and D. R. Hawtin. Alphabet-almost-simple 2-neighbour-transitive codes. *Ars Mathematica Contemporanea*, 14(2):345–357, 2017.
- [17] N. I. Gillespie and C. E. Praeger. Neighbour transitivity on codes in Hamming graphs. *Designs, Codes and Cryptography*, 67(3):385–393, 2013.
- [18] N. I. Gillespie and C. E. Praeger. Uniqueness of certain completely regular Hadamard codes. *Journal of Combinatorial Theory, Series A*, 120(7):1394 – 1400, 2013.
- [19] N. I. Gillespie and C. E. Praeger. Diagonally neighbour transitive codes and frequency permutation arrays. *Journal of Algebraic Combinatorics*, 39(3):733–747, 2014.
- [20] N. I. Gillespie and C. E. Praeger. Characterisation of a family of neighbour transitive codes. [arXiv:1405.5427](https://arxiv.org/abs/1405.5427), 2014.
- [21] N. I. Gillespie and C. E. Praeger. New characterisations of the Nordstrom-Robinson codes. *Bulletin of the London Mathematical Society*, 49(2):320–330, 2017.
- [22] M. Giudici. Completely transitive codes in Hamming graphs. M. Sc. Thesis, The University of Western Australia, Perth, Australia, 1998.
- [23] M. Giudici and C. E. Praeger. Completely transitive codes in Hamming graphs. *European Journal of Combinatorics*, 20(7):647–662, 1999.
- [24] D. R. Hawtin. *Algebraic symmetry of codes in hamming graphs*. PhD thesis, The University of Western Australia, 2017.
- [25] W. M. Kantor. Automorphism groups of designs. *Mathematische Zeitschrift*, 109(3):246–252, 1969.
- [26] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. Urbanke. Reed-Muller codes achieve capacity on erasure channels. *IEEE Transactions on information theory*, 63(7):4298–4316, 2017.
- [27] M. W. Liebeck. The affine permutation groups of rank three. *Proceedings of the London Mathematical Society*, 3(3):477–516, 1987.
- [28] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland Mathematical Library. North-Holland, 1978.
- [29] P. Solé. Completely regular codes and completely transitive codes. *Discrete Mathematics*, 81(2):193–201, 1990.
- [30] D. R. Stinson. *Combinatorial Designs: Construction and Analysis*. Springer, 2004.
- [31] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM Journal on Applied Mathematics*, 24(1):88–96, 1973.
- [32] J. A. Todd. A combinatorial problem. *J. Math. Phys.*, 12(1–4):321–333, 1933.
- [33] H. Wielandt, H. Booker, D. A. Bromley, and N. DeClaris. *Finite Permutation Groups*. Academic paperbacks. Elsevier Science, 2014.
- [34] V. A. Zinoviev and V. K. Leontiev. The nonexistence of perfect codes over Galois fields. *Problems of Control and Information*, 2(2):123–132, 1973.