Algebraic Symmetry of Codes in Hamming Graphs

Daniel R. Hawtin

This thesis is presented for the degree of
Doctor of Philosophy
of The University of Western Australia
Department of Mathematics & Statistics.
December, 2017

Thesis Declaration

I, Daniel Hawtin, certify that:

This thesis has been substantially accomplished during enrolment in the degree.

This thesis does not contain material which has been accepted for the award of any other degree or diploma in my name, in any university or other tertiary institution.

No part of this work will, in the future, be used in a submission in my name, for any other degree or diploma in any university or other tertiary institution without the prior approval of The University of Western Australia and where applicable, any partner institution responsible for the joint-award of this degree.

This thesis does not contain any material previously published or written by another person, except where due reference has been made in the text.

The work(s) are not in any way a violation or infringement of any copyright, trademark, patent, or other rights whatsoever of any person.

This research was supported at various times by: a grant associated with Australian Research Council Federation Fellowship FF0776186, an Australian Postgraduate Award (APA) and University of Western Australia Safety-Net-Top-Up Scholarship, and an Australian Government Research Training Program (RTP) Scholarship.

This thesis contains published work and/or work prepared for publication, some of which has been co-authored.

Signature and date:

31/8/2017

Authorship declaration: co-authored publications

This thesis contains work that has been published and prepared for publication.

Details of the work:
The manuscript [42] was submitted for publication and is available online.
Location in thesis:
Chapter 3.
Student contribution to work:
70% of the results and 90% of the preparation of the manuscript.
Coordinating supervisor signature and date:

31/8/2017

Details of the work:
The manuscript [55] has been prepared for publication.
Location in thesis:
Chapter 4.
Student contribution to work:
100% of the results and 100% of the preparation of the manuscript.
Coordinating supervisor signature and date:

31/8/2017

Details of the work:
The manuscript [40] has been published.
Location in thesis:
Chapter 5.
Student contribution to work:
70% of the results and 90% of the preparation of the manuscript.
Coordinating supervisor signature and date:

31/8/2017

Details of the work:
The manuscript [41] has been accepted for publication.
Location in thesis:
Chapter 6.
Student contribution to work:
50% of the results and 80% of the preparation of the manuscript.
Coordinating supervisor signature and date:

31/8/2017

Student signature and date:

31/8/2017

I, Cheryl Praeger, certify that the student statements
regarding their contribution to each of the works listed above are correct.
Coordinating supervisor signature and date:

3

Abstract

This thesis studies algebraic symmetry properties of error-correcting codes. A *code* is a subset C of the vertex set of a Hamming graph $H(m, q)$ (the vertices of which are functions from a set of entries M, of size m, to an alphabet Q, of size q). The elements of C are *codewords* and the *distance partition* with respect to C, of the vertex set of $H(m, q)$, is the partition $\{C = C_0, C_1, \ldots, C_\rho\}$, with each C_i being the set of vertices with nearest codeword at distance i, and where the largest i such that C_i is non-empty is the *covering radius* ρ.

A code C is said to be s*-neighbour-transitive* if its automorphism group $\mathrm{Aut}(C)$ (defined to be the stabiliser of C inside $\mathrm{S}_q^m \rtimes \mathrm{S}_m$) acts transitively on each of the sets $C_0, C_1, \ldots, C_s$. The main results are directed towards the possibility of an eventual classification of 2-neighbour-transitive codes in Hamming graphs with minimum distance at least 5.

It is shown that a 2-neighbour-transitive code C in $H(m, q)$ having a faithful action of $\mathrm{Aut}(C)$ on the set of entries, and minimum distance $\delta \geqslant 5$, is either the binary repetition code of length m or the even weight subcode of the punctured Hadamard code of length 12.

Let C be a 2-neighbour-transitive code with minimum distance $\delta \geqslant 3$ such that the kernel of the action of $\mathrm{Aut}(C)$ on M is non-trivial. It is known that the subgroup $\mathrm{Aut}(C)_i \leqslant \mathrm{Aut}(C)$ that fixes the entry $i \in M$ has either an affine or an almost-simple action on the alphabet Q in the entry i. It is proved that when the action of $\mathrm{Aut}(C)_i$ on Q is almost-simple, C is a repetition code in $H(3, q)$ with $q \geqslant 5$ and $\delta = 3$. Thus, for $\delta \geqslant 4$ the action of $\mathrm{Aut}(C)_i$ on Q is always affine. For $\delta \geqslant 5$, it is shown that the action on the alphabet is always soluble, with a list of possible actions given. For $q = 2$, a characterisation of binary 2-neighbour-transitive codes in $H(m, 2)$ is then provided, via a list of minimal subcodes. In the case $q \geqslant 3$, new infinite families of 2-neighbour-transitive codes are exhibited, involving the groups $\mathrm{AGL}_t(r)$, $\mathrm{Sz}(r)$, and $\mathrm{PSU}_3(r)$.

A code C is s*-elusive* if there exists an automorphism x of $H(m, q)$ which fixes C_s setwise, but $x \notin \mathrm{Aut}(C)$. Infinite families of examples of s-elusive codes with $s = 1$ and 2, plus a single example for $s = 3$, are exhibited. It is shown that an s-elusive code with $\delta \geqslant 2s + 1$ comes with an associated collection of q-ary s-$(m, 2s, 1)$-designs.

Finally, the possibility of extending the main results to 1-neighbour-transitive codes with an associated rank-3 action on $Q \times M$ is discussed. It is shown that many crucial results from the 2-neighbour-transitive case also hold in this setting.

Contents

Acknowledgements

First and foremost I would like to thank my supervisors, Cheryl Praeger, Michael Giudici and Neil Gillespie, for their guidance and support during my PhD; Cheryl for the opportunity to undertake this project in the first place, her vast wealth of knowledge and her rigour; Michael for his eye for detail and friendly, relaxed approach; and Neil for passing on his expertise in design and coding theory and for the many discussions we had in the early stages of my PhD.

I would also like to thank the members of the Centre for the Mathematics of Symmetry and Computation at the University of Western Australia, past and present, for their friendship, as well as the mathematics we have shared. In particular, Mark Ioppolo, Luke Morgan, Melissa Lee, John Bamberg, Irene Pivotto, Gabriel Verret, Tomasz Popiel and Eric Schwartz. More broadly, I thank everyone at the School of Mathematics and Statistics at the University of Western Australia, in particular, Thomas Stemler, for all of his support, and Konstantinos Sakellariou, for the many discussions we have had, mathematical and otherwise. Outside of the University of Western Australia I would like to mention Padraig Ó Catháin, Stacey Mendan and John Tsartsaflis for their friendship, as well as Peter and Sylvia Neumann for their hospitality while I was in Oxford.

Outside of mathematics, I thank Rory Petersen, Marcus Fort and Matthew Bowker, without whom I would not be the person I am today. I am also grateful to those I have made music with, which has helped to keep me sane during my PhD: Trevor Gerard, Haydn Mansell, Cain Munns, Justin Martins and Chris Chen. Further friends I would be remiss not to mention are: Kate Bowker, Lynn Chan, Imogen Bell and Leoni Mole. Undoubtedly, I thank my amazing partner Margrethe Mjelde Maalsnes for the unbelievable amount of love and understanding she has. Last, and indeed most of all, I thank my parents Neil and Kerrie Hawtin for their unending love and support over the years.

x

Introduction

Error-correcting codes have been an important tool in communications, and other transmissions of information, ever since Shannon's landmark paper [90]. Applications have included: the internet [85], data storage [59, 62], random access memory in computers [80], and deep-space telecommunications [1]. These days, coding theory has connections to many areas of mathematics, for instance: finite geometry [3], graph theory [23], group theory [21], representation theory [91], lattices [29], matroids [96], association schemes [34], and algebraic geometry [52].

This thesis studies symmetry properties of error-correcting codes using perspectives given by the theory of permutation groups. This study is motivated primarily by the historical investigation of combinatorial symmetry in error-correcting codes, but also the idea that it may culminate in new insights into the study of permutation groups and related combinatorial structures.

The first major result concerning the symmetry of codes occurred in 1973, when the parameters of all perfect codes over finite fields were classified (see [97] or [104]). In that same year, Delsarte [32] began the study of s-regular codes[1] in association schemes, whilst Biggs [10] began the study of perfect codes in distance-transitive graphs. This work takes inspiration from these two ideas; the main class of codes considered in these pages is that of s-neighbour-transitive codes[2], the algebraic analogue of s-regular codes, discussed in language traditionally used to study graph symmetries.

1.1 Symmetry in coding theory

This section takes a deeper look into the history surrounding the study of symmetry of codes in Hamming graphs, starting with the combinatorial point of view. Only those concepts required for this discussion are introduced here, for more complete definitions see Chapter 2.

The vertex set $V\Gamma$ of the Hamming graph $\Gamma = H(m, q)$ is the set of all functions from a set M, called the set of *entries*, into a set Q, called the *alphabet*, where M and Q have size m and q, respectively. Two functions are adjacent if they differ on precisely one element of M. A *code* is regarded as a subset C of the vertex set of a Hamming graph $H(m, q)$. Unless otherwise stated, it is assumed that C has size at least 2. The graph structure gives rise to the Hamming metric $d(\alpha, \beta)$, where $\alpha, \beta \in V\Gamma$. Given a code C, the Hamming metric in turn allows the following definitions to be made:

1. The *minimum distance* δ of C is the minimum value of $d(\alpha, \beta)$ taken over all distinct $\alpha, \beta \in C$.

2. The distance $d(\nu, C)$ from a vertex $\nu \in V\Gamma$ to the code C is the minimum value of $d(\nu, \alpha)$ over all $\alpha \in C$.

[1] See Definition 1.1.1.
[2] See Definition 1.1.2.

3. The *covering radius* ρ is the maximum value of $d(\nu, C)$, taken over all $\nu \in V\Gamma$.

4. The *distance partition* is the set $\{C = C_0, C_1, C_2, \ldots, C_\rho\}$, where C_i is given by the set of vertices $\nu \in V\Gamma$ such that $d(\nu, C) = i$. An element of C_s is called an s-*neighbour*.

The full automorphism group of the Hamming graph is the semi-direct product $\mathrm{Aut}(\Gamma) = B \rtimes L$, where $B \cong \mathrm{Sym}(Q)^m$ and $L \cong \mathrm{Sym}(M)$ (see [19, Theorem 9.2.1]). The automorphism group of a code C is the setwise stabiliser of C inside $\mathrm{Aut}(\Gamma)$, that is, $\mathrm{Aut}(C) = \mathrm{Aut}(\Gamma)_C$.

A *perfect* code C is one for which the covering radius ρ is equal to the error-correction capability e (defined as $e = \lfloor (\delta - 1)/2 \rfloor$). This is a highly restrictive condition, and indeed linear perfect codes, or (equivalently) the parameters of perfect codes over prime power alphabets, have been classified (see [97] or [104]).

Perfect codes may equivalently be defined as codes that attain a certain sphere packing bound. In particular, for a perfect code C, the set of all balls of radius e centered around the codewords of C partition the vertex set of the Hamming graph. The class of *nearly-perfect* codes generalise that of perfect codes, defined via a slightly more relaxed sphere packing bound (see [51]). The next notable classification result was the classification of linear nearly-perfect codes over finite fields [78]. *Uniformly packed* codes, defined in a more combinatorial manner [89], were introduced around the same time as nearly-perfect codes, and in fact generalise nearly-perfect codes. Certain classes of uniformly packed codes have been classified [99, 22]. Other classification results include codes with certain automorphism groups, such as the general linear group [31] (acting as "pure permutations" on M, see Section 2.3).

Though the notion of symmetry is implicit in all of the classes discussed above, the idea of combinatorial symmetry is the focal point of the definition of s-regular and completely regular codes (see [32]), presented below. Note that, for $\alpha \in V\Gamma$, the set of vertices at distance k from α is denoted $\Gamma_k(\alpha) = \{\beta \in V\Gamma \mid d(\alpha, \beta) = k\}$.

Definition 1.1.1. Let C be a code in $H(m, q)$ with covering radius ρ, and s be an integer with $0 \leqslant s \leqslant \rho$. Then,

1. C is s-*regular* if, for each $i \in \{0, 1, \ldots, s\}$, each $k \in \{0, 1, \ldots, m\}$, 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 ρ-regular.

Perfect codes, nearly-perfect codes and uniformly packed codes are all completely regular [32, 93]. Completely regular codes have been studied extensively since Delsarte introduced them. Not only are completely regular codes of interest to coding theorists, but, due to a result of Brouwer et al. [19, p.353], they are also the building blocks of certain types of distance regular graphs, and Neumaier [83] also studied completely regular codes using the theory of distance regular graphs.

A classification of completely regular codes is far from complete. Indeed, new families of completely regular codes continue to be found, [18, 38] for instance, while subfamilies continue

to be classified. For example, in [16] all linear completely regular codes that have *covering radius* $\rho = 2$ and an *antipodal* dual code are classified, as are linear completely regular codes with covering radius $\rho = 1$, with the first class shown to be the extended codes of the second. All of these codes are in fact completely transitive, as in the following definition.

Definition 1.1.2. Let C be a code in $H(m, q)$ with covering radius ρ, let $s \in \{1, \ldots, \rho\}$, and $X \leqslant \mathrm{Aut}(C)$. Then C is said to be

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

Completely transitive codes form a subfamily of completely regular codes, and (X, s)-neighbour transitive codes are a sub-family of s-regular codes, for each s. In particular, by results of Delsarte [32], this means that the set of minimum weight codewords of an (X, s)-neighbour transitive code forms a q-ary s-design[3], a fact of much use in later results.

The main family studied here is that of 2-neighbour-transitive codes. It is hoped that studying this class of 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. Also, codes with 2-transitive actions on the entries of the Hamming graph (which many 2-neighbour-transitive codes indeed have, see Proposition 2.5.3), have been of interest lately, where this fact has been used to prove that certain families of codes achieve capacity on erasure channels [71].

The two most extreme cases in the above definition, neighbour-transitive and completely transitive, have been studied previously. Neighbour-transitive codes are studied in [43, 46, 45], while completely-transitive codes are studied in [49]. In fact, completely transitive codes date back to 1987, when Solé [92] introduced what we refer to here as *coset-completely transitive codes*, a definition that only applies to linear codes in a Hamming graph[4]. Solé's definition was first published in 1990 [93].

In [14], Borges et al. classified binary coset-completely transitive codes with minimum distance at least 9, showing that the binary repetition code[5] is the unique code in this family. Other work has been done by Borges et al. in [13, 15, 17, 18].

[3] See Definition 2.6.2 and Lemma 2.6.4.

[4] Note that by simply replacing $H(m, q)$ by an arbitrary graph, in Definition 1.1.2, the definition generalises to any graph.

[5] See Definition 2.1.1.

There exist completely transitive codes that are not coset-completely transitive. For example, certain Hadamard codes [44] and the Nordstrom-Robinson code [47] are completely transitive, but as they are non-linear, they are not coset-completely transitive. Also, the repetition code of length 3 over a finite field $\mathbb{F}_q$ for $q \geqslant 9$ is an example of a linear completely transitive code that is not coset-completely transitive [49, Example 3.1].

Another concept related to algebraic symmetry of codes in Hamming graphs was encountered when Gillespie and Praeger were deciding upon the definition for a neighbour-transitive code (see [39]). The concept of an elusive code, first studied in [43], arose from the question of whether, given a code C, the automorphism group of the neighbour set C_1 must fix the code C setwise. This question is related to the next definition, in the case $s = 1$.

Definition 1.1.3. Let C be a code in $H(m, q)$, let $X = \mathrm{Aut}(C)$ and let $X_s = \mathrm{Aut}(C_s)$ be the setwise stabiliser of C_s in $\mathrm{Aut}(\Gamma)$. Then C is *s-elusive* if X_s is strictly larger than X. If C is 1-elusive then C is simply called *elusive*.

For a code C to be s-elusive, there must be some automorphism $x \in X_s \setminus X$. It follows that C^x and C are not equal, but are equivalent[6] codes, each with the same s-neighbour set C_s. As such, given only information about the s-neighbour set, full knowledge of the code remains elusive. Whether such codes exist seems to be related to the *minimum distance* δ of the code, namely the smallest distance between two distinct codewords. In [43] an infinite family of binary (that is, $q = 2$) elusive codes was constructed with minimum distance $\delta = 4$. It was also shown there that if C is an elusive code with minimum distance δ, then $\delta \leqslant 4$, and if $\delta = 4$ then $q = 2$. In [56] a family of elusive codes with $\delta = 3$ was exhibited, containing infinitely many examples for each $q \geqslant 3$. All known examples of elusive codes are such that the length m of the code is divisible by the alphabet size q. This led to the question [56, Question 1.3] being posed, asking if q must always divide m. This indeed holds true in the binary case, since $m(q-1) = m$ must be even, by [43, Theorem 1], regardless of δ.

1.2 Main results

Chapters 3 and 4 focus on s-elusive codes. Chapter 3 concerns the case $s = 1$, and Theorem 3.3 exhibits an infinite family of linear codes, each of which is both elusive and completely transitive. This family of examples provides answers to some questions asked in [56], as in Theorem 3.4. Theorem 3.2 also provides a partial answer to [56, Question 1.3]. However, through an argument provided by Andries Brouwer in private correspondence, Section 4.1 answers the question in full, showing that if C is an s-elusive code in $H(m, q)$ then q divides m.

In the next chapter, Lemma 4.2.6 generalises [43, Theorem 1], showing that if an s-elusive code with $\delta \geqslant 2s + 1$ exists in $H(m, q)$, then a combinatorial object known as a q-ary s-$(m, 2s, 1)$ design must exist. In particular, this means that certain divisibility requirements

[6] See Section 2.3.

must be satisfied. The existence of certain designs, in particular, binary 2-$(2^{2d}, 4, 1)$ designs (for $d \geqslant 2$) and a 3-$(22, 6, 1)$ design, leads here to the discovery that the Preparata codes are 2-elusive, proved in Lemma 4.2.7, and that the punctured code of the even weight subcode of the perfect Golay code of length 23 is 3-elusive, proved in Proposition 4.2.9.

Chapters 5 to 9 examine 2-neighbour-transitive codes, with an emphasis on classifying certain families of them. The analysis of 2-neighbour-transitive codes is attacked as three separate problems. The subdivision is based on the following argument. Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 3$. For each $i \in M$, let Q_i denote the copy of the alphabet Q in the entry i, and let

$$X_i^{Q_i} = X_i \Big/ X_{(Q_i)},$$

where X_i is the subgroup of X stabilising the entry i, and $X_{(Q_i)}$ is the subgroup of X_i fixing every element of Q_i (that is, the kernel of the action of X_i on Q_i). Proposition 2.5.3 shows that X acts transitively on M, so that $X_i^{Q_i}$ and $X_j^{Q_j}$ are isomorphic for all $i, j \in M$. Proposition 2.5.5, shows that $X_i^{Q_i}$ acts 2-transitively on Q_i. Since every 2-transitive group is either affine or almost-simple[7], by [20, Section 154], every $(X, 2)$-neighbour-transitive code satisfies precisely one of the definitions given below. Note that K is the kernel of the action of X on entries and $K = X \cap B$, where $B \cong \mathrm{S}_q^m$ is the subgroup of $\mathrm{Aut}(\Gamma)$ fixing M pointwise.

Definition 1.2.1. Let C be a code in $H(m, q)$, $X \leqslant \mathrm{Aut}(C)$ and K be the kernel of the action of X on M. 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.

Theorem 5.2 provides a classification of all $(X, 2)$-neighbour-transitive codes in $H(m, q)$ that are X-entry-faithful and have minimum distance $\delta \geqslant 5$. Such a code is proved to be equivalent to either the binary repetition code in $H(m, 2)$, where $\delta = m$, or the even-weight subcode of the punctured Hadamard code of length 12[8] in $H(11, 2)$, where $\delta = 6$. Conversely, these two codes are shown to indeed be 2-neighbour-transitive.

Chapter 6 concerns codes in $H(m, q)$ with minimum distance $\delta \geqslant 3$ that are $(X, 2)$-neighbour-transitive and X-alphabet-almost-simple. The results of that chapter rely on [45], which characterises X-alphabet-almost-simple and X-neighbour-transitive codes with $\delta \geqslant 3$. Theorem 6.1 states that the only $(X, 2)$-neighbour-transitive and X-alphabet-almost-simple

[7] See Section 2.4 for the definitions of affine and almost-simple.

[8] See Definition 5.2.1.

code in $H(m,q)$ having minimum distance $\delta \geqslant 3$, is the repetition code in $H(3,q)$, where $q \geqslant 5$ and $\delta = 3$.

The results of Chapter 6 are of interest from the point of view of the non-existence of perfect codes over an alphabet of non-prime-power size, since such a code cannot be X-alphabet-affine. The existence of perfect codes over non-prime-power alphabets, with covering radius 1 or 2, is still an open question [60]. By Theorem 6.1, if such codes exist, then they cannot be 2-neighbour-transitive, unless they have length 3. Note that in the prime power case, for every set of parameters such that a perfect code with covering radius $\rho \geqslant 2$ exists[9], there exists a code with those parameters that is both perfect and (at least) 2-neighbour transitive. That is to say, the repetition codes and Golay codes are 2-neighbour-transitive. In fact, the repetition, Hamming and Golay codes are completely transitive (by [49, Example 3.1] for the repetition codes, [93, Proposition 7.3] for the Hamming and binary Golay codes, and [48, Example 3.5.6] for the ternary Golay codes).

For a 2-neighbour-transitive code C with $\delta \geqslant 5$, this leaves the case that C is X-alphabet-affine, which is the subject of Chapters 7, 8 and 9. If C is X-alphabet-affine, then the vertex set $V\Gamma$ of the Hamming graph $H(m,q)$ is a vector space $\mathbb{Z}_p^{dm}$, where $q = p^d$. For the remainder of this section, it is assumed that C is an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$, with minimum distance $\delta \geqslant 5$, containing the zero vertex[10] $\mathbf{0}$, and $X_{\mathbf{0}}$ denotes the subgroup of X fixing $\mathbf{0}$.

First, Theorem 7.2 classifies C (with C as above) such that C contains a block U of imprimitivity[11] for the action of X on C and U is a subspace of $V\Gamma$ having $\mathbb{Z}_p$-dimension at most d. Such a code is shown to be one of either the binary repetition code in $H(m,2)$, so that $\delta = m$, the Hadamard code of length 12 in $H(12,2)$, in which case $\delta = 6$, or the punctured code of the Hadamard code of length 12 in $H(11,2)$, whence $\delta = 5$. Each of these codes are shown to be 2-neighbour-transitive and to contain a 1-dimensional $\mathbb{Z}_2$-vector space as a block of imprimitivity for the action of X on C.

Chapter 8 then examines more closely the structure of X and certain blocks of imprimitivity of C under the action of X. Theorem 8.1 contains the two main results of Chapter 8, relating to each of these two concepts. The first shows that C has a block of imprimitivity for the action of X on C that is an $FX_{\mathbf{0}}$-submodule[12] of the vertex set of $H(m,q)$[13], for some finite field F. The second states that the group $X_i^{Q_i}$ cannot be an arbitrary 2-transitive affine group but is in fact soluble. It follows from this that $X_{\mathbf{0},i}^{Q_i^\times}$ (the stabiliser in $X_i^{Q_i}$ of $\mathbf{0} \in C$) is either a transitive subgroup of $\Gamma\mathrm{L}_1(q)$ or $X_{\mathbf{0},i}^{Q_i^\times}$ and q are as in one of a (relatively small) finite number of cases[14].

Chapter 9 then focuses on the case that $X_{\mathbf{0},i}^{Q_i^\times} \cong \mathrm{AGL}_1(q)$ and $K_{\mathbf{0}} = \mathbb{F}_q^\times$, that is, codes

[9] The minimum covering radius required for 2-neighbour-transitivity is 2.

[10] This can be assumed by Lemma 2.5.1.

[11] See Section 2.4.

[12] See Section 2.8 for the definition of an FG-module.

[13] Where the vertex set $V\Gamma$ is itself regarded as an $FX_{\mathbf{0}}$-module.

[14] See Table 8.1.1.

satisfying the following definition, with $s = 2$.

Definition 1.2.2. Let C be a code in the Hamming graph $H(m, q)$ with vertex set an $\mathbb{F}_q$-vector space of dimension m. Then C is defined to be *linear-(X, s)-neighbour-transitive* if C is (X, s)-neighbour-transitive, $T_C \leqslant X$, and $X_{\mathbf{0},i}^{Q_i^\times} \cong K_{\mathbf{0}} = \mathrm{Diag}_m(\mathbb{F}_q^\times)$ for all $i \in M$.

Chapter 9 begins by constructing examples of linear-$(X, 2)$-neighbour-transitive codes as sets of polynomials. The use of polynomials allows codes to be defined via subsets of bounded degree. In Propositions 9.1.8 and 9.2.3, the Reed-Muller and projective Reed Muller codes[15] are shown to be 2-neighbour-transitive. Indeed they are often defined as sets of polynomials, and have been studied fairly thoroughly in the literature (see [8, 52, 69, 72, 73, 94, 102] for instance). Definitions 9.3.1, 9.4.1, 9.4.2, and 9.4.3 introduce codes related, respectively, to the following 2-transitive groups: the affine general linear groups, the Suzuki groups, the Ree groups, and the unitary groups. These codes are referred to here as the twisted Reed-Muller codes, the Suzuki codes, the Ree codes and the unitary codes. As far as the author is aware, these codes do not appear in the literature. In the case of the twisted Reed-Muller codes, the Suzuki codes, and the unitary codes, Propositions 9.3.3, 9.4.6 and 9.4.8, respectively, show that these families contain instances of 2-neighbour-transitive codes.

The other major result of Chapter 9 is Theorem 9.1, which gives a characterisation of $(X, 2)$-neighbour-transitive codes in $H(m, 2)$ with minimum distance δ satisfying $\delta \geqslant 5$. By Theorem 8.1, every such code satisfying $K \neq 1$ contains an $\mathbb{F}_2 X_{\mathbf{0}}$-module as a block of imprimitivity. Thus, the characterisation is achieved by finding all of the minimal submodules, in the sense that they contain no proper $X_{\mathbf{0}}$-submodules, except for possibly that corresponding to the binary repetition code. Table 9.7.1, gives certain parameters of these minimal blocks. While δ is not explicitly found in every case, bounds are given for those cases where δ is not known, some of which do not seem to have appeared elsewhere.

The remainder of Chapter 9 gives an outline of what is known in regards to linear-$(X, 2)$-neighbour-transitive codes in $H(m, q)$ with $q \geqslant 3$ and minimum distance $\delta \geqslant 5$, for each of the possible 2-homogeneous[16] actions of $X_{\mathbf{0}}$ on M. In particular, Proposition 9.8.1 narrows down the possibilities for q. Examples are given in many of the permissible cases, with the majority of infinite families included.

Chapter 10 contains some concluding remarks, giving a summary of results, open questions and new directions to take this research. In particular, different symmetry conditions codes in Hamming graphs are briefly discussed, as well as studies of codes in other contexts.

[15] See Definitions 9.1.6 and 9.2.1, respectively.

[16] See Proposition 2.5.3.

Preliminaries

This chapter is a summary of the language, preliminary/existing results, and mathematics used throughout this thesis.

2.1 Codes in Hamming graphs

Let M and Q be sets of size m and q referred to as the *set of entries* and the *alphabet*, respectively. Note that both m and q are assumed to be finite integers, and at least 2, throughout. The vertex set $V\Gamma$ of a 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 the product

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

An edge exists between two vertices 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 often be assumed to contain 0, which may be thought of as simply some distinguished element. For more in depth background material on coding theory see [25] or [79].

A code C is a non-empty subset of $V\Gamma$. A Roman uppercase C will usually be used to denote an arbitrary code, while an uppercase calligraphic font will generally be used for specific codes, for instance, $\mathcal{NR}$ denotes the Nordstrom-Robinson code. Generally, the lower case Greek letters $\alpha, \beta, \gamma, \mu, \nu$ refer to vertices in a Hamming graph, the lower case Roman i, j, k, ℓ refer to entries and a, b, c to elements of the alphabet.

If α is a vertex of $H(m, q)$ and $i \in M$ then α_i refers to the value of α in the i-th entry, so that $\alpha = (\alpha_1, \ldots, \alpha_m)$ when $M = \{1, \ldots, m\}$.

Let α, β 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 2.1.1.

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

There are several notions of a trivial code in $H(m, q)$, for instance, the complete code $C = V\Gamma$, a singleton vertex $C = \{\alpha\} \subseteq V\Gamma$, or the empty code. It is assumed throughout that $|C| \geqslant 2$, and almost always that $\delta \geqslant 3$; thus such codes are all but excluded from this discussion. The most interesting codes that one might consider trivial are the repetition codes, defined below, and those codes equivalent to one. Note that a repetition code is not generally excluded by the aforementioned conditions.

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
$\mathrm{diff}(\alpha, \beta) = \{i \in M \mid \alpha_i \neq \beta_i\}$	set of entries in which α and β differ
$\mathrm{supp}(\alpha) = \{i \in M \mid \alpha_i \neq 0\}$	support of α
$\mathrm{wt}(\alpha) = \lvert\mathrm{supp}(\alpha)\rvert$	weight of α
$d(\alpha, \beta) = \lvert\mathrm{diff}(\alpha, \beta)\rvert$	Hamming distance
$\Gamma_s(\alpha) = \{\beta \in V\Gamma \mid d(\alpha, \beta) = s\}$	set of s-neighbours of α
$\delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$	minimum distance of C
$d(\alpha, C) = \min\{d(\alpha, \beta) \mid \beta \in C\}$	distance from α 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
$\{C = C_0, C_1, \ldots, C_\rho\}$	distance partition of C

Table 2.1.1: Hamming graph notation.

Definition 2.1.1. The *repetition code* in $H(m, q)$, denoted by $\mathrm{Rep}(m, q)$, is equal to the set of vertices of the form $(a, \ldots, a)$, for all $a \in Q$. The code $\mathrm{Rep}(m, q)$ has minimum distance $\delta = m$.

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 $H(m, q)$ from 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 of a linear code is defined below.

Definition 2.1.2. Let C be a linear code in $H(m, q)$ with vertex set V. Then 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 [32, 4.3.2]) is a well known bound for the size of a code C in $H(m, q)$ with minimum distance δ, stating that $|C| \leqslant q^{m-\delta+1}$. For a linear code C this may be stated as $\delta^\perp - 1 \leqslant k \leqslant m - \delta + 1$, where k is the dimension of C, δ is the minimum distance of C and $\delta^\perp$ is the minimum distance of $C^\perp$.

2.2 Group actions

This section is a very short introduction to group actions, also known as permutation groups, containing only the core concepts most relevant to this work. For more background regarding groups acting on sets see, for instance, [24] or [36]. All groups and sets considered here are finite.

A group G acts on a set Ω if there exists a function χ from $\Omega \times G$ to Ω which both respects the group operation, and for which the identity of G induces the identity map 1_Ω on Ω. The

Notation	Explanation
G_ω	subgroup of G consisting of all elements that fix $\omega \in \Omega$
G_S	subgroup of G fixing S setwise
$G_{(S)}$	subgroup of G individually fixing each element of S
G^Ω	quotient of G by the kernel of the action of G on Ω - acts faithfully on Ω
$\mathbb{Z}_n$	cyclic group of order n
$\mathbb{F}_q$	finite field of prime power order q
$\mathbb{F}_q^\times$	multiplicative group of the finite field of order q
$\mathbb{F}_q^+$	additive group of the finite field of order q
$\Omega^{\{t\}}$	set of t-subsets of Ω
$\Omega^{(t)}$	set of t-tuples of distinct elements of Ω
$\mathrm{soc}(G)$	the socle of G - the product of all minimal normal subgroups of G
$\mathrm{Sym}(\Omega) = \mathrm{S}_n$	symmetric group on a set Ω of size n

Table 2.2.1: Group action and related notation.

kernel of the action of G on Ω is the collection of all elements of G which induce 1_Ω on Ω and the action is *faithful* if its kernel is trivial. In fact, the kernel of an action of G on Ω forms a normal subgroup H of G and the group G/H acts faithfully on Ω. The function χ is omitted almost entirely from this work, instead the exponentiation notation $\omega^g = \chi(\omega, g)$ is used.

If a group G acts on a set Ω, $\omega \in \Omega$ and $S \subseteq \Omega$ then Table 2.2.1 lists some frequently used notation for groups and sets. Note that each stabiliser subgroup is in fact the collection of all elements in G that stabilise the relevant structure. Also, $\mathbb{Z}_n$ is used to denote the cyclic group of order n in order to avoid confusion with C_s, the vertices of a Hamming graph at distance s from a code C. The reader should be aware that the precise meaning of $\mathbb{Z}_n$, $\mathbb{F}_q$, $\mathbb{F}_q^+$ and $\mathbb{F}_q^\times$ may sometimes need to be inferred from the context in which they are used.

2.3 Automorphisms of a Hamming graph

The automorphism group $\mathrm{Aut}(\Gamma)$ of the Hamming graph is the semi-direct product $B \rtimes L$, where $B \cong \mathrm{Sym}(Q)^m$ and $L \cong \mathrm{Sym}(M)$ (see [19, Theorem 9.2.1]). Note that B and L are called the *base group* and the *top group*, respectively, of $\mathrm{Aut}(\Gamma)$. Since we identify Q_i with Q, we also identify $\mathrm{Sym}(Q_i)$ with $\mathrm{Sym}(Q)$. If $h \in B$ and $i \in M$ then $h_i \in \mathrm{Sym}(Q_i)$ 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 σ act on α

explicitly via:

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

A subgroup $X \leqslant \mathrm{Aut}(\Gamma)$ gives rise to actions on M and Q. First, consider the quotient group X^M acting faithfully on the set M of entries, defined by the homomorphism:

$$\begin{array}{rccc} \mu: & X & \longrightarrow & \mathrm{Sym}(M) \\ & h\sigma & \longmapsto & \sigma \end{array}$$

Let K denote the kernel of this map and observe that $K = X \cap B$.

Next, consider the action of the stabiliser $X_i \leqslant X$ of the entry $i \in M$, on the alphabet Q_i. Then $X_i^{Q_i}$ is the quotient of X_i by the kernel of the homomorphism:

$$\begin{array}{rccc} \varphi_i: & X_i & \longrightarrow & \mathrm{Sym}(Q_i) \\ & h\sigma & \longmapsto & h_i \end{array}$$

Furthermore, consider the action of X on the disjoint union $\cup_{i\in M} Q_i$ defined by $a_i^x = ({a_i}^{h_i})_j$, where $a_i \in Q_i$, $i^\sigma = j$, and $x = h\sigma \in X$ with $h \in B$ and $\sigma \in L$. Note that the subscript here is used to denote that a_i is the copy of $a \in Q$ in Q_i. This action is faithful and imprimitive, with at least one system of imprimitivity $\{Q_i \mid i \in M\}$.

The automorphism group of a code C in $\Gamma = H(m, q)$ is $\mathrm{Aut}(C) = \mathrm{Aut}(\Gamma)_C$, the set-wise stabiliser of C in $\mathrm{Aut}(\Gamma)$. Note that any subset of $V\Gamma$ is a code, and hence has an automorphism group defined in this way. For instance the automorphism group of the set of s-neighbours of C is $\mathrm{Aut}(C_s) = \mathrm{Aut}(\Gamma)_{C_s}$.

Given a group $H \leqslant \mathrm{Sym}(Q)$ an important subgroup of $\mathrm{Aut}(\Gamma)$ is the *diagonal* group of H, denoted $\mathrm{Diag}_m(H)$, where an element of H acts the same in each entry. Formally, $\mathrm{Diag}_m(H) = \{g \in B \mid g_i = h, \forall h \in H\}$.

It is worth mentioning that coding theorists often consider more restricted groups of automorphisms, such as the group $\mathrm{PermAut}(C) = \{\sigma \mid h\sigma \in \mathrm{Aut}(C), h = 1 \in \mathrm{S}_q^m, \sigma \in \mathrm{S}_m\}$. 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 $x \in \mathrm{Aut}(\Gamma)$ 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 $\mathrm{Aut}(\Gamma)$ preserves distances in $H(m, q)$.

2.4 Primitive and multiply transitive group actions

This section introduces various standard classes of group actions, as well as some useful results regarding these classes.

The action of a group G on a set Ω is *transitive* if for all $\omega_1, \omega_2 \in \Omega$ there exists some $g \in G$ such that $\omega_1^g = \omega_2$. By considering the set of orbits of G on Ω, any group action can be broken down into a set of transitive actions. The Orbit-Stabiliser Theorem states that if G is transitive on a finite set Ω and $\omega \in \Omega$ then $|G| = |\Omega||G_\omega|$.

Let G be a group acting transitively on a set Ω. A G-invariant partition of Ω is a partition $\mathcal{B} = \{B_1, \ldots, B_k\}$ of Ω of size k such that for each $g \in G$ and $i \in \{1, \ldots, k\}$ there exists a $j \in \{1, \ldots, k\}$ such that $B_i^g = B_j$. The elements of $\mathcal{B}$ are called *blocks* and $\mathcal{B}$ is *trivial* if either $\mathcal{B}$ or a block in $\mathcal{B}$ has size 1. A non-trivial G-invariant partition of Ω is a *system of imprimitivity* for the action of G on Ω. The action of G on Ω is said to be *imprimitive* if it has a system of imprimitivity and *primitive* if no such system of imprimitivity exists. Primitive actions are the building blocks of all transitive group actions, in the sense that for any imprimitive action of G on Ω there exists a system of imprimitivity $\mathcal{B}$ such that G_B^B is primitive for all $B \in \mathcal{B}$. In particular, if N is a normal subgroup of G then the set of N-orbits forms a system of imprimitivity for the action of G on Ω, so that if G is primitive then N must either be transitive or the trivial group.

The action of a group G on a set Ω is *t-homogeneous* or *t-transitive* if the induced action of G on $\Omega^{\{t\}}$ or $\Omega^{(t)}$ (see Table 2.2.1), respectively, is transitive. The next result shows that a t-homogeneous or t-transitive group action is primitive provided $t \geqslant 2$.

Lemma 2.4.1. *Let G be a group acting 2-homogeneously on a set Ω. Then G acts primitively on Ω.*

Proof. Suppose that $\mathcal{B}$ is a system of imprimitivity for the action of G on Ω. Since $\mathcal{B}$ is a non-trivial G-invariant partition of Ω, there exist distinct blocks B and B' of $\mathcal{B}$ such that $B \cap B' = \emptyset$ and $\alpha, \beta, \gamma \in \Omega$ such that $\alpha, \beta \in B$ and $\gamma \in B'$. Since G is 2-homogeneous on Ω, there exists some $g \in G$ such that $\{\alpha, \beta\}^g = \{\beta, \gamma\}$. It follows that $B^g \neq B$, since $\gamma \in B^g$. However, $B^g \cap B$ is non-empty, since it contains β. This gives rise to a contradiction. □

Lemma 2.4.2. *Let G be a 2-homogeneous group acting faithfully on a set Ω such that the order of G is even. Then G is 2-transitive on Ω.*

Proof. Since G has even order there exists some $g \in G$ such that g has even order, say $2k$. Thus g^k has order 2. Let $\alpha \in \Omega$ such that $\alpha^g \neq \alpha$. Then $\alpha^{g^2} = \beta^g = \alpha$ for some $\beta \in \Omega$. Since G is 2-homogeneous, for any distinct $\mu, \nu \in \Omega$ there exists some $h \in G$ such that $\{\mu, \nu\}^h = \{\alpha, \beta\}$. Hence, either $(\mu, \nu)^h = (\alpha, \beta)$ or $(\mu, \nu)^{hg} = (\alpha, \beta)$. Thus G is 2-transitive on Ω. □

Theorems 2.4.3, 2.4.4, 2.4.5 and 2.4.6 give the classification of all 2-homogeneous groups. Proofs or statements of each can be found in [74, Lemma 4.7], [75], [24, Table 7.4], and [67], respectively. Descriptions of the groups may be found in the given references or in most standard texts, such as [103]. Note that a group action is *affine* if $\mathrm{soc}(G) \cong \mathbb{Z}_p^t$ (see Table 2.2.1 for the definition of $\mathrm{soc}(G)$) and G is a subgroup of the affine general linear group $\mathrm{AGL}_t(p)$ acting on $\Omega = \mathbb{Z}_p^t$. An action of a group G on Ω is *almost-simple* if the socle is a non-abelian simple group S. Identifying S with its inner automorphism group $\mathrm{Inn}(S)$ we have $S \leqslant G \leqslant \mathrm{Aut}(S)$.

Theorem 2.4.3. *Let $q = p^t$ be a prime power and $G_0 \leqslant \Gamma\mathrm{L}_1(q)$ and transitively on $\Omega = \mathbb{F}_q^\times$. Then G_0 can be expressed uniquely as $G_0 = \langle \omega^d, \omega^e \xi^s \rangle \leqslant \Gamma\mathrm{L}_1(q)$, where ω is a fixed multiplicative generator of $\mathbb{F}_q^\times$, ξ is the Frobenius automorphism of $\mathbb{F}_q$ and either:*

1. *$d = 1$, $e = 0$ and s divides t, or,*
2. *d divides $p^t - 1$, s divides t and $0 < e < d$ such that d divides $e(p^{ds} - 1)/(p^s - 1)$ but does not divide $e(p^{d's} - 1)/(p^s - 1)$ for any d' with $1 < d' < d$.*

Theorem 2.4.4. *Let $G_0 \leqslant \mathrm{GL}_t(p)$ act transitively on the set ${\mathbb{Z}_p^t}^\times$ of non-zero vectors. Then either:*

1. *G_0 is a transitive subgroup of $\Gamma\mathrm{L}_1(p^t)$, as in Theorem 2.4.3,*
2. *k divides t and $\mathrm{SL}_{t/k}(p^k) \trianglelefteq G_0$,*
3. *k divides t, t/k is even and $\mathrm{Sp}_{t/k}(p^k) \trianglelefteq G_0$,*
4. *$t = 6k$ and $\mathrm{G}_2(2^k)' \trianglelefteq G_0$,*
5. *$p = 5, 7, 11, 23$, $t = 2$ and $\mathrm{SL}_2(3) \trianglelefteq G_0$,*
6. *$p = 11, 19, 29, 59$, $t = 2$ and $\mathrm{SL}_2(5) \trianglelefteq G_0$,*
7. *$p = 2, t = 4$, $n = 6$ or 7, and $\mathrm{A}_n \trianglelefteq G_0$,*
8. *$p = 3, t = 4$ and $\mathrm{SL}_2(5) \trianglelefteq G_0$,*
9. *$p = 3, t = 4$ and $2_-^{1+4} \trianglelefteq G_0$, or,*
10. *$p = 3, t = 6$ and $\mathrm{SL}_2(13) \trianglelefteq G_0$.*

Theorem 2.4.5. *Let G be a group acting 2-transitively on a set Ω of size n. Then G is either affine and $G \cong T \rtimes G_0 \leqslant \mathrm{AGL}_t(p)$ where $T \cong \mathbb{Z}_p^d$, $n = p^d$ and G_0 is a transitive linear group, or G is almost-simple and $\mathrm{soc}(G)$, n are one of the following:*

1. *A_n,*
2. *$\mathrm{Sp}_{2t}(2)$ and $n = 2^{2t-1} \pm 2^{t-1}$,*
3. *$\mathrm{PSL}_t(r)$ and $n = \frac{r^t - 1}{r - 1}$,*
4. *$\mathrm{Sz}(r)$ and $n = r^2 + 1$,*
5. *$\mathrm{PSL}_2(8)$ and $n = 28$,*
6. *$\mathrm{Ree}(r)$ and $n = r^3 + 1$,*
7. *$\mathrm{PSU}_3(r)$ and $n = r^3 + 1$,*

8. $\mathrm{PSL}_2(11)$ *and* $n = 11$,

9. A_7 *and* $n = 15$,

10. M_n *and* $n = 11, 12, 22, 23, 24$,

11. M_{11} *and* $n = 12$,

12. HS *and* $n = 176$, *or,*

13. Co_3 *and* $n = 276$.

Theorem 2.4.6. *The action a group G on a set Ω is 2-homogeneous if and only if one of the following holds:*

1. *G acts 2-transitively on Ω, or,*

2. *G acts 2-homogeneously, but not 2-transitively, on $\Omega = \mathbb{F}_q^+$, where $q = p^t \equiv 3 \pmod 4$ is a prime power, $G \cong \mathbb{F}_q^+ \rtimes \langle \omega^2, \xi^s \rangle$ is a subgroup of the affine general semi-linear group $\mathrm{A\Gamma L}_1(q)$, s divides t, ω is the multiplicative generator of $\mathbb{F}_q^\times$ and ξ is the Frobenius automorphism of $\mathbb{F}_q$.*

2.5 s-Neighbour-transitive codes

This section contains some of the most fundamental results which make the possible the work in later chapters. First, it is shown that working with equivalent codes makes it possible to assume the existence of certain explicit codewords.

Lemma 2.5.1. *Let C be a code in $H(m, q)$ with minimum distance δ, $|C| \geqslant 2$. Then there exists an equivalent code C' in $H(m, q)$ such that $\mathbf{0}$ and $\alpha = (a^\delta, 0^{m-\delta})$ lie in C', and for any $\beta \in C'$ such that $\mathrm{supp}(\beta) = \mathrm{supp}(\alpha)$ there exists some $b \in Q$ such that $\beta = (b^\delta, 0^{m-\delta})$.*

Proof. Since C has minimum distance δ, there exists a subset J of M of size δ and a subset S of C, of size at least 2, such that $\mathrm{diff}(\mu, \nu) = J$ for all distinct $\mu, \nu \in S$. Assume S is maximal, in the sense that there does not exist a $\gamma \in C \setminus S$ and $\nu \in S$ such that $\mathrm{diff}(\gamma, \nu) = J$. Choose some distinguished element $\mu \in S$. Now, $\mathrm{Aut}(\Gamma) \cong \mathrm{S}_q^m \rtimes \mathrm{S}_m$ acts m-transitively on M and q-transitively on Q in each entry (see Section 2.4 for the definition of t-transitivity). Thus, there exists $x = h\sigma \in \mathrm{Aut}(\Gamma)$, with $h \in B$ and $\sigma \in L$, such that $J^\sigma = \{1, \ldots, \delta\}$, $\mu_i^{h_i} = 0$ for all $i \in M$, and for each distinct $\nu \in S \setminus \{\mu\}$ there exists a distinct $a \in Q^\times$ (dependent on ν) such that $\nu_i^{h_i} = a$ for all $i \in J$. Hence, $S^x \subseteq \{(a^\delta, 0^{\delta-m}) \mid a \in Q\}$, $S^x \subseteq C'$, and $C' = C^x$ is equivalent to C. □

Lemma 2.5.2. *Let $\mathbf{0}$, α and β be vertices in $H(m, q)$ and let $x = h\sigma \in \mathrm{Aut}(\Gamma)_{\mathbf{0}}$, where $h \in B$ and $\sigma \in L$, such that $\alpha^x = \beta$. Then $\mathrm{supp}(\alpha)^\sigma = \mathrm{supp}(\beta)$.*

Proof. Now $\alpha_i^{h_i} \neq 0$ for all $i \in \mathrm{supp}(\alpha)$, since h_i fixes 0 for all $i \in M$. Hence, $\mathrm{supp}(\alpha)^\sigma \subseteq \mathrm{supp}(\beta)$. Also, $|\mathrm{supp}(\alpha)| = |\mathrm{supp}(\beta)|$, since $x \in X_{\mathbf{0}}$ preserves distance in $H(m,q)$ and thus $d(\alpha, \mathbf{0}) = d(\beta, \mathbf{0})$. □

A code C is (X,s)-neighbour-transitive if $X \leqslant \mathrm{Aut}(C)$ is transitive on each of the sets $C = C_0, C_1, \ldots, C_s$, as in Definition 1.1.2. Proposition 2.5.3 is used regularly throughout this work. The proof, primarily due to Giudici [48, Theorem 5.2.7] in relation to completely transitive codes, appears as [40, Proposition 2.5] and is included here for completeness.

Proposition 2.5.3. *Let C be an (X,s)-neighbour transitive code in $H(m,q)$, with minimum distance δ. Then for $\alpha \in C$ and $i \leqslant \min\{s, \lfloor \frac{\delta-1}{2} \rfloor\}$, the stabiliser X_α fixes setwise and acts transitively on $\Gamma_i(\alpha)$. In particular, X_α acts i-homogeneously on M.*

Proof. Assume $\alpha = \mathbf{0}$ by applying Lemma 2.5.1. First, $X_{\mathbf{0}} \leqslant X_{\Gamma_i(\mathbf{0})}$ since automorphisms of a Hamming graph preserve distances between vertices. Let $\nu_1, \nu_2 \in \Gamma_i(\mathbf{0})$. As C_i is an X-orbit, and because $\Gamma_i(\mathbf{0}) \subseteq C_i$, there exists $x \in X$ such that $\nu_1^x = \nu_2$. Suppose $x \notin X_{\mathbf{0}}$. Then $\mathbf{0} \neq \mathbf{0}^x \in C$, and so $d(\mathbf{0}, \mathbf{0}^x) \geqslant \delta$. However, the triangle inequality gives $d(\mathbf{0}, \mathbf{0}^x) \leqslant 2i < \delta$, which is a contradiction. Thus $x \in X_{\mathbf{0}}$, and hence $X_{\mathbf{0}}$ acts transitively on $\Gamma_i(\mathbf{0})$.

Let J_1, J_2 be i-subsets of M, and ν, γ be vertices in $H(m,q)$ such that $\mathrm{supp}(\nu) = J_1$ and $\mathrm{supp}(\gamma) = J_2$. It follows that $\nu, \gamma \in \Gamma_i(\mathbf{0}) \subseteq C_i$. As $X_{\mathbf{0}}$ acts transitively on $\Gamma_i(\mathbf{0})$, there exists $x = g\sigma \in X_{\mathbf{0}}$, with $g \in B$ and $\sigma \in L$, such that $\nu^x = \gamma$. By Lemma 2.5.2, $J_1^\sigma = \mathrm{supp}(\nu)^\sigma = \mathrm{supp}(\gamma) = J_2$. Hence $X_{\mathbf{0}}$ acts i-homogeneously on M. □

Corollary 2.5.4. *Let C be an (X,s)-neighbour transitive code in $H(m,q)$, with minimum distance δ. Then for each $i \leqslant \min\{s, \lfloor \frac{\delta-1}{2} \rfloor\}$ and $I \in M^{\{i\}}$, the setwise stabiliser X_I acts transitively on C.*

Proof. By definition C is (X,i)-neighbour transitive and, by Proposition 2.5.3, X_α acts transitively on the set $M^{\{i\}}$ of i-subsets of M. Hence X is transitive on $C \times M^{\{i\}}$, and so X_I is transitive on C. □

Another useful result is stated below. Originally due to Gillespie [39, Proposition 4.55], the proof here is a slight simplification of that given for [40, Proposition 2.7].

Proposition 2.5.5. *Let C be an $(X,1)$-neighbour transitive code in $H(m,q)$, with $\delta \geqslant 3$ and $|C| > 1$. Then $X_i^{Q_i}$ acts 2-transitively on Q_i for all $i \in M$.*

Proof. Following Lemma 2.5.1, assume that $\alpha = \mathbf{0}$ and $\beta = (a^\delta, 0^{m-\delta}) \in C$. Since $\delta \geqslant 3$, Proposition 2.5.3 implies that $X_{\mathbf{0}}$ acts transitively on $\Gamma_1(\mathbf{0})$. Let $b \in Q_1^\times$. Since $(a, 0^{m-1})$ and $(b, 0^{m-1})$ are in $\Gamma_1(\mathbf{0})$ there exists some $x \in X_{\mathbf{0}}$ such that $(a, 0^{m-1})^x = (b, 0^{m-1})$. By Lemma 2.5.2, $x \in X_{\mathbf{0},1}$. Since $b \in Q_1^\times$ was arbitrary, $X_{\mathbf{0},1}$ acts transitively on $Q_1^\times$. By Corollary 2.5.4, X_1 acts transitively on C. Thus, there exists some $y \in X_1$ such that $\beta^y = \mathbf{0}$. Hence, there exists $h \in B$ and $\sigma \in L$ such that $y = h\sigma$ and $a^{h_1} = 0$. It follows that X_1

acts 2-transitively on Q_1. By Proposition 2.5.3, X^M acts transitively on M, so that the result follows. □

Propositions 2.5.3 and 2.5.5 allow the classification of 2-homogeneous groups to be applied with the hope of classifying $(X, 2)$-neighbour-transitive codes with minimum distance at least 5. The next result gives divisibility conditions for the orders of the groups X and $X_{\mathbf{0}}$ when C is an $(X, 2)$-neighbour transitive code containing $\mathbf{0}$.

Lemma 2.5.6. *If C is an $(X, 2)$-neighbour transitive code in $H(m, q)$ with $\delta \geqslant 5$ and $\mathbf{0} \in C$, then $\binom{m}{2}(q-1)^2$ divides $|X_{\mathbf{0}}|$, and hence $|X|$. In particular, if $|X_{\mathbf{0}}| = m(m-1)/2$ then $q = 2$.*

Proof. Since $\delta \geqslant 5$ it follows that $X_{\mathbf{0}}$ is transitive on $\Gamma_2(\mathbf{0})$ by Proposition 2.5.3. Thus $|\Gamma_2(\mathbf{0})| = \binom{m}{2}(q-1)^2$ divides $|X_{\mathbf{0}}|$. □

2.6 Regular codes and designs

Recall the definitions of s-regular codes and of the repetition code from Definition 1.1.1 and Definition 2.1.1, respectively. The proof of the following result is due to Gillespie, appearing as [40, Lemma 2.15].

Lemma 2.6.1. *Let C be a code in $H(m, q)$ with $|C| \geqslant 2$ and $\delta = m$. Then there exists C' equivalent to C with $C' \subseteq \mathrm{Rep}(m, q)$. Moreover, if C is 1-regular then $C' = \mathrm{Rep}(m, q)$; if C is 2-regular and $m \geqslant 4$ then $C' = \mathrm{Rep}(m, 2)$.*

Proof. Let $0, a \in Q$. Since $\delta = m$, Lemma 2.5.1 implies that there is a code C' equivalent to C which contains $\alpha = \mathbf{0}$ and $\beta = (a^m)$, and each $\gamma \in C' \backslash \{\alpha, \beta\}$ at distance $\delta = m$ from α is of the form (b^m) for some $b \in Q \backslash \{0, a\}$. Thus, C' is a subset of the repetition code $\mathrm{Rep}(m, q)$, and in particular $|C| = |C'| \leqslant q$.

Assume C, and hence C', is 1-regular. Suppose $|C'| < q$. Then there exists $b \in Q \backslash \{0, a\}$ such that b does not appear in any codeword of C'. Let $\nu_1 = (a, 0^{m-1})$ and $\nu_2 = (b, 0^{m-1})$. Then $\nu_1, \nu_2 \in C'_1$. However, $|\Gamma_{m-1}(\nu_1) \cap C'| = 2$ if $m = 2$, and 1 if $m \geqslant 3$, while $|\Gamma_{m-1}(\nu_2) \cap C'| = 1$ if $m = 2$ and 0 if $m \geqslant 3$, which is a contradiction. Therefore $|C'| = q$ and $C' = \mathrm{Rep}(m, q)$.

Now assume that C, and hence C', is 2-regular, and that $m \geqslant 4$. Let $\nu_3 = (a^2, 0^{m-2})$. As ν_3 has weight 2 and $\delta = m \geqslant 4$, we have $\nu_3 \in C'_2$. Let $\gamma = (c^m)$ be an arbitrary element of C'. Then,

$$d(\nu_3, \gamma) = \begin{cases} 2 & \text{if} \quad c = 0 \\ m-2 & \text{if} \quad c = a \\ m & \text{if} \quad c \in Q \backslash \{0, a\} \end{cases}.$$

Since $m \geqslant 4$ it follows that $\Gamma_{m-1}(\nu_3) \cap C = \emptyset$. Therefore, because C' is 2-regular, $\Gamma_{m-1}(\nu) \cap C' = \emptyset$ for all $\nu \in C'_2$. Now suppose that $q \geqslant 3$ and consider $\nu_4 = (b, a, 0^{m-2}) \in C'_2$, where $b \neq 0, a$. Then $d(\nu_4, \beta) = m - 1$, which gives a contradiction. Therefore $q = 2$, and the result follows, since $\mathrm{Rep}(m, 2)$ is 2-regular. □

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 ν of $H(m,q)$ is said to be *covered* by α if $\nu_i = \alpha_i$ for every $i \in M$ such that $\nu_i \neq 0$. A binary design, obtained by setting $q = 2$ in the below definition, is usually defined as a collection of subsets of some ground set, satisfying equivalent conditions. In particular, the concept of covering a vertex just described, corresponds to containment of a subset.

Definition 2.6.2. A q-*ary* s-(v,k,λ) *design* is a subset $\mathcal{D}$ of vertices of $\Gamma_k(\mathbf{0})$ (where $k \geqslant s$) such that each vertex $\nu \in \Gamma_s(\mathbf{0})$ is covered by exactly λ vertices of $\mathcal{D}$. When $q = 2$, $\mathcal{D}$ is simply the set of characteristic vectors of an s-design. The elements of $\mathcal{D}$ are called *blocks*.

The following equations can be found, for instance, in [95]. Let $\mathcal{D}$ be a binary s-(v,k,λ) design with $|\mathcal{D}| = b$ blocks and let r be the number of blocks incident with a point. Then $vr = bk$, $r(k-1) = \lambda(v-1)$ and

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

The following is [99, Theorem 2.4.7]. Note that if C contains no codewords of a given weight then the theorem below gives the empty design, that is, where $\lambda = 0$.

Theorem 2.6.3. *Let C be an s-regular code in $H(m,q)$ such that $\mathbf{0} \in C$ and $\delta \geqslant 2s$. Then for each k such that $0 \leqslant k \leqslant m$, the set of codewords from C of weight k forms a q-ary s-(m,k,λ) design, for some λ.*

The following shows that an (X,s)-neighbour-transitive code is s-regular, allowing the above result to be applied. The fact that the codewords of weight k in a (X,s)-neighbour-transitive code C with $\delta \geqslant 2s+1$ and $\mathbf{0} \in C$ form a q-ary s-(m,k,λ) design can also be deduced directly from Proposition 2.5.3.

Lemma 2.6.4. *Let C be an (X,s)-neighbour transitive code. Then C is s-regular. Moreover, if $\mathbf{0} \in C$ and $\delta \geqslant 2s$ then the set of codewords of weight $k \leqslant m$ forms a q-ary s-(m,k,λ) design, for some λ.*

Proof. Let i be such that $0 \leqslant i \leqslant s$ and $\nu, \mu \in C_i$. Then there exists an $x \in X$ such that $\nu^x = \mu$. It follows that $|\Gamma_k(\nu) \cap C| = |\Gamma_k(\mu) \cap C|$ for all k with $0 \leqslant k \leqslant m$ and C is s-regular. If $\mathbf{0} \in C$ then applying Theorem 2.6.3 completes the proof. □

2.7 Projections

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

Let X_J be the setwise stabiliser of a subset $J = \{j_1, \ldots, j_k\} \subseteq M$. For $x = h\sigma \in X_J$, with $h \in B$ and $\sigma \in L$, define the *projection of* x with respect to J, denoted $\chi_J(x)$, so that

$$\pi_J(\alpha)^{\chi_J(x)} = \pi_J(\alpha^x).$$

To be well defined, this requires $x \in X_J$. It follows that

$$\chi_J(x) = (h_{j_1}, \ldots, h_{j_k})\hat{\sigma} \in \mathrm{Aut}(H(k,q)),$$

where $\hat{\sigma}$ is the element of $\mathrm{Sym}(J)$ induced by σ. Finally, define $\chi_J(X) = \{\chi_J(x) \mid x \in X_J\}$.

2.8 Representation theory

A *linear representation* or *projective representation* of a group G is a homomorphism ϕ from G into $\mathrm{GL}(V)$ or $\mathrm{PGL}(V)$, respectively, for some vector space V. If F is the field underlying V, then the vector space V is called an FG*-module* and any subspace $U \leqslant V$ such that $U^G = U$, where the action of G is induced by ϕ, is called an FG*-submodule* of V, and is itself an FG-module. Either of F or G may be omitted if the context is clear. An FG-module V is called *irreducible* if it contains no non-trivial submodule, that is, if $U \leqslant V$ such that $U^G = U$ then $U = V$ or $U = 0$. (In fact these definitions are usually given in a slightly more general form, but suffice for the purposes of later chapters. For further background see [65], for instance.)

Suppose that C is a linear code (see Section 2.1), so that $V\Gamma \cong \mathbb{F}_q^m$, and C is (X, s)-neighbour-transitive with $X = T_C \rtimes X_{\mathbf{0}}$. Then $X_{\mathbf{0}}$ and $X_{\mathbf{0}}^M$ are naturally embedded in $\mathrm{GL}(V\Gamma)$ and $\mathrm{PGL}(V\Gamma)$, respectively. Thus, $V\Gamma$ is both an $\mathbb{F}_q X_{\mathbf{0}}$-module and an $\mathbb{F}_q X_{\mathbf{0}}^M$-module, and C is a submodule of $V\Gamma$.

Table 2.8.1 gives lower bounds for the minimal (non-trivial) dimension of an irreducible projective representation in cross-characteristic for certain simple groups. This information will be useful later in the treatment of linear-2-neighbour-transitive codes in Chapter 9. Theorem 2.8.1 is a portion of [100, Theorem 1.3] and is also applied in Chapter 9.

Theorem 2.8.1. *Let $n = 2^{w_1} + \cdots + 2^{w_s}$ with $w_1 < w_2 < \cdots < w_s$. Also, let F be a field of characteristic not 2. Then the dimension of any proper projective representation of A_n or S_n over F is divisible by $2^{\lfloor (n-s-1)/2 \rfloor}$ or $2^{\lfloor (n-s)/2 \rfloor}$, respectively.*

G	min. deg.	exceptions
$\mathrm{PSL}_2(r)$	$(r-1)/\gcd(2,r-1)$	$2,3$ for $r=4,9$ resp.
$\mathrm{PSL}_t(r)$, $t \geqslant 3$	$(r^t-1)/(r-1)-2$	$2,4$ if $t=3$ and $r=2,4$ resp.
		$7,26$ if $t=4$ and $r=2,3$ resp.
$\mathrm{PSp}_{2t}(r)$, $t \geqslant 2$, r odd	$(r^t-1)/2$	-
r even	$(r^t-1)(r^t-r)/2(r+1)$	2 for $t=2, r=2$
$\mathrm{PSU}_3(r)$	$r(r-1)$	-
$\mathrm{G}_2(r)$	$r(r^2-1)$	$14,12$ for $r=3,4$ resp.
$\mathrm{Sz}(r)$	$\sqrt{r/2}(r-1)$	8 for $r=8$
$\mathrm{Ree}(r)$	$r(r-1)$	-

Table 2.8.1: Lower bounds for the minimal dimension of an irreducible cross-characteristic projective representation, of dimension at least 1, for selected simple groups. Excerpt from [88].

Structure of Elusive Codes

As in Definition 1.1.3 a code C is *elusive* if $\mathrm{Aut}(C_1)$ is strictly larger than $\mathrm{Aut}(C)$. That is, if there exists an automorphism of the neighbour set of C that is not an automorphism of C. This chapter gives some examples of elusive codes and investigates some properties related to them. Recall that the notation $X = \mathrm{Aut}(C)$ and $X_1 = \mathrm{Aut}(C)_1$ is used when considering elusive codes.

Definition 3.1. Let C be an elusive code in $H(m, q)$ with minimum distance δ, and let $x \in X_1 \setminus X$ and $\alpha \in C$ such that $\alpha^x \notin C$. Then (C, α, x) is an *elusive triple* with parameters (m, q, δ).

Let C be an elusive code in $H(m, q)$ with minimum distance $\delta \geqslant 3$, and (C, α, x) be an elusive triple. Throughout this chapter let $X = \mathrm{Aut}(C)$ and $X_1 = \mathrm{Aut}(C_1)$. Since C^x is an equivalent code to C and $C_1^x = C_1$, each $\nu \in C_1$ is adjacent to some vertex π of C^x. That is, if $\nu \in \Gamma_1(\alpha) (\subseteq C_1$ since $\delta \geqslant 3)$, then there exists some vertex $\pi \in \Gamma_1(\nu) \cap C^x$. Now, x fixes C_1 and $\pi = \beta^x$ for some $\beta \in C$, so $\pi \notin \Gamma_1(\alpha)$. By definition, π is distance at most 2 from α and it follows that $\pi \in \Gamma_2(\alpha)$. We call such a vertex $\pi \in \Gamma_2(\alpha) \cap C^x$ a (C, α, x)-*associate*, or simply an *associate* if the elusive triple is clear from the context. The *set of* (C, α, x)-*associates* is $\Gamma_2(\alpha) \cap C^x$, and is the set of vertices in the code C^x which share at least one neighbour with α.

(Note that [43, 56] use the notation $\mathrm{Pre}(\alpha, x)$ to refer to the set of *pre-codewords*, which consist of all $\pi \in \Gamma_2(\alpha) \cap C^{x^{-1}}$. The notation introduced here aims to be a little more intuitive and succinct. In general, replacing x by x^{-1} allows most results to be carried over.)

Let π and π' be distinct (C, α, x)-associates. Then $\alpha \in C \cap \Gamma_2(\pi) \cap \Gamma_2(\pi')$ and we call α a *mutual codeword* of π and π'. Let $\mathrm{MC}(\pi, \pi')$ denote the number $|C \cap \Gamma_2(\pi) \cap \Gamma_2(\pi')|$ of mutual codewords of π and π'. Corollary 3.2.6 shows that $1 \leqslant \mathrm{MC}(\pi, \pi') \leqslant 3$. Moreover, since $\alpha \in \Gamma_2(\pi) \cap \Gamma_2(\pi')$ the vertices π, π' are at distance at most 4, and if they are at distance 4 it is proved that $\mathrm{MC}(\pi, \pi') \leqslant 2$ (Lemma 3.2.3). If $\delta = 4$ then $d(\pi, \pi') = 4$, since π and π' are elements of the equivalent code C^x, which has the same minimum distance as C, by Lemma 2.5.1. Hence $\mathrm{MC}(\pi, \pi')$ can be 3 only if $\delta = 3$. Every elusive triple (C, α, x) with $\delta = 3$ presented in Section 3.3, has the property that *for all distinct associates* $\pi, \pi' \in \Gamma_2(\alpha) \cap C^x$ *at distance* 3*, the parameter* $\mathrm{MC}(\pi, \pi') = 3$ (see Proposition 3.3.9). The main result of this chapter shows that if this condition on mutual codewords holds for just *one* elusive triple, then the parameter m must be a multiple of q.

Theorem 3.2. *Let* (C, α, x) *be an elusive triple, with parameters* $(m, q, 3)$*. Suppose that all* (C, α, x)*-associates* π, π'*, such that* $d(\pi, \pi') = 3$*, satisfy* $\mathrm{MC}(\pi, \pi') = 3$*. Then* $q \mid m$*.*

Lemma 3.1.4 shows that when $q \geqslant 3$ there must exist associates π, π' such that $d(\pi, \pi') = 3$, so that the hypotheses in Theorem 3.2 are not vacuously satisfied. If $q = 2$ then there are no associates π, π' at distance 3 from each other, however q still divides m by [43, Theorem 1].

An infinite family of examples is presented in Section 3.5 such that no elusive triple satisfies the hypotheses of Theorem 3.2 (see Theorem 3.3 below). However for each of the examples it holds that $q \mid m$. A specific example is also given for which $\mathrm{MC}(\pi, \pi') = 1$, for some associates π, π', thus achieving the lower bound of Corollary 3.2.6.

Theorem 3.3 exhibits an infinite family of elusive and completely-transitive codes (see Section 3.5 and see Definition 1.1.2 for the definition of completely-transitive). Each code is the dual of a first order q-ary Reed-Muller code and is contained in the dual of the repetition code of the respective length. Fix:

$$k = (q-1)d - 2 \tag{3.1}$$

throughout this chapter. Let q be a prime power, $Q = \mathbb{F}_q$ and $M = \mathbb{F}_q^d$. Recall the definitions of the repetition code and a dual code from Definitions 2.1.1 and 2.1.2, respectively. Define $\mathcal{RM}_q(k+1, d)$ and $\mathcal{RM}_q(k, d)$, the $k+1$- and k-th order q-ary Reed-Muller codes, in the Hamming graph $H(q^d, q)$ as:

$$\mathcal{RM}_q(k+1, d) = \{\alpha \in V\Gamma \mid \sum_{v \in M} \alpha_v = 0\} = \mathrm{Rep}(q^d, q)^{\perp}, \quad \text{and} \tag{3.2}$$

$$\mathcal{RM}_q(k, d) = \{\alpha \in \mathrm{Rep}(q^d, q)^{\perp} \mid \sum_{v \in M} \alpha_v v = 0\}. \tag{3.3}$$

Note that $\mathcal{RM}_q(k, d)$ has minimum distance $\delta = 3$ unless $q = 2$, in which case $\mathcal{RM}_2(k, d)$ is the extended Hamming code with minimum distance $\delta = 4$. These codes are part of the larger class of q-ary Reed-Muller codes (see Definition 9.1.6 or [2, Section 5.4]). The following result is proved in Section 3.5.

Theorem 3.3. *Let $C = \mathcal{RM}_q(k, d)$, where $k = (q-1)d - 2$, and let $X = \mathrm{Aut}(C)$. Then the code C is X-completely transitive and 1-elusive. Moreover, if $q \geqslant 5$ and (C, α, x) is an elusive triple, then there exist associates π, π' such that $d(\pi, \pi') = 3$ and $\mathrm{MC}(\pi, \pi') \neq 3$.*

The family of examples from Theorem 3.3 provides answers to some questions raised in [56].

1. In that paper there are only two images of each example code C under X_1; [56, Question 1.4] asks if this is always the case.

2. In [56, Question 1.5] it is asked whether the images under X_1 of a 1-elusive code C which is X-neighbour-transitive must be pairwise disjoint (for the definition of X-neighbour-transitive see Definition 1.1.2).

Theorem 3.4. *Let C be as in Theorem 3.3, $X = \mathrm{Aut}(C)$ and $X_1 = \mathrm{Aut}(C_1)$. If q is a power of the prime p then:*

1. *there are at least p distinct images of C under X_1; and,*

2. *there exists some $x \in X_1 \setminus X$ such that $\mathbf{0} \in C \cap C^x$.*

3.1 Elusive codes

Let (C, α, x) be an elusive triple where C has minimum distance $\delta \geqslant 2$. Then $\{\beta \in \Gamma \mid d(\beta, C_1) = 1\} = C \cup C_2$. In other words the 'set of neighbours' of C_1 is $C \cup C_2$. Thus, using [43, Lemma 3] (which states that $X \leqslant X_1$) with C_1 as the code, it follows that $X_1 \leqslant \mathrm{Aut}(C \cup C_2)$. Hence for all $\beta \in C$ and $y \in X_1$, $\beta^y \in C \cup C_2$.

The next Lemma is a combination [43, Lemma 6 (i) and (ii)] and [43, Lemma 7 (ii) and (iii)] respectively. (Note that $\Gamma_2(\alpha) \cap C^x = \mathrm{Pre}(\alpha, x^{-1})$). Each part of the partitions has size 2 by [43, Lemma 1].

Lemma 3.1.1. *Let (C, α, x) be an elusive triple with parameters (m, q, δ) where $\delta \geqslant 3$, and $\pi \in \Gamma_2(\alpha) \cap C^x$. Then*

1. *$\{\Gamma_1(\alpha) \cap \Gamma_1(\pi') \mid \pi' \in \Gamma_2(\alpha) \cap C^x\}$ forms a partition of $\Gamma_1(\alpha)$ with $m(q-1)/2$ parts of size 2.*

2. *$\{\Gamma_1(\pi) \cap \Gamma_1(\beta) \mid \beta \in \Gamma_2(\pi) \cap C\}$ forms a partition of $\Gamma_1(\pi)$ with $m(q-1)/2$ parts of size 2.*

When asking questions about elusive codes, the following lemma allows us to consider an equivalent code, and the elusive triples which arise from it. In particular, we often assume the zero vertex is part of our code, which we are able to do since $\mathrm{Aut}(\Gamma)$ is transitive on $H(m, q)$.

Lemma 3.1.2. *Let (C, α, x) be an elusive triple. Then $(C^y, \alpha^y, y^{-1}xy)$ is an elusive triple for any $y \in \mathrm{Aut}(\Gamma)$. Moreover, $(\Gamma_2(\alpha) \cap C^x)^y = \Gamma_2(\alpha^y) \cap C^{xy}$.*

Proof. Any element of $\mathrm{Aut}(\Gamma)$ preserves distances in the Hamming graph. Hence, $(C_1)^y = (C^y)_1$, and $(C^y)_1^{y^{-1}xy} = C_1^{xy} = C_1^y$. We have $\alpha^y \in C^y$. However $\alpha^{y(y^{-1}xy)} = \alpha^{xy} \notin C^y$, since $\alpha^x \notin C$, so $(C^y, \alpha^y, y^{-1}xy)$ is an elusive triple. Suppose $\pi \in \Gamma_2(\alpha) \cap C^x$, then $2 = d(\pi, \alpha) = d(\pi^y, \alpha^y)$ and $\pi \in C^x$ so $\pi^y \in C^{xy}$. Similarly, suppose $\pi \in \Gamma_2(\alpha^y) \cap C^{xy}$, then $2 = d(\pi, \alpha^y) = d(\pi^{y^{-1}}, \alpha)$ and $\pi \in C^{xy}$ so $\pi^{y^{-1}} \in C^x$. Thus $(\Gamma_2(\alpha) \cap C^x)^y = \Gamma_2(\alpha^y) \cap C^{xy}$. □

Some notation to refer to specific elements of $\Gamma_r(\alpha)$ for $\alpha \in H(m, q)$ will be useful for the next lemma. Let $\alpha \in H(m, q)$, $a_i \in Q$ and $k_i \in M$, for $i = 1, \ldots, r$, where the k_i are pairwise distinct, and define

$$\gamma(\alpha|k_1, \ldots, k_r|a_1, \ldots, a_r)_i = \begin{cases} a_j & \text{if } i = k_j \\ \alpha_i & \text{otherwise} \end{cases}.$$

For example, if $\alpha = (0, \ldots, 0)$, $r = 2$, $k_1 = 1$ and $k_2 = 2$, then

$$\gamma(\alpha|k_1, k_2|a, b) = (a, b, 0, \ldots, 0).$$

Since

$$\gamma(\alpha|k_1, \ldots, k_r|a_1, \ldots, a_r)$$

differs from α in at most r entries, we have

$$\gamma(\alpha|k_1,\ldots,k_r|a_1,\ldots,a_r) \in \cup_{i\leqslant r}\Gamma_i(\alpha),$$

and if $a_i \neq \alpha_{k_i}$ for each i, then

$$\gamma(\alpha|k_1,\ldots,k_r|a_1,\ldots,a_r) \in \Gamma_r(\alpha).$$

The next lemma is a restatement of the result [56, Lemma 3.11].

Lemma 3.1.3. *If two vertices $\alpha,\beta \in \Gamma$ are at distance 2 with $\mathrm{diff}(\alpha,\beta) = \{i,j\}$, then they are part of a unique 4-cycle with vertices $\alpha, \gamma(\alpha|i|\beta_i), \beta(=\gamma(\alpha|i,j|\beta_i,\beta_j))$ and $\gamma(\alpha|j|\beta_j)$.*

The next result shows that the conditions of Theorem 3.2 do not vacuously hold. Recall that $\mathrm{diff}(\alpha,\beta)$ is the subset of entries $i \in M$ such that $\alpha_i \neq \beta_i$ (see Table 2.1.1).

Lemma 3.1.4. *Let (C,α,x) be an elusive triple with $\delta, q \geqslant 3$. Then there exist (C,α,x)-associates π_1,π_2 such that $d(\pi_1,\pi_2) = 3$.*

Proof. It is stated in [43, Theorem 1] that if $\delta \geqslant 3$ then $\delta = 3$, or $q = 2$ and $\delta = 4$. Thus $\delta = 3$, since $q \neq 2$. Lemma 3.1.2 allows us to assume $\alpha = \mathbf{0}$, the zero codeword. By Lemma 3.1.1 (i), $\{\Gamma_1(\alpha)\cap\Gamma_1(\pi') \mid \pi' \in \Gamma_2(\alpha)\cap C^x\}$ form a partition of $\Gamma_1(\alpha)$. Furthermore, again by Lemma 3.1.2, it can be assumed that $\pi_1 = \gamma(\mathbf{0}|1,2|1,1)$ is a (C,α,x)-associate, and thus the neighbours $\gamma(\mathbf{0}|1|1)$ and $\gamma(\mathbf{0}|2|1)$ appear in the same part of the partition, by Lemma 3.1.3. The neighbour $\gamma(\mathbf{0}|1|2)$ must also appear in a part, corresponding to an associate $\pi_2 = \gamma(\mathbf{0}|1,i|2,a)$, for some $i \neq 1$, $a \neq 0$. If $i = 2$ then $d(\pi_1,\pi_2) \leqslant 2$; however $\pi_1,\pi_2 \in C^x$, which is equivalent to C and so has minimum distance 3. So $\mathrm{diff}(\pi_1,\pi_2) = \{1,2,i\}$ and thus $d(\pi_1,\pi_2) = 3$. □

The reader will notice a difference in terminology from [56], where the concept of an *elusive pair* was used, a code-group pair (C,X'), where X' fixes C_1 setwise, but not C. This implies that there exists an element $x \in X'$ such that $x \in X_1 \setminus X$, and hence also a codeword α such that $\alpha^x \notin C$, implying that (C,α,x) is an elusive triple. Conversely, if (C,α,x) is an elusive triple then for $X' = \langle x\rangle$, (C,X') is an elusive pair. Hence the two concepts are equivalent.

3.2 Mutual codewords

This section investigates the way in which the structure of the Hamming graph affects the configuration of codewords. The strategy in this section is to find, for vertices α and β with $d(\alpha,\beta) \leqslant 4$, a way to express those vertices which are at distance 2 from both α and β, apply this to the case that α and β are mutual codewords of associates π,π', and then use this condition to bound the size of $\mathrm{MC}(\pi,\pi')$.

Lemma 3.2.1. *Let $\alpha,\beta,\gamma \in \Gamma$ such that $\alpha,\beta \in \Gamma_2(\gamma)$. Then,*

1. $d(\alpha, \beta) = 4$ *if and only if* $\operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma) = \emptyset$ *and,*

2. $d(\alpha, \beta) = 3$ *implies* $|\operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma)| = 1$.

Proof. First, note that $\operatorname{diff}(\alpha, \beta) \subseteq \operatorname{diff}(\alpha, \gamma) \cup \operatorname{diff}(\beta, \gamma)$, since $\alpha_i = \beta_i = \gamma_i$ for any $i \notin \operatorname{diff}(\alpha, \gamma) \cup \operatorname{diff}(\beta, \gamma)$. By hypothesis, $|\operatorname{diff}(\alpha, \gamma)| = |\operatorname{diff}(\beta, \gamma)| = 2$.

Suppose $d(\alpha, \beta) = 4$, or equivalently, $|\operatorname{diff}(\alpha, \beta)| = 4$. It then follows, from the above, that $\operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma) = \emptyset$. Conversely, if $\operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma) = \emptyset$, then there are entries $i_1, i_2, j_1, j_2 \in M$ such that $\alpha_{i_k} = \gamma_{i_k} \neq \beta_{i_k}$ and $\beta_{j_k} = \gamma_{j_k} \neq \alpha_{j_k}$, for $k = 1, 2$. Thus $\operatorname{diff}(\alpha, \beta) = \{i_1, i_2, j_1, j_2\}$ and $d(\alpha, \beta) = 4$.

Assume $|\operatorname{diff}(\alpha, \beta)| = 3$. Then $\operatorname{diff}(\alpha, \beta) \subseteq \operatorname{diff}(\alpha, \gamma) \cup \operatorname{diff}(\beta, \gamma)$ implies that either $|\operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma)| = 1$ or $\operatorname{diff}(\alpha, \gamma)$ and $\operatorname{diff}(\beta, \gamma)$ are disjoint and $\operatorname{diff}(\alpha, \beta)$ is a proper subset of the above. However, by (i), $\operatorname{diff}(\alpha, \gamma)$ and $\operatorname{diff}(\beta, \gamma)$ disjoint implies $d(\alpha, \beta) = 4$. Thus $|\operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma)| = 1$. □

Lemma 3.2.2. *Suppose* $\alpha, \beta \in \Gamma$ *and* $d(\alpha, \beta) = 4$. *Then* $\Gamma_2(\alpha) \cap \Gamma_2(\beta)$ *consists of the six vertices* $\gamma(\alpha|i, j|\beta_i, \beta_j)$ *for* $i, j \in \operatorname{diff}(\alpha, \beta), i \neq j$.

Proof. Without loss of generality let $\alpha = \mathbf{0}$, the zero codeword, and let

$$\beta = \gamma(\mathbf{0}|1, 2, 3, 4|1, 1, 1, 1)$$

so that $\operatorname{diff}(\alpha, \beta) = \{1, 2, 3, 4\}$. Any element of $\Gamma_2(\alpha)$ has the form $\gamma(\mathbf{0}|i, j|a, b)$ where $a, b \neq 0$ and $i \neq j$. Moreover, $\gamma(\mathbf{0}|i, j|a, b) \in \Gamma_2(\beta)$ if and only if $a = b = 1$ and $i, j \in \operatorname{diff}(\alpha, \beta)$. □

Lemma 3.2.3. *Let* (C, α, x) *be an elusive triple with* $\delta \geqslant 3$ *and let* $\pi, \pi' \in \Gamma_2(\alpha) \cap C^x$ *such that* $d(\pi, \pi') = 4$. *Then* $1 \leqslant \mathrm{MC}(\pi, \pi') \leqslant 2$.

Proof. By Lemma 3.1.2 we can assume $\alpha = \mathbf{0}$, $\pi = \gamma(\mathbf{0}|1, 2|1, 1)$ and $\pi' = \gamma(\mathbf{0}|3, 4|1, 1)$, since by Lemma 3.2.1 $\operatorname{diff}(\alpha, \pi)$ and $\operatorname{diff}(\alpha, \pi')$ are disjoint. By Lemma 3.2.2, and running through each choice for i, j,

$$\Gamma_2(\pi) \cap \Gamma_2(\pi') = \{\mathbf{0}, \gamma(\mathbf{0}|1, 2, 3, 4|1, 1, 1, 1), \gamma(\mathbf{0}|i, j|1, 1) \mid i \in \{1, 2\}, j \in \{3, 4\}\}.$$

Since $\mathbf{0} \in C$ we have $1 \leqslant \mathrm{MC}(\pi, \pi')$ and as $\delta \geqslant 3$ the only other possible element in $C \cap \Gamma_2(\pi) \cap \Gamma_2(\pi')$ is $\gamma(\mathbf{0}|1, 2, 3, 4|1, 1, 1, 1)$ and thus $\mathrm{MC}(\pi, \pi') \leqslant 2$. □

Lemma 3.2.4. *Suppose* $q \geqslant 3$, $\alpha, \beta \in \Gamma$ *and* $d(\alpha, \beta) = 3$. *Then*

$$\Gamma_2(\alpha) \cap \Gamma_2(\beta) = \{\gamma(\alpha|i, j|a, \beta_j) \mid i, j \in \operatorname{diff}(\alpha, \beta), i \neq j, a \neq \alpha_i, \beta_i\},$$

and $|\Gamma_2(\alpha) \cap \Gamma_2(\beta)| = 6(q - 2)$.

Proof. Let $\gamma \in \Gamma_2(\alpha) \cap \Gamma_2(\beta)$. By Lemma 3.2.1, there is a unique (for γ) $i \in \operatorname{diff}(\alpha, \gamma) \cap \operatorname{diff}(\beta, \gamma)$, which implies that $\gamma = \gamma(\alpha|i, j|a, \beta_j)$ where $j \in \operatorname{diff}(\alpha, \beta) \setminus \{i\}$ and $a \neq \alpha_i, \beta_i$. There are $\binom{3}{2} = 6$ choices for $\{i, j\}$, and there are $q - 2$ choices for a. □

Lemma 3.2.5. *Let (C, α, x) be an elusive triple with $\delta = 3$ and $q \geqslant 3$. If $\pi, \pi' \in \Gamma_2(\alpha) \cap C^x$ with $d(\pi, \pi') = 3$, then $1 \leqslant \mathrm{MC}(\pi, \pi') \leqslant 3$. Moreover, if $\mathrm{MC}(\pi, \pi') = 3$ and $\{i, j\} = \mathrm{diff}(\alpha, \pi)$, $\{j, k\} = \mathrm{diff}(\alpha, \pi')$, then*

$$C \cap \Gamma_2(\pi) \cap \Gamma_2(\pi') = \{\alpha, \gamma(\alpha|i, j, k|\pi_i, \pi'_j, a), \gamma(\alpha|i, j, k|c, \pi_j, \pi'_k)\},$$

for some $a \neq \alpha_k, \pi'_k$, and some $c \neq \alpha_i, \pi_i$.

Proof. Note that $\mathrm{diff}(\alpha, \pi) \cap \mathrm{diff}(\alpha, \pi') = \{j\}$. Since this proof concerns only the entries i, j, k, abbreviate $\gamma(\alpha|i, j, k|a, b, c)$ to simply abc. Let $S = \Gamma_2(\pi) \cap \Gamma_2(\pi') \cap C$. Then $\alpha \in S$, so $|S| \geqslant 1$. By Lemma 3.2.4

$$\begin{aligned}\Gamma_2(\pi) \cap \Gamma_2(\pi') &= \{\gamma(\pi|s, t|a, \pi'_t) \mid s, t \in \mathrm{diff}(\pi, \pi'), s \neq t, a \neq \pi_s, \pi'_s\} \\ &= \{\pi_i\pi'_j a,\ \ \pi_i b\pi'_k,\ \ \pi'_i\pi_j a,\ \ c\pi_j\pi'_k,\ \ \pi'_i b\pi_k,\ \ c\pi'_j\pi_k \\ &\qquad \mid a \neq \pi_k, \pi'_k; b \neq \pi_j, \pi'_j; c \neq \pi_i, \pi'_i\}.\end{aligned}$$

Since $\delta = 3$, $\pi_k = \alpha_k$ and $\pi'_i = \alpha_i$, the set $S \setminus \{\alpha\}$ cannot contain vertices which agree with π and π' in the entries k and i respectively. Thus, $\pi_i\pi'_j a, \pi_i b\pi'_k$ and $c\pi_j\pi'_k$ represent the possible elements of $S \setminus \{\alpha\}$. In particular, $\delta \geqslant 3$ implies each form is present in S for unique values of a, b or c respectively. Suppose $\pi_i b\pi'_k \in S$ for some $b \neq \alpha_j, \pi_j, \pi'_j$. Then, since $\delta \geqslant 3$, $\pi_i\pi'_j a, c\pi_j\pi'_k \notin S$, as they agree with $\pi_i b\pi'_k$ in entry i and k respectively. In this case, $|S| = 2$.

On the other hand, if $\pi_i b\pi'_k \notin S$ then it follows that $|S| \leqslant 3$, since at most one of each of $\pi_i\pi'_j a$ and $b\pi_j\pi'_k$ is in S. If $\mathrm{MC}(\pi, \pi') = 3$ then S contains the vertices α, $\gamma(\alpha|i, j, k|\pi_i, \pi'_j, a)$ and $\gamma(\alpha|i, j, k|c, \pi_j, \pi'_k)$, for some $a \in Q \setminus \{\pi_k, \pi'_k\}$ and $c \in Q \setminus \{\pi_i, \pi'_i\}$. □

Corollary 3.2.6. *Let (C, α, x) be an elusive triple with $\delta \geqslant 3$ and π, π' be distinct (C, α, x)-associates. Then $1 \leqslant \mathrm{MC}(\pi, \pi') \leqslant 3$.*

Proof. Combining Lemma 3.2.3 and Lemma 3.2.5 gives the result. □

3.3 Permutation codes

This section examines the infinite family of elusive codes presented in [56]. The main purpose of this is as motivation for the hypothesis in Theorem 3.2. In particular we find the full automorphism groups of the codes and their neighbour sets, and show that $\mathrm{MC}(\pi, \pi') = 3$ for any two associates π, π' at distance 3. These examples are instances of *permutation codes* and *frequency permutation arrays*, which have been studied, in particular, by Blake, Cohen and Deza in [11], and Huczynska and Mullen in [61], respectively.

Definition 3.3.1. Let $Q = \{1, \ldots, q\}$ and S_q be the symmetric group on Q. Associate with each permutation $g \in \mathrm{S}_q$ the vertex $\alpha(g) = (1^g, \ldots, q^g)$ in $H(q, q)$. Now let $N = \{1, \ldots, n\}$, $M = Q \times N$ and, for $T \subseteq \mathrm{S}_q$, let $C(T, n)$ be the set of nq-tuples $(\alpha(g_1), \alpha(g_2), \ldots, \alpha(g_n))$ in $H(nq, q)$ such that the product $g_1 \cdots g_n \in T$. Denote $C(T) = C(T, 1)$.

For example, $C(\mathrm{A}_q, n)$ consists of all nq-tuples obtained by concatenating n permutation codewords $\alpha(g_i)$, such that an even number of the g_i are odd permutations. Similarly, $C(\mathrm{S}_q, n)$ is the code consisting of all nq-tuples obtained by concatenating n permutation codewords $\alpha(g_i)$, with no restriction on the g_i.

The following two actions of S_q on $H(q, q)$, when combined with results from [39] and [46], allows us to describe the full automorphism groups of $C(\mathrm{A}_q)$ and $C(\mathrm{S}_q)$.

For $y \in \mathrm{S}_q$, let $x_y = (y, \ldots, y) \in B \cong Sym(Q)^q$ and let σ_y be the permutation in $L \cong Sym(M) (\cong Sym(Q)$ since $n = 1)$ induced by y. Then x_y and σ_y act on codewords in $C(\mathrm{S}_q)$ via $\alpha(g)^{x_y} = \alpha(gy)$ and $\alpha(g)^{\sigma_y} = \alpha(y^{-1}g)$ for all $y \in \mathrm{S}_q$, by [46].

There are two natural subgroups which arise from these actions:

$$\mathrm{Diag}_q(T) = \{x_y \mid y \in T\} \quad \text{and} \quad A(T) = \{x_y\sigma_y \mid y \in T\}.$$

The aim of the next few results is to show that if π, π' are $(C(\mathrm{A}_q, n), \alpha, x)$-associates and $d(\pi, \pi') = 3$ then $\mathrm{MC}(\pi, \pi') = 3$. This is done determining $X_1 = \mathrm{Aut}(C(\mathrm{A}_q, n)_1)$ in each case. Generally, $X_1 = \mathrm{Aut}(C(\mathrm{S}_q, n))$. However, there are two exceptions to this, presented in the next example.

Example 3.3.2. *Let $C = C(\mathrm{A}_3) = \{123, 231, 312\}$, as defined in Definition 3.3.1. Since each codeword is generated from a permutation, the neighbour set consists of every vertex containing a repeated entry, for example $113 \in C_1$. Another code with the same neighbour set is $C(\mathrm{S}_3 \setminus \mathrm{A}_3) = \{132, 213, 321\}$, constructed from the odd permutations. In this case the repetition code $\mathrm{Rep}(3, 3) = \{111, 222, 333\}$ also has the same neighbour set and is equivalent to C under the automorphism $x = (1, (123), (132))$ in the base group B of $\mathrm{Aut}(\Gamma)$. There are no other codes with the same neighbour set and minimum distance. To see this note that $H(3, 3)$ is the disjoint union $C(\mathrm{A}_3) \cup C(\mathrm{S}_3 \setminus \mathrm{A}_3) \cup \mathrm{Rep}(3, 3) \cup C_1$, and any two vertices $\alpha, \beta \notin C_1$ from different codes are at distance 2.*

As a second example, let $C = C(\mathrm{A}_2, 2) = \{1212, 2121\}$. Then C_1 is made up of vertices with an odd number of each symbol and $C(\mathrm{S}_2 \setminus \mathrm{A}_2, 2) = \{1221, 2112\}$ shares the same neighbour set. Additionally the code $\mathrm{Rep}(2, 4) = \{1111, 2222\}$ has neighbour set C_1 and is equivalent to C under the automorphism $x = (1, (12), 1, (12)) \in B$.

Lemma 3.3.3. *The full automorphism groups of $C(\mathrm{A}_q)$ and $C(\mathrm{S}_q)$ are the semi-direct products $\mathrm{Aut}(C(\mathrm{A}_q)) = \mathrm{Diag}_q(\mathrm{A}_q) \rtimes A(\mathrm{S}_q)$ and $\mathrm{Aut}(C(\mathrm{S}_q)) = \mathrm{Diag}_q(\mathrm{S}_q) \rtimes A(\mathrm{S}_q)$ respectively.*

Proof. As A_q and S_q are 2-transitive, [39, Lemma 5.1.7] can be applied, which states that $\mathrm{Aut}(C(G)) = \mathrm{Diag}_q(G) \rtimes A(N_{\mathrm{S}_q}(G))$ for any 2-transitive group G, where $N_{\mathrm{S}_q}(T)$ is the normaliser of T in S_q. The result then follows, since $N_{\mathrm{S}_q}(\mathrm{A}_q) = N_{\mathrm{S}_q}(\mathrm{S}_q) = \mathrm{S}_q$. □

The next result is simply a re-wording of [56, Lemma 3.9].

Lemma 3.3.4. *$C(\mathrm{A}_q, n)$ is an elusive code.*

The above result tells us that elusive triples (C, α, x) exist with $C = C(\mathrm{A}_q, n)$. The remainder of this section provides results which allow us to decide if a triple (C, β, y), where $\beta \in C(\mathrm{A}_q, n)$ and $y \in \mathrm{Aut}(\Gamma)$, is an elusive triple.

Lemma 3.3.5. *The automorphism group of $C(\mathrm{S}_q, n)$ contains the wreath product*

$$(\mathrm{Diag}_q(\mathrm{S}_q) \rtimes A(\mathrm{S}_q)) \wr \mathrm{S}_n\,.$$

Proof. This follows from [56, Corollary 3.6]. □

The next result shows that $\mathrm{Aut}(C(\mathrm{S}_q, n))$ acts imprimitively on M, which allows the full automorphism group to be found. As in Definition 3.3.1 the set of entries is $M = Q \times N$, where $N = \{1, \ldots, n\}$ so that entries are labelled by tuples (i, j), where $i \in Q$ and $j \in N$. For $j \in N$ define (Q, j) to be the subset $\{(i, j) \mid i \in Q\}$ of $Q \times N$.

Lemma 3.3.6. *If $n \geqslant 2$ then the partition $\{(Q,1), \ldots, (Q,n)\}$ is a system of imprimitivity for the action of $\mathrm{Aut}(C(\mathrm{S}_q, n))$ on $M = Q \times N$. Moreover, $\mathrm{Aut}(C(\mathrm{S}_q, n)) = (\mathrm{Diag}_q(\mathrm{S}_q) \rtimes A(\mathrm{S}_q)) \wr \mathrm{S}_n$.*

Proof. If $\alpha \in C(\mathrm{S}_q, n)$ then $(\alpha_{(1,i)}, \ldots, \alpha_{(q,i)}) = \alpha(g)$, for some permutation $g \in \mathrm{S}_q$, which implies that $\alpha_s \neq \alpha_t$ whenever $s, t \in (Q, i)$ for some $i \in N$. We preemptively refer to $\{(Q,1), \ldots, (Q,n)\}$ as blocks. If s and t are in different blocks, then it is claimed that there is no element of $\mathrm{Aut}(C(\mathrm{S}_q, n))^M$ mapping s and t to the same block. It follows from this claim that for any $x \in \mathrm{Aut}(C(\mathrm{S}_q, n))$ and $i \in N$, either $(Q, i)^x \cap (Q, i) = \emptyset$ or $(Q, i)^x = (Q, i)$, since otherwise there exists $s \in (Q, i)^x \cap (Q, i)$ and $t \in (Q, i)$, with $t \in (Q, j)^x$ for some $j \neq i$. Thus, the claim implies $\{(Q,1), \ldots, (Q,n)\}$ is a system of imprimitivity for the action of $\mathrm{Aut}(C(\mathrm{S}_q, n))$ on $M = Q \times N$.

The claim is proved as follows. Suppose $s = (i, j)$ and $t = (i', j')$, where $j \neq j'$. By Lemma 3.3.5, there exists a permutation $\sigma \in (\mathrm{Diag}_q(\mathrm{S}_q) \rtimes A(\mathrm{S}_q)) \wr \mathrm{S}_n$ such that $(i, j)^\sigma = (1, 1)$ and $(i', j')^\sigma = (1, 2)$. Hence, it suffices to prove the claim when $s = (1, 1)$ and $t = (1, 2)$. For each $i \in Q$, let $\beta(i) = (\alpha(1), \alpha(g_i), \alpha(g), \ldots, \alpha(g))$ with $n-2$ entries $\alpha(g)$, for some $g, g_i \in \mathrm{S}_q$ with $1^{g_i} = i$. Then $\beta(i) \in C(\mathrm{S}_q, n)$ for all $i \in Q$. Let $x = h\sigma \in \mathrm{Aut}(C(\mathrm{S}_q, n))$ where $h \in \mathrm{S}_q^{nq}$ and σ is an element of S_{nq}, the full symmetric group on M (note that this does not assume that σ preserves the Cartesian product $M = Q \times N$). Suppose $(1, 1)^\sigma = (j, k)$ and $(1, 2)^\sigma = (j', k)$ for some $j, j' \in Q$ and $k \in N$. If $1^{h_{(1,1)}} = r$, then $(\beta(i)_{(1,1)})^{h_{(1,1)}} = r$, for all $i \in Q$. However, there exists an s such that $(\beta(s)_{(1,2)})^{h_{(1,2)}} = r$. This means $(\beta(s)^x)_{(j,k)} = (\beta(s)^x)_{(j',k)} = r$, so $((\beta(s)^x)_{(1,k)}, \ldots, (\beta(s)^x)_{(q,k)}) \neq \alpha(g')$ for any $g' \in \mathrm{S}_q$, a contradiction. This proves the claim.

Since $\{(Q,1), \ldots, (Q,n)\}$ is a system of imprimitivity for the action of $\mathrm{Aut}(C(\mathrm{S}_q, n))$ on $M = Q \times N$ we have $\mathrm{Aut}(C(\mathrm{S}_q, n)) \leqslant H \wr \mathrm{S}_n$, for some $H \leqslant \mathrm{S}_q \wr \mathrm{S}_q$. Any codeword $\alpha \in C(\mathrm{S}_q, n)$ satisfies $\alpha_{(Q,1)} = \alpha(g)$, for some g. Also for any $g \in \mathrm{S}_q$ we have $(\alpha(g), \ldots, \alpha(g)) \in C(\mathrm{S}_q, n)$. Hence projecting the code $C(\mathrm{S}_q, n)$ onto $(Q, 1)$ gives $C(\mathrm{S}_q)$. Thus, the group induced by $\mathrm{Aut}(C(\mathrm{S}_q, n))$ on $(Q, 1)$ is a subgroup of $\mathrm{Aut}(C(\mathrm{S}_q))$, so we may assume that

$H = \mathrm{Aut}(C(\mathrm{S}_q))$. By Lemma 3.3.3, $H = \mathrm{Diag}_q(\mathrm{S}_q) \rtimes A(\mathrm{S}_q)$. Since $\mathrm{Aut}(C(\mathrm{S}_q, n)) \geqslant (\mathrm{Diag}_q(\mathrm{S}_q) \rtimes A(\mathrm{S}_q)) \wr \mathrm{S}_n$ by Lemma 3.3.5, it follows that $\mathrm{Aut}(C(\mathrm{S}_q, n)) = H \wr \mathrm{S}_n$. □

By the above result and the fact that $|C(\mathrm{S}_q, n)| = 2|C(\mathrm{A}_q, n)|$,

$$\mathrm{Aut}(C(\mathrm{A}_q, n)) = \{(x_{y_1} z_1, \ldots, x_{y_n} z_n) \mid y_i \in \mathrm{S}_q, z_i \in A(\mathrm{S}_q), y_1 \cdots y_n \in \mathrm{A}_q\},$$

since the above group has index 2 in $\mathrm{Aut}(C(\mathrm{S}_q, n))$.

Lemma 3.3.7. *Let $\beta = (\beta_1, \ldots, \beta_n) \in H(nq, q)$, where $\beta_i \in C(\mathrm{S}_q)_{k_i}$, for $i = 1 \ldots, n$. Then $\beta \in C(\mathrm{S}_q, n)_k$, where $k = k_1 + \cdots + k_n$.*

Proof. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a codeword in $C(\mathrm{S}_q, n)$, where $\alpha_i \in C(\mathrm{S}_q)$, for $i = 1, \ldots, n$. Then $d(\alpha_i, \beta_i) \geqslant k_i$ for all $i = 1, \ldots, n$ so $d(\alpha, \beta) \geqslant k_1 + \cdots + k_n$. In particular, for each $i = i, \ldots, n$, there exists some $\gamma_i \in C(\mathrm{S}_q)$ such that $d(\beta_i, \gamma_i) = k_i$, so $d(\beta, \gamma) = k_1 + \cdots + k_n$, where $\gamma = (\gamma_1, \ldots, \gamma_n) \in H(nq, q)$. □

Set $X = \mathrm{Aut}(C(\mathrm{A}_q, n))$ and $X_1 = \mathrm{Aut}(C(\mathrm{A}_q, n)_1)$. The next result shows that, apart from two exceptions, the group $X_1 = \mathrm{Aut}(C(\mathrm{S}_q, n))$.

Lemma 3.3.8. *Suppose $(q, n) \neq (3, 1)$ or $(2, 2)$. Then $C(\mathrm{S}_q, n)$ is not an elusive code and $X_1 = \mathrm{Aut}(C(\mathrm{S}_q, n))$.*

Proof. By [43, Lemma 3],

$$\mathrm{Aut}(C(\mathrm{S}_q, n)) \leqslant \mathrm{Aut}(C(\mathrm{S}_q, n)_1) = \mathrm{Aut}(C(\mathrm{A}_q, n)_1),$$

since $C(\mathrm{A}_q, n)_1 = C(\mathrm{S}_q, n)_1$ by [56, Lemma 3.8]. So $\mathrm{Aut}(C(\mathrm{S}_q, n)) \leqslant X_1$. Moreover, it follows by definition that if we show that $C(\mathrm{S}_q, n)$ is not elusive, then $\mathrm{Aut}(C(\mathrm{S}_q, n)) = X_1$. We show that $C(\mathrm{S}_q, n)$ is not elusive by showing no elusive triples exist. For the case $(q, n) = (2, 1)$, $H(2, 2) = C(\mathrm{S}_2) \cup C(\mathrm{S}_2)_1$, thus $C(\mathrm{S}_2)_2$ is empty and there is no $\beta \in C(\mathrm{S}_2)_2$ such that $\alpha^x = \beta$. Assume now that $(q, n) \neq (2, 1)$.

Suppose that there exists an elusive triple $(C(\mathrm{S}_q, n), \alpha, x)$. Then let $\beta = \alpha^x \in C(\mathrm{S}_q, n)_2$. Now $\nu \in \Gamma_1(\alpha)$ implies $\nu^x \in C_1$, so that $\Gamma_1(\beta) \subseteq C(\mathrm{S}_q, n)_1$. We now show that there exists $\gamma \in \Gamma_1(\beta) \cap C(\mathrm{S}_q, n)_3$, which contradicts $\beta = \alpha^x \in C(\mathrm{S}_q, n)_2$. Thus if x maps α to β then $x \notin X_1$ and so no such elusive triple exists.

If $\beta \in C(\mathrm{S}_q, n)_2$, then either β differs from a codeword in two entries of a single block (Q, s), so that $\beta_{(Q,s)} = \nu \in C(\mathrm{S}_q)_2$, and $\beta_{(Q,j)} = \alpha(g_j)$ for $j \neq s$, where $g_j \in \mathrm{S}_q$; or β differs from a codeword in one entry of each of two distinct blocks (Q, s) and (Q, t), so that $\beta_{(Q,s)} = \mu$ and $\beta_{(Q,t)} = \nu$, where $\mu, \nu \in C(\mathrm{S}_q)_1$, and $\beta_{(Q,j)} = \alpha(g_j)$ for $j \neq s, t$, where $g_j \in \mathrm{S}_q$.

Let $n \geqslant 3$, with β taking either of the above forms, and choose $r \neq s, t$. Let $\beta'_{(Q,r)} = \nu'$, for some $\nu' \in \Gamma_1(\alpha(g_r))$, and $\beta'_{(Q,j)} = \beta_{(Q,j)}$ for $j \neq r$. Then β is adjacent to β' and β' lies in $C(\mathrm{S}_q, n)_3$ by Lemma 3.3.7.

Let $n = 2$, $q \geqslant 3$. If $\beta = (\nu, \alpha(g))$ where $\nu \in C(\mathrm{S}_q)_2$, then let $\beta' = (\nu, \mu)$ where $\mu \in \Gamma_1(\alpha(g))$. Similarly if $\beta = (\alpha(g), \nu)$. If $\beta = (\mu, \nu)$ where $\mu, \nu \in C(\mathrm{S}_q)_1$, then let $\beta' = (\mu, \nu')$ where $\nu' \in \Gamma_1(\nu) \cap C(\mathrm{S}_q)_2$ (note that $C(\mathrm{S}_q)_2 \neq \emptyset$ since $q \geqslant 3$). In either case, β is adjacent to β' and, by Lemma 3.3.7, β' lies in $C(\mathrm{S}_q, n)_3$.

Finally, let $n = 1$, $q \geqslant 4$. Any $\nu \in C(\mathrm{S}_q)_2$ either has two entries repeated twice, or one entry repeated three times. Without loss of generality we may assume that ν is either $\gamma(\alpha(1)|2,3|1,1)$ or $\gamma(\alpha(1)|2,4|1,3)$, that is, $(1,1,1,4,\ldots,q)$ or $(1,1,3,3,5,\ldots,q)$. In either case, ν is adjacent to a vertex $\beta' \in C(\mathrm{S}_q)_3$: in the first case we have $\beta' = \gamma(\alpha(1)|2,3,4|1,1,1)$ and in the second $\beta' = \gamma(\alpha(1)|2,4,5|1,3,1)$. Note that this uses $q \geqslant 5$ in the second case. For $q = 4$, $(1,1,3,3)$ is not adjacent to any $\beta' \in C(\mathrm{S}_4)_3$, so in this case we prove there is no $x \in X_1$ which maps an element of $C(\mathrm{S}_4)$ to $(1,1,3,3)$. Suppose $\alpha' = \alpha(g)$ for some $g \in \mathrm{S}_4$ and $\alpha'^x = (1,1,3,3)$, for some $x = (h_1,h_2,h_3,h_4)\sigma \in X_1$, where $(h_1,h_2,h_3,h_4) \in \mathrm{S}_4^4$, $\sigma \in \mathrm{S}_4$. Let $i \in M$ such that $i^\sigma = 1$. Then there exists $a \in Q \setminus \{\alpha'_i\}$ such that $a^{h_i} = 3$. Therefore $\gamma(\alpha'|i|a) \in C(\mathrm{S}_4)_1$ and $\gamma(\alpha'|i|a)^x = (3,1,3,3) \notin C(\mathrm{S}_4)_1$. This implies $x \notin X_1$, giving us a contradiction. □

Lemma 3.3.8 leaves out the two cases $(q,n) = (3,1)$ and $(2,2)$. For these parameters, $C(\mathrm{S}_q, n)$ is an elusive code with $\delta = 2$, since there are elements of X_1 which do not fix $C(\mathrm{S}_q, n)$ (see Example 3.3.2).

The following proposition tells us that every elusive triple arising from $C(\mathrm{A}_q, n)$ satisfies the conditions of Theorem 3.2.

Proposition 3.3.9. *Let $(C(\mathrm{A}_q,n),\alpha,x)$ be an elusive triple. Then, for any $(C(\mathrm{A}_q,n),\alpha,x)$-associates π,π' such that $d(\pi,\pi') = 3$, we have $\mathrm{MC}(\pi,\pi') = 3$.*

Proof. If $(q,n) = (3,1)$ then $C = C(\mathrm{A}_3)$ and we consider $\pi,\pi' \in \{111,222,333\}$ or $\pi,\pi' \in \{132,321,213\}$ (see Example 3.3.2). However, it is easily checked that any choices of π and π' are each at distance two from any $\alpha \in C$ and so $\mathrm{MC}(\pi,\pi') = 3$. By Lemma 3.3.8, either $(q,n) = (3,1)$ or $\pi,\pi' \in C(\mathrm{S}_q \setminus \mathrm{A}_q, n)$. We need only consider $q \geqslant 3$, since when $q = 2$ either $n = 1$ and there is only one codeword in $C(\mathrm{A}_q,n)$ or $n \geqslant 2$ and $\delta = 4$. Thus, if $q = 2$ there is either only one associate or for all distinct $\pi,\pi' \in \Gamma_2(\alpha) \cap C^x$ we have $d(\pi,\pi') = 4$, and hence there do not exist $(C(\mathrm{A}_q,n),\alpha,x)$-associates π,π', such that $d(\pi,\pi') = 3$.

Let $C = C(\mathrm{A}_q,n)$ and $\alpha = (\alpha(g_1),\alpha(g_2),\ldots,\alpha(g_n)) \in C$. Then, by Lemma 3.3.8, each associate $\pi \in \Gamma_2(\alpha) \cap C^x$ has the form $\pi = (\alpha(h_1),\ldots,\alpha(h_n))$ where $h_s = g_s(ij)$ for some s and $i \neq j$, and $h_t = g_t$ if $t \neq s$. Consider another associate $\pi' = (\alpha(h'_1),\ldots,\alpha(h'_n))$ where $h'_{s'} = g_{s'}(i'j')$ for some s' and $i' \neq j'$, and $h'_t = g_t$ if $t \neq s'$. If $s \neq s'$ then $d(\pi,\pi') \geqslant 4$, so we must have $s = s'$. Moreover, $d(\pi,\pi') = 3$ if and only if $h'_s = g_s(jk)$, $k \neq i,j$ and $h'_t = h_t$ for $t \neq s$. Then $C \cap \Gamma_2(\pi) \cap \Gamma_2(\pi') = \{\alpha, (\alpha(b_1),\ldots,\alpha(b_n)) \mid b_s = g_s(ijk) \text{ or } g_s(ikj); b_t = g_t, t \neq s\}$, and $\mathrm{MC}(\pi,\pi') = 3$. □

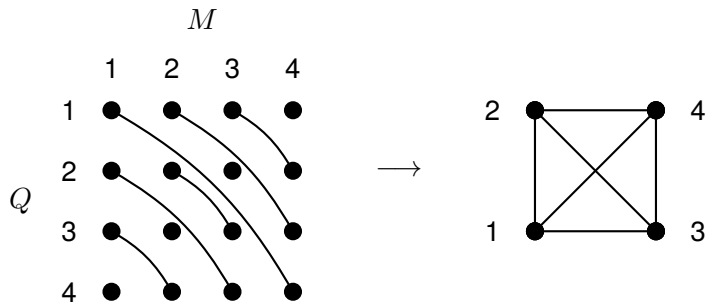

Figure 3.4.1: The graph on the right is $\Pi = \Pi(C(\mathrm{A}_4), \alpha, (12))$ (as in Definition 3.4.1) associated with the codeword $\alpha = \alpha(1) = 1234$, the permutation $(12) \in C(\mathrm{S}_4) \cap L$, where L is the top group of $\mathrm{Aut}(\Gamma)$. The vertices of Π are labelled by M. In the graph on the left, the vertex set is $Q \times M$ and the edges are pairs $(a, i), (b, j) \in Q \times M$ such that there exists a $(C(\mathrm{A}_q), \alpha, (12))$-associate π where $\pi_i = a \neq \alpha_i$ and $\pi_j = b \neq \alpha_j$.

3.4 Associate graphs

In order to analyse the structure of an elusive code, the next definition introduces a graph with vertex set M and edges given by an appropriate set of associates. From there, the property exhibited by $C(\mathrm{A}_q, n)$ in Proposition 3.3.9 is used to give a condition which guarantees $q \mid m$ in an elusive code.

Definition 3.4.1. Let (C, α, x) be an elusive triple. The *associate graph* $\Pi(C, \alpha, x)$ is the graph with vertex set M and an edge between $i, j \in M$ whenever there is a (C, α, x)-associate $\pi = \gamma(\alpha|i, j|a, b) \in \Gamma_2(\alpha) \cap C^x$ for some $a \neq \alpha_i$ and $b \neq \alpha_j$.

Lemma 3.4.2. *Let (C, α, x) be an elusive triple with $\delta \geqslant 3$. Then the graph $\Pi(C, \alpha, x)$, as in Definition 3.4.1, is a simple, regular graph with valency $q - 1$.*

Proof. There are no loops in $\Pi(C, \alpha, x)$ since $\pi = \gamma(\alpha|i, j|a, b) \in \Gamma_2(\alpha) \cap C^x$ implies $i \neq j$. Suppose $\pi = \gamma(\alpha|i, j|a, b)$ and $\pi' = \gamma(\alpha|i, j|a', b')$ are distinct associates. Then $d(\pi, \pi') \leqslant 2$, but π, π' are in the code C^x, which is equivalent to C, so this contradicts $\delta \geqslant 3$. Thus, there are no multiple edges in $\Pi(C, \alpha, x)$ and it is simple. By Lemma 3.1.1, the set of associates $\Gamma_2(\alpha) \cap C^x$ corresponds to a partition of $\Gamma_1(\alpha)$ with $m(q-1)/2$ parts of size 2, and each part corresponds to an edge of $\Pi(C, \alpha, x)$, namely the associate $\pi = \gamma(\alpha|i, j|a, b)$ corresponds to the part $\{\gamma(\alpha|i|a), \gamma(\alpha|j|b)\}$ and the edge $\{i, j\}$ of $\Pi(C, \alpha, x)$. Since we have a partition of $\Gamma_1(\alpha)$, for any i the vertex $\gamma(\alpha|i|a)$ appears in a part for each $a \in Q \setminus \{\alpha_i\}$. Hence the vertex i of $\Pi(C, \alpha, x)$ is incident with exactly $q-1$ edges, so $\Pi(C, \alpha, x)$ is regular of valency $q-1$. □

Corollary 3.4.3. *Suppose (C, α, x) is an elusive triple with parameters (m, q, δ), where $\delta \geqslant 3$. Then $m \geqslant q$.*

Proof. The associate graph $\Pi(C, \alpha, x)$ has m vertices, each adjacent to $q - 1$ other vertices by Lemma 3.4.2, so $m \geqslant q$. □

Lemma 3.4.4. *Let (C, α, x) be an elusive triple with $\delta \geqslant 3$ and π be a (C, α, x)-associate. Then there are $2q-4$ associates π' such that $d(\pi, \pi') = 3$.*

Proof. In the associate graph $\Pi(C, \alpha, x)$, an associate $\pi = \gamma(\alpha|i, j|a, b)$ represents an edge between vertices i and j. Any other edge incident with vertex i or j represents an associate π' such that $d(\pi, \pi') = 3$. Since $\Pi(C, \alpha, x)$ is $(q-1)$-regular, by Lemma 3.4.2, there are $q-2$ other edges incident with each vertex i and j. Hence there are $2(q-2)$ such π'. □

Finally in this section we prove Theorem 3.2.

Proof of Theorem 3.2. Let (C, α, x) be an elusive triple with parameters $(m, q, 3)$ such that, for distinct $\pi, \pi' \in \Gamma_2(\alpha) \cap C^x$ with $d(\pi, \pi') = 3$ we have $\mathrm{MC}(\pi, \pi') = 3$. Without loss of generality, let $M = \{0, \ldots, m-1\}$, $Q = \{0, \ldots, q-1\}$ and $\alpha = \mathbf{0}$. Consider the graph $\Pi(C, \alpha, x)$, defined in Definition 3.4.1, and the vertex $i \in M$. Using the automorphism $\sigma = (0, i) \in K \cong \mathrm{S}_m$ we can set $i = 0$ by Lemma 3.1.2, replacing C with C^σ.

By Lemma 3.4.2 there are edges between 0 and $q-1$ other vertices, say $j_1, \ldots, j_{q-1}$, with corresponding associates $\pi_i = \gamma(\mathbf{0}|0, j_i|a_i, b_i)$ for some $a_i, b_i \in Q \setminus \{0\}$. Again we apply Lemma 3.1.2, using an automorphism $y = \sigma h \in \mathrm{Aut}(\Gamma)$, where $\sigma \in K$ such that $j_i^\sigma = i$ and $h = (h_0, \ldots, h_{m-1}) \in N \cong \mathrm{S}_q^m$ such that $a_i^{h_0} = i$ and $h_i = (b_i, 1)$ for $i \in \{1, \ldots, q-1\}$ with $h_i = 1$ for $q \leqslant i \leqslant m$. Replacing C by C^y, we may assume that the vertex $0 \in M$ is adjacent to the vertices $i = 1, \ldots, q-1 \in M$, each edge having corresponding associate $\pi_i = \gamma(\mathbf{0}|0, i|i, 1)$. Recall that $\mathrm{diff}(\mu, \nu)$ denotes the set of entries in which vertices $\mu, \nu \in H(m, q)$ differ. Then, for each i, $\mathrm{diff}(\mathbf{0}, \pi_i) = \{0, i\}$, and for $i \neq j$, $\mathrm{diff}(\pi_i, \pi_j) = \{0, i, j\}$ so $d(\pi_i, \pi_j) = 3$.

Since $d(\pi_1, \pi_i) = 3$ for $i \in Q \setminus \{0, 1\}$, and by assumption $\mathrm{MC}(\pi_1, \pi_i) = 3$, we can apply Lemma 3.2.5. In particular $\mathrm{diff}(\mathbf{0}, \pi_1) \cap \mathrm{diff}(\mathbf{0}, \pi_i) = \{0\}$, so for each $i \in Q \setminus \{0, 1\}$ the third codeword listed in Lemma 3.2.5, applied to π_1, π_i, is $\beta_i = \gamma(\mathbf{0}|1, 0, i|a_i, 1, 1) \in C$, for some $a_i \in Q \setminus \{0, 1\}$ (note that we write this as $\gamma(\mathbf{0}|0, 1, i|1, a_i, 1)$ below). Moreover, the a_i are pairwise distinct, since $\delta = 3$. Note that this implies that every possible value for a_i occurs, since there are $q-2$ choices for both i and a_i.

Suppose the connected component of $\Pi(C, \alpha, x)$ containing the vertex 0 has more than q vertices. The vertex 0 is connected to the vertices $1, \ldots, q-1$, so there would need to be an edge from some vertex $i \in \{1, \ldots, q-1\}$ to a vertex $j \geqslant q$. Then we have a corresponding associate $\pi' = \gamma(\mathbf{0}|i, j|b_i, b_j)$. Let $\sigma = (1, i)(q, j) \in K$ and $h = (h_0, \ldots, h_{m-1})$ with $h_0 = (1, i)$, $h_i = (2, b_i)$, $h_j = (1, b_j)$ and $h_k = 1$ otherwise. Then $h\sigma$ swaps π_1 with π_i and fixes π_k for $k \neq 1, i$. Thus, replacing C by $C^{h\sigma}$, we can assume that $i = 1$ and $j = q$, the edge corresponds to the associate $\pi' = \gamma(\mathbf{0}|1, q|2, 1)$, and $\mathrm{diff}(\mathbf{0}, \pi') = \{1, q\}$.

Again, Lemma 3.2.5 allows us to determine the form of some codewords. In particular, substituting $\pi_1, \pi' \in \Gamma_2(\alpha) \cap C^x$ into the codeword given by the second element of the set (3.2.5) gives $\beta' = \gamma(\mathbf{0}|0, 1, q|1, 2, b) \in C$, for some $b \in Q \setminus \{0, 1\}$. However, from the previous

paragraph there exists i such that $a_i = 2$ and for this i the codeword $\beta_i = \gamma(\mathbf{0}|0,1,i|1,2,1) \in C$. This gives us a contradiction, since $d(\beta', \beta_i) = 2$. Thus there are q vertices in each connected component of $\Pi(C, \alpha, x)$ and, as the number of vertices in total is m, we see that q must divide m. □

Corollary 3.4.5. *If the hypotheses of Theorem 3.2 hold for the elusive triple (C, α, x) then the associate graph $\Pi(C, \alpha, x) = \frac{m}{q} \mathrm{K}_q$.*

3.5 Elusive Reed-Muller codes

Throughout this section let $M = \mathbb{F}_q^d$, $Q = \mathbb{F}_q$ and, as in (3.1), let $k = (q-1)d - 2$. Let $C = \mathcal{RM}_q(k, d)$ and $C' = \mathcal{RM}_q(k+1, d) = \mathrm{Rep}(q^d, q)^\perp$, see (3.2) and (3.3), in $H(q^d, q)$ with $X = \mathrm{Aut}(C)$ and $X_1 = \mathrm{Aut}(C_1)$. The next lemma states some well-known facts about C', the dual of the repetition code, which can be found, for instance, in [79].

Lemma 3.5.1. *The code C' is linear with dimension $q^d - 1$, minimum distance $\delta' = 2$, covering radius $\rho' = 1$ and $|{C'}_1| = (q-1)q^{q^d-1}$.*

Whilst the next result is known (see [2, Corollary 5.5.4 and Theorem 5.4.1]), it is included here because of the fact that it introduces ideas used in subsequent proofs.

Lemma 3.5.2. *The code C has covering radius $\rho = 2$, dimension $q^d - (d+1)$, and minimum distance*

$$\delta = \begin{cases} 4 & \text{if} \quad q = 2, d \geqslant 2, \\ 3 & \text{if} \quad q \geqslant 3, d \geqslant 1. \end{cases}$$

Furthermore, the set of neighbours satisfies $C_1 = {C'}_1$.

Proof. Let δ' and ρ' be the minimum distance and covering radius, respectively, of C', as in Lemma 3.5.1.

The conditions in (3.2) and (3.3) comprise $d+1$ independent linear equations. To see this, consider the matrix formed by the coefficients of (3.3). The columns are the vectors of $\mathbb{F}_q^d$ and thus this matrix has rank d. Moreover, the coefficient of α_0 is 0 in each equation from (3.3), but is 1 in (3.2). Hence, C is linear of dimension $q^d - (d+1)$.

Note that $C \subseteq C'$, so $\delta \geqslant \delta' = 2$, by Lemma 3.5.1. Let α be a weight 2 vertex in $H(q^d, q)$. Then, there exists some $u, v \in M$ with $u \neq v$, $\alpha_u = a$, $\alpha_v = b$, and $\alpha_w = 0$ for all $w \neq u, v$. By (3.2) we have $b = -a$. However then $\sum_{w \in M} \alpha_w w = au - av$, and thus $\alpha \notin C$, since $u \neq v$. If $q = 2$, then no weight 3 vector satisfies (3.2). Moreover, let α be the weight 4 vertex $\alpha_0 = 1$, $\alpha_{e_1} = 1$, $\alpha_{e_2} = 1$, $\alpha_{e_1+e_2} = 1$, and $\alpha_v = 0$ for $v \neq 0, e_1, e_2, e_1 + e_2$. Then $\alpha \in C$. If $q \geqslant 3$, let α be the weight 3 vertex such that $\alpha_0 = 1$, $\alpha_{e_1} = 1$, $\alpha_{-e_1} = 1$, and $\alpha_v = 0$ for $v \neq 0, e_1, -e_1$. Then $\alpha \in C$. Thus δ is as above.

Let $\beta \in H(q^d, q)$, $a = \sum_{v \in M} \beta_v$ and $u = \sum_{v \in M} \beta_v v$. If $a \neq 0$, then there exists $\beta' \in C$ with $d(\beta, \beta') = 1$, where $\beta'_{a^{-1}u} = \beta_{a^{-1}u} - a$, and $\beta'_v = \beta_v$ for $v \neq a^{-1}u$. If $a = 0$ and $u = 0$

then $\beta \in C$. If $u \neq 0$ then there exists $\beta' \in C$ with $d(\beta, \beta') = 2$, where $\beta'_u = \beta_u - 1$, $\beta'_0 = \beta_0 + 1$ and $\beta'_v = \beta_v$ for $v \neq 0, u$. Thus $\rho = 2$.

Now, $|C| = q^{q^d-(d+1)}$. Since $\delta' = 2$ and $C \subset C'$ it follows that $C_1 \subseteq C'_1$. Also, since $\delta \geqslant 3$, $|C_1| = m(q-1)|C| = q^d(q-1)q^{q^d-(d+1)} = q^{q^d} - q^{q^d-1}$, and thus $C_1 = C'_1$ by Lemma 3.5.1. □

Lemma 3.5.3. *The Reed-Muller code $C = \mathcal{RM}_q(k, d)$ is an elusive code.*

Proof. Now $X_1 = \mathrm{Aut}(C'))$ because, by Lemma 3.5.2, $C_1 = C'_1$, and, by Lemma 3.5.1, $V\Gamma = C' \cup C'_1$. Since C' is linear, $X_1 (= \mathrm{Aut}(C'))$ contains the translation t_α for each $\alpha \in C'$. If $\alpha \in C' \setminus C$ then t_α does not fix C setwise, so $t_\alpha \notin X$, and hence the image $C^{t_\alpha} \neq C$, so C is 1-elusive. □

Recall from Section 2.3 that $\mathrm{PermAut}(C) = \mathrm{Aut}(C) \cap L$ is the group of pure permutations on entries fixing the code C. By [7, Theorem 5], $\mathrm{PermAut}(C) \cong \mathrm{AGL}(d, q)$. Since C' is the dual of the repetition code in $H(m, q)$, it follows that $\mathrm{PermAut}(\mathcal{RM}_q(k+1, d)) \cong \mathrm{S}_m$.

Proof of Theorem 3.4. If p is the characteristic of the field $\mathbb{F}_q$, then any non-trivial translation in X_1 has order p. As in the proof of Lemma 3.5.3 there is a translation in $X_1 \setminus X$, so there are at least p distinct images of C under elements of X_1. Note also that $\sigma \in \mathrm{Aut}(C')$ for any $\sigma \in \mathrm{Sym}(M)$, where σ acts by permuting entries. However, by [7, Theorem 5], $\sigma \in \mathrm{PermAut}(C)$ if and only if $\sigma \in \mathrm{AGL}(d, q)$. Thus if $\sigma \in \mathrm{Sym}(M) \setminus \mathrm{AGL}(d, q)$, then $C^\sigma \neq C$. However $\mathbf{0} \in C^\sigma \cap C$. □

Lemma 3.5.4. *The Reed-Muller code $C = \mathcal{RM}_q(k, d)$ is X-completely transitive.*

Proof. Since C is linear, X is transitive on C. Since $\delta \geqslant 3$, $\mathbf{0} \in C$ and X is transitive on C, to prove that X is transitive on C_1 it is sufficient to prove $X_{\mathbf{0}}$ is transitive on the set of weight one vertices. Let ν be the weight one vertex with $\nu_k = a \in Q^\times$ for a unique $k \in M$. By [7, Theorem 5], $\mathrm{PermAut}(\mathcal{RM}_q(k, d)) \cong \mathrm{AGL}(d, q)$ acting 2-transitively as pure permutations on entries. Since C is linear X also contains a subgroup isomorphic to the multiplicative group $\mathbb{F}_q^\times$ acting as scalar multiplication. Hence, multiplying by a^{-1} and then applying a permutation of the entries $\sigma \in X$ which maps k to $0 \in M$, will map ν to the weight one vertex μ with $\mu_0 = 1$.

We now prove X is transitive on C_2. Recall $C' = \mathcal{RM}_q(k+1, d)$. Now $\Gamma_2(\mathbf{0})$ consists of the weight two vertices ν with $\nu_j = a \in Q^\times$, $\nu_k = -a$ for distinct $j, k \in M$. To see this, first note that each such vertex ν satisfies the condition in (3.2), but not the conditions in (3.3) and so $\nu \in C \setminus C'$. By Lemma 3.5.1, C' has minimum distance 2 and, by Lemma 3.5.2, $C_1 = C'_1$, and thus $\nu \in C_2$. Now let ν' be an arbitrary vertex in $\Gamma_2(\mathbf{0})$, with $\nu'_j \neq 0$,$\nu'_k \neq 0$, for some $j \neq k$. If $\nu_j \neq -\nu_k$ then $\nu \in C_1$ since then, by (3.3), C contains the weight three vertex $\alpha \in \Gamma_1(\nu)$ with $\alpha_j = \nu'_j$, $\alpha_k = \nu'_k$ and $\alpha_{j+k} = -\nu'_j - \nu'_k$. Finally, we can map $\nu \in \Gamma_2(\mathbf{0}) \cap C_2$ to the weight two vertex μ, where $\mu_0 = 1$, $\mu_{e_1} = -1$, by multiplying by a^{-1} and then applying a permutation of entries $\sigma \in X$ which maps the pair (u, v) to $(0, e_1)$. □

The next two results show that most of the elusive triples in this section do not satisfy the conditions of Theorem 3.2.

Proposition 3.5.5. *Let $C = \mathcal{RM}_q(s-1,d)$, (C,α,x) be an elusive triple, and π be a (C,α,x)-associate. Then if,*

1. $q \equiv 0 \pmod 3$ *there are at most two (C,α,x)-associates π' such that* $\mathrm{MC}(\pi,\pi') = 3$,
2. $q \equiv 1 \pmod 3$ *there are at most four (C,α,x)-associates π' such that* $\mathrm{MC}(\pi,\pi') = 3$,
3. $q \equiv 2 \pmod 3$ *there are no (C,α,x)-associates π' such that* $\mathrm{MC}(\pi,\pi') = 3$.

Proof. Since X is transitive on C, by Lemma 3.1.2, we can assume $\alpha = \mathbf{0}$. By (3.2) any associate has the form $\pi = \gamma(\mathbf{0}|u,v|a,-a)$. However, by Lemma 3.1.2 and the fact that $\mathrm{AGL}(d,q)$ is 2-transitive, using an appropriate automorphism $\sigma \in \mathrm{AGL}(d,q) \leqslant \mathrm{PermAut}(C)$ and scalar multiplication by a^{-1}, we can, without loss of generality, let $\pi = \gamma(\mathbf{0}|0,e_1|1,-1)$.

By Lemma 3.4.4, there are a total of $(2q-4)$ $(C,\mathbf{0},x)$-associates at distance 3 from π. These are $\pi_{u,a} = \gamma(\mathbf{0}|u,v|a,-a)$, for some $v \in M$, by (3.2), where $u = 0$ and $a \in Q \setminus \{0,1\}$, or $u = e_1$ and $a \in Q \setminus \{0,-1\}$.

Suppose $\mathrm{MC}(\pi,\pi_{u,a}) = 3$, for some choice of u and a. By Lemma 3.2.5, $C \cap \Gamma_2(\pi) \cap \Gamma_2(\pi_{u,a})$ contains, depending on u and a, $\gamma(\mathbf{0}|0,e_1,v|a,-1,b_1)$ and $\gamma(\mathbf{0}|0,e_1,v|1,b_2,-a)$, if $u = 0$, or $\gamma(\mathbf{0}|0,e_1,v|b_3,-1,-a)$ and $\gamma(\mathbf{0}|0,e_1,v|1,a,b_4)$, if $u = e_1$, where $b_1 \in Q \setminus \{0,-a\}$, $b_2 \in Q \setminus \{0,-1\}$, $b_3 \in Q \setminus \{0,1\}$, and $b_4 \in Q \setminus \{0,-a\}$.

By (3.2), $b_1 = 1-a$ and $b_2 = a-1$, if $u = 0$, or $b_3 = a+1$ and $b_4 = -a-1$, if $u = e_1$. By (3.3), we then have $(1-a)v = e_1$ and $(a-1)e_1 = av$, if $u = 0$, or $e_1 = -av$ and $ae_1 = (a+1)v$, if $u = e_1$. Thus $(1-a)(a-1) = a$, if $u = 0$, or $-a^2 = a+1$, if $u = e_1$, that is, $a^2 - a + 1 = 0$, if $u = 0$, or $a^2 + a + 1 = 0$, if $u = e_1$.

Consider the case $u = 0$. Here a is a solution to the equation $x^2 - x + 1 = 0$. If $a = -1$ then $a^2 - a + 1 = 3 \equiv 0 \pmod q$, hence, $q \equiv 0 \pmod 3$. In this case $x^2 - x + 1 = x^2 + 2x + 1 = (x+1)^2$, and $x = a = -1$ is the only solution. Suppose $a \neq -1$, then a is a solution of $(1+x)(x^2 - x + 1) = x^3 + 1$ so $a = -c, -c^2$, where c is a primitive cube root of 1 in $\mathbb{F}_q$, and hence $3 \mid q-1$. We can deduce that $x^2 - x + 1$ is irreducible over $\mathbb{F}_q$ if $q \equiv 2 \pmod 3$.

Now let $u = e_1$. So a is a solution to the equation $x^2 + x + 1 = 0$. If $a = 1$ then $a^2 + a + 1 = 3 \equiv 0 \pmod q$, and thus $q \equiv 0 \pmod 3$. We then have $x^2 + x + 1 = x^2 - 2x + 1 = (x-1)^2$, and $x = a = 1$ is the only solution. Suppose $a \neq 1$, then a is a solution to $(x-1)(x^2 + x + 1) = x^3 - 1$ so $a = c, c^2$, where c is a primitive cube root of 1 in $\mathbb{F}_q$, and hence $3 \mid q-1$. We can deduce that $x^2 + x + 1$ is irreducible over $\mathbb{F}_q$ if $q \equiv 2 \pmod 3$.

If $q \equiv 2 \pmod 3$ there are no solutions to the required equations, so there are no associates at distance 3 from π with three mutual codewords.

If $q \equiv 0 \pmod 3$ we have at most two associates, one choice of a for each $u \in \{0,e_1\}$, namely $\pi_{0,-1} = \gamma(\mathbf{0}|0,-e_1|-1,1)$ and $\pi_{e_1,1} = \gamma(\mathbf{0}|e_1,-e_1|1,-1)$ at distance 3 from π, with the mutual codewords $\mathbf{0}$, $\gamma(\mathbf{0}|0,e_1,-e_1|1,1,1)$, and $\gamma(\mathbf{0}|0,e_1,-e_1|-1,-1,-1)$.

If $q \equiv 1 \pmod 3$, then there are at most four associates, since given $u \in \{0, e_1\}$ there are two choices for a. These are $\pi_{0,-c} = \gamma(\mathbf{0}|0, (1+c)^{-1}e_1| - c, c)$, $\pi_{0,-c^2} = \gamma(\mathbf{0}|0, (1+c^2)^{-1}e_1| - c^2, c^2)$, $\pi_{e_1,c} = \gamma(\mathbf{0}|e_1, -c^{-1}e_1|c, -c)$, and $\pi_{e_1,c^2} = \gamma(\mathbf{0}|e_1, -c^{-2}e_1|c^2, -c^2)$. □

Corollary 3.5.6. *If $q \neq 3, 4$ and $C = \mathcal{RM}_q(s-1, d)$, then there is no elusive triple (C, α, x) satisfying the hypotheses of Theorem 3.2.*

Proof. Let π be a (C, α, x)-associate. If $q = 2$, then there are no associates π' at distance 3 from π. Hence, by Lemma 3.2.3, $\mathrm{MC}(\pi, \pi') \neq 3$ for all associates π'. Suppose $q \geqslant 5$. By Lemma 3.4.4 there are 6 associates π' such that $d(\pi, \pi') = 3$. However by Proposition 3.5.5 at most four of these have $\mathrm{MC}(\pi, \pi') = 3$. Hence it is not possible that $\mathrm{MC}(\pi, \pi') = 3$ for all (C, α, x)-associates π, π' at distance 3. □

The three results Lemma 3.5.3, Lemma 3.5.4 and Corollary 3.5.6 combine to give a proof of Theorem 3.3. Finally, we give an example with $\mathrm{MC}(\pi, \pi') = 1$ for some associates π, π', showing that the lower bound in Corollary 3.2.6 can be attained.

Example 3.5.7. *Consider $C = \mathcal{RM}_2(1, 3)$. Let $x = t_\beta\sigma$, where t_β is the translation induced by $\beta = \gamma(\mathbf{0}|e_1, e_1+e_2+e_3|1, 1)$, and $\sigma = (\mathbf{0}, e_1+e_2+e_3)$. Then $\pi, \pi' \in \Gamma_2(\mathbf{0}) \cap C^x$, where $\pi = \gamma(\mathbf{0}|0, e_1|1, 1)$ and $\pi' = \gamma(\mathbf{0}|e_2, e_3|1, 1)$, since $\mathbf{0}^x = \pi$ and*

$$\gamma(\mathbf{0}|e_1, e_2, e_3, e_1+e_2+e_3|1, 1, 1, 1)^x = \pi'.$$

By Lemma 3.2.2, if $\alpha \in \Gamma_2(\pi) \cap \Gamma_2(\pi')$ then $\alpha = \mathbf{0}$ or $\gamma(\mathbf{0}|0, e_1, e_2, e_3|1, 1, 1, 1)$. However, by (3.3), $\gamma(\mathbf{0}|0, e_1, e_2, e_3|1, 1, 1, 1) \notin C$ since $e_1+e_2+e_3 \neq \mathbf{0}$. Thus $\mathrm{MC}(\pi, \pi') = 1$.

Designs and s-Elusive Codes

A construction was given in [56] for each $q \geqslant 3$ of an infinite family of 1-elusive codes with $\delta = 3$. It was observed in that paper that for all known examples the length m of the code is divisible by the alphabet size q. This led the authors to ask if q must always divide m [56, Question 1.3]. This was known to be true in the binary case, since $m(q-1) = m$ must be even by [43, Theorem 1], regardless of δ. We would like to record that the answer to the question is 'yes', for all q (Lemma 4.1.2). We thank Andries Brouwer for sending us this argument in private correspondence, generalising partial results of the author in [42].

In Section 4.2 we show that any s-elusive code has a set of q-ary s-$(m, 2s, 1)$ designs associated to it. This fact allows us to identify infinitely many 2-elusive codes, and even a 3-elusive code. See Section 4.2 for the definition of $\mathcal{P}(2d)$.

Theorem 4.1. *1. The Preparata codes $\mathcal{P}(2d)$ are 2-elusive with minimum distance $\delta = 6$.*

2. The punctured code of the even weight binary perfect Golay code is 3-elusive with minimum distance $\delta = 7$.

4.1 Alphabet size divides length

We were made aware of the following argument in private correspondence with Andries Brouwer.

The *adjacency matrix* of a graph has rows and columns indexed by the vertices of the graph, with an entry 1 if the corresponding vertices are adjacent and 0 otherwise. Let A be the adjacency matrix of the Hamming graph. A subset of the vertex set of a graph, and hence a code C, can be represented by a *characteristic vector* $u = u(C)$, where the entries are labelled by the vertices of the graph and take the value 1 if the vertex is in C and 0 otherwise. If the entries of A and u are thought of as elements of $\mathbb{R}$, it follows that Au is related to the characteristic vector of C_1, in that the entry of Au is $|\Gamma_1(\beta) \cap C|$. In particular, if $\delta \geqslant 3$ then $Au = u(C_1)$. A similar argument shows that, if $\delta \geqslant 2s+1$, then $A^s u(C) = u(C_s)$.

Proposition 4.1.1. *Let $s \in \{1, \ldots, \rho\}$ and suppose there exist distinct codes C and C' in $H(m, q)$ such that $C_s = C'_s$, with both C and C' having minimum distance at least $2s+1$. Then q divides m.*

Proof. Let A be the adjacency matrix of the Hamming graph $H(m, q)$ and let $u = u(C)$, $v = u(C')$. Since both C and C' have minimum distance at least $2s+1$, we have $A^s u = A^s v$. Since $u \neq v$, A is singular and has at least one zero eigenvalue. The Hamming graph is the Cartesian product of m copies of the complete graph on q vertices K_q. Hence, by [30, Theorem 2.3.4], and the fact that the eigenvalues of K_q are -1 and $q-1$, we see that the Hamming graph has eigenvalues $(m-i)(q-1) - i = (q-1)m - iq$, where $0 \leqslant i \leqslant m$. Since A has an eigenvalue zero, we have $(q-1)m - iq = 0$, for some integer i, and hence $q \mid m$. □

Corollary 4.1.2. *Let C be an s-elusive code in $H(m,q)$ with $\delta \geqslant 3$. Then q divides m.*

Proof. If C is an s-elusive code, then there exists $x \in X \setminus X_s$ such that $C^x \neq C$ but $C_s^x = C_s$. Hence we can apply Lemma 4.1.1. □

4.2 s-Elusive codes

Recall, for a code C we let $X = \mathrm{Aut}(C)$ and $X_s = \mathrm{Aut}(C_s)$, and C is *s-elusive* if X_s is strictly larger than X. Note that for any $x \in X_s$ we have that C^x is an equivalent code to C, and thus has the same size and minimum distance, and has conjugate automorphism group.

Lemma 4.2.1. *Let C be an s-elusive code and $x \in X_s$. Then $(C_s)^x = (C^x)_s = C_s$.*

Proof. Note that $x \in \mathrm{Aut}(C_s)$ and thus fixes C_s setwise, so it follows that $(C_s)^x = C_s$. It remains to show that $(C^x)_s = C_s$. Let $\nu \in C_s$ be distance s from $\alpha \in C$. Then $d(\nu^x, \alpha^x) = s$. Suppose there exists some $\beta \in C^x$ such that $d(\nu, \beta) < s$. Then $d(\nu^{x^{-1}}, \beta^{x^{-1}}) < s$, however $\beta^{x^{-1}} \in C$, contradicting the fact that x fixes C_s setwise. Hence $\nu \in (C^x)_s$ and thus $(C^x)_s = C_s$, as these sets have the same size. □

If C is an s-elusive code then there exists an automorphism $x \in X_s \setminus X$. This implies that $C^x \neq C$, so that there is some codeword $\alpha \in C$ such that $\alpha^x \notin C$.

Definition 4.2.2. Let C be an s-elusive code in $H(m,q)$, $x \in X_s \setminus X$ and $\alpha \in C$ such that $\alpha^x \notin C$. Then we call the triple (C, α, x) an *s-elusive triple*.

Lemma 4.2.3. *Let (C, α, x) be an s-elusive triple in $H(m,q)$ with $\delta \geqslant 2s+1$. For all $\nu \in \Gamma_s(\alpha)$ there exists a unique $\pi \in C_{2s} \cap \Gamma_s(\nu)$ such that $\pi \in C^x$.*

Proof. Since $\delta \geqslant 2s+1$, we have the disjoint union $C_s = \cup_{\gamma \in C} \Gamma_s(\gamma)$. Now C^x is equivalent to C and, by Lemma 4.2.1, $C_s^x = C_s$. Thus each $\nu \in C_s$ is distance s from some vertex π in C^x. That is, if $\nu \in \Gamma_s(\alpha)$ then there exists some vertex $\pi \in \Gamma_s(\nu) \cap C^x$. Now, $d(\alpha, \pi) \leqslant d(\alpha, \nu) + d(\nu, \pi) = 2s$ and hence $\pi \notin C$ since $\delta \geqslant 2s+1$. Moreover, this means $\pi \in C_k$, for some k such that $1 \leqslant k \leqslant 2s$.

Suppose $\pi \in C_k$, where $1 \leqslant k < 2s$. Then there exists $\beta \in C$ such that $\pi \in \Gamma_k(\beta)$, in particular there is a path of length k from β to π. Choose a vertex μ on this path, such that $\mu \in \Gamma_s(\beta)$. Then $\mu \in C_s$, however $d(\pi, \mu) = k - s < s$ contradicting the fact that $C_s^x = C_s$.

Suppose there exists $\pi' \in \Gamma_s(\nu) \cap C^x$ such that $\pi' \neq \pi$. Then π, π' are in the code C^x which is equivalent to C. However $d(\pi, \pi') \leqslant d(\pi, \nu) + d(\nu, \pi') = 2s$ contradicting $\delta = 2s+1$. Thus π is unique. □

The next definition introduces the concept of a q-ary t-design, which allows us to describe the structure of an s-elusive code. Designs arise in many other contexts, for instance when considering s-regular codes [32]. First we need the notion of *covering* a vertex.

Definition 4.2.4. Let $0 \in Q$; $\nu, \alpha \in H(m,q)$. The vertex ν is said to be *covered* by α, if for every $i \in M$ such that $\nu_i \neq 0$ we have $\nu_i = \alpha_i$.

In other words α *covers* ν if each non-zero entry of ν agrees with the corresponding entry of α.

Definition 4.2.5. A q-*ary* t-(m,k,λ) *design* consists of a subset $\mathcal{D}$ of vertices of $\Gamma_k(\mathbf{0})$ such that each vertex $\nu \in \Gamma_t(\mathbf{0})$ is covered by exactly λ vertices of $\mathcal{D}$. When $q = 2$, $\mathcal{D}$ is simply a t-(m,k,λ) design and if additionally $\lambda = 1$, $\mathcal{D}$ is called an $S(t,k,m)$-Steiner system.

Lemma 4.2.6. *Let $(C, \mathbf{0}, x)$ be an s-elusive triple in $H(m,q)$ with $\delta \geqslant 2s+1$. The set $\Gamma_{2s}(\mathbf{0}) \cap C^x$ forms a q-ary s-$(m,2s,1)$-design. In particular, if $q = 2$, then $\Gamma_{2s}(\mathbf{0}) \cap C^x$ forms an $S(s,2s,m)$-Steiner system.*

Proof. By Lemma 4.2.3, every vertex of $\Gamma_s(\mathbf{0})$ is covered by a unique element of $\Gamma_{2s}(\mathbf{0}) \cap C^x$, with respect to $\mathbf{0}$ and thus the result follows. □

The Preparata codes are a family of binary codes of length 2^{2d} for each integer $d \geqslant 2$. For a full definition see [25, (16.12)], taking note that we denote their $\bar{\mathcal{P}}(\sigma)$ as $\mathcal{P}(2d)$, with σ arbitrary. Also, since $q = 2$ in the following, we write $\mathcal{RM}(2d,2d) = \mathcal{RM}_2(2d,2d)$.

Lemma 4.2.7. *The Preparata codes $\mathcal{P}(2d)$ are 2-elusive codes.*

Proof. To prove this we will show that the 2-neighbour sets $\mathcal{P}(2d)_2$ and $\mathcal{RM}(2d,2d)_2$ are equal and that $\mathcal{P}(2d)$ is properly contained in $\mathcal{RM}(2d,2d)$. It will then follow that the automorphism group of $\mathcal{RM}(2d,2d)$ fixes $\mathcal{P}(2d)_2$ but not $\mathcal{P}(2d)$, since $\mathrm{Aut}(\mathcal{RM}(2d,2d))$ contains the translations by any codeword. Thus $\mathcal{P}(2d)$ is 2-elusive.

By [25, (16.12) (a) and (b)] we have $\mathcal{P}(2d) \subset \mathcal{RM}(2d,2d)$. Since $\delta(\mathcal{RM}(2d,2d)) = 4$ it follows that $\mathcal{P}(2d)_2 \subset \mathcal{RM}(2d,2d)_2$. We now show that the 2-neighbour sets have the same size, and are thus equal. Now, by Lemma 3.5.2, $\mathcal{RM}(2d,2d)$ has covering radius 2 and dimension $2^{2d} - 2d - 1$. Hence $H(2^{2d},2) = \mathcal{RM}(2d,2d) \cup \mathcal{RM}(2d,2d)_1 \cup \mathcal{RM}(2d,2d)_2$. This gives

$$\begin{aligned}|\mathcal{RM}(2d,2d)_2| &= |H(2^{2d},2)| - |\mathcal{RM}(2d,2d)| - |\mathcal{RM}(2d,2d)_1| \\ &= 2^{2^{2d}} - 2^{2^{2d}-2d-1} - 2^{2^{2d}-2d-1}.2^{2d} \\ &= 2^{2^{2d}-1} - 2^{2^{2d}-2d-1}.\end{aligned}$$

Furthermore, by [25, (16.16)], $\mathcal{P}(2d)$ has minimum distance 6 so is properly contained in $\mathcal{RM}(2d,2d)$. This also gives,

$$\begin{aligned}|\mathcal{P}(2d)_2| &= |\mathcal{P}(2d)|\binom{m}{2}(q-1)^2 \\ &= 2^{2^{2d}-4d}2^{2d-1}(2^{2d}-1) \\ &= 2^{2^{2d}-1} - 2^{2^{2d}-2d-1}.\end{aligned}$$

□

Corollary 4.2.8. *Let $\alpha \in \mathcal{P}(2d)$ and $x \in X_2 \backslash X$. Then $\Gamma_4(\mathbf{0}) \cap \mathcal{P}(2d)^x$ is an $S(2, 4, 2^{2d})$-Steiner system.*

Proof. This follows from Lemma 4.2.6 and Lemma 4.2.7. □

There exists a 3-$(22, 6, 1)$-design, namely the Witt design W_{22}. This suggests an elusive code with these parameters may exist. Indeed, if we take the even weight subcode of the binary perfect Golay code $\mathcal{G}_{23}$ and puncture the resulting code we find that this code is 3-elusive.

Proposition 4.2.9. *Let $\mathcal{PG}$ and $\mathcal{EG}$ be the codes obtained by puncturing the binary perfect Golay code $\mathcal{G}_{23}$ and the even weight subcode of the Golay code $\mathcal{G}_{23}$, respectively. Then $\mathcal{PG}_3 = \mathcal{EG}_3$ and $\mathcal{EG}$ is 3-elusive with minimum distance $\delta = 7$.*

Proof. Now $\mathcal{G}_{23}$ is a linear $[23, 12, 7]$ code with covering radius 3, and $\mathrm{Aut}(\mathcal{G})^M \cong \mathrm{M}_{23}$ is transitive on M. Thus, puncturing $\mathcal{G}_{23}$ results in the linear $[22, 12, 6]$ code $\mathcal{PG}$ with covering radius $\rho = 3$. The even weight subcode of $\mathcal{G}$ is a linear $[23, 11, 8]$ code, again with M_{23} acting on entries, so puncturing results in the $[22, 11, 7]$ code $\mathcal{EG}$.

Since $\mathcal{PG}$ has covering radius 3 and minimum distance 6 it follows that $V\Gamma = \mathcal{PG} \cup \mathcal{PG}_1 \cup \mathcal{PG}_2 \cup \mathcal{PG}_3$, where this union is disjoint. So,

$$\begin{aligned}
|\mathcal{PG}_3| =& |V\Gamma| - |\mathcal{PG}| - |\mathcal{PG}_1| - |\mathcal{PG}_2| \\
=& 2^{22} - 2^{12} - 2^{12}.22 - 2^{12}.\frac{22.21}{2} \\
=& 2^{12}(2^{10} - 1 - 22 - 11.21) \\
=& 2^{13}5.7.11
\end{aligned}$$

Now, $\mathcal{EG}$ has minimum distance 7, so $|\mathcal{EG}_3| = 2^{11}.22.21.20/6 = 2^1 3.5.7.11 = |PG_3|$. Since $\mathcal{PG}$ is linear, any translation by a vertex in $\mathcal{PG} \setminus \mathcal{EG}$ fixes $\mathcal{PG}_3 = \mathcal{EG}_3$. However this automorphism is not an element of $\mathrm{Aut}(\mathcal{EG})$. □

Entry-Faithful 2-Neighbour-Transitive Codes

This chapter begins the task of classifying those $(X, 2)$-neighbour-transitive codes, by considering the case where the action of X on the entries of the Hamming graph has trivial kernel. In other words, the codes investigated in this chapter are $(X, 2)$-neighbour-transitive and also X-entry-faithful (see Definition 1.2.1). The following result allows the classification of 2-transitive groups to be applied.

Corollary 5.1. *Let C be an X-entry-faithful and $(X, 2)$-neighbour-transitive code in $H(m, q)$, with $|C| \geqslant 2$ and $\delta \geqslant 5$. Then X acts 2-transitively on M.*

Proof. By Lemma 2.5.1, assume $\mathbf{0} \in C$. By Proposition 2.5.3, $X_{\mathbf{0}}$ acts 2-homogeneously on M, and so X has a faithful 2-homogeneous action on M. By Proposition 2.5.5, X_i^Q acts 2-transitively on Q. Thus X_i^Q has even order, and, since X acts faithfully on M, it follows that X^M has even order. The result is then implied by Lemma 2.4.2. □

A classification of X-entry-faithful and $(X, 2)$-neighbour-transitive codes allows for the assumption that $K = X \cap B \neq 1$ in subsequent chapters. The main result of the chapter is as follows.

Theorem 5.2. *Let C be a code in $H(m, q)$ with $|C| \geqslant 2$, minimum distance $\delta \geqslant 5$ and $X \leqslant \mathrm{Aut}(C)$. Then C is X-entry-faithful and $(X, 2)$-neighbour-transitive if and only if C is equivalent to either:*

1. *a binary repetition code with $\delta = m$ and X, $X_{\mathbf{0}}$ are as in Table 5.1, or*
2. *the even weight subcode of the punctured Hadamard code of length 12 with $\delta = 6$, $X_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$ and $X \cong \mathrm{M}_{11}$.*

The punctured Hadamard code $\mathcal{P}$, of length 12, and the even weight subcode $\mathcal{E}$ of $\mathcal{P}$ are defined in Section 5.2. The Hadamard and punctured Hadamard codes, of length 11 and 12 respectively, are known to be completely transitive (see [44]). Lemma 5.2.2 shows that,

X	m	$X_{\mathbf{0}} < X$
$\leqslant \mathrm{A\Gamma L}_d(r)$	r^d	a 2-homogeneous index 2 subgroup
S_m	m	A_m
$\mathrm{M}_{22} \rtimes \mathbb{Z}_2$	22	M_{22}
$\trianglerighteq \mathrm{PSU}_3(r)$	$r^6 + 1$	an index 2 subgroup
$\trianglerighteq \mathrm{PSL}_d(r)$	$\frac{r^d-1}{r-1}$	an index 2 subgroup

Table 5.1: Groups X, $X_{\mathbf{0}}$ such that the binary repetition code in $H(m, 2)$ is X-entry-faithful and $(X, 2)$-neighbour-transitive.

although $\mathcal{E}$ has covering radius at least 3, $\mathcal{E}$ is not $(X, 3)$-neighbour-transitive for any group X. This leads to the following result with regards to X-entry-faithful and X-completely transitive codes:

Theorem 5.3. *Let C be a code in $H(m, q)$ with $|C| \geqslant 2$ and minimum distance $\delta \geqslant 5$. Then C is X-entry-faithful and X-completely transitive for some group X, if and only if $q = 2$ and C is equivalent to the binary repetition code. In this case $X \cong \mathrm{S}_m$ and $X_{\mathbf{0}} \cong \mathrm{A}_m$.*

Remark 5.4. Observe that X in Theorem 5.2 and 5.3 is not necessarily the full automorphism group of C, for example the binary repetition code has automorphism group $2 \times \mathrm{S}_m$. Note that there exist other completely transitive codes with minimum distance $\delta \geqslant 5$, for example, the Golay codes of length 23 and 24 (which are in fact coset-completely transitive) [93] and the Nordstrom-Robinson code [47], but these codes are not X-entry-faithful and $(X, 2)$-neighbour-transitive for any group X.

Proposition 5.2.3 classifies all 2-regular codes in $H(11, 2)$ with minimum distance $\delta \geqslant 5$ and $|C| \geqslant 2$. Such a code is either the repetition code, the punctured code of the Hadamard code of length 12, or the even weight subcode of the punctured Hadamard code. This can be seen as an extension of [44, Theorem 1.1(b)], which gives the punctured code of the Hadamard 12 code as the only completely regular code with minimum distance $\delta = 5$ in $H(11, 2)$.

The results in this chapter require the identification of all finite 2-transitive groups not containing the alternating group, but containing a 2-homogeneous subgroup with a different socle. Proposition 5.2.4 gives a classification of all groups $G < H \leqslant \mathrm{S}_m$ such that G is 2-transitive of degree m, H is 2-homogeneous of degree m, the socle of G is not A_m and the socles of G and H are not equal.

The proof of Theorem 5.2 hinges on Propositions 2.5.3 and 2.5.5, and Corollary 5.1, which imply that X is involved in two different 2-transitive actions and that $X_{\mathbf{0}}$ must have a 2-homogeneous action on entries. This allows the use of the powerful results in [35] and [86]. Section 5.1 covers the cases that the socle of X (the group generated by all minimal normal subgroups of X) is either A_m or is equal to the socle of $X_{\mathbf{0}}$. Section 5.2 deals with the case that the socle of X is not A_m and not equal to the socle of $X_{\mathbf{0}}$.

5.1 The socle and the stabiliser

Proposition 2.5.5, Proposition 2.5.3 and Corollary 5.1 show that if C is an $(X, 2)$-neighbour-transitive code, then X has two different 2-transitive actions, and that the stabiliser $X_{\mathbf{0}}$ of the zero codeword is 2-homogeneous on M. A 2-homogeneous group G is either *affine* or *almost-simple*, depending on the structure of the *socle* of G, denoted $\mathrm{soc}(G)$, that is, the group generated by all the minimal normal subgroups of G (see, for example, [36]). A group is affine if its socle is a regular elementary abelian group, and a group is almost-simple if its socle is a non-abelian simple group.

The following remark, which relies directly on [35, Theorem 1.4], vastly reduces the search space for the parameters of an X-entry-faithful and $(X, 2)$-neighbour-transitive code C of a given group X.

Remark 5.1.1. Let C be an X-entry-faithful and $(X, 2)$-neighbour-transitive code in $H(m, q)$. Then, by Proposition 2.5.5, X_i acts 2-transitively on Q in the first entry and, by Corollary 5.1, X acts 2-transitively on M. It follows that $X_i^Q (\leqslant \mathrm{Sym}(Q))$, $X^M (\leqslant \mathrm{S}_m)$ and X satisfy [35, Hypothesis 1] (G there being our X). That is, X_i^Q and X^M are 2-transitive, $X \leqslant X_i^Q \wr X^M$ acting imprimitively on $Q \times M$, with X projecting onto X^M, and X_i^Q being, what is referred to there as, the component of X. Thus, since X is almost simple and acts faithfully on M, we can apply [35, Theorem 1.4], so that the possible values of X, m, and q are listed, as G, n, and $|B|$, in one of the lines of [35, Tables 2 or 3].

The socle of $X_{\mathbf{0}}$ may or may not be the same as the socle of X. In the case that they are the same, the next lemma shows that the size of an $(X, 2)$-neighbour-transitive code is at most 2.

Lemma 5.1.2. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ such that $|C| \geqslant 2$, $\delta \geqslant 5$, and $\mathrm{soc}(X) = \mathrm{soc}(X_{\mathbf{0}})$. Then C is the binary repetition code. If, in addition, C is X-entry-faithful, then X is isomorphic to one of the groups in Table 5.1.*

Proof. By Lemma 2.5.1, it can be assumed that $\mathbf{0} \in C$. By Proposition 2.5.3, $X_{\mathbf{0}}$ acts 2-homogeneously on M, and thus $X_{\mathbf{0}}$ acts primitively on M. Since $H = \mathrm{soc}(X_{\mathbf{0}})$ is a normal subgroup of $X_{\mathbf{0}}$, it follows that H^M acts transitively on M. Moreover, as X is transitive on C, the stabiliser of each codeword is conjugate in X to $X_{\mathbf{0}}$. Since $H = \mathrm{soc}(X)$, it is normal in X, and thus H is contained in the stabiliser of every codeword from C.

Let $\beta \in C$ such that $d(\mathbf{0}, \beta) = \delta$. Without loss of generality, by Lemma 2.5.1, $\beta = (b^\delta, 0^{m-\delta})$. Let $x = (h_1, \ldots, h_m)\sigma \in H$. Then x fixes $\mathbf{0}$, and so h_i fixes 0 for all i. Since x also fixes β, it follows that σ fixes each of the two subsets of entries $\{1, \ldots, \delta\}$ and $\{\delta + 1, \ldots, m\}$ setwise. This is true for each $x \in H$, so H fixes $\{1, \ldots, \delta\}$ setwise. Since H acts transitively on M, it follows that $\delta = m$. Finally, we apply Lemma 2.6.1, since any 2-neighbour-transitive code is also 2-regular, and conclude that $q = 2$ and C is equivalent to the binary repetition code.

Now assume that X acts faithfully on entries. Since X^M is 2-transitive, it is thus affine or almost simple. Suppose X is affine. In this case, since $|X : X_{\mathbf{0}}| = |C| = 2$, it follows that X is any 2-transitive subgroup of $\mathrm{AGL}_d(q)$, which contains an index two subgroup $X_{\mathbf{0}}$ acting 2-homogeneously on M, with $\mathrm{soc}(X) = \mathrm{soc}(X_{\mathbf{0}})$ as in line 1 of Table 5.1. Suppose, then, that X is almost simple. By Remark 5.1.1, X, m, and q appear (as G, n, and $|B|$ respectively) in [35, Tables 2 and 3]. We also require X to have a 2-homogeneous (and hence, by [68], 2-transitive) index two subgroup $X_{\mathbf{0}}$, with $\mathrm{soc}(X) = \mathrm{soc}(X_{\mathbf{0}})$. All possibilities for X are then contained in Table 5.1. □

X	m	q	$\lvert X\rvert$	$\binom{m}{2}(q-1)^2$	Lemma 2.5.6
$\mathrm{A}_m, \mathrm{S}_m$	m	$m-1$			
S_m	m	2			
S_5	5	3	$2^3 \cdot 3 \cdot 5$	$2^3 \cdot 5$	
A_6	6	6	$2^3 \cdot 3^2 \cdot 5$	$3 \cdot \mathbf{5^3}$	fail
S_6	6	6	$2^4 \cdot 3^2 \cdot 5$	$3 \cdot \mathbf{5^3}$	fail
A_7	7	10	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	$\mathbf{3^5} \cdot 7$	fail
S_7	7	10	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$\mathbf{3^5} \cdot 7$	fail
A_8	8	15	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot \mathbf{7^3}$	fail
A_9	9	15	$2^6 \cdot 3^4 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot \mathbf{7^2}$	fail

Table 5.1.1: Candidate groups X, with $soc(X) = \mathrm{A}_m$, such that C is an X-entry-faithful and $(X, 2)$-neighbour-transitive code in $H(m, q)$.

The next result deals with the possibility that $X \cong \mathrm{A}_m$ or S_m.

Lemma 5.1.3. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$, such that $\delta \geqslant 5$ and $|C| \geqslant 2$, where $X \cong \mathrm{A}_m$ or S_m. Then C is equivalent to the binary repetition code and $X \cong \mathrm{S}_m$.*

Proof. By Remark 5.1.1 the values of X, m, and q appear as G, n, and $|B|$ respectively, in [35, Table 2]. Such groups, with the additional requirement that $\mathrm{soc}(X) = \mathrm{A}_m$, are compiled in Table 5.1.1. Those cases which fail to satisfy Lemma 2.5.6 are marked as such. Thus, we are left with the cases $q = m - 1$; $X \cong \mathrm{S}_m$ and $q = 2$; and $X \cong \mathrm{S}_5$, $m = 5$ and $q = 3$. Note that $m \geqslant 5$, since $\delta \geqslant 5$, and $X_{\mathbf{0}}$ is 2-homogeneous on M, by Proposition 2.5.3.

First, let $m = 5$, $q = 3$ and $X \cong \mathrm{S}_5$. Table 5.1.1 and Lemma 2.5.6 imply that $X_{\mathbf{0}}$ is isomorphic to an index 3 subgroup of S_5, which does not exist.

Now, let $X \cong \mathrm{S}_m$ and $q = 2$. If $X_{\mathbf{0}} \cong \mathrm{A}_m$ then, by Lemma 5.1.2, C is the binary repetition code. Suppose $X_{\mathbf{0}} \neq \mathrm{A}_m$. Now, $X_{\mathbf{0}}$ is 2-homogeneous, and hence primitive. Thus we can then apply a result from [12], which says that the index of a primitive group, not containing A_m, in S_m is at least $\lfloor (m+1)/2 \rfloor !$. Now, $|C| = |X : X_{\mathbf{0}}| \geqslant \lfloor (m+1)/2 \rfloor !$. By the Singleton bound $|C| \leqslant 2^{m-\delta+1} \leqslant 2^{m-4}$. Hence m must satisfy $2^{m-4} \geqslant \lfloor (m+1)/2 \rfloor !$, which does not hold for $m \geqslant 5$.

Suppose $X \cong \mathrm{A}_m$ or S_m and $q = m - 1$. If $X_{\mathbf{0}}$ is 2-homogeneous, but not 2-transitive, then $X_{\mathbf{0}} \leqslant \mathrm{A\Gamma L}_1(m)$ and $m \equiv 3 \pmod 4$, by [68]. So m is a prime power, that is $m = r^t$, and $|X_{\mathbf{0}}|$ divides $tm(m-1)/2$. However, by Lemma 2.5.6, $\binom{m}{2}(q-1)^2 = m(m-1)(m-2)^2/2$ must divide $|X_{\mathbf{0}}|$, that is, $(m-2)^2$ must divide t. This does not occur for $m \geqslant 5$, so $X_{\mathbf{0}}$ is 2-transitive.

Suppose $m \neq 7$. If $X = \mathrm{A}_m$ or S_m, then the stabiliser X_i of $1 \in M$ is A_{m-1} or S_{m-1}, respectively. Now X_i is 2-transitive of degree $m-1$ on Q in the first entry, by Proposition 2.5.5,

and 2-transitive of degree $m-1$ on $M \setminus \{1\}$, since X is at least 3-transitive on M. Let $x \in Q \setminus \{0\}$. Since A_{m-1} and S_{m-1} only have one 2-transitive representation of degree $m-1$ [24, Table 7.4], up to permutational isomorphism, it follows that $X_{1,x} = X_{1,i}$, for some $i \in M$.

Now, consider the stabiliser $X_{\mathbf{0},1}$ of the zero codeword and the entry $1 \in M$. Since $X_{\mathbf{0}}$ is transitive on the neighbours of $\mathbf{0}$, it follows that $X_{\mathbf{0},1}$ is transitive on the vertices of the form $\nu = (y, 0^{m-1})$ in $\Gamma_1(\mathbf{0})$, where $y \in Q \setminus \{0\}$. Hence, $X_{\mathbf{0},1}$ is transitive on $Q \setminus \{0\}$. Thus, for $x \in Q \setminus \{0\}$ the stabiliser $X_{\mathbf{0},1,x}$, has index $m-2$ in $X_{\mathbf{0},1}$. Note that $X_{\mathbf{0},1,x} = (X_{1,x})_{\mathbf{0}} = X_{1,i,\mathbf{0}}$, and we have just proved that this subgroup has index $m(m-2)$ in $X_{\mathbf{0}}$. Since $X_{\mathbf{0}}$ is 2-transitive on M, it follows that $X_{\mathbf{0},1,i}$ has index $m(m-1)$ in $X_{\mathbf{0}}$, which is a contradiction.

Suppose $m = 7$. We have that $|X|$ divides 7!. However, $(q-1)^2\binom{m}{2} = 3.5^2.7$ must divide $|X|$, by Lemma 2.5.6, which does not hold. □

5.2 Different socles

The even weight subcode of the punctured Hadamard code of length 12, below, is an example of an X-entry-faithful and $(X,2)$-neighbour-transitive code, where $\mathrm{soc}(X) \neq \mathrm{soc}(X_{\mathbf{0}})$.

Definition 5.2.1. Let $\mathcal{P}$ be the punctured Hadamard 12 code, obtained as follows (see [79, Part 1, Section 2.3]). First, we construct a normalised Hadamard matrix H_{12} of order 12 using the Paley construction. Let $M = \mathbb{F}_{11} \cup \{*\}$ and let H_{12} be the 12×12 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 $((-1)^{12})$. The Hadamard code $\mathcal{H}$ of length 12 in $H(12,2)$ then consists of the vertices α 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 $u_a = -1$. 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^{11}), 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. The even weight subcode $\mathcal{E}$ of $\mathcal{P}$ is the code consisting of the zero codeword and the 2-$(11,6,3)$ design. Both $\mathcal{D}$ and its complement are unique up to isomorphism [98].

Lemma 5.2.2. *Let $\mathcal{E}$ be the even weight subcode of the punctured Hadamard 12 code, defined above. Then $\mathcal{E}$ is X-entry-faithful and $(X,2)$-neighbour-transitive, if and only if $X = \mathrm{Aut}(\mathcal{E}) \cong \mathrm{M}_{11}$. Moreover $\mathrm{Aut}(\mathcal{E})$ acts faithfully on entries. Furthermore, $\mathcal{E}$ is not $(X,3)$-neighbour-transitive for any group X, in particular, $\mathcal{E}$ is not completely transitive.*

Proof. By [44] the Hadamard 12 code $\mathcal{H}$ has automorphism group the non-split extension $2\,\mathrm{M}_{12}$ and $\mathrm{Aut}(\mathcal{H})^M = \mathrm{M}_{12}$ is 5-transitive on the entries of $H(12,2)$ [54]. Since $\mathcal{P}$ is obtained by deleting an entry from $\mathcal{H}$, and since the Schur multiplier of M_{11} is trivial, we have that $\mathrm{Aut}(\mathcal{P}) = H \times \mathrm{M}_{11} \cong 2 \times \mathrm{M}_{11}$, where $H = \langle((01),\ldots,(01))\rangle$.

Let Y be the stabiliser in $\mathrm{Aut}(\Gamma)$ of the set of even weight vertices of $H(11,2)$, noting that $|\mathrm{Aut}(\Gamma) : Y| = 2$. Now, either $\mathrm{Aut}(\mathcal{P}) \leqslant Y$ or $Y \cap \mathrm{Aut}(\mathcal{P})$ is an index 2 subgroup of $\mathrm{Aut}(\mathcal{P})$. Since $\mathcal{P}$ contains the weight 11 codeword (1^{11}) and $\mathrm{Aut}(\mathcal{P})$ is transitive on $\mathcal{P}$, it follows that $Y \cap \mathrm{Aut}(\mathcal{P})$ must be an index 2 subgroup of $\mathrm{Aut}(\mathcal{P})$. As M_{11} is the unique index 2 subgroup of $\mathrm{Aut}(\mathcal{P})$ we have $\mathrm{M}_{11} = Y \cap \mathrm{Aut}(\mathcal{P})$. Since $\mathrm{Aut}(\mathcal{P})$ is transitive on $\mathcal{P}$, M_{11} has two orbits on $\mathcal{P}$; the even weight codewords $\mathcal{E}$ and the odd weight codewords $\mathcal{P} \setminus \mathcal{E}$. Hence $\mathrm{M}_{11} \leqslant \mathrm{Aut}(\mathcal{E})$ and M_{11} is transitive on $\mathcal{E}$.

By [98], $\mathrm{PSL}_2(11)$ is the automorphism group of the weight 6 codewords forming the 2-$(11,6,3)$ design $\mathcal{D}$. Thus $\mathrm{Aut}(\mathcal{E})_{\mathbf{0}} \leqslant \mathrm{PSL}_2(11)$. Now,

$$|\mathrm{Aut}(\mathcal{E})| = 12|\mathrm{Aut}(\mathcal{E})_{\mathbf{0}}| \leqslant 12|\mathrm{PSL}_2(11)|.$$

Hence $\mathrm{Aut}(\mathcal{E}) \cong \mathrm{M}_{11}$ and $\mathrm{Aut}(\mathcal{E})_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$. Moreover, M_{11} acts faithfully on entries since it contains no non-trivial normal subgroups and $\mathrm{Aut}(\mathcal{E})^M$ is non-trivial, since it contains $\mathrm{PSL}_2(11)$.

Now, M_{11} is transitive on $\mathcal{E}$. Moreover, $\mathrm{Aut}(\mathcal{E})_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$ acts 2-transitively on entries. Thus, it follows that $\mathrm{Aut}(\mathcal{E})_{\mathbf{0}}$ is transitive on the sets of weight 1 and weight 2 vertices of $H(11,2)$. Hence, $\mathcal{E}$ is $(\mathrm{Aut}(\mathcal{E}),2)$-neighbour-transitive.

Suppose X is a proper subgroup of $\mathrm{Aut}(\mathcal{E})$ such that $\mathcal{E}$ is $(X,2)$-neighbour-transitive. Since X is transitive on $\mathcal{E}$, it follows that $X_{\mathbf{0}}$ is a proper subgroup of $\mathrm{PSL}_2(11)$. Then, as $X_{\mathbf{0}}$ is transitive on $\Gamma_2(\mathbf{0})$, we have that $X_{\mathbf{0}}$ is 2-homogeneous, and hence primitive on M. The only 2-homogeneous proper subgroup of $\mathrm{PSL}_2(11)$ in its action of 11 points is F_{55}, and thus $X_{\mathbf{0}} \cong F_{55}$. Also X^M is 2-transitive on 11 points, with order $|C| \cdot |X_{\mathbf{0}}| = 12 \cdot 55$, implying $X \cong \mathrm{PSL}_2(11)$. However, $\mathrm{Aut}(\mathcal{E})$ has a unique conjugacy class of subgroups isomorphic to $\mathrm{PSL}_2(11)$, see [28, p. 18], and hence X is conjugate to $\mathrm{Aut}(\mathcal{E})_{\mathbf{0}}$. This implies that X fixes a codeword, which is a contradiction.

Suppose $\mathcal{E}$ is $(X,3)$-neighbour-transitive, for some $X \leqslant \mathrm{Aut}(\mathcal{E})$. Then, by Lemma 2.6.4, the weight six codewords of $\mathcal{E}$ would form a 3-$(11,6,\lambda)$ design, for some integer λ. The equation

$$b = \frac{v(v-1)(v-2)}{k(k-1)(k-2)}\lambda$$

gives $\lambda = 11 \cdot 6 \cdot 5 \cdot 4/(11 \cdot 10 \cdot 9) = 4/3$, a contradiction. Since $\delta \geqslant 6$, it follows that $\rho \geqslant 3$ and hence $\mathcal{E}$ is not completely transitive. □

Proposition 5.2.3. *Let C be a 2-regular code in $H(11,2)$ with $\delta \geqslant 5$ and $|C| \geqslant 2$. 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 $\mathcal{P}$, or*
3. *$\delta = 6$ and C is equivalent to $\mathcal{E}$.*

Proof. Suppose C is a 2-regular code. By Lemma 2.5.1 we can assume $\mathbf{0} \in C$. Weight δ codewords must exist, and form a 2-$(11, \delta, \lambda)$ design, by Lemma 2.6.4. If $\delta = 11$ we get the trivial design with one block, that is $|C| = 2$ and C is equivalent to the binary repetition code. Suppose $\delta < 11$. Using the equation $vr = bk$, we have $11r = b\delta$. So, since $\delta < 11$, 11 divides b. Now, Table 1 in [9] gives $|C| \leqslant 24$, so that $b = 11$ or 22. The equation

$$b = \frac{v(v-1)}{k(k-1)}\lambda = \frac{11 \cdot 10}{\delta(\delta-1)}\lambda$$

then gives $a\delta(\delta - 1) = 10\lambda$, where $a = 1$ or 2, so that $\delta = 5, 6$ or 10. If $\delta = 10$ then $a = 1$, $\lambda = 9$ and the design consists of every weight 10 vector. However, $d((1^{10}, 0), (0, 1^{10})) = 2$, which contradicts $\delta = 10$.

Suppose $\delta = 5$. Then the weight 5 codewords of C form a 2-$(11, 5, \lambda)$ design, and since $a \cdot 5 \cdot 4 = 10\lambda$, we see $\lambda = 2$ or 4. Consider distinct weight 5 codewords α, β which share 2 non-zero entries. Without loss of generality, $\alpha = (1^5, 0^6)$ and $\beta = (1^i, 0^{5-i}, 1^{5-i}, 0^{i+1})$, for some $i \in \{2, 3, 4\}$. Now, $d(\alpha, \beta) = 10 - 2i \geqslant \delta = 5$, so $i = 2$ and $d(\alpha, \beta) = 6$. Since the code is 2-regular, and in particular 0-regular, this implies there are weight 6 vertices in the code. Hence the weight 6 codewords form a 2-$(11, 6, \lambda')$ design, with the equation $vr = bk$ implying 11 divides b. The bound $|C| \leqslant 24$ then implies that $b = 11$ in both designs. Hence $\lambda' = 3$ and $\lambda = 2$ and the designs are equivalent to $\mathcal{D}$ and its complementary design respectively (see Definition 5.2.1).

As we have just seen, it is impossible to form a design from weight k vertices for $k \neq 0, 5, 6, 11$. Hence the distance distribution of C is $(1, 0, 0, 0, 0, 11, 11, 0, 0, 0, 0, a_{11})$ where $a_{11} = 0$ or 1. Let ν be a weight 5 codeword. By regularity, we have $|\Gamma_5(\nu) \cap C| = 11$. Since $\mathbf{0} \in \Gamma_5(\nu) \cap C$, there must be some weight 6 codeword ν' which is not at distance 5 from ν. Moreover, since ν is weight 5 and ν' is weight 6, $d(\nu, \nu')$ is odd. It follows that $a_{11} = 1$. Regularity then implies the designs are indeed the complementary designs of each other, not just equivalent to these, hence $C = \mathcal{P}$.

Suppose $\delta = 6$. By a similar argument to above we see that the weight 6 codewords form a 2-$(11, 6, \lambda)$ design. Table 1 in [9] gives $|C| \leqslant 12$, and so we see that $b = 11$ and $\lambda = 3$. Thus C consists of the zero codeword and the characteristic vectors of the blocks of $\mathcal{D}$, that is, $C = \mathcal{E}$. □

The results of the previous section leave only the possibility that X and $X_{\mathbf{0}}$ have different socles. The next proposition gives a classification of the inclusions of 2-homogeneous groups in 2-transitive groups with different socles.

Proposition 5.2.4. *Let G, H be groups such that $G < H \leqslant \mathrm{S}_m$, H is 2-transitive of degree m with $\mathrm{soc}(H) \neq \mathrm{A}_m$, and G is 2-homogeneous of degree m with $\mathrm{soc}(G) \neq \mathrm{soc}(H)$. Then G, H, and m are as in Table 5.2.1.*

G	H	degree	Table of [76]
$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	$\mathrm{PSL}_3(2)$	7	I
$\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$	$\mathrm{PSL}_2(11)$ or M_{11}	11	I
$\mathbb{Z}_{23} \rtimes \mathbb{Z}_{11}$	M_{23}	23	I
$\mathrm{PSL}_2(7)$	$\mathrm{AGL}_3(2)$	8	II
A_7	A_8	15	III
$\mathrm{PSL}_2(11)$	M_{11}	11	IV
$\mathrm{PSL}_2(11)$ or M_{11}	M_{12}	12	IV
$\mathrm{PSL}_2(23)$	M_{24}	24	IV

Table 5.2.1: Groups $G < H \leqslant \mathrm{S}_m$ where H is 2-transitive, G is 2-homogeneous, $\mathrm{soc}(H) \neq \mathrm{A}_m$ and $\mathrm{soc}(G) \neq \mathrm{soc}(H)$.

Proof. We use the classification of 2-transitive groups, [36, Section 7.7], and [36, Theorem 9.4B] which gives those groups which are 2-homogeneous, but not 2-transitive. Now, G and H are 2-homogeneous and 2-transitive, respectively, and thus either almost-simple or affine. Moreover, G is not maximal in A_m or S_m, since then $\mathrm{soc}(H) = \mathrm{A}_m$. If G is affine, part (I) of the main result from [76] tells us that G is in [76, Table I] of type (c), giving the examples in Table 5.2.1, lines 1–3 (we note that the group $\mathbb{Z}_{17} \rtimes \mathbb{Z}_8$, in $H = \mathrm{P\Gamma L}_2(16)$ is not 2-homogeneous).

Suppose G is almost simple. If H is affine then part (II) of the main result from [76] tells us that H is of type (c) and listed in [76, Table II], giving Table 5.2.1, line 4. If H is almost simple, part (II) of the main result from [76] gives us that $\mathrm{soc}(G)$ and $\mathrm{soc}(H)$ are listed in [76, Tables III, IV, V, and VI], giving Table 5.2.1, lines 5–8. □

It is now possible to prove the main results.

Proof of Theorem 5.2. By Lemma 2.5.1 we may assume $\mathbf{0} \in C$. By Corollary 5.1 and Proposition 2.5.3, we have that X acts 2-transitively on M and $X_{\mathbf{0}}$ acts 2-homogeneously on M. By Lemma 5.1.2 if $\mathrm{soc}(X) = \mathrm{soc}(X_{\mathbf{0}})$ then C is the binary repetition code and X is one of the groups listed in Table 5.1. Suppose $\mathrm{soc}(X) \neq \mathrm{soc}(X_{\mathbf{0}})$. Since X^M is 2-transitive, X is either affine or almost simple.

Suppose X is affine. Then, by Proposition 5.2.4, $m = 8$ and $X \cong \mathrm{AGL}_3(2)$. Hence $X_i \cong \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$, acting 2-transitively on Q, and so $q = 7$ or 8. Since $\delta \geqslant 5$, $X_{\mathbf{0}}$ must be transitive on $\Gamma_2(\mathbf{0})$. However, $|\Gamma_2(\mathbf{0})| = m(m-1)(q-1)^2/2 = 4 \cdot 7 \cdot 6^2$ or $4 \cdot 7^3$ respectively, neither of which divides $|X| = 8 \cdot 7 \cdot 3$. Thus X is almost simple.

If $\mathrm{soc}(X) = \mathrm{A}_m$ then, by Lemma 5.1.3, C is equivalent to the binary repetition code, and so $X = \mathrm{S}_m$, $X_{\mathbf{0}} = \mathrm{A}_m$, contradicting the assumption that $\mathrm{soc}(X) \neq \mathrm{soc}(X_{\mathbf{0}})$. Thus $\mathrm{soc}(X) \neq \mathrm{A}_m$.

Since X is almost-simple acts 2-transitively on M with $\mathrm{soc}(X) \neq \mathrm{A}_m$, and $X_{\mathbf{0}}$ acts 2-homogeneously on M with $\mathrm{soc}(X_{\mathbf{0}}) \neq \mathrm{soc}(X)$, we can apply Proposition 5.2.4. Hence, $X, X_{\mathbf{0}}$

$X_{\mathbf{0}}$	X	m	q	$\lvert X_{\mathbf{0}}\rvert$	$\binom{m}{2}(q-1)^2$	Lemma 2.5.6
$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	$\mathrm{PSL}_3(2)$	7	2	$3 \cdot 7$	$3 \cdot 7$	
$\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$	$\mathrm{PSL}_2(11)$	11	2	$5 \cdot 11$	$5 \cdot 11$	
	M_{11}	11	2		$5 \cdot 11$	
$\mathbb{Z}_{23} \rtimes \mathbb{Z}_{11}$	M_{23}	23	22	$11 \cdot 23$	$\mathbf{3^2} \cdot 7^2 \cdot 11 \cdot 23$	fail
A_7	A_8	15	7	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	$2^2 \cdot \mathbf{3^3} \cdot 5 \cdot 7$	fail
			8		$3 \cdot 5 \cdot \mathbf{7^3}$	fail
$\mathrm{PSL}_2(11)$	M_{11}	11	2	$2^2 \cdot 3 \cdot 5 \cdot 11$	$5 \cdot 11$	
			10		$\mathbf{3^4} \cdot 5 \cdot 11$	fail
	M_{12}	12	11		$\mathbf{2^3} \cdot 3 \cdot \mathbf{5^2} \cdot 11$	fail
			12		$2 \cdot 3 \cdot \mathbf{11^3}$	fail
M_{11}	M_{12}	12	11	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	$2^3 \cdot 3 \cdot \mathbf{5^2} \cdot 11$	fail
			12		$2 \cdot 3 \cdot \mathbf{11^3}$	fail
$\mathrm{PSL}_2(23)$	M_{24}	24	23	$2^4 \cdot 3 \cdot 11 \cdot 23$	$2^4 \cdot 3 \cdot \mathbf{11^2} \cdot 23$	fail

Table 5.2.2: Groups $X, X_{\mathbf{0}} \leqslant \mathrm{Aut}(\Gamma)$ such that X is faithful and almost simple 2-transitive on M, $X_{\mathbf{0}}$ is 2-homogeneous on M, $\mathrm{soc}(X) \neq \mathrm{A}_m$ and $\mathrm{soc}(X_{\mathbf{0}}) \neq \mathrm{soc}(X)$.

and m are as in Table 5.2.1, with $X = H$ and $X_{\mathbf{0}} = G$. Moreover, by Remark 5.1.1, the values of X, m, and q appear (as G, n, and $|B|$ respectively) in one of the lines of [35, Tables 2 or 3]. The groups which appear both in Table 5.2.1 and in one of the lines of [35, Tables 2 or 3] are listed in Table 5.2.2, along with the corresponding value of q, noting that Lemma 2.5.6 tells us that if $|X_{\mathbf{0}}| = m(m-1)/2$ then $q = 2$. Furthermore, Lemma 2.5.6 allows us to obtain the last column in Table 5.2.2, where a group is marked with 'fail' if it does not satisfy the first part of this result. Dealing with the remaining cases here will complete the proof. In each case $q = 2$.

Suppose $m = 7$, $X_{\mathbf{0}} = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ and $X = \mathrm{PSL}_3(2)$. It follows that $|C| = 8$. Since $\delta \geqslant 5$, there are 7 non-zero codewords, each having weight either $5, 6$ or 7. Since $m = 7$, the supports of two such codewords intersect in at least three entries. Hence the distance between two such codewords is at most 4, a contradiction. Suppose $m = 11$, $X_{\mathbf{0}} = \mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ and $X = \mathrm{PSL}_2(11)$. Then $|C| = 12$, so Proposition 5.2.3 says that C is equivalent to the even weight subcode of the punctured Hadamard 12 code, however this contradicts Lemma 5.2.2. Suppose $m = 11$, $X_{\mathbf{0}} = \mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ and $X = \mathrm{M}_{11}$. Then $|C| = 2^4 \cdot 3^2$, which contradicts the Singleton bound $|C| \leqslant 2^{m-\delta+1} \leqslant 2^7$. If $m = 11$, $X_{\mathbf{0}} = \mathrm{PSL}_2(11)$ and $X = \mathrm{M}_{11}$, then $|C| = 12$. By Proposition 5.2.3, C is equivalent to the even weight subcode $\mathcal{E}$ of the punctured Hadamard 12 code. Moreover, by Lemma 5.2.2, C is indeed $(X, 2)$-neighbour-transitive. □

Proof of Theorem 5.3. Suppose $q = 2$ and C is equivalent to the binary repetition code. We show that C is X-completely transitive with $X \cong \mathrm{S}_m$. It is clear that the top group $L \cong \mathrm{S}_m$ of $\mathrm{Aut}(\Gamma)$ is a subgroup of $\mathrm{Aut}(C)$ and that $H = \langle (h, \ldots, h) \rangle \leqslant \mathrm{Aut}(C)$, where $1 \neq h \in \mathrm{S}_2$.

$\delta = m$	5	6	7	8	9	10
X	–	$\mathrm{PGL}_2(5)$	$\mathrm{AGL}_1(7)$	$\mathrm{PGL}_2(7)$	$\leqslant \mathrm{AGL}_2(3)$	$\leqslant \mathrm{P\Gamma L}_2(9)$

Table 5.2.3: Groups $X \neq \mathrm{S}_m$ from Table 5.1, for $m \leqslant 10$.

Now let X be the group consisting of automorphisms of the form $x = (h, \ldots, h)\sigma$ if σ is an odd permutation and $x = \sigma$ if σ is an even permutation. Then $X \cong \mathrm{S}_m$, $X_{\mathbf{0}} \cong \mathrm{A}_m$, $X \cap \mathrm{S}_q^m = 1$, and X acts transitively on C. The covering radius of C is $\lfloor \frac{m}{2} \rfloor$ and C_i consists of the vertices of weights i and $m-i$, for $i = 0, \ldots, \lfloor \frac{m}{2} \rfloor$. Let $\nu_1, \nu_2 \in C_i$. If ν_1, ν_2 both have the same weight, then because A_m acts i-homogeneously on M for all $i \leqslant m$ it follows that there exists $\sigma \in X_{\mathbf{0}}$ such that $\nu_1^\sigma = \nu_2$. Now suppose ν_1 and ν_2 have different weights, say ν_1 has weight i and ν_2 has weight $m-i$. Then there exists $x \in X$ such that ν_2^x has weight i. Consequently there exists $\sigma \in X_\alpha$ such that $\nu_1^\sigma = \nu_2^x$, thus $\nu_1^{\sigma x^{-1}} = \nu_2$. Hence X acts transitively on C_i and so C is X-completely transitive.

Conversely, suppose C is X-entry-faithful and X-completely transitive, for some group X. Since $\delta \geqslant 5$, and so $\rho \geqslant 2$, C is $(X, 2)$-neighbour-transitive. Thus, by Theorem 5.2, either C is the even weight subcode $\mathcal{E}$ of the Hadamard code of length 12, or C is the binary repetition code. By Lemma 5.2.2, $\mathcal{E}$ is not X-completely transitive for any group X. Thus, $q = 2$ and C is equivalent to the binary repetition code, and X is listed in Table 5.1. Note that in this case $\mathrm{soc}(X) = \mathrm{soc}(X_{\mathbf{0}})$. If $\mathrm{soc}(X) = \mathrm{A}_m$ then $X = \mathrm{S}_m$, $X_{\mathbf{0}} = \mathrm{A}_m$ and C is X-completely transitive by the above.

Suppose that $\mathrm{soc}(X) \neq \mathrm{A}_m$. By Proposition 2.5.3, $X_{\mathbf{0}}$ (and so X also) is i-homogeneous on M for all $i \leqslant \lfloor \frac{\delta-1}{2} \rfloor = \lfloor \frac{m-1}{2} \rfloor$. By [36, Section 7.7 and Theorem 9.4B], we see that the groups in Table 5.1 are at most 4-homogeneous, and so $m \leqslant 10$. Comparing the possible values for m with those groups in Table 5.1 satisfying the conditions of the last column, we arrive at Table 5.2.3. By [36, Section 7.7 and Theorem 9.4B], we see that $\mathrm{AGL}_1(7)$, $\mathrm{AGL}_2(3)$ and $\mathrm{P\Gamma L}_2(9)$ do not have $\lfloor \frac{\delta-1}{2} \rfloor$-homogeneous subgroups. Suppose $X = \mathrm{PGL}_2(7)$ and $m = 8$. Then X must be transitive on the set of weight 4 vertices, of which there are $\binom{8}{4} = 70$ such vertices. However, 5 does not divide $|X|$.

Suppose $X \cong \mathrm{PGL}_2(5)$ and $m = 6$. Then $X_{\mathbf{0}} \cong \mathrm{PSL}_2(5)$. Since $q = 2$ we have $X_{\mathbf{0}} = X \cap L \leqslant L \cong \mathrm{S}_m$. Let $h = ((01), \ldots, (01)) \in \mathrm{S}_2^6$. As every $x \in X \setminus X_{\mathbf{0}}$ must map the zero codeword to the vector $(1, \ldots, 1)$, it follows that for some $\sigma \in \mathrm{PGL}_2(5) \setminus \mathrm{PSL}_2(5) \subseteq X^M$ we have $x = h\sigma$. By [36, Section 7.7 and Theorem 9.4B], $\mathrm{PGL}_2(5)$ is 3-transitive, but $\mathrm{PSL}_2(5)$ is not 3-homogeneous. In fact, by [39, Sec. 2.4 and Lem. 9.1.1], $\mathrm{PSL}_2(5)$ has two orbits on the set of weight 3 vertices, and these are the characteristic vectors of complementary 2-$(6, 3, 2)$ designs. Denote these orbits as $\mathcal{O}_1, \mathcal{O}_2$, and note that for $\sigma \in \mathrm{PGL}_2(5) \setminus \mathrm{PSL}_2(5) \subseteq \mathrm{Sym}(M)$ we have $\mathcal{O}_1^\sigma = \mathcal{O}_2$. Since the designs are complementary, we have $\mathcal{O}_1^h = \mathcal{O}_2$. Thus, for $x = h\sigma \in X \setminus X_{\mathbf{0}}$, where $\sigma \in \mathrm{PGL}_2(5) \setminus \mathrm{PSL}_2(5)$, we have $\mathcal{O}_1^x = \mathcal{O}_1^{h\sigma} = \mathcal{O}_1$. Hence X is not transitive on the set of weight 3 vertices. □

Alphabet-Almost-Simple 2-Neighbour Transitive Codes

Chapter 5 classified all $(X, 2)$-neighbour-transitive codes for which the group X acts faithfully on the set of entries of the Hamming graph. This chapter begins the study of $(X, 2)$-neighbour-transitive codes such that the action of X on the entries has a non-trivial kernel. If C is an $(X, 2)$-neighbour-transitive code with minimum distance $\delta \geqslant 3$, then the subgroup X_i of X stabilising the entry $i \in M$ has a 2-transitive action on the alphabet Q_i (see Proposition 2.5.5). Recall that $B \cong \mathrm{S}_q^m$ and $L \cong \mathrm{S}_m$ are the base group and the top group, respectively, of $\mathrm{Aut}(\Gamma)$. Also, a code C in $H(m, q)$ is X-alphabet-almost-simple (see Definition 1.2.1) if $K = X \cap B \neq 1$, X acts transitively on M, and $X_i^{Q_i}$ is a 2-transitive almost-simple group. The main result of this chapter concerns the non-existence of codes that are X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive with minimum distance $\delta \geqslant 4$.

Theorem 6.1. *Let C be an X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 3$. Then $\delta = 3$ and C is equivalent to the repetition code in $H(3, q)$, where $q \geqslant 5$.*

Section 6.1 contains results on the structure of X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive codes, as well as some questions about codes for which the action of X_i on the alphabet in the first entry is affine. Some example codes with properties of interest in relation to the results here are presented in Section 6.2. Finally we give a classification of *diagonally $(X, 2)$-neighbour-transitive* codes (see Definition 6.1.1), as well as prove Theorem 6.1, in Section 6.3.

6.1 Structural results

Codes C that are X-alphabet-almost-simple and X-neighbour-transitive with $\delta \geqslant 3$ have been characterised in [45]. This chapter is reliant on certain results of [45], which are compiled below. The following definition is needed first. Recall that $\mathrm{Diag}_m(T) = \{(h, \ldots, h) \in B \mid h \in T\}$ for $T \leqslant \mathrm{S}_q$.

Definition 6.1.1. A code C in $H(m, q)$ is *diagonally (X, s)-neighbour-transitive*, if C is (X, s)-neighbour-transitive and $X \leqslant \mathrm{Diag}_m(\mathrm{S}_q) \rtimes L$.

Each part of Proposition 6.1.2 is proved in the relevant citation of [45]. Recall the definitions of: $\pi_J(C)$ and $\chi_J(X)$ (see Section 2.7), $\mathrm{soc}(G)$ (see Section 2.2), and the kernel $K = X \cap B$ for the action of X on M (see Section 2.3), where $B \cong \mathrm{S}_m$ is the base group of $\mathrm{Aut}(\Gamma)$. Note also that G is a *sub-direct* subgroup of a direct product $\prod_{i=1}^n T_i$ of isomorphic groups $T_i \cong T$, where $i \in \{1, \ldots, n\}$ if the projection of G in each coordinate is isomorphic to T.

Proposition 6.1.2. *Suppose C is an X-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 3$. Then the following hold:*

1. *Let $\mathcal{J}$ be an X-invariant partition of M and $J \in \mathcal{J}$ such that $\pi_J(C)$ is not the complete code. Then $\pi_J(C)$ is $\chi_J(X)$-neighbour-transitive [45, Proposition 3.4]. (Note that the assumption that $\pi_J(C)$ is not the complete code does not appear in [45], but is necessary since the proof assumes that $\pi_J(C)_1$ is non-empty.)*

2. *Let $\mathcal{J}$ be an X-invariant partition of M and $J \in \mathcal{J}$ such that $\pi_J(C)$ is not the complete code. Then $\pi_J(C)$ has minimum distance at least 2 [45, Corollary 3.7].*

3. *If C is X-alphabet-almost-simple, then $\mathrm{soc}(K)$ is a sub-direct subgroup of*

$$\prod_{i \in M} \mathrm{soc}(X_i^{Q_i}) \quad \textit{[45, Proposition 5.2].}$$

While the next result is not explicitly stated in [45], it is the basis of the characterisation contained in it.

Proposition 6.1.3. *Let C be an X-alphabet-almost-simple and X-neighbour-transitive code with $\delta \geqslant 3$. Then there exists an X-invariant partition $\mathcal{J}$ of M such that for all $J \in \mathcal{J}$ the code $\pi_J(C)$ is equivalent to a diagonally $\chi_J(X)$-neighbour-transitive with minimum distance $\delta(\pi_J(C)) \geqslant 2$.*

Proof. Let T be the non-abelian simple socle of the almost-simple 2-transitive group $X_i^{Q_i}$. By part 3 of Proposition 6.1.2, the group $\mathrm{soc}(K)$ is a sub-direct subgroup of $\prod_{i \in M} \mathrm{soc}(X_i^{Q_i})$. Following the discussion after [45, Proposition 5.2], Scott's Lemma [87, p. 328] can be applied to give a partition $\mathcal{J}$, of M such that $\mathrm{soc}(K) = \prod_{J \in \mathcal{J}} D_J$, where each $D_J \cong \mathrm{Diag}_k(T)$ acts on $\pi_J(V\Gamma)$, for all $J \in \mathcal{J}$, where $k = |J|$. Moreover, by [45, Remark 5.5], $\mathcal{J}$ is X-invariant. By examining $\mathrm{soc}(K)$, it can be shown [45, Section 5] that, up to equivalence, two possibilities occur. Either $\chi_J(X) \leqslant \mathrm{Diag}_k(\mathrm{S}_q) \rtimes \mathrm{S}_k$, where $k = |J|$, for all $J \in \mathcal{J}$, or $\mathcal{J}$ can be replaced by a more refined X-invariant partition $\hat{\mathcal{J}}$ of M such that $\chi_J(X) \leqslant \mathrm{Diag}_k(\mathrm{S}_q) \rtimes \mathrm{S}_k$, where $k = |J|$, for all $J \in \hat{\mathcal{J}}$.

In either case, it follows from parts 1 and 2 of Proposition 6.1.2 that, for all $J \in \mathcal{J}$ or $\hat{\mathcal{J}}$ respectively, $\chi_J(X)$ acts transitively on $\pi_J(C)$ and either $\pi_J(C)$ is the complete code or it is $\chi_J(X)$-neighbour-transitive with minimum distance at least 2. Since $\chi_J(X)$ is a diagonal subgroup, we deduce that $\pi_J(C)$ is as in the second case, since no diagonal subgroup acts transitively on the complete code. □

Proposition 6.1.4. *Let C be an $(X, 2)$-neighbour-transitive code with $\delta \geqslant 3$ in $H(m, q)$, and suppose $\mathcal{J}$ is an X-invariant partition of M. Then for all $J \in \mathcal{J}$, either;*

1. *$\pi_J(C)$ is the complete code, $\delta(\pi_J(C)) = 1$, and $\chi_J(X)$ is transitive on $\pi_J(C)$;*

2. *$\pi_J(C)$ has covering radius 1, $\delta(\pi_J(C)) = 2$ or 3, and is $(\chi_J(X), 1)$-neighbour-transitive; or,*

3. $\pi_J(C)$ *is* $(\chi_J(X), 2)$*-neighbour-transitive.*

Proof. Let $\bar{C} = \pi_J(C)$. The fact that $\chi_J(X)$ is transitive on $\bar{C}$ and $\bar{C}_1$, if $\bar{C}_1$ is non-empty, follows from part 1 of Proposition 6.1.2. From this we deduce parts 1 and 2. Now, part 2 of Proposition 6.1.2 gives us that $\delta(\pi_J(C)) \geqslant 2$, and $\delta(\pi_J(C))$ is at most 3 in part 2. Moreover, to prove part 3, we need only show that if $\bar{C}_2$ is non-empty, then $\chi_J(X)$ is transitive on $\bar{C}_2$.

Suppose $\bar{C}$ has covering radius at least 2. Let $\mu, \nu \in \bar{C}_2$. Then there exists $\alpha, \beta \in C$ such that $d(\mu, \pi_J(\alpha)) = d(\nu, \pi_J(\beta)) = 2$. Let $\hat{\nu} \in H(m, q)$ with $\hat{\nu}_u = \nu_u$ for u in J and $\hat{\nu}_v = \alpha_v$ otherwise. Similarly, let $\hat{\mu} \in H(m, q)$ with $\hat{\mu}_u = \mu_u$ for u in J and $\hat{\mu}_v = \beta_v$ otherwise. We claim that $\hat{\nu}, \hat{\mu} \in C_2$. We show this for $\hat{\nu}$ and note that an identical argument holds for $\hat{\mu}$. First, note that $d(\alpha, \hat{\nu}) = 2$ and $\delta \geqslant 3$, so $\hat{\nu} \notin C$. Suppose $\hat{\nu} \in C_1$. Then there exists $\alpha' \in C$ such that $d(\hat{\nu}, \alpha') = 1$. We then have $d(\nu, \pi_J(\alpha')) \leqslant 1$. However, this contradicts $\nu \in \bar{C}_2$. Hence $\hat{\mu}, \hat{\nu} \in C_2$.

As C is $(X, 2)$-neighbour-transitive, there exists an $x = h\sigma \in X$ mapping $\hat{\nu}$ to $\hat{\mu}$. We claim $x \in X_J$. Suppose $x \notin X_J$. Then, since $\mathcal{J}$ is a system of imprimitivity for the action of X on M, there exists $J' \in \mathcal{J}$ such that $J \neq J'$ and $J'^{\sigma} = J$. Since $\pi_{J'}(\hat{\nu}) = \pi_{J'}(\alpha)$, this implies that $\pi_J(\hat{\nu}^x) = \pi_J(\alpha^x) \in \bar{C}$ and hence $\pi_J(\hat{\nu}^x) \neq \mu$, which contradicts the fact that $\hat{\nu}^x = \hat{\mu}$. Thus $x \in X_J$ and

$$\nu^{\chi_J(x)} = \pi_J(\hat{\nu})^{\chi_J(x)} = \pi_J(\hat{\nu}^x) = \pi_J(\hat{\mu}) = \mu.$$

□

Proposition 6.1.5. *Let* C *be an* $(X, 2)$*-neighbour-transitive code in* $H(m, q)$ *with* $\delta \geqslant 3$*, and* $\mathcal{J}$ *be an* X*-invariant partition of* M*. Then, for all* $J \in \mathcal{J}$*,*

1. $\chi_J(X)_i^Q$ *is* 2*-transitive on* Q*; and,*
2. *for* $\alpha \in C$*,* $\chi_J(X)_{\pi_J(\alpha)}$ *is transitive on* J*.*

Proof. As C is X-neighbour-transitive with $\delta \geqslant 3$, we have that X_i^Q is 2-transitive and X^M is transitive. One then deduces that X_i^Q is 2-transitive for all i. Now, because $\mathcal{J}$ is an X-invariant partition, it follows that $X_i = (X_J)_i$ for all $i \in J$. This in turn implies that $\chi_J(X)_i = \chi_J(X_i)$. It is now straight forward to show that $\chi_J(X_i)^Q = X_i^Q$.

Now, since X_α is transitive on M and $\mathcal{J}$ is an X-invariant partition of M, it follows that $(X_\alpha)_J$ is transitive on J. Thus $\chi_J(X_\alpha) \leqslant \chi_J(X)_{\pi(\alpha)}$ is transitive on J. □

The previous two propositions suggest studying $(X, 2)$-neighbour-transitive codes where X acts primitively on M with $\delta \geqslant 2$. An answer to the following questions would provide us with the building blocks for $(X, 2)$-neighbour-transitive codes with $\delta \geqslant 3$.

Question 6.1.6. Can we classify all $(X, 2)$-neighbour-transitive codes with $\delta \geqslant 2$ such that X^M is primitive and $X_i^{Q_i}$ is 2-transitive?

Question 6.1.7. Can we classify all $(X, 1)$-neighbour-transitive codes with $\delta = 2$ or 3 and $\rho = 1$ such that X^M is primitive and $X_i^{Q_i}$ is 2-transitive?

Recall the definition of X-entry-faithful from Definition 1.2.1. If C is a code in $H(m, q)$ and $X \leqslant \mathrm{Aut}(C)$ such that, X^M is transitive, and $X_i^{Q_i}$ is and affine 2-transitive group, we say C is *X-alphabet-affine*. Questions 6.1.6 and 6.1.7 can be further broken down into X-entry-faithful and non-trivial kernel cases, that is, X-alphabet-affine and X-alphabet-almost-simple. By the main result of this chapter, the outstanding cases of Question 6.1.6 are X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive with $\delta = 2$, and X-alphabet-affine and $(X, 2)$-neighbour-transitive, where X^M is primitive and $X_i^{Q_i}$ is 2-transitive.

Given Proposition 6.1.3, a third question is the following.

Question 6.1.8. Can we contrsuct $(X, 2)$-neighbour-transitive codes with $\delta \geqslant 3$ by taking copies of $(X, 1)$-neighbour-transitive codes with $\delta = 2$ or 3 and $\rho = 1$.

6.2 Examples

We begin this section by considering some examples of codes which have properties relating to the results of the previous section. We first introduce the operators Prod and Rep which allow the construction of new codes from old ones. For an arbitrary code C in $H(m, q)$ we define $\mathrm{Prod}(C, \ell)$ and $\mathrm{Rep}_\ell(C)$ in $H(m\ell, q)$ as

$$\mathrm{Prod}(C, \ell) = \{(\alpha_1, \ldots, \alpha_\ell) \mid \alpha_i \in C\},$$

and

$$\mathrm{Rep}_\ell(C) = \{(\alpha, \ldots, \alpha) \mid \alpha \in C\}.$$

The *repetition code* $\mathrm{Rep}(m, q)$ in $H(m, q)$ is the set of all vertices $(a, \ldots, a)$ consisting of a single element $a \in Q$ repeated m times.

The next two examples are codes which are X-alphabet-almost-simple and X-completely transitive, though the second has $\delta = 2$.

Example 6.2.1. *Let $C = \mathrm{Rep}(3, q)$, where $q \geqslant 5$, and $X = \mathrm{Diag}_3(\mathrm{S}_q) \rtimes \mathrm{S}_3$, as in [49, Example 3.1]. Now,*

$$C_1 = \{(a, a, b), (a, b, a), (b, a, a) \mid a, b \in Q; a \neq b\},$$

and

$$C_2 = \{(a, b, c) \mid a, b, c \in Q; a \neq b \neq c \neq a\}.$$

Since S_q acts 3-transitively on Q and S_3 acts transitively on M, it follows that X acts transitively on C, C_1 and C_2. Thus C is $(X, 2)$-neighbour-transitive and X-completely transitive, since C has covering radius $\rho = 2$. Also, $X_i^{Q_i} \cong \mathrm{S}_q$ is almost-simple, since $q \geqslant 5$, and $X^M \cong \mathrm{S}_3$ is transitive on M. Hence C is X-alphabet-almost-simple and X-completely transitive.

Example 6.2.2. *Let $q \geqslant 5$, $\ell \geqslant 2$, $C = \mathrm{Prod}(\mathrm{Rep}(2,q),\ell)$ and $X = (\mathrm{Diag}_2(\mathrm{S}_q))^\ell \rtimes U$, where $\mathrm{Diag}_2(\mathrm{S}_q)$ is a subgroup of the base group of $\mathrm{Aut}(H(2,q))$ and $U = \mathrm{S}_2 \wr \mathrm{S}_\ell = \mathrm{S}_2^\ell \rtimes \mathrm{S}_\ell$ is a subgroup of the top group of $\mathrm{Aut}(H(2\ell,q))$. Let $\mathcal{J} = \{J_1,\ldots,J_\ell\}$, with $J_i = \{2i-1, 2i\}$, be the partition of M preserved by U. Note that $\delta = 2$. Let $R \subseteq \{1,\ldots,\ell\}$ of size s, and $\nu \in H(m,q)$ be such that $\pi_{J_i}(\nu) = (a,b)$, where $a \neq b$ for all $i \in R$, and $a = b$ for all $i \notin R$. Any codeword β is at least distance s from ν, since $d(\pi_{J_i}(\nu), \pi_{J_i}(\beta)) \geqslant 1$ for each $i \in R$. Also, there exists some codeword α with $\pi_{J_i}(\alpha) = (a,a)$ whenever $\pi_{J_i}(\nu) = (a,b)$ for $i \in \{1,\ldots,\ell\}$, and hence $d(\alpha,\nu) = s$. So $\nu \in C_s$. Any vertex ν of $H(2\ell,q)$ can be expressed in this way, for some R, since $\pi_{J_i}(\nu) = (a,b)$ has either $a = b$ or $a \neq b$. Thus, for each s, C_s consists of all such vertices ν where $|R| = s$. It also follows from this that $\rho = \ell$.*

Let $\nu \in C_s$, with R as above. Let $x = (h_{J_1},\ldots,h_{J_\ell})\sigma \in X$ where $h_{J_i} \in \mathrm{Diag}_2(\mathrm{S}_q)$ such that $\pi_{J_i}(\nu)^{h_{J_i}} = (1,2)$, for $i \in R$, and $\pi_{J_i}(\nu)^{h_{J_i}} = (1,1)$, for all $i \notin R$. Moreover, since S_ℓ is ℓ-transitive, there exists $\sigma \in \mathrm{S}_\ell \leqslant \mathrm{S}_2 \wr \mathrm{S}_\ell$ mapping $\{J_{i_1},\ldots,J_{i_s}\}$ to $\{J_1,\ldots,J_s\}$ (where $R = \{i_1,\ldots,i_s\}$), whilst preserving order within each J_i. Then $\nu^x = \gamma \in C_s$, where $\pi_{J_i}(\gamma) = (1,2)$ for all $i \in \{1,\ldots,s\}$ and $\pi_{J_i}(\gamma) = (1,1)$ for all $i \notin \{s+1,\ldots,\ell\}$. Since we can map any such ν to γ, X is transitive on C_s for each $s \in \{1,\ldots,\ell\}$. Hence C is X-completely transitive, and in particular $(X,2)$-neighbour-transitive for $\ell \geqslant 2$. Since $X_i^{Q_i} \cong \mathrm{S}_q$ and $X^M \cong \mathrm{S}_2 \wr \mathrm{S}_\ell$ is transitive on M, C is X-alphabet-almost-simple.

Lemma 6.2.3. *Suppose C is an $(X,2)$-neighbour-transitive code in $H(m,q)$, with $q \geqslant 3$, and $\mathcal{J}$ is an X-invariant partition of M, such that $\pi_J(C) = \mathrm{Rep}(k,q)$, for all $J \in \mathcal{J}$ where $k = |J|$. Then either $\delta = k = 2$, or $\mathcal{J}$ is a trivial partition.*

Proof. Let $x = (h_1,\ldots,h_m)\sigma \in X$ and $J \in \mathcal{J}$. By the hypothesis it follows that for all $a \in Q$, there exists $\alpha \in C$ such that $\pi_J(\alpha) = (a,\ldots,a)$. Suppose $J^\sigma = J' \in \mathcal{J}$. Then $\pi_{J'}(\alpha^x) = (a^{h_{i_1}},\ldots,a^{h_{i_k}})\sigma = (b,\ldots,b)$ for some $b \in Q$, that is, $a^{h_{i_s}} = a^{h_{i_t}}$ for all $i_s, i_t \in J$. In particular $\chi_J(x\sigma^{-1}) = (h,\ldots,h)$ for some $h \in \mathrm{S}_q$, and $X \leqslant \mathrm{Diag}_k(\mathrm{S}_q) \wr U$, where U is the stabiliser of $\mathcal{J}$ in the top group.

Now suppose that $\mathcal{J}$ is a non-trivial partition, so $k, \ell \geqslant 2$. Since $C \subseteq \mathrm{Prod}(\mathrm{Rep}(k,q),\ell)$, which has minimum distance k, it follows that $\delta \geqslant k \geqslant 2$.

Suppose $\delta \geqslant 3$. As C is a subset of $\mathrm{Prod}(\mathrm{Rep}(k,q),\ell)$ we can replace C by an equivalent code contained in $\mathrm{Prod}(\mathrm{Rep}(k,q),\ell)$ containing $\alpha = (1,\ldots,1)$ and such that

$$\mathcal{J} = \{\{1,\ldots,k\},\{k+1,\ldots,2k\},\cdots,\{m-k+1,\ldots,m\}\}.$$

Consider,

$$\mu = (2,3,1,1,\ldots,1,1,1,1,\ldots,1,\cdots,1,\ldots,1) \quad \text{and}$$
$$\nu = (\underbrace{2,1,1,1,\ldots,1}_{k \text{ entries}},\underbrace{2,1,1,\ldots,1}_{k \text{ entries}},\cdots,\underbrace{1,\ldots,1}_{k \text{ entries}}).$$

If $k = 2$, then we claim $\mu \in C_2$. Any vertex $\beta \in \mathrm{Prod}(\mathrm{Rep}(2,q),\ell) \supseteq C$ with $d(\mu,\beta) = 1$ is of the form $\gamma = (a,a,1,\ldots,1)$, where $a = 2$ or 3. However, no such γ is an element of C,

since each is distance 2 from α. If $k \geqslant 3$ then $\mu \in C_2$ since $d(\alpha, \mu) = 2$ and there is no closer codeword as $\pi_{J_1}(\mu) \in \pi_{J_1}(C)_2$. In both cases $\nu \in C_2$ since $d(\alpha, \nu) = 2$ and no codeword is closer, as $\pi_{J_i}(\nu) \in \pi_{J_i}(C)_1$ for $i = 1, 2$. Let $x = (h_1, \ldots, h_m)\sigma \in X$ such that $\mu^x = \nu$. We reach a contradiction here, since $h_1 = h_2 = \cdots = h_k = h$ cannot, assuming $k \geqslant 3$, map the set $\{1, 2, 3\}$ to either of the sets $\{1, 2\}$ or $\{1\}$. In the case $k = 2$, in at least one block we must map the set $\{1\}$ to $\{1, 2\}$, which is not possible. Hence $2 \geqslant \delta \geqslant k \geqslant 2$. □

Suppose $\mathcal{J}$ is a system of imprimitivity for the action of X on M and C is an X-neighbour-transitive code, with $\delta \geqslant 3$. The next example shows that it is possible that the projection of C onto each block of $\mathcal{J}$ gives the complete code.

Example 6.2.4. *Let $\bar{C} = \mathrm{Prod}(C, \ell)$ be a code in $\Gamma = H(m, q)$, where $m = k\ell$ and C is an X-neighbour-transitive code in $H(k, q)$ where $X \cap B$ is transitive on C and $\delta \geqslant 3$. Let $\bar{X} = \langle (X \cap B)^\ell, \mathrm{Diag}_\ell(X), \mathrm{S}_\ell \rangle$ preserve the partition*

$$\mathcal{J} = \{\{1, \ldots, k\}, \ldots, \{m - k + 1, \ldots, m\}\} = \{J_1, \ldots, J_\ell\},$$

of M, where $\chi_J((X \cap B)^\ell) = X \cap B$ and $\chi_J(\mathrm{Diag}_\ell(X)) = X$ for all $J \in \mathcal{J}$, and S_ℓ acts as pure permutations by permuting the blocks of $\mathcal{J}$ whilst preserving the order of entries within a given block. It follows that we preserve two $\bar{X}$-invariant partitions. These being $\mathcal{J}$ and $\mathcal{J}'$, where $\mathcal{J}'$ is attained by taking the corresponding entries, by order, from each copy of C to form each block:

$$\mathcal{J}' = \{\{1, k + 1, \ldots, m - k + 1\}, \ldots, \{\ell, k + \ell, \ldots, m\}\}.$$

Given any $\alpha = (\alpha_1, \ldots, \alpha_\ell) \in \bar{C}$, $\alpha_i \in C$, and $\beta = (\beta_1, \ldots, \beta_\ell) \in \bar{C}$, $\beta_i \in C$ there exists an $x \in (X \cap B)^\ell$ mapping α to β since $X \cap B$ is transitive on C. Hence $\bar{X}$ is transitive on $\bar{C}$. Given any two neighbours $\mu, \nu \in \Gamma_1(\alpha)$, where μ, ν differ from α in the respective blocks J_i and J_j, we can map J_j to J_i via some element $\sigma \in \mathrm{S}_\ell$. Then, since X_{α_i} is transitive on $\Gamma_1(\alpha_i)$, there exists an element $x \in \mathrm{Diag}_\ell(X)$ such that $\pi_{J_i}(\nu^{\sigma x}) = \pi_{J_i}(\mu)$. We can then map $\nu^{\sigma x}$ to μ via some element $h \in (X \cap B)^\ell$, where $\chi_{J_i}(h) = 1$, since each $\pi_{J_t}(\nu^{\sigma x})$ and $\pi_{J_t}(\mu)$ are elements of C for $t \neq i$ and $X \cap B$ is transitive on C. Hence $\sigma x h$ maps ν to μ and $\bar{X}$ is transitive on $\bar{C}_1$.

When we consider the projection $\pi_J(\bar{C})$ for any $J \in \mathcal{J}'$ we are left with the complete code. To see this, consider that for $(\alpha_1, \ldots, \alpha_\ell) \in \bar{C}$, $\alpha_i \in C$, we may choose an arbitrary element of C as α_i for each i. Since $X_i^{Q_i}$ is 2-transitive on Q, each element appears in the first entry for some codeword. Thus, as $\pi_J((\alpha_1, \ldots, \alpha_\ell))$ when $J = \{1, k+1, \ldots, m-k+1\}$ is the first entry of each α_i, we have that $\pi_J(\bar{C})$ is the complete code.

6.3 Alphabet-almost-simple 2-neighbour-transitive codes

Before we prove the final results we define the codes used in this section, which first requires the following definition.

Definition 6.3.1. Define the *composition* of a vertex $\alpha \in H(m,q)$ to be the set

$$Q(\alpha) = \{(a_1, p_1), \ldots, (a_q, p_q)\},$$

where p_i is the number of entries of α which take the value $a_i \in Q$. For $\alpha \in H(m,q)$ define the set

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

where (p_i, s_i) means that s_i distinct elements of Q appear precisely p_i times in α.

Definition 6.3.2. We define the following codes:

1. $\mathrm{Inj}(m,q)$, where $m < q$, is the set of all vertices $\alpha \in H(m,q)$ such that $\mathrm{Num}(\alpha) = \{(1,m)\}$;
2. for m odd, $W([m/2],2)$ is the set of vertices in $\alpha \in H(m,2)$ such that $\mathrm{Num}(\alpha) = \{(m+1)/2, 1), (m-1)/2, 1)\}$; and,
3. $\mathrm{All}(pq,q)$, where $pq = m$, is the set of all vertices $\alpha \in H(m,q)$ such that $\mathrm{Num}(\alpha) = \{(p,q)\}$.

For more information on these codes see [46, Definition 2]. The following lemma is [46, Lemma 4].

Lemma 6.3.3. *Let α be a vertex in $H(m,q)$. Then $\mathrm{Num}(\alpha)$ is preserved by $\mathrm{Diag}_m(\mathrm{S}_q) \rtimes L$.*

The last result, when combined with the classification of diagonally neighbour-transitive codes [46, Theorem 4.3], allows us to prove the next result.

Proposition 6.3.4. *Suppose C is a diagonally $(X,2)$-neighbour-transitive code in $H(m,q)$. Then one of the following holds:*

1. *$q = 2$ and $C = \{(a, \ldots, a)\}$;*
2. *$m = 3$ or $q = 2$, and $C = \mathrm{Rep}(m,q)$;*
3. *$C = \mathrm{Inj}(3,q)$;*
4. *m is odd and $C = W([m/2],2)$; or,*
5. *$m = q = 3$ or $q = 2$, and there exists some p such that $m = pq$ and C is a subset of $\mathrm{All}(pq,q)$.*

Proof. By [46, Theorem 4.3], a diagonally neighbour-transitive code C is one of: $\{(a, \ldots, a)\}$ for some $a \in Q$, $\mathrm{Rep}(m,q)$, $\mathrm{Inj}(m,q)$ with $m < q$, $W([m/2],2)$ with m odd, or there exists a p such that $m = pq$ and C is a subset of $\mathrm{All}(pq,q)$. Here we consider $m \geqslant 2$, since if $m = 1$

C conditions	$\mu \in C_2$ $\mathrm{Num}(\mu)$	$\nu \in C_2$ $\mathrm{Num}(\nu)$
$\{(a,\dots,a)\}$ $q \geqslant 3$	$(b,b,a,\dots,a)$ $\{(m-2,1),(2,1)\}$	$(b,c,a,\dots,a)$ $\{(m-2,1),(1,2)\}$
$\mathrm{Rep}(m,q)$ $m > q \geqslant 3$	$(2,2,1,\dots,1)$ $\{(m-2,1),(2,1)\}$	$(2,3,1,\dots,1)$ $\{(m-2,1),(1,2)\}$
$\mathrm{Inj}(m,q)$ $m \geqslant 4$	$(1,1,1,4,5,\dots,m)$ $\{(3,1),(1,m-3)\}$	$(1,1,3,3,5,6,\dots,m)$ $\{(2,2),(1,m-4)\}$
$\subseteq \mathrm{All}(q,q)$ $q \geqslant 4$	$(1,1,1,4,5,\dots,q)$ $\{(3,1),(1,q-3)\}$	$(1,1,3,3,5,6,\dots,q)$ $\{(2,2),(1,q-4)\}$
$\subseteq \mathrm{All}(pq,q)$ $q > p \geqslant 2$	$(\hat{\mu},\alpha,\dots,\alpha)$ $\{(p-1,2),(p,q-3),(p+2,1)\}$	$(\hat{\nu},\hat{\nu},\alpha,\dots,\alpha)$ $\{(p-2,1),(p,q-2),(p+2,1)\}$

Table 6.3.1: Diagonally neighbour-transitive codes C which are not diagonally 2-neighbour-transitive, and elements of C_2 which illustrate this. Note: $\hat{\mu} = (1,1,1,4,5,\dots,q)$, $\hat{\nu} = (1,1,3,4,5,\dots,q)$ and $\alpha = (1,2,3,\dots,q)$.

then C_2 is empty, so C is not $(X,2)$-neighbour-transitive. Also to prove some C is $(X,2)$-neighbour-transitive, we need only find some $X \leqslant \mathrm{Aut}(C)$ such that $X \leqslant \mathrm{Diag}_m(\mathrm{S}_q) \rtimes L$ and X is transitive on C_2, since C is already X-neighbour-transitive, for some X, by [46, Theorem 4.3].

First, if $C = \mathrm{Inj}(2,q)$ then C_2 is empty. Thus, C is not $(X,2)$-neighbour-transitive. Table 6.3.1 lists the remaining cases that are not $(X,2)$-neighbour-transitive. The second and third columns give a pair $\mu,\nu \in C_2$ such that $\mathrm{Num}(\mu) \neq \mathrm{Num}(\nu)$. Hence, by Lemma 6.3.3, X is not transitive on C_2. It can be deduced from $\mathrm{Num}(\mu), \mathrm{Num}(\nu)$ that $\mu,\nu \in C_2$, since this makes it clear that we must change μ,ν in at least two entries to get a vertex in C. Note that we let $\alpha = (1,2,3,\dots,q) \in H(q,q)$ and in the second last and last rows we assume $\alpha \in C$ and $(\alpha,\dots,\alpha) \in C$, respectively, and observe for the last row $\hat{\mu} = (1,1,1,4,5,\dots,q)$, $\hat{\nu} = (1,1,3,4,5,\dots,q)$ are in $\Gamma_2(\alpha)$.

Now we prove the result for the cases which are 2-neighbour-transitive. Suppose $C = \{(a,\dots,a)\}$ for some $a \in Q$. Let $q = 2$ and $Q = \{0,1\}$. Then $L = \mathrm{S}_m = \mathrm{Aut}(C)$. Without loss of generality, let $a = 0$ so that C_2 is the set of weight two vertices. Since L is transitive on the sets of weight 2 and weight 1 vertices, it follows C is diagonally $(X,2)$-neighbour-transitive. Let $C = \mathrm{Rep}(m,q)$. It follows from Example 6.2.1 that $\mathrm{Rep}(3,q)$ is $(\mathrm{Diag}_3(\mathrm{S}_q) \rtimes \mathrm{S}_3, 2)$-neighbour-transitive. If $q = 2$ then $\mathrm{Aut}(C) \cong \mathrm{Diag}_m(\mathrm{S}_2) \rtimes \mathrm{S}_m$ and C is completely transitive [49, Example 3.1]. Consider $C = \mathrm{Inj}(m,q)$ with $3 = m < q$ and $q \geqslant 4$. If $\nu \in C_2$ then $\nu_1 = \nu_2 = \nu_3$, since otherwise $\nu \in C$ or C_1. Since $\mathrm{Diag}_m(\mathrm{S}_q) \leqslant \mathrm{Aut}(C)$, we are transitive on C_2. Suppose $C = W([m/2],2)$ and m is odd. Then by [46, Corollary 3.4] C is $\mathrm{Diag}(\mathrm{S}_2) \rtimes \mathrm{S}_m$-completely

transitive. Finally, suppose C is a subset of $\mathrm{All}(pq, q)$ for some p such that $m = pq$. Let $p \geqslant 2$, $q = 2$ and $C = \mathrm{All}(2p, 2)$. Then C_2 is the set of all weight $p \pm 2$ vertices, which $\mathrm{Diag}_2(\mathrm{S}_2) \rtimes \mathrm{S}_m \leqslant \mathrm{Aut}(C)$ is transitive on. Let $p = 1$, $q = 3$ and $C = \mathrm{All}(3, 3)$. Then $C_2 = \mathrm{Rep}(3, q)$ and is $\mathrm{Aut}(C)$-completely transitive by Example 6.2.1. □

With the classification of diagonally $(X, 2)$-neighbour-transitive codes from the previous result, Propositions 6.1.3 and 6.1.4 mean we are now in a position to prove the main theorem.

Proof of Theorem 6.1. Suppose C is an X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive code with $\delta \geqslant 3$ such that $X \cap B \neq 1$. By Proposition 6.1.3, there exists an X-invariant partition $\mathcal{J}$, of size ℓ, for the action of X on M. Moreover, for all $J \in \mathcal{J}$ the code $\pi_{J_i}(C)$ has minimum distance at least 2 and is diagonally $\chi_J(X)$-neighbour-transitive. By Proposition 6.1.4, either $\pi_J(C)$ has covering radius $\rho \leqslant 1$, or $\pi_J(C)$ is also $(\chi_J(X), 2)$-neighbour-transitive. Note $\rho \neq 0$, that is, $\pi_J(C)$ is not the complete code, since $\pi_J(C)$ has minimum distance at least 2.

Suppose $\pi_J(C)$ has covering radius $\rho \geqslant 2$. Since $X_i^{Q_i}$ is almost-simple, it follows that $q \geqslant 5$. By Proposition 6.3.4, the only diagonally 2-neighbour-transitive code with $q \geqslant 5$ and $\delta \geqslant 2$ is $\mathrm{Rep}(3, q)$ for $q \geqslant 5$ (note that $\delta = 1$ for $\mathrm{Inj}(3, q)$). Then Lemma 6.2.3 implies $\mathcal{J}$ is a trivial partition. Since $|J| = k = 3 > 1$, it follows that $\ell = 1$, $k = m$, and $C = \mathrm{Rep}(3, q)$.

Suppose $\pi_J(C)$ has covering radius $\rho = 1$. By [46, Thm. 4 and Cor. 2], the only diagonally neighbour-transitive code with $\delta \geqslant 2$ and $\rho = 1$ is $\mathrm{Rep}(2, q)$. If $l = 1$ then $\delta = 2$, a contradiction. Suppose $l \geqslant 2$. Then Lemma 6.2.3 implies $\delta = 2$, a contradiction. □

Extensions of 2-Neighbour-Transitive Codes

This chapter takes another direction in classifying the family of 2-neighbour transitive codes. Since the action on the alphabet is 2-transitive (see Proposition 2.5.5) it is either almost-simple or affine. Chapter 6 considered the case where the action on the alphabet is almost-simple. Moreover, Chapter 5 studied 2-neighbour-transitive codes with a trivial kernel for the action on entries. Hence, it is assumed here that the action on the alphabet is affine and the kernel of the action on entries is non-trivial. Recall that K denotes the kernel of the action of X on entries, where $X \leqslant \mathrm{Aut}(\Gamma)$, and $K = X \cap B$, where $B \cong \mathrm{S}_q^m$ is the base group in $\mathrm{Aut}(\Gamma)$.

Definition 7.1. Let $q = p^d$, $V = \mathbb{F}_p^{dm}$ and W be a non-trivial subspace of V. Identify V with the vertex set of the Hamming graph $H(m, q)$. An $(X, 2)$-*neighbour-transitive extension* of W is an $(X, 2)$-neighbour-transitive code C containing $\mathbf{0}$ such that $T_W \leqslant X$ and $K = K_W$, where T_W is the group of translations by elements of W and K_W is the stabiliser of W in K. Note that $T_W \leqslant X$ and $\mathbf{0} \in C$ means that $W \subseteq C$. If $C \neq W$ then the extension is said to be *non-trivial*.

Identify $V = \mathbb{F}_p^{dm}$ with the vertex set of the Hamming graph $H(m, q)$. The main result for this chapter classifies all $(X, 2)$-neighbour-transitive extensions of W, supposing W is a k-dimensional $\mathbb{F}_p$-subspace of V, where $k \leqslant d$.

Theorem 7.2. *Let $V = \mathbb{F}_p^{dm}$ be the vertex set of the Hamming graph $H(m, q)$ and C be an $(X, 2)$-neighbour-transitive extension of W with $\delta \geqslant 5$, where the subspace $W \leqslant V$ has $\mathbb{F}_p$-dimension $k \leqslant d$. Then $p = 2$, $d = 1$ and one of the following holds:*

1. *$C = W$ is the binary repetition code, with $\delta = m$,*
2. *$C = \mathcal{H}$, where $\mathcal{H}$ is the Hadamard code of length 12, as in Definition 5.2.1, 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 5.2.1, with $\delta = 5$.*

Moreover, in each case C is an $(\mathrm{Aut}(C), 2)$-neighbour-transitive extension of the binary repetition code in the appropriate Hamming graph.

Note that if C is an $(X, 2)$-neighbour-transitive extension of a k-dimensional subspace W of V, with $k > 0$, then $T_W \leqslant K_W \leqslant K$ so that $K \neq 1$. Since $K \neq 1$, X^M is transitive, by Proposition 2.5.3, and $X_i^{Q_i}$ is a subgroup of $\mathrm{AGL}_d(p)$, it follows that C is X-alphabet-affine (see Definition 1.2.1).

7.1 Extensions of the binary repetition code

In this section it will be shown that the hypotheses of Theorem 7.2 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 2-neighbour-transitive codes and blocks of imprimitivity is proved.

Lemma 7.1.1. *Suppose C is an $(X, 2)$-neighbour transitive code with $\delta \geqslant 5$ and that Δ is a block of imprimitivity for the action of X on C. Then Δ is an $(X_\Delta, 2)$-neighbour transitive code with minimum distance $\delta_\Delta \geqslant 5$.*

Proof. Since Δ is a block of imprimitivity for the action of X on C, it follows that X_Δ is transitive on Δ. Since $\delta \geqslant 5$ and $\Delta \subseteq C$ it follows that $\delta_\Delta \geqslant 5$. Since X_Δ fixes Δ, we have that X_Δ fixes Δ_1 and Δ_2. It remains to show that X_Δ is transitive on Δ_i for $i = 1, 2$. Let $i \in \{1, 2\}$ and $\mu, \nu \in \Delta_i$. Then, since $\delta_\Delta \geqslant 5$, 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 $\delta \geqslant 5$. Hence, there exists $x \in X$ such that $\mu^x = \nu$ and, since $\delta \geqslant 5$, $\alpha^x = \beta$. Since Δ is a block of imprimitivity, it follows that x fixes Δ, so that $x \in X_\Delta$. Thus X_Δ is transitive on Δ_i for $i = \{1, 2\}$. □

Corollary 7.1.2. *Let C be an $(X, 2)$-neighbour-transitive extension of W, and C have minimum distance $\delta \geqslant 5$. 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 $\delta_W \geqslant 5$.*

Proof. Now, $K = K_W$ is normal in X and $T_W \leqslant K_W$ is transitive on W from which it follows (see Section 2.4) that W is an orbit of K on C and hence is a block of imprimitivity for the action of X on C. Thus, the result is implied by Lemma 7.1.1. □

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 $1 \leqslant k \leqslant d$.

Lemma 7.1.3. *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 subspace of V, with $1 \leqslant k \leqslant d$, such that W is an $(X, 2)$-neighbour-transitive code with minimum distance $\delta \geqslant 5$. Then $q = 2$ and W is the binary repetition code in $H(m, 2)$.*

Proof. It is claimed that $\delta = m$. As any $(X, 2)$-neighbour transitive code is also 2-regular, by Lemma 2.6.4, and $\mathbf{0} \in W$, proving the claim implies the result, by Lemma 2.6.1. Suppose $\delta < m$. Then there exists $\alpha \in W$, with $d(\alpha, \mathbf{0}) = \delta$, and distinct $i, j \in M$ such that $\alpha_i = 0$ and $\alpha_j \neq 0$. Now, $X_j^{Q_j^\times}$ acts transitively on $Q_j^\times$, by Proposition 2.5.5, and thus for all $a \in \mathbb{F}_p^d$ there exists some $x \in X_{\mathbf{0},j}$ such that $(\alpha^x)_j = a$. Hence $k \geqslant d$, so that $k = d$. By Proposition 2.5.3, $X_{\mathbf{0}}$ 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 $\beta = \alpha^y \in W$ and $\beta_i \neq 0$. It follows that $\dim(C) > d$, a contradiction. So $\delta = m$. □

Lemma 7.1.3 implies part 1 of Theorem 7.2 and also that, given the hypotheses of Theorem 7.2, it can be assumed that $q = 2$ and W is the repetition code in $H(m, 2)$.

Lemma 7.1.4. *Let C be an $(X, 2)$-neighbour-transitive extension of W, where W is the repetition code in $H(m, 2)$, with $\delta \geqslant 5$. 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 7.1.2 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 $K = T_W$. □

Lemma 7.1.5. *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 $\delta \geqslant 5$. 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, $\beta = \alpha + (1, \ldots, 1) \in C$, since $T_W \leqslant X$, which implies $\pi_J(\beta) = (1, 0) \in P$. Thus, P is the complete code in the Hamming graph $H(2, 2)$. By Corollary 2.5.4 $X_{\{i,j\}}$ 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 7.1.4, $K = T_W$ so that $|K| = 2$. Thus 2 divides $|X/K|$. Lemma 2.4.2 and Proposition 2.5.3 then imply that $X/K = X^M$ is 2-transitive.

By Corollary 7.1.2, W is $(X_W, 2)$-neighbour-transitive. Thus, by Proposition 2.5.3, 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, $|X_{\{i,j\}}^P| \leqslant 8$, since $\mathrm{Aut}(H(2, 2)) = (\mathrm{S}_2 \times \mathrm{S}_2) \rtimes \mathrm{S}_2$. Furthermore, $|X_{\{i,j\}}^P : X_{W,\{i,j\}}^P| = 2$, since $X_{\{i,j\}}^P$ acts transitively on P. Thus $X_{\{i,j\}}^P = (\mathrm{S}_2 \times \mathrm{S}_2) \rtimes \mathrm{S}_2$, 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,

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

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 $X_{i,j}^M$ index 2. □

Recall that the socle of a primitive 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 7.1.6. *Let C be a non-trivial $(X, 2)$-neighbour-transitive extension of W with $\delta \geqslant 5$, where W is the repetition code in $H(m, 2)$. Then $\mathrm{soc}(X/K) \neq \mathrm{soc}(X_W/K)$.*

Proof. Let $H \leqslant X$ such that $K < H$ and $H/K = \mathrm{soc}(X/K)$. Note that this implies that $H \trianglelefteq X$. By Lemma 7.1.4, $X_W = K \rtimes X_{\mathbf{0}}$. Suppose $H/K = \mathrm{soc}(X_W/K)$, and note that by Lemma 7.1.5, $X_W^M = X_W/K$ acts 2-homogeneously on M and $X^M \cong X/K$ acts 2-transitively on M.

By considering vertices as characteristic vectors, identify the set of all subsets of M with the vertex set $V \cong \mathbb{F}_2^m$ of $H(m,2)$. By Lemma 7.1.4, $K = T_W \cong \mathbb{Z}_2$. 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 $X_{\mathbf{0}}$ on the set:

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

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 K maps $J \subseteq M$ to $\bar{J}$, 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 $X_{(\mathcal{O})} \leqslant X_W$. By Lemma 7.1.4, $X_W = K \rtimes X_{\mathbf{0}}$. It follows that $X_{(\mathcal{O})}/K \trianglelefteq X_W/K$, and, since $H/K = \mathrm{soc}(X_W/K)$, either $X_{(\mathcal{O})}/K = 1$, or $H/K \trianglelefteq X_{(\mathcal{O})}$.

Suppose that $H/K \leqslant X_{(\mathcal{O})}/K$. 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 $H/K = \mathrm{soc}(X_W/K)$ 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 Theorem 2.4.6, $2|m$ implies that $X_{\mathbf{0}}$ acts 2-transitively on M. By [20, Theorem IX, p. 192], a 2-transitive group with an imprimitive socle is affine, so that $X_W^M \leqslant \mathrm{AGL}_d(2)$ and $M \cong \mathbb{F}_2^d$. 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 $X_{\mathbf{0},i}$ 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 $X_{\mathbf{0},i}$ 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 $K \leqslant X_W \leqslant X$ implies $|C|/|W| = |X|/|X_W| = |X^M|/|X_W^M|$. 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 (see Theorem 2.4.4). Thus, $X_{(\mathcal{O})}/K = 1$.

By Lemma 7.1.5, X^M acts 2-transitively on M. Since $H/K = \mathrm{soc}(X/K)$, 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 $H \leqslant X_W/K$. If H/K fixes each element of $\mathcal{O}$ then $H/K \leqslant X_{(\mathcal{O})}/K$, giving a contradiction. Thus $\mathrm{soc}(X/K) \neq \mathrm{soc}(X_W/K)$. □

Lemma 7.1.7. *Let C be a non-trivial $(X,2)$-neighbour-transitive extension of W with $\delta \geqslant 5$, where W is the repetition code in $H(m,2)$. Then $\mathrm{soc}(X^M) \neq \mathrm{A}_m$.*

Proof. Suppose $\mathrm{soc}(X^M) = \mathrm{A}_m$. By Lemma 7.1.5, $X_W/K \cong X_W^M$ is a 2-homogeneous group and thus primitive, and, by Lemma 7.1.6, $\mathrm{soc}(X_W/K) \neq \mathrm{soc}(X/K)$. By Lemma 7.1.4, $|C| = |X : X_{\mathbf{0}}| = 2|X : X_W| = 2|X/K : X_W/K|$. Since X_W^M is primitive, it follows from [12]

(which gives a lower bound on the index of a primitive non-trivial subgroup of the alternating group), that $|X/K : X_W/K| \geqslant \lfloor (m+1)/2 \rfloor !$. Hence $|C| \geqslant 2\lfloor (m+1)/2 \rfloor !$. However, by the Singleton bound we have $|C| \leqslant 2^{m-\delta+1} \leqslant 2^{m-4}$. Combining these equations we have $2\lfloor (m+1)/2 \rfloor ! \leqslant 2^{m-4}$, which does not hold for $m \geqslant 5$. □

The main theorem of this chapter can now be proved.

Proof of Theorem 7.2. Suppose C is an $(X, 2)$-neighbour-transitive extension of W with $\delta \geqslant 5$, where W is a k-dimensional subspace of $V = \mathbb{F}_p^{dm}$ and $1 \leqslant k \leqslant d$. By Lemma 7.1.3, 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 7.1.5, $\delta \neq m$, X^M acts 2-transitively on M and either $X^M_{i,j}$ has an index 2 normal subgroup, or X^M_W acts 2-homogeneously, but not 2-transitively, on M. Also, by Lemma 7.1.6, the socles of X^M and X^M_W are not equal. Moreover, $\mathrm{soc}(X^M) \neq \mathrm{A}_m$, by Lemma 7.1.7. Thus the possibilities for X^M and X^M_W are as in Table 5.2.1.

Now $T_W \leqslant X$ implies that if there exists some weight k codeword in C, then there is also a weight $m-k$ codeword. Thus $\delta \leqslant m/2$ and $\delta \geqslant 5$ implies $m \geqslant 10$. In particular, $X^M \neq \mathrm{PSL}_3(2)$ or $\mathrm{AGL}_3(2)$. Suppose $X^M \cong \mathrm{PSL}_2(11)$ and $m = 11$. Then $\delta = 5$ and, by Proposition 5.2.3, 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. Moreover, as in the proof of Proposition 5.2.3, the only copy of $\mathrm{PSL}_2(11)$ in $\mathrm{Aut}(\mathcal{P})$ fixes $\mathbf{0}$, and hence $X^M_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$, a contradiction.

Suppose $m = 23$, $X^M \cong \mathrm{M}_{23}$ and $X^M_W \cong \mathbb{Z}_{23} \rtimes \mathbb{Z}_{11}$. Since $|C| = |X|/|X_{\mathbf{0}}| = 2|X^M|/|X^M_W|$, it follows that $|C| = 80640$. However, this contradicts the bounds given in [9, Table I].

Suppose $m = 15$, $X^M \cong \mathrm{A}_8$ and $X^M_W \cong \mathrm{A}_7$. Then $X^M_{i,j} \cong \mathrm{A}_6$ is simple, contradicting Lemma 7.1.5.

Suppose $m = 11$, $X^M \cong \mathrm{M}_{11}$ and $X^M_W \cong \mathrm{PSL}_2(11)$. Then, by Proposition 5.2.3, 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 $X = \mathrm{Aut}(\mathcal{P}) \cong 2 \times \mathrm{M}_{11}$ with $X_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$ and $K = T_W$. By [44, Theorem 1.1] $\mathcal{P}$ is an $(X, 2)$-neighbour-transitive extension of W, as in outcome 3.

Suppose $m = 12$, $X^M \cong \mathrm{M}_{12}$ and $X^M_W \cong \mathrm{M}_{11}$ or $\mathrm{PSL}_2(11)$. If $X^M_W \cong \mathrm{PSL}_2(11)$ then, as the index of $\mathrm{PSL}_2(11)$ in M_{12} is 144, we have $|C| = 288$. However, since $\delta \geqslant 5$, the Singleton bound gives $|C| \leqslant 2^{m-\delta+1} \leqslant 256$. Thus $X^M_W \cong \mathrm{M}_{11}$ and $|C| = 24$. If weight 5 codewords exist then there are $b = 2 \cdot 11\lambda/5$ of them, for some λ divisible by 5. Since there are the same number of weight 7 codewords it follows that $\lambda = 0$. Thus $\delta \geqslant 6$, and as $\delta \leqslant m/2 = 6$, it follows that $\delta = 6$. The Hadamard code $\mathcal{H}$ of length 12 with $X = \mathrm{Aut}(\mathcal{H}) \cong 2.\mathrm{M}_{12}$, $X_{\mathbf{0}} \cong \mathrm{M}_{12}$ and $K = T_W$ is then the unique $(X, 2)$-neighbour-transitive extension of W with these parameters, by [44, Theorem 1.1], as in outcome 2.

Finally, suppose $m = 24$, $X^M \cong \mathrm{M}_{24}$ and $X_W^M \cong \mathrm{PSL}_2(23)$. Then $X_{i,j}^M \cong \mathrm{M}_{22}$ is simple, contradicting Lemma 7.1.5. □

Alphabet-Affine 2-Neighbour-Transitive Codes

Recall that Definition 1.2.1 partitions $(X, 2)$-neighbour-transitive codes with $\delta \geqslant 3$ into three different classes, X-entry-faithful, X-alphabet-almost-simple, and X-alphabet-affine codes. Chapter 5 classified the $(X, 2)$-neighbour-transitive codes where X acts faithfully on the set M of entries and C has minimum distance $\delta \geqslant 5$, and Chapter 6 classified the $(X, 2)$-neighbour-transitive codes where $K = X \cap B \neq 1$, $\delta \geqslant 3$ and $X_i^{Q_i}$ is an almost-simple group. This chapter concerns X-alphabet-affine codes, that is codes C in $H(m, q)$ such that $X \leqslant \mathrm{Aut}(C)$, $K = X \cap B \neq 1$, X acts transitively on M, and $X_i^{Q_i}$ is a 2-transitive affine group. It is assumed that $\mathbf{0} \in C$ throughout this chapter (see Lemma 2.5.1).

The two main results of the chapter are stated in the theorem below. The first result characterises any X-alphabet-affine and $(X, 2)$-neighbour-transitive code as having a block of imprimitivity that is an $FX_{\mathbf{0}}$-module, for some finite field F. The second gives strong restrictions on the affine 2-transitive group $X_i^{Q_i}$. Recall Definition 7.1 of an $(X, 2)$-neighbour-transitive extension.

Theorem 8.1. *Let $q = p^d$ and C be an X-alphabet-affine and $(X, 2)$-neighbour-transitive code in $H(m, q)$ with minimum distance $\delta \geqslant 5$. Then:*

1. *C is an $(X, 2)$-neighbour-transitive extension of $W = \mathbf{0}^{O_p(K)}$, the orbit of $\mathbf{0}$ under the p-core $O_p(K)$ of K, and W is an $\mathbb{F}_p X_{\mathbf{0}}$-module.*

2. *$X_i^{Q_i}$ is soluble. In particular, $X_{\mathbf{0},i}^{Q_i^\times}$ is a transitive linear group of degree $q - 1$, as in Table 8.1.1.*

It follows from Theorem 6.1 that there do not exist X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive codes with minimum distance $\delta \geqslant 4$. If it is assumed that $\delta \geqslant 5$ and $K \neq 1$, this means that an $(X, 2)$-neighbour-transitive code is X-alphabet-affine. Note that many results in this chapter does not assume Theorem 6.1. In particular, several results in Section 8.1 apply to 2-neighbour-transitive codes in general, while some apply even more generally.

Section 8.1 concerns the automorphism group of an $(X, 2)$-neighbour-transitive code with minimum distance $\delta \geqslant 5$. Most results in that section do not in fact assume that C is X-alphabet-affine. A key result is that $K_{\mathbf{0}}$ must be soluble and, in some sense, be small. Moreover, it is proved that there is at least some 'part' of the action on the alphabet that can be found as a quotient of the action on entries. These results provide the framework for the following sections, which involve a mixture of case-by-case and structural analysis.

Part 1 of Theorem 8.1 is proved in Section 8.2. Section 8.3 classifies all X-alphabet-affine and $(X, 2)$-neighbour-transitive codes with $\delta \geqslant 5$ and $m \leqslant 8$. Dealing with these small cases before Section 8.4, where part 2 of Theorem 8.1 is proved, allows $m \geqslant 9$ to be assumed.

8.1 The stabiliser of a codeword

Suppose C is an $(X, 2)$-neighbour-transitive code with $\delta \geqslant 5$. The next lemma takes a closer look at K^{Q_i} and $K_{\mathbf{0}}$, the group induced by $K = X \cap B$ on Q_i and the stabiliser of the zero codeword inside K, respectively. Recall (Section 2.3) the definition of $\mathrm{Diag}_m(H) = \{g \in B \mid g_i = h, \forall h \in H\}$, for $H \leqslant \mathrm{Sym}(Q)$.

Lemma 8.1.1. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ with minimum distance $\delta \geqslant 5$ and containing $\mathbf{0}$. Then $K_{\mathbf{0}} \cong \mathrm{Diag}_m(H)$ where H acts semi-regularly on $Q_i^\times$ for all $i \in M$.*

Proof. Let $h = (h_1, \ldots, h_m) \in K_{\mathbf{0}}$. If $q = 2$ then, since each h_i fixes 0 and thus also fixes $1 \in Q$, it follows that $h = 1$, $K_{\mathbf{0}} = 1$, and the conclusion holds with $H = 1$. Assume $q \geqslant 3$ and $K_{\mathbf{0}} \neq 1$.

By Proposition 2.5.3, $X_{\mathbf{0}}$ acts transitively on M. Thus $K_{\mathbf{0}}^{Q_i^\times} \cong K_{\mathbf{0}}^{Q_j^\times}$ for all distinct $i, j \in M$. Let $h = (h_1, \ldots, h_m) \in K_{\mathbf{0}}$, with $h \neq 1$, choose $i \in M$ such that $h_i \neq 1$, and $a \in Q_i^\times$ such that $a^{h_i} \neq a$. Let $j \neq i$ and $b \in Q_j^\times$. By Lemma 2.6.4, the weight δ codewords of C form a q-ary 2-(m, δ, λ) design. Thus, there exists a weight δ codeword $\alpha \in C$ with $\alpha_i = a$ and $\alpha_j = b$. Now, $\mathrm{supp}(\alpha) = \mathrm{supp}(\alpha^h)$ since $K_{\mathbf{0}}$ acts trivially on M and fixes $\mathbf{0}$. Since $a^{h_i} \neq a$ we then have $1 \leqslant d(\alpha, \alpha^h) \leqslant \delta$. Suppose $b^{h_j} = b$. Then $d(\alpha, \alpha^h) < \delta$ which contradicts $\alpha^h \in C$. Thus $h_j \neq 1$. Since this holds for all $j \neq i$, for any non-trivial $h \in K_{\mathbf{0}}$ we have that $h_k \neq 1$ for all $k \in M$ and thus $K_{\mathbf{0}} \cong \mathrm{Diag}_m(H)$ where $H \cong K_{\mathbf{0}}^{Q_i^\times}$. Now, for all $a' \in Q_i^\times$ with $a' \neq a$, there exists a weight δ codeword $\alpha' \in C$ such that $\alpha'_i = a'$ and $\alpha'_j = b$. By a similar argument to that involving b, we also have $(a')^{h_i} \neq a'$ and thus h_i fixes no point of $Q_i^\times$.

Since i may be chosen arbitrarily, for any $h \in K_{\mathbf{0}}$ such that $h \neq 1$ we have that h_i has no fixed points in $Q_i^\times$. It follows from this, that for any $a \in Q_i^\times$ we have $K_{\mathbf{0},a}^{Q_i^\times} = 1$ so that $K_{\mathbf{0}}^{Q_i^\times}$ acts semi-regularly on $Q_i^\times$. □

Lemma 8.1.2. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$, with $\delta \geqslant 5$ and $\mathbf{0} \in C$. Then, there exists an equivalent code C^y such that $K_{\mathbf{0}}^y = \mathrm{Diag}_m(H) \leqslant \mathrm{Aut}(C^y)$, where $K_{\mathbf{0}} \cong H$ and $y \in \mathrm{Aut}(\Gamma)_{\mathbf{0}}$.*

Proof. Lemma 2.6.4 allows Lemma 8.1.1 to be applied so that $K_{\mathbf{0}} \cong \mathrm{Diag}_m(H)$ and H acts semi-regularly on $Q_i^\times$, for all $i \in M$. Thus $K_{\mathbf{0}} = \{(h, h^{\tau_2}, \ldots, h^{\tau_m}) \mid h \in H\}$, where $\tau_i \in \mathrm{Aut}(H)$ for $i = 2, \ldots, m$. Let r be the number of orbits of H on $Q_i^\times$. Then we can identify $Q_i^\times$ with a disjoint union of r copies of H, and thereby identify each τ_i with an element of $\mathrm{Sym}(Q_i^\times)$. Let $y = (1, \tau_2^{-1}, \ldots, \tau_m^{-1})$. Then $y \in \prod_{i \in M} \mathrm{Sym}(Q_i^\times) \leqslant (\mathrm{Aut}(\Gamma))_{\mathbf{0}}$ and,

$$\begin{aligned}(h, h^{\tau_2}, \ldots, h^{\tau_m})^y &= (h, h^{\tau_2\tau_2^{-1}}, \ldots, h^{\tau_m\tau_m^{-1}}) \\ &= (h, h, \ldots, h)\end{aligned}$$

Hence $\mathrm{Diag}_m(H) \leqslant (\mathrm{Aut}(C^y))_{\mathbf{0}}$. □

From Proposition 2.5.5, if an $(X, 2)$-neighbour-transitive code C satisfies $\delta \geqslant 5$ then $X_{\mathbf{0},i}^{Q_i^\times}$ acts transitively on $Q_i^\times$. The following lemma shows that in fact $X_{\mathbf{0},i,j}^{Q_i^\times}$ also acts transitively on $Q_i^\times$, which allows a connection to be made between $X_{\mathbf{0},i,j}^{Q_i^\times}$ and $X_{\mathbf{0},i,j}^{M}$ in Lemma 8.1.4.

Lemma 8.1.3. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 5$ and $\mathbf{0} \in C$. Then the stabiliser $X_{\mathbf{0},i,j}$ of distinct $i, j \in M$ is transitive on each of the sets $Q_i^\times$ and $Q_j^\times$, and has at most two orbits on $Q_i^\times \times Q_j^\times$. If there are two orbits on $Q_i^\times \times Q_j^\times$, then they have equal size.*

Proof. Now $X_{\mathbf{0}}$ acts transitively on $\Gamma_2(\mathbf{0})$, by Proposition 2.5.3, since $\delta \geqslant 5$. Thus, it can be deduced 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. By Proposition 2.5.3, $X_{\mathbf{0}}$ acts 2-homogeneously on M. Suppose $X_{\mathbf{0}}$ is 2-homogeneous, but not 2-transitive, on M. It follows that $X_{\mathbf{0},i,j} = X_{\mathbf{0},\{i,j\}}$ has one orbit on $Q_i^\times \times Q_j^\times$ and is thus transitive on $Q_i^\times$ and $Q_j^\times$. Suppose $X_{\mathbf{0}}$ is 2-transitive on M and $X_{\mathbf{0},i,j}$ has two orbits on $Q_i^\times \times Q_j^\times$. 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, say k, 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 $Q_i^\times \times Q_j^\times$ which implies $k = 1$, since if $k \geqslant 2$ then $k^2 \geqslant 4$, a contradiction. □

Lemma 8.1.4. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 5$, and $i, j \in M$ be distinct. Then,*

1. $X_{\mathbf{0},i}^{Q_i^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times}$ *is isomorphic to a quotient of* $X_{\mathbf{0},i}^{M}$*, and,*
2. $X_{\mathbf{0},i,j}^{Q_i^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times}$ *and* $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times \times Q_j^\times}$ *are isomorphic to quotients of* $X_{\mathbf{0},i,j}^{M}$.

Proof. Recall that round brackets indicate that we are fixing a set point-wise. To obtain part 1, let $Y = X_{\mathbf{0},i}$, $H = X_{\mathbf{0},(Q_i)}$ and $\Omega = Q_i^\times$ in the following. To obtain part 2, let

$$(Y, H, \Omega) = (X_{\mathbf{0},i,j}, X_{\mathbf{0},(Q_i),j}, Q_i^\times) \quad \text{and} \quad (X_{\mathbf{0},i,j}, X_{\mathbf{0},(Q_i),(Q_j)}, Q_i^\times \times Q_j^\times),$$

respectively. In each case, H is the kernel of the action of Y on Ω. Lemma 8.1.1 implies that $H \cap K_{\mathbf{0}} = 1$, since each H fixes an element of $Q_i^\times$. Thus, $K_{\mathbf{0}} = K_{\mathbf{0}}/(H \cap K_{\mathbf{0}}) \cong K_{\mathbf{0}}H/H$ and $K_{\mathbf{0}}H/K_{\mathbf{0}} \cong H/(H \cap K_{\mathbf{0}}) = H$. Hence,

$$Y^\Omega \Big/ K_{\mathbf{0}}^\Omega \cong Y/H \Big/ K_{\mathbf{0}}H/H \cong Y \Big/ (K_{\mathbf{0}}H) \cong Y/K_{\mathbf{0}} \Big/ K_{\mathbf{0}}H/K_{\mathbf{0}} \cong (Y/K_{\mathbf{0}})/H \cong Y^M/H.$$

□

The following divisibility conditions, implied by Lemma 8.1.3, will prove to be useful later in the elimination of many pairs of groups and codes.

Lemma 8.1.5. *Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 5$. Then,*

1. $(q-1)^2$ *divides each of* $2\left|X_{\mathbf{0},i,j}\right| = 2\left|K_{\mathbf{0}}\right|\left|X^M_{\mathbf{0},i,j}\right|$ *and* $2\left|X^{Q_i^\times \times Q_j^\times}_{\mathbf{0},i,j}\right|$,
2. $q-1$ *divides* $2\left|X^M_{\mathbf{0},i,j}\right|$, *and,*
3. $\left|X^{Q_i^\times}_{\mathbf{0},i} : X^{Q_i^\times}_{\mathbf{0},i,j}\right|$ *divides* $m-1$.

Proof. By Lemma 8.1.3, $X^{Q_i^\times \times Q_j^\times}_{\mathbf{0},i,j}$ is either transitive on $Q_i^\times \times Q_j^\times$, or has two, equal sized, orbits. Thus, $2\left|X^{Q_i^\times \times Q_j^\times}_{\mathbf{0},i,j}\right|$ and $2\left|X_{\mathbf{0},i,j}\right| = 2\left|K_{\mathbf{0}}\right|\left|X^M_{\mathbf{0},i,j}\right|$ are divisible by $(q-1)^2$, since $X^{Q_i^\times \times Q_j^\times}_{\mathbf{0},i,j}$ is a quotient of $X_{\mathbf{0},i,j}$, by Lemma 8.1.4. Since $X^M_{\mathbf{0},i,j} \cong X_{\mathbf{0},i,j}/K_{\mathbf{0}}$ and Lemma 8.1.1 implies $|K_{\mathbf{0}}|$ divides $q-1$, we have that $q-1$ divides $2\left|X^M_{\mathbf{0},i,j}\right|$.

Since X acts 2-homogeneously on M, by Proposition 2.5.3, it follows that $\left|X^M_{\mathbf{0},i} : X^M_{\mathbf{0},i,j}\right| = m-1$ or $(m-1)/2$. By Lemma 8.1.4, there exist $N_1 \trianglelefteq X^M_{\mathbf{0},i}$ and $N_2 \trianglelefteq X^M_{\mathbf{0},i,j}$ such that $X^{Q_i^\times}_{\mathbf{0},i}/K^{Q_i^\times}_{\mathbf{0}} \cong X^M_{\mathbf{0},i}/N_1$ and $X^{Q_i^\times}_{\mathbf{0},i,j}/K^{Q_i^\times}_{\mathbf{0}} \cong X^M_{\mathbf{0},i,j}/N_2$. This implies that $|K_{\mathbf{0}}|\,|N_1| = \left|X_{\mathbf{0},(Q_i)}\right|$ and $|K_{\mathbf{0}}|\,|N_2| = \left|X_{\mathbf{0},(Q_i),j}\right|$. Now, $X_{\mathbf{0},(Q_i),j} = X_{\mathbf{0},i,j} \cap X_{\mathbf{0},(Q_i)}$, so that $|N_2|$ divides $|N_1|$. Let $n = |N_1|\,/\,|N_2|$. Then,

$$\left|X^{Q_i^\times}_{\mathbf{0},i} : X^{Q_i^\times}_{\mathbf{0},i,j}\right| = \frac{\left|X^{Q_i^\times}_{\mathbf{0},i} \Big/ K^{Q_i^\times}_{\mathbf{0}}\right|}{\left|X^{Q_i^\times}_{\mathbf{0},i,j} \Big/ K^{Q_i^\times}_{\mathbf{0}}\right|} = \frac{\left|X^M_{\mathbf{0},i}/N_1\right|}{\left|X^M_{\mathbf{0},i,j}/N_2\right|} = \frac{k}{n},$$

where $k = m-1$ or $(m-1)/2$. Thus, $\left|X^{Q_i^\times}_{\mathbf{0},i} : X^{Q_i^\times}_{\mathbf{0},i,j}\right|$ divides $m-1$. □

Given that C is $(X, 2)$-neighbour-transitive with $\delta \geqslant 5$, Proposition 2.5.5 and Lemma 8.1.3 imply that both $X^{Q_i^\times}_{\mathbf{0},i}$ and $X^{Q_i^\times}_{\mathbf{0},i,j}$ act transitively on $Q_i^\times$. Moreover, $K^{Q_i^\times}_{\mathbf{0}} \trianglelefteq X^{Q_i^\times}_{\mathbf{0},i}$ and $K^{Q_i^\times}_{\mathbf{0}} \trianglelefteq X^{Q_i^\times}_{\mathbf{0},i,j}$, with $K^{Q_i^\times}_{\mathbf{0}}$ acting semi-regularly on $Q_i^\times$, by Lemma 8.1.1. Also, Lemma 8.1.4 provides connections between actions of various subgroups of $X_{\mathbf{0}}$ on the alphabet and on the entries. None of these results have required that C is X-alphabet-affine. Imposing this condition now enables the use of the classification of finite transitive linear groups. Tables 8.1.1 and 8.1.2 list the soluble and insoluble, respectively, transitive linear groups $G_0 \leqslant \mathrm{GL}_d(p)$ and their semi-regular normal subgroups N. Note that any semi-regular normal subgroup $N \leqslant G_0$ is either soluble, or contains $\mathrm{SL}_2(5)$ as a subgroup.

Lemma 8.1.6. *Let C be an X-alphabet-affine and $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 5$. Then $K_{\mathbf{0}}$ is soluble.*

Proof. Suppose $K_{\mathbf{0}}$ is insoluble. Now, $X^{Q_i^\times}_{\mathbf{0},i} \leqslant \mathrm{GL}_d(p)$ is transitive on $Q_i^\times$, by Proposition 2.5.5. Also, $K_{\mathbf{0}} \cong K^{Q_i^\times}_{\mathbf{0}} \trianglelefteq X^{Q_i^\times}_{\mathbf{0},i}$ and $K_{\mathbf{0}}$ acts semi-regularly on $Q_i^\times$, by Lemma 8.1.1. Thus, Table 8.1.2 implies that $\mathrm{SL}_2(5) \trianglelefteq K_{\mathbf{0}}$ and $q = p^d$ with $p = 11, 19, 29$ or 59 and $d = 2$.

G_0	parameters	semi-regular N
$G_0 \leqslant \Gamma\mathrm{L}_1(p^d)$	$q = p^d$	numerous
$\mathrm{SL}_2(3) \trianglelefteq G_0$	$p = 3, 5, 7, 11, 23$, $d = 2$	$N \leqslant \mathbb{F}_p^\times$, or $p = 3$ and $N = Q_8$
$2_-^{1+4} \trianglelefteq G_0$	$p^d = 3^4$	$N \leqslant \mathbb{F}_3^\times$

Table 8.1.1: The soluble transitive linear groups G_0 and their semi-regular normal subgroups N.

G_0	parameters $q = p^d$	semi-regular N
$\mathrm{SL}_{d/k}(p^k) \trianglelefteq G_0$	$(d/k, p^k) \neq (2,2), (2,3)$	$N \leqslant \mathbb{F}_{p^k}^\times$
$\mathrm{Sp}_{d/k}(p^k) \trianglelefteq G_0$	d/k even	$N \leqslant \mathbb{F}_{p^k}^\times$
$\mathrm{G}_2(2^k)' \trianglelefteq G_0$	$d = 6k$, $k \geqslant 1$	$N \leqslant \mathbb{F}_{2^k}^\times$
$\mathrm{SL}_2(5) \trianglelefteq G_0$	$p = 11, 19, 29, 59$, $d = 2$	$\mathrm{SL}_2(5) \trianglelefteq N$ or $N \leqslant \mathbb{F}_p^\times$
$\mathrm{A}_6 \trianglelefteq G_0$	$p = 2, d = 4$	trivial
$\mathrm{A}_7 \trianglelefteq G_0$	$p = 2, d = 4$	trivial
$\mathrm{SL}_2(5) \trianglelefteq G_0$	$p = 3, d = 4$	$N \leqslant \mathbb{F}_9^\times$
$2_-^{1+4}.\mathrm{A}_5 \trianglelefteq G_0$	$p^d = 3^4$	$N \leqslant \mathbb{F}_3^\times$
$\mathrm{SL}_2(13) \trianglelefteq G_0$	$p = 3, d = 6$	$N \leqslant \mathbb{F}_3^\times$

Table 8.1.2: The insoluble transitive linear groups $G_0 \leqslant \mathrm{GL}_d(p)$ and semi-regular normal subgroups $N \trianglelefteq G_0$. Note that in the third from last line $G_0 \leqslant \Gamma\mathrm{L}_2(9)$ and $\mathrm{SL}_2(5)$ is not semi-regular.

By Lemma 8.1.2 we may assume that $D = \{(h,h) \mid h \in S\} \trianglelefteq X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$, where $S \cong \mathrm{SL}_2(5)$. Hence, $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ is contained in the normaliser $N_{A\times A}(D)$, where $A = N_{\mathrm{GL}_d(p)}(S)$. Now $(h_1, h_2) \in N_{A\times A}(D)$ implies $h_1 h_2^{-1}$ is an element of the centraliser $C_A(S) = \mathbb{F}_p^\times$ so that $h_1 \in N_A(S)$ and $h_2 = h_1 h'$ for some $h' \in C_A(S)$. Hence, $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ has order dividing $|A||Z(A)| = 60(p-1)^2$, as S_5 is not a subgroup of $\mathrm{PGL}_2(p)$. By Lemma 8.1.5, $(q-1)^2 = (p+1)^2(p-1)^2$ must divide $2\left|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}\right|$ so that $(p+1)^2$ divides 120, which gives a contradiction. □

Combining Lemmas 8.1.4 and 8.1.6 gives the following connection between non-abelian composition factors of different actions of X.

Lemma 8.1.7. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 5$. Then any non-abelian composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$ appears as a composition factor of $X_{\mathbf{0},i}^M$, and any non-abelian composition factor of $X_{\mathbf{0},i,j}^{Q_i^\times}$ or $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ appears as a composition factor of $X_{\mathbf{0},i,j}^M$.*

Proof. By Lemma 8.1.6, $K_{\mathbf{0}}$ is soluble, and so it follows, from Lemma 8.1.4, that each of $X_{\mathbf{0},i}^{Q_i^\times}$,

$X_{\mathbf{0},i,j}^{Q_i^\times}$ and $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ are insoluble precisely when the relevant quotient

$$X_{\mathbf{0},i}^{Q_i^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times}, \quad X_{\mathbf{0},i,j}^{Q_i^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times} \quad \text{or} \quad X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times \times Q_j^\times},$$

is insoluble. Hence, any non-abelian composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$ appears as a composition factor of $X_{\mathbf{0},i}^{M}$, and of $X_{\mathbf{0},i,j}^{Q_i^\times}$ and $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ appears as a composition factor of $X_{\mathbf{0},i,j}^{M}$. □

8.2 Modules as blocks of imprimitivity

The previous section has provided tools with which to analyse groups $X_{\mathbf{0}} \leqslant \mathrm{Aut}(\Gamma)$ that act transitively on $\Gamma_2(\mathbf{0})$. Section 8.4 puts these tools to work. This section instead focuses on the structure of an $(X, 2)$-neighbour-transitive code. Investigating the kernel K of the action of X on M allows blocks of imprimitivity to be identified. Note that, for a group G and a prime p, the *p-core* $O_p(G)$ is the largest normal p-subgroup of G.

Lemma 8.2.1. *Let C be an X-alphabet-affine code in $H(m, q)$, where $q = p^d$ for some prime p, and $i \in M$. Then the p-core $O_p(K^{Q_i})$ of K^{Q_i} is the unique minimal normal subgroup of $X_i^{Q_i}$.*

Proof. By Definition 1.2.1, X^M is transitive, $K \neq 1$ and $X_i^{Q_i}$ is a 2-transitive affine group. It follows that X_i and X_j are conjugate in X for all $i, j \in M$. Since $K \lhd X$ it follows that $K^{Q_i} \lhd X_i^{Q_i}$ for each $i \in M$, and since X^M is transitive it follows that K^{Q_i} is isomorphic to K^{Q_j}. Now $K \leqslant \prod_{i \in M} K^{Q_i}$ which implies, since $K \neq 1$, that $K^{Q_i} \neq 1$ for all $i \in M$. By hypothesis, we have $X_i^{Q_i} \cong T_i \rtimes G_0$, where $T_i \cong \mathbb{Z}_p^d$ is the minimal normal subgroup of $X_i^{Q_i}$ and G_0 acts transitively on $Q_i^\times$. Hence K^{Q_i} contains T_i as a normal subgroup. Since T_i is a normal p-subgroup of K^{Q_i}, it is contained in $O_p(K^{Q_i})$. Since $O_p(K^{Q_i})$ is characteristic in K^{Q_i} it follows that $O_p(K^{Q_i}) \leqslant O_p(X_i^{Q_i})$. We claim that $O_p(X_i^{Q_i}) = T_i$, from which the result follows.

Suppose $O_p(X_i^{Q_i})$ strictly contains T_i. Then there exists a normal p-subgroup P of G_0 such that $O_p(X_i^{Q_i}) = T_i \rtimes P$. Consider the orbits of P on the non-zero vectors of $V = \mathbb{F}_p^d$. The length of each orbit is divisible by p^s, for some s. However, there are $p^d - 1$ non-zero vectors and so there is at least one fixed point. Now, G_0 is transitive on the non-zero vectors and P is normal in G_0, and thus each orbit on non-zero vectors has the same size. It follows that P fixes each vector, and is thus trivial. □

Lemma 8.2.2. *Let C be an X-alphabet-affine code in $H(m, q)$ where $q = p^d$. Let $G = \prod_{i \in M} K^{Q_i}$ and T_i be the minimal normal subgroup of $X_i^{Q_i}$. Then $O_p(G) = \prod_{i \in M} T_i$ acts regularly on the vertex set of $H(m, q)$.*

Proof. Let $T = \prod_{i \in M} T_i \cong \mathbb{Z}_p^{dm}$. Suppose T is strictly contained in some normal p-subgroup N of G. Let $N_i = N^{Q_i} \trianglelefteq K^{Q_i}$ for each $i \in M$. Since N is a p-group, so is N_i. Thus, by Lemma 8.2.1, $N_i \leqslant T_i$. Now, $N \leqslant \prod_{i \in M} N_i \leqslant \prod_{i \in M} T_i = T$ contradicting the assumption

that T is strictly contained in N. Finally, T_i acts regularly on Q_i, so that $O_p(G) = \prod_{i\in M} T_i$ acts regularly on $\prod_{i\in M} Q_i$, the vertex set of $H(m,q)$. □

Lemma 8.2.3. *Let C be an X-alphabet-affine code in $H(m,q)$ with $q = p^d$, and G, T_i be as in Lemma 8.2.2. Then $O_p(K) = K \cap O_p(G)$ is normal in X, the orbit of the vertex $\mathbf{0}$ under $O_p(K)$ is an $FX_{\mathbf{0}}$-module, where F has characteristic p, and $K = O_p(K) \rtimes K_{\mathbf{0}}$.*

Proof. Now, because $O_p(G)$ is normal in G and $K \leqslant G$, it follows that $K \cap O_p(G) \trianglelefteq K$, and as $K \cap O_p(G)$ is a p-group it lies in $O_p(K)$. Suppose $O_p(K)$ strictly contains $K \cap O_p(G)$. Then Lemma 8.2.2 implies that there exists an $i \in M$ such that $O_p(K)^{Q_i}$ strictly contains $O_p(G)^{Q_i} \cong T_i$. Since $O_p(K)$ is normal in K, it follows that $O_p(K)^{Q_i}$ is a normal p-subgroup of K^{Q_i} strictly containing T_i. However, $O_p(K^{Q_i}) = T_i$, by Lemma 8.2.1. Hence $O_p(K) = K \cap O_p(G)$ and $\mathbf{0}^{O_p(K)}$ is an $FX_{\mathbf{0}}$-submodule of $T = \prod_{i\in M} T_i \cong \mathbb{Z}_p^{dm}$. Now, $G_{\mathbf{0}} = \prod_{i\in M} K_{\mathbf{0}}^{Q_i^\times}$, so that $O_p(G) \cap G_{\mathbf{0}} = 1$. Also, $O_p(G) = T$ is transitive on the set of vertices of $H(m,q)$, so that $G = O_p(G) \rtimes G_{\mathbf{0}}$. Thus $K = O_p(K) \rtimes K_{\mathbf{0}}$. □

Lemma 8.2.3 is the major idea of this section. The next result is needed for Proposition 8.2.5, which proves part 1 of Theorem 8.1.

Lemma 8.2.4. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 5$, and $C \neq \mathrm{Rep}(m,2)$ if $q = 2$, such that the group T_C of translations by codewords of C is contained in X. Then $X_{i,j}$ acts transitively on $Q_i \times Q_j$.*

Proof. By Lemma 2.6.4, the weight δ codewords form a q-ary 2-(m,δ,λ) design, for some $\lambda > 0$. Thus, for all $a \in Q_i^\times$ and $b \in Q_j^\times$, there exists at least one weight δ codeword α such that $\alpha_i = a$ and $\alpha_j = b$. Hence, for all $a \in Q_i^\times$ and $b \in Q_j^\times$, there exists $h \in T_C$ such that $0^{h_i} = a$ and $0^{h_j} = b$. Since $C \neq \mathrm{Rep}(m,2)$ it follows from Lemma 2.6.1 that $\delta \neq m$. Thus, there exist $\beta \in C$ and distinct $i', j' \in M$ such that $\beta_{i'} = 0$ and $\beta_{j'} = c'$, for some $c' \in Q_{j'}^\times$. By Proposition 2.5.3, $X_{\mathbf{0}}$ acts 2-homogeneously on M, so there exists some $\gamma \in C$ such that either $\gamma_i = 0$ and $\gamma_j = c$, for some $c \in Q_j^\times$, or $\gamma_i = c$ and $\gamma_j = 0$, for some $c \in Q_i^\times$. Suppose $\gamma \in C$ where $\gamma_i = c$ and $\gamma_j = 0$, for some $c \in Q_i^\times$. Now, for all $b \in Q_j^\times$ there exists an $\alpha \in C$ and $t_\alpha \in X$, with $\alpha_i = -c$ and $\alpha_j = b$, so that $\gamma' = \gamma^{t_\alpha} \in C$ where ${\gamma'}_i = 0$ and ${\gamma'}_j = b$. Also, for all $a \in Q_i^\times$ there exists an $\alpha' \in C$ and $t_{\alpha'} \in X$, with ${\alpha'}_i = a$ and ${\alpha'}_j = -b$, so that $\gamma'' = {\gamma'}^{t_{\alpha'}} \in C$ where ${\gamma''}_i = a$ and ${\gamma''}_j = 0$. A similar argument holds if $\gamma \in C$ where $\gamma_i = 0$ and $\gamma_j = c$, for some $c \in Q_j^\times$. Thus, for all $a \in Q_i$ and $b \in Q_j$ there exists some $\alpha \in C$, and hence $t_\alpha \in T_C$, such that $\alpha_i = a$ and $\alpha_j = b$. Since, by assumption, $T_C \leqslant X$ and hence $T_C \leqslant X_{i,j}$, it follows that $X_{i,j}$ acts transitively on $Q_i \times Q_j$. □

Recall Definition 7.1 of an $(X,2)$-neighbour-transitive extension.

Proposition 8.2.5. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in the Hamming graph $H(m,q)$ with $q = p^d$, $\delta \geqslant 5$ and $\mathbf{0} \in C$. Then C is an $(X,2)$-neighbour-transitive extension of W, where W is the code formed by the orbit of $\mathbf{0}$ under $O_p(K)$, where $K = X \cap B$. It follows that:*

1. $X_W = O_p(K) \rtimes X_{\mathbf{0}}$,
2. W *is* X_W*-alphabet-affine,*
3. W *is* $(X_W,2)$*-neighbour-transitive with minimum distance* $\delta_W \geqslant 5$,
4. W *is an* $FX_{\mathbf{0}}$*-module for some characteristic* p *field* F*, and,*
5. *if* $W \neq \mathrm{Rep}(m,2)$ *then* q^2 *divides* $|W|$.

Proof. By Lemma 8.2.3, $W = \mathbf{0}^{O_p(K)}$ is an $FX_{\mathbf{0}}$-module, for some field F of characteristic p, $O_p(K) \trianglelefteq X$, and $K = O_p(K) \rtimes K_{\mathbf{0}}$. In particular, part 4 is proved. By Lemma 8.2.2, $O_p(G) \cong \mathbb{Z}_p^{dm}$ acts regularly on the vertex set of $H(m,q)$, from which it follows that $T_W = O_p(K) \trianglelefteq X$. Now, $T_W \trianglelefteq X$ implies that W is a block of imprimitivity for the action of X on C. By assumption W contains $\mathbf{0}$, which implies that $X_{\mathbf{0}}$, and thus $K_{\mathbf{0}}$, fixes W. Thus $K = K_W$, and so C is an $(X,2)$-neighbour-transitive extension of W. As T_W is transitive on W, we have $X_W = T_W \rtimes X_{\mathbf{0}}$, proving part 1. By Lemma 7.1.2, W is $(X_W,2)$-neighbour-transitive and $\delta_W \geqslant 5$, which gives part 3. Now, T_W, and hence K, is non-trivial, $X_{W,i}^{Q_i} \leqslant X_i^{Q_i} \leqslant \mathrm{AGL}_d(p)$ and, by Proposition 2.5.3, $X_{\mathbf{0}}$ acts transitively on M, so that W is X_W-alphabet-affine, establishing part 2.

Suppose $W \neq \mathrm{Rep}(m,2)$ and fix $i,j \in M$ with $i \neq j$. Suppose there are k codewords $\alpha \in W$ such that $\alpha_i = \alpha_j = 0$. Lemma 8.2.4 implies that $X_{W,i,j}$ acts transitively on $Q_i \times Q_j$. Thus, for any $a \in Q_i$ and $b \in Q_j$ there are a constant number k of codewords $\beta \in W$ such that $\beta_i = a$ and $\beta_j = b$. Therefore, $|W| = kq^2$, proving part 5. □

By Proposition 8.2.5, every X-alphabet-affine and $(X,2)$-neighbour-transitive code with $\delta \geqslant 5$ is an $(X,2)$-neighbour-transitive extension of some $\mathbb{F}_p$-subspace W of the vertex set $V \cong \mathbb{F}_p^{dm}$ of $H(m,q)$. Since W must also be $(X_W,2)$-neighbour-transitive, classifying $(X,2)$-neighbour-transitive codes requires knowledge of all subspaces of V which form 2-neighbour-transitive codes, and all $(X,2)$-neighbour-transitive extensions of them. In fact, given a subgroup $X_{\mathbf{0}}$ of $\mathrm{Aut}(\Gamma)_{\mathbf{0}}$ such that $X_{\mathbf{0}}$ acts transitively on $\Gamma_2(\mathbf{0})$, any $\mathbb{F}_pX_{\mathbf{0}}$-submodule W, with minimum distance $\delta_W \geqslant 5$, of V will be $(X_W,2)$-neighbour-transitive, with $X_W = T_W \rtimes X_{\mathbf{0}}$. This suggests first classifying all such groups $X_{\mathbf{0}}$ and then considering $\mathbb{F}_pX_{\mathbf{0}}$-submodules of V.

Suppose $X_{\mathbf{0}}$ acts transitively on $\Gamma_2(\mathbf{0})$. If $q = 2$, this occurs precisely when $X_{\mathbf{0}} \cong X_{\mathbf{0}}^M$ acts 2-homogeneously on M, since in this case $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ is trivial. In Section 9.7, submodules of 2-homogeneous $\mathbb{F}_2$ permutation modules are considered in some detail. Conversely, if $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$

is trivial, then Lemma 8.1.5 implies $(q-1)^2 \leqslant 2$, and hence $q = 2$. Thus, in the remainder of the chapter it is assumed that $q \geqslant 3$.

The result below will be useful in the next section.

Corollary 8.2.6. *Suppose C is an X-alphabet-affine and $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $q = p^d$, $\delta \geqslant 5$ and $|C| = q^2$. Then C is a vector subspace of the vertex set $V \cong \mathbb{F}_p^{dm}$ of $H(m, q)$ and $X = T_C.X_{\mathbf{0}}$, where T_C is the group of translations by codewords in C.*

Proof. By Theorem 7.2, C is not an $(X, 2)$-neighbour-transitive extension of $\mathrm{Rep}(m, 2)$, since $|C| = q^2$. By Proposition 8.2.5, C is an $(X, 2)$-neighbour-transitive extension of W, where W is an $FX_{\mathbf{0}}$-module, $X_W = T_W \rtimes X_{\mathbf{0}}$, and q^2 divides $|W|$. Since $|C| = q^2$ it follows that $C = W$. □

8.3 Codes of length at most 8

This section considers particular small cases of m and q. Suppose $q \geqslant 3$ and C is an X-alphabet-affine and $(X, 2)$-neighbour-transitive code in $H(m, q)$ with $\delta \geqslant 5$. Then $m \geqslant 6$, since if $m = 5$ then $\delta = 5$ and C is equivalent to the binary repetition code, by Lemma 2.6.1. The next few results deal with the cases $m = 6, 7$ and 8, allowing it to be assumed that $m \geqslant 9$ in the remainder of the chapter. This is simply to avoid having to consider the many isomorphisms between small groups in Section 8.4. First, a general result.

Lemma 8.3.1. *Let C be a 2-regular code in $H(m, q)$ with $\mathbf{0} \in C$, $\delta \geqslant 4$ and $m = \delta + 1$. Then $q = \delta$ and $|C| = q^2$. Moreover, if C is X-alphabet-affine and $(X, 2)$-neighbour-transitive then $q = p^d$, C is an $\mathbb{F}_p X_{\mathbf{0}}$-submodule of $\mathbb{F}_p^{dm}$ and $X = T_C \rtimes X_{\mathbf{0}}$, where T_C is the group of translations by codewords in C.*

Proof. The weight δ codewords form a q-ary 2-design, by Lemma 2.6.4, with $m(q-1)^2\lambda/(m-2)$ blocks, for some $\lambda \geqslant 1$. Let α, β be weight $m-1$ codewords with $\alpha_i = \beta_i$ for $i = 1, 2$. Then $d(\alpha, \beta) \leqslant m-2$ and, since $\delta = m-1$, it follows that $\alpha = \beta$, $\lambda = 1$ and there are exactly $m(q-1)^2/(m-2)$ weight $m-1$ codewords. Since $m \geqslant 5$, it follows that $\gcd(m, m-2)$ divides 2. Thus, $(m-2)/\gcd(2, m)$ divides $q-1$. Let $i \in M$ and consider the code $C[i]$ in $H(m-1, q)$ obtained by projecting the set of all codewords α with $\alpha_i = 0$ onto the set of entries $M \setminus \{i\}$. Now, $C[i]$ is 1-regular with minimum distance m and, by Lemma 2.6.1, is equivalent to the repetition code. Thus $C[i]$ contains $q-1$ weight δ codewords. Since the pre-images of $C[i]$ and $C[j]$ are disjoint for distinct $i, j \in M$, there are exactly $m(q-1)$ weight δ codewords in C. Hence $m-2 = q-1$, so $q = m-1 = \delta$, and there are $m(q-1) = q^2-1$ weight δ codewords.

Suppose there exists a weight $\delta+1 = m$ codeword α. For distinct $i, j \in M$, there must exist, by Lemma 2.6.4, a weight δ codeword β such that $\beta_i = \alpha_i$ and $\beta_j = \alpha_j$. It follows that $d(\alpha, \beta) \leqslant m-2 = \delta-1$ and there are no weight m codewords. The remaining assertions follow from Corollary 8.2.6. □

The projective Reed-Muller codes are defined in generality in Section 9.2, via polynomials from $\mathbb{F}_q^t$ into $\mathbb{F}_q$. The results of this section require some specific instances to be defined. For any prime power q,

$$\mathcal{PRM}_q(1,2) = \{ax_1 + bx_2 \mid a, b \in \mathbb{F}_q\}.$$

Then $\mathcal{PRM}_q(1,2)$ is a code in $H(q+1,q)$ with entry set M equal to the set of all 1-dimensional subspaces of $\mathbb{F}_q^2$, and alphabet Q_i the set of all functions f from the 1-dimensional subspace i into $\mathbb{F}_q$ such that $f(ax) = af(x)$, for all $a \in \mathbb{F}_q$ and $x \in i$. For instance, if $i = \langle(1,1)\rangle \in M$ and $f(x) = ax_1 + bx_2$, then $(f(x))_i = (a+b)x_1$, since $x_1 = x_2$. If $a = b = 0$ then $ax_1 + bx_2$ is the vertex $\mathbf{0}$ of $H(q+1,q)$. Otherwise, $ax_1 + bx_2 = 0$ when $bx_2 = -ax_1$, that is, for x in precisely the 1-space $(b, -a) \in M$. Thus, $\mathcal{PRM}_q(1,2)$ has minimum distance q. Below, it is shown that if p is prime then, up to equivalence, $\mathcal{PRM}_p(1,2)$ is the only 2-neighbour-transitive in $H(p+1,p)$ with minimum distance p.

Lemma 8.3.2. *Let $p \geqslant 5$ be prime and C be an $(X,2)$-neighbour-transitive code in $H(p+1,p)$ with $\delta = p$. Then C is equivalent to the projective Reed-Muller code $\mathcal{PRM}_p(1,2)$. Moreover, $X_{\mathbf{0}}^M$ is not affine.*

Proof. Since $\delta \geqslant 5$ and $q \geqslant 6$, Theorem 5.2 implies that $K = X \cap B \neq 1$. Thus C is either X-alphabet-almost-simple or X-alphabet-affine. Theorem 6.1 and $\delta \geqslant 5$ then imply that C is X-alphabet-affine. Thus $Q = \mathbb{F}_p$. Let $M = \mathbb{F}_p \cup \{*\}$. By Lemma 8.3.1 we have $|C| = p^2$ and C is an $\mathbb{F}_p$-module. By Lemma 2.6.4, the weight δ codewords form a q-ary 2-design with $b = (p+1)(p-1)^2\lambda/(p-1) = (p^2-1)\lambda$ blocks, for some $\lambda \geqslant 1$. Thus $\lambda = 1$ and C contains only vertices of weight p or 0.

Lemma 2.5.1 allows it to be assumed that $\alpha \in C$ where $\alpha_* = 0$ and $\alpha_i = 1$ for all $i \in \mathbb{F}_p$. Since $X_{\mathbf{0}}$ acts transitively on M, by Proposition 2.5.3, there exists some $\beta \in C$ such that $\beta_0 = 0$. Now C is an $\mathbb{F}_p$-submodule, so it can be assumed that $\beta_* = 1$. Also, for all $a \in \mathbb{F}_p^\times$ the vertex $a\alpha + \beta \in C$ must have weight δ, which implies that there exists a unique $i \in \mathbb{F}_p^\times$ such that $\beta_i = -a$. Thus, up to equivalence, β satisfies $\beta_i = i$ for all $i \in \mathbb{F}_p$ and $C = \langle\alpha, \beta\rangle$. Let $R = \{(1,0), (a,1) \mid a \in \mathbb{F}_p\}$ be a set of representatives for the set of all 1-dimensional subspaces of $\mathbb{F}_p^2$. Let $f_\alpha(x) = x_2 \in \mathcal{PRM}_p(1,2)$ and $f_\beta(x) = x_1 \in \mathcal{PRM}_p(1,2)$. Then $f_\alpha((1,0)) = \alpha_*$, $f_\beta((1,0)) = \beta_*$ and $f_\alpha((1,i)) = \alpha_i$, $f_\beta((1,i)) = \beta_i$ for all $i \in \mathbb{F}_p$. Thus C is equivalent to $\mathcal{PRM}_p(1,2)$.

Suppose T is a regular normal subgroup of $X_{\mathbf{0}}^M$ and let Y be the smallest normal subgroup of $X_{\mathbf{0}}$ that projects onto T. Then either $Y \cong T$ or $Y \cong 2.T$, since $K_{\mathbf{0}} \leqslant \mathbb{F}_p^\times$ and $\gcd(m, q-1) = \gcd(p+1, p) = 1$ or 2. Since $p = \delta \geqslant 5$, it follows that Y does not act transitively on $\cup_{i\in M} Q_i^\times$, which has size $(p-1)|T|$, and the orbits of Y form a system of imprimitivity for the action of $X_{\mathbf{0}}$ on $\cup_{i\in M} Q_i^\times$. Since T acts transitively on M,there exists distinct $i, j \in M$, $a \in Q_i$ and $b \in Q_j$ such that a and b are in the same orbit under Y. However, there also exists some $c \in Q_j$ that is contained in a different Y-orbit to a. It follows that $X_{\mathbf{0}}$ cannot map (a,b) to (a,c), contradicting the fact that $X_{\mathbf{0}}$ acts transitively on $\Gamma_2(\mathbf{0})$. □

The next three results find all X-alphabet-affine and $(X,2)$-neighbour-transitive codes in $H(m,q)$ with $m = 6, 7$ or 8. The only codes which arise are projective Reed-Muller codes when $m = 6$ or 8.

Lemma 8.3.3. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(6,q)$ with $\delta \geqslant 5$ and $q \neq 2$. Then $q = 5$ and C is equivalent to the projective Reed-Muller code $\mathcal{PRM}_5(1,2)$.*

Proof. If $\delta = 6$ then Lemma 2.6.1 implies $q = 2$, so $\delta = 5$. By Lemma 8.3.2 C is equivalent to the projective Reed-Muller code $\mathcal{PRM}_5(1,2)$. □

Lemma 8.3.4. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 5$ and $q \neq 2$. Then $m \neq 7$.*

Proof. Suppose $m = 7$. If $\delta = 7$ then Lemma 2.6.1 implies $q = 2$, so $\delta \leqslant 6$. Suppose $\delta = 6$. Then Lemma 8.3.1 gives $q = 6$, which is not a power of a prime. Thus $\delta = 5$. Then the Singleton bound (see Section 2.1) and Proposition 8.2.5 together give $q^2 \leqslant |C| \leqslant q^3$. The set of weight 5 codewords forms a q-ary design with $21(q-1)^2\lambda_5/10$ blocks, for some integer $\lambda_5 \geqslant 1$. Since $\delta = 5$, there is at least one weight 5 codeword, so 10 divides $(q-1)\lambda_5$. Let $i,j \in M$ be distinct and consider the projection $C[i,j]$ of the set of all weight 5 codewords α with $\alpha_i = \alpha_j = 0$, into the Hamming graph $H(5,q)$ with entry set $M \setminus \{i,j\}$. Note, $C[i,j]$ has minimum distance 5, and is thus, by Lemma 2.6.1, a subset of the repetition code. Hence, considering $C[i,j]$ for each choice of distinct $i,j \in M$, there are at most $21(q-1)$ weight 5 codewords. It follows that $(q-1)\lambda_5 \leqslant 10$, and here equality holds, so $(q,\lambda_5) = (3,5)$ or $(11,1)$, since $q \neq 2$ and is a prime power. If $q = 3$ then this implies there are at least $21(q-1)^2\lambda_5/10 = 21 \cdot 2$ codewords, contradicting $|C| \leqslant q^3$, so $q = 11$.

By Proposition 2.5.3 $X_{\mathbf{0}}^M$ is a 2-homogeneous group acting on 7 points, so is one of $\mathrm{PSL}_3(2)$, A_7, S_7 or a subgroup of $\mathrm{AGL}_1(7)$ which have 2-point stabilisers $\mathbb{Z}_2 \times \mathbb{Z}_2$, A_5, S_5 or 1, respectively. By Lemma 8.1.5 we have $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \cong \mathbb{F}_{11}^\times \times \mathbb{F}_{11}^\times$, or the unique index 2 subdirect subgroup of this, and 10 divides $2|X_{\mathbf{0},i,j}^M|$. Thus $X_{\mathbf{0},i,j}^M \cong \mathrm{A}_5$ or S_5, contradicting Lemma 8.1.7, since A_5 is not a composition factor of $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ and $\left| X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \Big/ K_{\mathbf{0}}^{Q_i^\times \times Q_j^\times} \right| \geqslant 5$. □

Lemma 8.3.5. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(8,q)$ with $\delta \geqslant 5$ and $q \neq 2$. Then $q = 7$ and C is equivalent to a projective Reed-Muller code $\mathcal{PRM}_7(1,2)$ and $X \cong \mathrm{PSL}_2(7)$ or $\mathrm{PGL}_2(7)$.*

Proof. If $\delta = 8$ then Lemma 2.6.1 implies $q = 2$, so we have $\delta \leqslant 7$. By Proposition 2.5.3, $X_{\mathbf{0}}^M$ is a 2-homogeneous group on 8 points, that is, one of: $\mathrm{AGL}_1(8)$, $\mathrm{A\Gamma L}_1(8)$, $\mathrm{AGL}_3(2)$, $\mathrm{PSL}_2(7)$, $\mathrm{PGL}_2(7)$, A_8, or S_8. Thus $X_{\mathbf{0},i,j}^M$ is one of:

$$1, \mathbb{Z}_3, \mathrm{S}_4, \mathbb{Z}_3, \mathbb{Z}_6, \mathrm{A}_6, \quad \text{or,} \quad \mathrm{S}_6, \tag{8.3.1}$$

respectively.

Suppose $\delta = 7$. Then C is equivalent to the projective Reed-Muller code $\mathcal{PRM}_7(1,2)$, by Lemma 8.3.2.

Suppose $\delta = 6$. Then the weight 6 codewords form a q-ary 2-design with $28(q-1)^2\lambda_6/15$ blocks, for some integer $\lambda_6 \geqslant 1$. Fix $i, j \in M$, with $i \neq j$, $a \in Q_i^\times$ and $b \in Q_j^\times$. Let

$$S = \{\{k,\ell\} \mid \alpha \in \Gamma_6(\mathbf{0}) \cap C; \alpha_i = a, \alpha_j = b, \alpha_k = 0, \alpha_\ell = 0, k \neq \ell\}.$$

If $\{k,\ell\} \in S$ then $\{k,\ell\} \subseteq M \setminus \{i,j\}$. Also, any two elements of S intersect trivially, since $\delta = 6$. Thus $|S| \leqslant 3$ and $\lambda_6 \leqslant 3$. Let $i, j \in M$ be distinct and $C[i,j]$ be the code in $H(6,q)$ obtained by projecting the set of all weight 6 codewords α such that $\alpha_i = \alpha_j = 0$ onto the entries $M \setminus \{i,j\}$. The code $C[i,j]$ as minimum distance 6, and so, by Lemma 2.6.1, has size at most $q-1$. It follows that there are at most $28(q-1)$ weight 6 codewords, by considering $C[i,j]$ for all distinct $i, j \in M$. Hence $(q-1)\lambda_6 \leqslant 15$ and we have $(q, \lambda_6) = (16, 1)$, since $q \neq 2$ and is a prime power and $\lambda_6 \leqslant 3$. We consider this case below.

Suppose $\delta = 5$. The weight 5 codewords form a q-ary 2-design with $14(q-1)^2\lambda_5/5$ blocks, for some integer $\lambda_5 \geqslant 1$. Since $\delta = 5$, no two weight 5 codewords α, β with $\alpha_1 = \beta_1 = a$ and $\alpha_2 = \beta_2 = b$ can have $\alpha_i = \beta_i = \alpha_j = \beta_j = 0$, for distinct $i, j \neq 1, 2$. Let

$$\mathcal{D} = \{\{i,j,k\} \subseteq M \mid \alpha_i = \alpha_j = \alpha_k = 0, \exists \alpha \in C \cap \Gamma_5(\mathbf{0}), \alpha_1 = a, \alpha_2 = b\}.$$

If $|\mathcal{D}| = 5$, then $\mathcal{D}$ would form the block set of a binary 2-$(6,3,1)$ design. The fact that such a configuration does not exist (see [27, Table 3.3]), shows that $\lambda_5 \leqslant 4$. Thus 5 divides $q-1$.

Let $i, j, k \in M$ be distinct and $C[i,j,k]$ be the code in $H(5,q)$ obtained by projecting the set of all weight 5 codewords α such that $\alpha_i = \alpha_j = \alpha_k = 0$ onto the set of entries $M \setminus \{i,j,k\}$. Considering that $C[i,j,k]$ is a subset of the repetition code, by Lemma 2.6.1, for each choice of i, j, k gives us at most $56(q-1)$ weight 5 codewords. So $(q-1)\lambda_5 = 5, 10, 15$ or 20. This gives $(q, \lambda_5) = (11,1)$, $(11,2)$ or $(16,1)$, since q is a prime power. Suppose $q = 11$. Lemma 8.1.5 implies $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \cong \mathbb{F}_{11}^\times \times \mathbb{F}_{11}^\times$, or the unique index 2 subdirect subgroup of this, so that $K_{\mathbf{0}} \leqslant \mathbb{F}_{11}^\times$. Now, by Lemma 8.1.4, $\mathbb{F}_{11}^\times$ is a quotient of $X_{\mathbf{0},i,j}^M$, which does not occur for the possibilities of $X_{\mathbf{0},i,j}^M$ listed at 8.3.1.

We have that if $\delta = 5$ or 6 then $q = 16$. Thus Lemma 8.1.5 implies 15 divides the order of $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} / K_{\mathbf{0}}^{Q_i^\times \times Q_j^\times}$ and so, by Lemma 8.1.4, divides $|X_{\mathbf{0},i,j}^M|$, which gives $X_{\mathbf{0}}^M \cong \mathrm{A}_8$ or S_8 and $X_{\mathbf{0},i,j}^{Q_i^\times} \cong \mathrm{A}_6$ or S_6. Thus $K_{\mathbf{0}}$ is trivial, by Lemma 8.1.1, which implies $(q-1)^2$ divides $X_{\mathbf{0},i,j}^M$, a contradiction. □

To lead back to the main ideas of this chapter, Corollary 8.3.6 summarises the results of this section in the context of the next. Corollary 8.3.6 follows directly from Lemmas 8.3.3, 8.3.4 and 8.3.5.

Corollary 8.3.6. *Suppose C is an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 5$. Then the following hold:*

1. *If* $m \leqslant 8$ *then* $X_{\mathbf{0},i}^{Q_i^\times}$ *is soluble, and either* $q = 2$*, or* C *is equivalent to one of two projective Reed-Muller codes* $\mathcal{PRM}_5(1,2)$*, with* $(m,q,\delta) = (6,5,5)$*, or* $\mathcal{PRM}_7(1,2)$*, with* $(m,q,\delta) = (8,7,7)$*.*
2. *If* $X_{\mathbf{0},i}^{Q_i^\times}$ *is insoluble, then* $m \geqslant 9$*.*

8.4 Soluble entry stabiliser

The aim of this section is to show that $X_{\mathbf{0},i}^{Q_i^\times}$ is soluble. The proof relies mainly on Lemmas 8.1.6 and 8.1.7, along with the classification of 2-transitive groups. In particular, by Lemma 8.1.7, if either of $X_{\mathbf{0},i}^{Q_i^\times}$ or $X_{\mathbf{0},i,j}^{Q_i^\times}$ is insoluble then $X_{\mathbf{0},i}^M$ or $X_{\mathbf{0},i,j}^M$, respectively, is also insoluble.

Lemma 8.4.1. *Let* C *be an* X*-alphabet-affine and* $(X,2)$*-neighbour-transitive code in* $H(m,q)$ *with* $\delta \geqslant 5$ *such that* $X_{\mathbf{0},i}^{Q_i^\times}$ *is insoluble. Then* m *and* $X_{\mathbf{0}}^M$ *satisfy one of the following,*

1. $X_{\mathbf{0}}^M$ *is an insoluble affine* 2*-transitive group,*
2. $\mathrm{soc}(X_{\mathbf{0}}^M) = \mathrm{A}_9$ *with* $m = 9$*,*
3. $\mathrm{soc}(X_{\mathbf{0}}^M) = \mathrm{Sp}_6(2)$ *with* $m = 28$ *or* 36*,*
4. $\mathrm{soc}(X_{\mathbf{0}}^M) = \mathrm{PSL}_t(r)$*,* $t \geqslant 3$ *and* $(t,r) \neq (3,2),(3,3)$*, with* $m = \frac{r^t-1}{r-1}$*,*
5. $X_{\mathbf{0}}^M = \mathrm{PSL}_2(11)$ *with* $m = 11$*,*
6. $X_{\mathbf{0}}^M = \mathrm{A}_7$ *with* $m = 15$*,*
7. $X_{\mathbf{0}}^M = \mathrm{M}_{11}$ *with* $m = 11$ *or* 12*, or,*
8. $\mathrm{soc}(X_{\mathbf{0}}^M) = \mathrm{M}_{22}$ *with* $m = 22$*.*

Proof. By Corollary 8.3.6, $m \geqslant 9$. By Lemma 8.1.6, $K_{\mathbf{0}}$ is soluble. It follows that $X_{\mathbf{0},i}^{Q_i^\times}$ is insoluble if and only if $X_{\mathbf{0},i}^{Q_i^\times}/K_{\mathbf{0}}^{Q_i^\times}$ is insoluble. By Lemma 8.1.4, $X_{\mathbf{0},i}^{Q_i^\times}/K_{\mathbf{0}}^{Q_i^\times}$ is a quotient of $X_{\mathbf{0},i}^M$, and so $X_{\mathbf{0},i}^M$ must have a non-abelian composition factor which appears as a composition factor of an insoluble transitive linear group, by Lemma 8.1.7. These are listed in Table 8.1.2. By Proposition 2.5.3, $X_{\mathbf{0}}^M$ is 2-homogeneous, in fact 2-transitive since it is insoluble, and thus is affine or almost-simple. If $X_{\mathbf{0}}^M$ is affine, then $X_{\mathbf{0},i}^M$ is a transitive linear group, giving 1.

Suppose $X_{\mathbf{0}}^M$ is almost-simple. If $\mathrm{soc}(X_{\mathbf{0}}) = \mathrm{A}_m$ then A_{m-1} is a composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$, but since A_n is only a composition factor of an insoluble transitive linear group for $n \in \{5,6,7,8\}$, and by hypothesis $m \geqslant 9$, we have $m = 9$, so that 2 holds. Suppose $\mathrm{soc}(X_{\mathbf{0}}) = \mathrm{Sp}_{2t}(2)$ with $m = 2^{2t-1} \pm 2^{t-1}$. The non-abelian composition factor of the point stabiliser is $\Omega_{2t}^{\pm}(2)$, which is only a composition factor of a transitive linear group through the isomorphisms (noting that $m \geqslant 9$) $\Omega_6^-(2) \cong \mathrm{PSp}_4(3)$ and $\Omega_6^+(2) \cong \mathrm{PSL}_4(2)$ when $t = 3$, leading to 3. If $\mathrm{soc}(X_{\mathbf{0}})^M \cong \mathrm{PSL}_t(r)$ then $X_{\mathbf{0},i}^M$ is insoluble, except for when $t = 2$ or when $t = 3$ and $r = 2$ or

3, and the non-abelian composition factor of $X^M_{\mathbf{0},i}$ is also a composition factor of some transitive linear group, producing 4. If $\mathrm{soc}(X_{\mathbf{0}})^M$ is $\mathrm{Sz}(r)$, $\mathrm{Ree}(r)$, $\mathrm{PSU}_3(r)$, or $\mathrm{PSL}_2(8)$ acting on 28 points, then $X^M_{\mathbf{0},i}$ is soluble. The sporadic 2-transitive almost-simple groups M_{12}, M_{23}, M_{24}, HS, and Co_3 have point stabilisers M_{11}, M_{22}, M_{23}, $\mathrm{PSU}_3(5)$, and McL, none of which appears as a composition factor of a transitive linear group. This leaves $\mathrm{PSL}_2(11)$, A_7, M_{11}, and M_{22}, leading to the final four possibilities. □

Y	conditions
$\mathrm{SL}_t(r)$	$t \geqslant 2$, $(t,r) \neq (3,2), (3,3)$
$\mathrm{Sp}_t(r)$	t even, $t \geqslant 4$
$\mathrm{G}_2(r)'$	$t = 6$, r even

Table 8.4.1: Possibilities for the normal subgroup Y of the insoluble transitive linear group $X^M_{\mathbf{0},i}$ in the case that $X^M_{\mathbf{0}}$ is affine, as in Lemma 8.4.2.

Lemma 8.4.2. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$. Suppose $X^M_{\mathbf{0}}$ is affine and $X^{Q_i^\times}_{\mathbf{0},i}$ is insoluble. Then $X^M_{\mathbf{0},i}$ contains either Y as a normal subgroup, where Y satisfies one of the lines of Table 8.4.1.*

Proof. By Corollary 8.3.6 $m \geqslant 9$. By Lemma 8.1.6, $K_{\mathbf{0}}$ is soluble and so any non-abelian composition factor of $X^{Q_i^\times}_{\mathbf{0},i}$ must appear as a composition factor of $X^M_{\mathbf{0},i}$, by Lemma 8.1.7. Showing that $X^M_{\mathbf{0},i}$ cannot be an exceptional insoluble transitive linear action is enough to prove the result, since $\mathrm{SL}_t(r)$, $\mathrm{Sp}_{2t}(r)$ and $\mathrm{G}_2(r)'$ are quasi-simple normal subgroups of the infinite families of insoluble transitive linear groups.

Suppose $X^M_{\mathbf{0},i}$ contains $\mathrm{SL}_2(5)$ as a normal subgroup, $m = r^2$ where $r = 11, 19, 29$ or 59. We then have that $q = q_0^2$, where $q_0 = 4, 5, 9, 11, 19, 29$ or 59. For $r = 11, 19, 29$ and 59 we have that $|X^M_{\mathbf{0},i,j}|$ divides $5, 3, 2$ and 1, respectively. Now, $2|X^M_{\mathbf{0},i,j}|$ must be divisible by $q-1$, by Lemma 8.1.5. This gives a contradiction since $q - 1 \geqslant 15$.

Suppose $X^M_{\mathbf{0},i}$ contains A_6 as a normal subgroup and $m = 2^4$. We have that $q = 2^4$ or 9^2, since $\mathrm{PSL}_2(9) \cong \mathrm{A}_6$. Here $|X^M_{\mathbf{0},i,j}|$ divides $2^4 \cdot 3$. Now, by Lemma 8.1.5, $q-1$ must divide $2|X^M_{\mathbf{0},i,j}|$, but 5 divides $q-1$.

Suppose $X^M_{\mathbf{0},i}$ contains A_7 as a normal subgroup and $m = 2^4$. Here $q = 2^4$, $X^M_{\mathbf{0},i,j} \cong \mathrm{PSL}_3(2)$ and $|X^M_{\mathbf{0},i,j}| = 2^3 \cdot 3 \cdot 7$. Now, by Lemma 8.1.5, $q-1$ must divide $2|X^M_{\mathbf{0},i,j}|$, but 5 divides $q-1$.

Suppose $X^M_{\mathbf{0},i}$ contains $\mathrm{SL}_2(5)$ as a normal subgroup and $m = 3^4$. We then have that $q = q_0^2$, where $q_0 = 4, 5, 9, 11, 19, 29$ or 59. Here $|X^M_{\mathbf{0},i,j}|$ divides 12, but $q - 1 \geqslant 15$ must divide $2|X^M_{\mathbf{0},i,j}|$ by Lemma 8.1.5.

Suppose $X^M_{\mathbf{0},i}$ contains the extra-special group 2^{1+4}_- as a normal subgroup, contains A_5 as a composition factor, and $m = 3^4$. Since $\mathrm{A}_5 \cong \mathrm{PSL}_2(5)$ we have that $q = q_0^2$, where

$q_0 = 4, 5, 9, 11, 19, 29$ or 59. Now, $|X^M_{\mathbf{0},i,j}|$ divides $2^4 \cdot 3$. By Lemma 8.1.5 $q-1$ must divide $2|X^M_{\mathbf{0},i,j}|$, but 5 divides $q-1$ except for when $q_0 = 5$. Let $q_0 = 5$. Then $K_{\mathbf{0}} \leqslant \mathbb{F}_5^\times$ and $|X_{\mathbf{0},i,j}| = |K_{\mathbf{0}}||X^M_{\mathbf{0},i,j}|$ divides $2^6 \cdot 3$. By Lemma 8.1.5, $(q-1)^2$ must divide $2|X_{\mathbf{0},i,j}|$, but 3^2 does not divide $|X_{\mathbf{0},i,j}|$.

Suppose $X^M_{\mathbf{0},i}$ contains $\mathrm{SL}_2(13)$ as a normal subgroup and $m = 3^6$. Then either $q = 13^2$ or 3^6. We have $2|X^M_{\mathbf{0},i,j}|$ divides 3, which is not divisible by $q-1$, contradicting Lemma 8.1.5. □

$\mathrm{soc}(X^M_{\mathbf{0}})$	m	S_i	$S_{i,j}$	conditions	possible q
A_9	9	A_8	A_7	-	2^4
$\mathrm{Sp}_6(2)$	28	$\mathrm{PSp}_4(3)$	A_5	-	3^4
$\mathrm{PSL}_t(r)$	$\frac{r^t-1}{r-1}$	$\mathrm{PSL}_{t-1}(r)$	$\mathrm{PSL}_{t-2}(r)$	$t \geqslant 4$, $(t,r) \neq (4,2), (4,3)$	none
M_{11}	12	$\mathrm{PSL}_2(11)$	A_5	-	11^2
M_{22}	22	$\mathrm{PSL}_3(4)$	A_5	-	none

Table 8.4.2: Non-abelian composition factors S_i and $S_{i,j}$ of $X^{Q_i^\times}_{\mathbf{0},i}$ and $X^{Q_i^\times}_{\mathbf{0},i,j}$, respectively, for the almost-simple groups $X^M_{\mathbf{0}}$ that satisfy Lemma 8.4.1 and have an insoluble two point stabiliser. Note that if $X_{\mathbf{0}} = \mathrm{Sp}_6(2)$ and $m = 36$ then $X^M_{\mathbf{0},i,j}$ is soluble.

Having narrowed down the possibilities for $X^M_{\mathbf{0},i}$ and $X^M_{\mathbf{0},i,j}$, the following two lemmas consider the solubility of $X^{Q_i^\times}_{\mathbf{0},i,j}$ and $X^M_{\mathbf{0},i,j}$.

Lemma 8.4.3. *Let C be an alphabet-affine $(X,2)$-neighbour-transitive code in $H(m,q)$, with $\delta \geqslant 5$, such that $X^M_{\mathbf{0}}$ is an almost-simple group. Then $X^{Q_i^\times}_{\mathbf{0},i,j}$ is soluble.*

Proof. Suppose $X^{Q_i^\times}_{\mathbf{0},i,j}$ is insoluble. Then Corollary 8.3.6 implies that $m \geqslant 9$. Also $X^{Q_i^\times}_{\mathbf{0},i}$ is insoluble, since $X^{Q_i^\times}_{\mathbf{0},i,j} \leqslant X^{Q_i^\times}_{\mathbf{0},i}$. By Lemma 8.1.7, $X^{Q_i^\times}_{\mathbf{0},i}$ and $X^{Q_i^\times}_{\mathbf{0},i,j}$ share a non-abelian composition factor with $X^M_{\mathbf{0},i}$ and $X^M_{\mathbf{0},i,j}$, respectively. By Proposition 2.5.5 and Lemma 8.1.3, $X^{Q_i^\times}_{\mathbf{0},i}$ and $X^{Q_i^\times}_{\mathbf{0},i,j}$ are transitive linear groups. Table 8.4.2 lists the almost-simple groups from Lemma 8.4.1 for which $X^M_{\mathbf{0},i}$ and $X^M_{\mathbf{0},i,j}$ are insoluble. It also gives the possibilities for $X^M_{\mathbf{0}}$, and the possible values of q for which the non-abelian composition factor of both the one and two point stabilisers in the action of $X_{\mathbf{0}}$ on M have a transitive linear action, as in Tables 8.1.1 and 8.1.2. Lemma 8.1.5 gives divisors of various group orders in terms of the parameters m and q, and is enough to eliminate the remaining cases, which we examine below.

Suppose $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{A}_9$ and $m = 9$. We have that $X^{Q_i^\times}_{\mathbf{0},i}$ and $X^{Q_i^\times}_{\mathbf{0},i,j}$ have $\mathrm{A}_8 \cong \mathrm{PSL}_4(2)$ and A_7, respectively, as composition factors. Comparing the transitive linear actions involving these groups forces $X^{Q_i^\times}_{\mathbf{0},i} \cong \mathrm{A}_8$, $X^{Q_i^\times}_{\mathbf{0},i,j} \cong \mathrm{A}_7$, and $q = 2^4$. Since there are no non-trivial semi-regular subgroups of A_8 in this action, $K_{\mathbf{0}}$ is trivial. Since $K_{\mathbf{0}}$ is the kernel of the action of $X_{\mathbf{0}}$ on M, it follows that $X_{\mathbf{0}} \cong X^M_{\mathbf{0}}$. Hence $X_{\mathbf{0}} \cong \mathrm{A}_9$ or S_9 and $X_{\mathbf{0},i,j} \cong \mathrm{A}_7$ or S_7. Now, $(q-1)^2 = 15^2$ must divide $2|X^{Q_i^\times \times Q_j^\times}_{\mathbf{0},i,j}|$. However, 5^2 does not divide $|\,\mathrm{S}_7\,|$.

Suppose $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{Sp}_6(2)$ and $m = 28$. Now, $\Omega_6^-(2) \cong \mathrm{PSp}_4(3)$ and $\Omega_4^-(2) \cong \mathrm{PSL}_2(5)$. This gives $q = 3^4$. The only transitive linear group with composition factor $\mathrm{PSp}_4(3)$ is $\mathrm{Sp}_4(3)$. The only nontrivial normal subgroup of $\mathrm{Sp}_4(3)$ is $\mathbb{F}_3^\times$ and hence the order of $K_{\mathbf{0}}$ divides 2. Now, $|X_{\mathbf{0},i,j}^M| = 2^5|\,\mathrm{A}_5\,|$. Also, $(q-1)^2 = 80^2$ must divide $2|K_{\mathbf{0}}||X_{\mathbf{0},i,j}^M|$. However, $|\,\mathrm{A}_5\,|$ is not divisible by 5^2.

Suppose $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{PSL}_t(r)$ and $m = (r^t-1)/(r-1)$. Since $X_{\mathbf{0},i,j}$ is insoluble, we require $t \geqslant 4$. Since $t-1 \geqslant 3$, consideration of the linear actions involving $\mathrm{PSL}_{t-1}(r)$ gives $q = r^{t-1}$, with the exception of $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ allowing $q = 2^7$. We can eliminate this exception since then $X_{\mathbf{0},i,j}$ would be soluble. We thus require $\mathrm{PSL}_{t-2}(r)$, the non-abelian composition factor of $X_{\mathbf{0},i,j}$, to be involved in a transitive linear action of degree $r^{t-1}-1$, which does not occur.

Suppose $X_{\mathbf{0}}^M = \mathrm{M}_{11}$ and $m = 12$. The one and two point stabilisers have non-abelian composition factors $\mathrm{PSL}_2(11)$ and $\mathrm{PSL}_2(5)$, respectively. Then $q = 11^2$, since $\mathrm{PSL}_2(11)$ is a composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$. Now, $\mathrm{PSL}_2(5)$ is involved in a transitive linear action of the same degree and we have $K_{\mathbf{0}} \leqslant \mathbb{F}_{11}^\times$. It follows from Lemma 8.1.5 that $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ has order dividing $|K_{\mathbf{0}}||X_{\mathbf{0},i,j}^M| = 2^3 \cdot 3 \cdot 5^2$. However, $(q-1)^2/2 = 2^6 \cdot 3^2 \cdot 5^2$ must divide $2|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}|$, a contradiction.

Suppose $X_{\mathbf{0}}^M = \mathrm{M}_{22}$ and $m = 22$. The one and two point stabilisers have $\mathrm{PSL}_3(4)$ and $\mathrm{PSL}_2(5)$ as composition factors. Now, $\mathrm{PSL}_3(4)$ implies $q = 4^3$, but $\mathrm{PSL}_2(5)$ is not involved in a transitive linear action of the same degree. □

Lemma 8.4.4. *Let C be an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$, with $\delta \geqslant 5$, such that $X_{\mathbf{0}}^M$ is affine. Then $X_{\mathbf{0},i,j}^{Q_i^\times}$ is soluble.*

Proof. Suppose that $X_{\mathbf{0},i,j}^{Q_i^\times}$ is insoluble. Then Corollary 8.3.6 implies $m \geqslant 9$. By Lemma 8.1.6, $K_{\mathbf{0}}$ is soluble and so, by Lemma 8.1.7, any non-abelian composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$ or $X_{\mathbf{0},i,j}^{Q_i^\times}$ must appear as a composition factor of $X_{\mathbf{0},i}^M$ or $X_{\mathbf{0},i,j}^M$, respectively. By Lemma 8.4.2 we only need to consider for $X_{\mathbf{0},i}^M$ the infinite families of insoluble transitive linear groups acting on $M \setminus \{i\}$ in their natural action.

Suppose $X_{\mathbf{0},i}^M$ contains $\mathrm{SL}_t(r)$ as a normal subgroup and $m = r^t$. Now $t \geqslant 3$ and $(r,t) \neq (2,3)$ or $(3,3)$, since otherwise $X_{\mathbf{0},i,j}^M$ is soluble. It follows then that $q = r^t$. Now, $X_{\mathbf{0},i,j}^{Q_i^\times}$ has $\mathrm{PSL}_{t-1}(r)$ as a composition factor, by Lemma 8.1.7. Since $\mathrm{PSL}_{t-1}(r)$ is not a composition factor of a transitive linear group of degree r^t-1, in this case $X_{\mathbf{0},i,j}^{Q_i^\times}$ must be soluble, giving a contradiction.

Suppose $X_{\mathbf{0},i}^M$ has a normal subgroup $\mathrm{Sp}_{2t}(r)$ with $m = r^{2t}$, where $t \geqslant 2$. Then, if $t = 2$ then $r \neq 2,3$, since otherwise $X_{\mathbf{0},i,j}^M$ is soluble. For $t \geqslant 2$, $\mathrm{PSp}_{2t}(r)$ only occurs as a composition factor of a transitive linear group of degree $r^{2t}-1$. However, $\mathrm{PSp}_{2t-2}(r)$ is never a composition factor of a transitive linear group of degree $r^{2t}-1$. So this case does not occur.

Thus $X_{\mathbf{0},i}^M$ has the exceptional Lie type group $\mathrm{G}_2(r)'$ as a composition factor and $m = r^6$,

with r even. Now, $X^M_{\mathbf{0},i,j}$ is soluble if $r = 2$. Suppose $r \geqslant 4$. By considering $X^{Q_i^\times}_{\mathbf{0},i}$ it follows that $q = m$. Now, $X^M_{\mathbf{0},i,j}$ has non-abelian composition factor $\mathrm{PSL}_2(r)$ which does not have a transitive linear action of degree $r^6 - 1$. □

$\mathrm{soc}(X^M_{\mathbf{0}})$	m	S_i	$A_{i,j}$
A_9	9	A_8	$\mathbb{Z}_2$
$\mathrm{Sp}_6(2)$	28	$\mathrm{PSp}_4(3)$	$\mathbb{Z}_2$
$\mathrm{Sp}_6(2)$	36	$\mathrm{PSL}_4(2)$	$\mathrm{AGL}_2(2)^2 \rtimes \mathbb{Z}_2$
$\mathrm{PSL}_3(r)$	$\frac{r^3-1}{r-1}$	$\mathrm{PSL}_2(r)$	$\mathrm{AGL}_1(r)^2 \rtimes \mathbb{Z}_e$
$\mathrm{PSL}_4(r)$, $r = 2, 3$	$\frac{r^4-1}{r-1}$	$\mathrm{PSL}_3(r)$	$\mathbb{Z}_r^4(\mathrm{GL}_2(r) \times \mathbb{F}_r^\times)$
$\mathrm{PSL}_t(r)$	$\frac{r^t-1}{r-1}$	$\mathrm{PSL}_{t-1}(r)$	$\mathrm{GL}_1(r)^2 \rtimes \mathbb{Z}_e$
$\mathrm{PSL}_2(11)$	11	A_5	S_3
A_7	15	$\mathrm{PSL}_2(7)$	A_4
M_{11}	11	A_6	$3^2 \rtimes Q_8$
M_{11}	12	$\mathrm{PSL}_2(11)$	1
M_{22}	22	$\mathrm{PSL}_3(4)$	$\mathbb{Z}_2$

Table 8.4.3: For almost-simple $X^M_{\mathbf{0}}$ with $m \geqslant 9$ from Lemma 8.4.1 we have the non-abelian composition factor S_i of $X^{Q_i^\times}_{\mathbf{0},i}$ and the largest possible soluble quotient $A_{i,j}$ of $X^{Q_i^\times}_{\mathbf{0},i,j}$, such that $X^{Q_i^\times}_{\mathbf{0},i,j} \leqslant X^{Q_i^\times}_{\mathbf{0},i} \leqslant \mathrm{GL}_d(p)$.

The notion of the *largest soluble quotient* of a group is introduced in the next lemma. It is needed for the final proofs of the chapter. Note that N, the group that is factored out below, is trivial if and only if G is soluble.

Lemma 8.4.5. *Let G be a finite group. Then there exists a largest soluble quotient $S \cong G/N$, for some $N \trianglelefteq G$, in the sense that if there exists some soluble $S_1 \cong G/N_1$, for some $N_1 \trianglelefteq G$, and S_1 is soluble, then $N \leqslant N_1$.*

Proof. If G is soluble, then $S = G$. Assume G is insoluble. Let $S_1 = G/N_1$ and $S_2 = G/N_2$ be soluble quotients of G. Now

$$N_1 \big/ N_1 \cap N_2 \cong N_1N_2 \big/ N_2 \trianglelefteq G \big/ N_2 .$$

Moreover,

$$G/(N_1 \cap N_2) \Big/ N_1/(N_1 \cap N_2) \cong G \big/ N_1 .$$

Hence $G/(N_1 \cap N_2)$ is soluble. The required S is thus the quotient of G by N, where N is the intersection of all normal subgroups of G having soluble quotients. □

Lemma 8.4.6. *Let C be an X-alphabet-affine and $(X, 2)$-neighbour-transitive code in $H(m, q)$, with $X^{Q_i^\times}_{\mathbf{0},i}$ insoluble and $\delta \geqslant 5$. Then the largest possible soluble quotient $A_{i,j}$ of $X^M_{\mathbf{0},i,j}$ is stated in Table 8.4.3, if $X^M_{\mathbf{0}}$ is almost-simple, and Table 8.4.4, if $X^M_{\mathbf{0}}$ is affine.*

Proof. First, consider Table 8.4.3 and note that $X_{\mathbf{0}}$ satisfies Lemma 8.4.1. If $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{A}_9$ then $X_{\mathbf{0},i,j}^M = \mathrm{A}_7$ or S_7, and so $A_{i,j} = \mathbb{Z}_2$. If $X_{\mathbf{0}}^M \cong \mathrm{Sp}_6(2)$ and $m = 28$ then $X_{\mathbf{0},i,j}^M = 2^4 \rtimes \mathrm{P\Gamma L}_2(4)$ with minimal normal subgroup 2^4 so that $A_{i,j} = \mathbb{Z}_2$. If $X_{\mathbf{0}}^M \cong \mathrm{Sp}_6(2)$ and $m = 36$ then $X_{\mathbf{0},i,j}^M = \mathrm{AGL}_2(2)^2 \rtimes \mathbb{Z}_2$ is soluble, so $A_{i,j} = \mathrm{AGL}_2(2)^2 \rtimes \mathbb{Z}_2$. Suppose $\mathrm{soc}(X_{\mathbf{0}})^M \cong \mathrm{PSL}_3(r)$. Any matrix stabilising the 1-spaces $\langle e_1 \rangle$ and $\langle e_2 \rangle$, in the row-space, has the form:

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ a & b & \lambda_3 \end{bmatrix},$$

and thus $A_{i,j} \cong \mathrm{AGL}_1(r)^2 \rtimes \mathbb{Z}_e$, where e is the degree of the extension of $\mathbb{F}_r$ over its prime field. Suppose $\mathrm{soc}(X_{\mathbf{0}})^M \cong \mathrm{PSL}_t(r)$ and $t \geqslant 4$. If $r = 2$ or 3 then $X_{\mathbf{0},i}^M$ is soluble and $A_{i,j} = \mathbb{Z}_r^4(\mathrm{GL}_2(r) \times \mathbb{F}_r^\times)$. If $r \geqslant 4$, then $\mathrm{PSL}_{t-2}(r)$ is a composition factor of $X_{\mathbf{0},i,j}^M$. Considering matrices, similar to the previous case, gives $A_{i,j} \cong \mathrm{GL}_1(r)^2 \rtimes \mathbb{Z}_e$, where e is the degree of the extension of $\mathbb{F}_r$ over its prime field. If $X_{\mathbf{0}}^M \cong \mathrm{PSL}_2(11)$ then $X_{\mathbf{0},i,j} \cong \mathrm{S}_3$, so $A_{i,j} \cong \mathrm{S}_3$. If $X_{\mathbf{0}}^M \cong \mathrm{A}_7$ then $X_{\mathbf{0},i,j}^M \cong \mathrm{A}_4$, so $A_{i,j} \cong \mathrm{A}_4$. If $X_{\mathbf{0}}^M \cong \mathrm{M}_{11}$ and $m = 11$, then $X_{\mathbf{0},i,j}^M \cong 3^2 \rtimes Q_8$, so $A_{i,j} \cong 3^2 \rtimes Q_8$. If $X_{\mathbf{0}}^M \cong \mathrm{M}_{11}$ and $m = 12$, then $X_{\mathbf{0},i,j} \cong \mathrm{A}_5$ so that $A_{i,j} = 1$. If $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{M}_{22}$ and $m = 22$, then $X_{\mathbf{0},i,j} \cong 2^4 \rtimes \mathrm{A}_5$ or $(2^4 \rtimes \mathrm{A}_5).2$, with minimal normal subgroup 2^4, so that $A_{i,j} \cong \mathbb{Z}_2$.

Consider now Table 8.4.4. Since $X_{\mathbf{0}}^M$ is affine, it follows that $X_{\mathbf{0},i}^M \leqslant \mathrm{GL}_{d_0}(p_0)$, for some prime p_0 and integer d_0, and, by Lemma 8.4.2, $X_{\mathbf{0},i}^M$ is as in Table 8.4.1. If $X_{\mathbf{0},i}^M$ has one of $\mathrm{SL}_2(r)$, $\mathrm{SL}_3(2)$, $\mathrm{SL}_3(3)$, $\mathrm{Sp}_4(2)'$, or $\mathrm{G}_2(2)'$ as a normal subgroup, then $X_{\mathbf{0},i,j}^M$ is soluble. In these cases, $A_{i,j}$ is taken to be the stabiliser $N_G(X_{\mathbf{0},i}^M)_j$ of $j \in M$ inside the normaliser of $X_{\mathbf{0},i}^M$ in $G = \mathrm{GL}_{d_0}(p_0)$. If $\mathrm{SL}_t(r), \mathrm{Sp}_t(r)$ or $G'(r) \trianglelefteq X_{\mathbf{0},i}^M$, then $X_{\mathbf{0},i,j}^M$ is insoluble and so $A_{i,j} \cong \Gamma\mathrm{L}_1(r)$. □

S_i	m	$A_{i,j}$	conditions
$\mathrm{PSL}_2(r)$	r^2	$\mathrm{A\Gamma L}_1(r)$	$r \neq 2, 3$
$\mathrm{PSL}_3(r)$	r^3	$\mathrm{AGL}_2(r)$	$r = 2, 3$
$\mathrm{PSL}_t(r)$	r^t	$\Gamma\mathrm{L}_1(r)$	$t \geqslant 3$, $(t, r) \neq (3, 2), (3, 3)$
$\mathrm{Sp}_4(2)'$	16	$\mathbb{Z}_2 \times \mathrm{S}_4$	-
$\mathrm{PSp}_t(r)$	r^t	$\Gamma\mathrm{L}_1(r)$	t even, $t \geqslant 2$, $(t, r) \neq (2, 2)$
$\mathrm{G}_2(2)'$	2^6	$\mathbb{Z}_4^2 \rtimes \mathrm{D}_{12}$	-
$\mathrm{G}_2(r)'$	r^6	$\Gamma\mathrm{L}_1(r)$	$r = 2^f$, $f \geqslant 2$

Table 8.4.4: Composition factor S_i of $X_{\mathbf{0},i}^{Q_i^\times}$ and largest soluble quotient $A_{i,j}$ of $X_{\mathbf{0},i,j}^{Q_i^\times}$, where $X_{\mathbf{0},i}^M$ is an insoluble transitive linear group belonging to an infinite family, with $m \geqslant 9$.

Finally, Propositions 8.4.7 and 8.4.8 consider the connections between $X_{\mathbf{0},i}^{Q_i^\times}$, $X_{\mathbf{0},i}^M$ and

$X_{\mathbf{0},i,j}^{Q_i^\times}$, the last known now to be soluble. These two results, together with Proposition 8.2.5, complete the proof of Theorem 8.1.

Proposition 8.4.7. *Suppose C is an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$, with $\delta \geqslant 5$, such that $X_{\mathbf{0}}^M$ is almost-simple. Then $X_{\mathbf{0},i}^{Q_i^\times}$ is soluble.*

Proof. Suppose $X_{\mathbf{0},i}^{Q_i^\times}$ is insoluble. By Corollary 8.3.6, $m \geqslant 9$. By Lemma 8.4.3 we have that $X_{\mathbf{0},i,j}^{Q_i^\times}$ is soluble. Table 8.4.3 lists the possibilities for the socle of $X_{\mathbf{0}}^M$, given by Lemma 8.4.1, with the corresponding non-abelian composition factor S_i of $X_{\mathbf{0},i}^M$ and largest soluble quotient $A_{i,j}$ of $X_{\mathbf{0},i,j}^M$, following from Lemma 8.4.6. Proposition 8.1.7 implies that S_i is a composition of $X_{\mathbf{0},i}^{Q_i^\times}$. The possible values for q and $K_{\mathbf{0}}$ are then obtained from Table 8.1.2 by considering those transitive linear groups with composition factor S_i. We then refer to Lemma 8.1.5 for the divisibility conditions required to complete each case.

Suppose $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{A}_9$. Then $X_{\mathbf{0},i}^{Q_i^\times} \cong \mathrm{A}_8$ so that $q = 2^4$ and $K_{\mathbf{0}} = 1$. Hence, $|X_{\mathbf{0},i,j}^{Q_i^\times}|$ divides 2 and is thus not transitive on $Q_i^\times$.

Suppose $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{Sp}_6(2)$ and $m = 28$. Since $X_{\mathbf{0},i}^{Q_i^\times}$ has $\mathrm{PSp}_4(3)$ as a composition factor it follows that $q = 3^4$ and $|K_{\mathbf{0}}|$ divides 2. Hence $|X_{\mathbf{0},i,j}^{Q_i^\times}|$ divides $|K_{\mathbf{0}}||A_{i,j}| = 4$, and is thus not transitive on $Q_i^\times$.

Suppose $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{Sp}_6(2)$ and $m = 36$. Then $X_{\mathbf{0},i}^{Q_i^\times}$ has $\mathrm{PSL}_4(2)$ as a composition factor, so $q = 2^4$ and $K_{\mathbf{0}} = 1$. Hence, $|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}|$, which divides $|K_{\mathbf{0}}||A_{i,j}|$, is not divisible by 5. However, by Lemma 8.1.5, $(q-1)^2 = 15^2$ must divide $2|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}|$.

Suppose $\mathrm{soc}(X_{\mathbf{0}}^M) \cong \mathrm{PSL}_3(r)$ and $m = r^2 + r + 1$. Now $X_{\mathbf{0},i}^{Q_i^\times}$ has composition factor $\mathrm{PSL}_2(r)$, $r \neq 2, 3$, and $X_{\mathbf{0},i,j}^M \leqslant \mathrm{AGL}_1(r)^2 \rtimes \mathbb{Z}_e = A_{i,j}$, where e is the degree of extension of $\mathbb{F}_r$ over its prime field. First, suppose $q = r^2$ and $X_{\mathbf{0},i}^{Q_i^\times}$ contains $\mathrm{SL}_2(r)$, so $K_{\mathbf{0}}$ is a subgroup of $\mathbb{F}_r^\times$. By Lemma 8.1.5 we require $(q-1)^2 = (r-1)^2(r+1)^2$ to divide $2|K_{\mathbf{0}}||X_{\mathbf{0},i,j}^M|$, which does not occur. Suppose now that $X_{\mathbf{0},i}^{Q_i^\times}$ is a linear group with $\mathrm{PSL}_2(5) \cong \mathrm{PSL}_2(4)$ as a composition factor, with $q = q_0^2$ where $q_0 = 4, 9, 11, 19, 29$ or 59 and $K_{\mathbf{0}} \leqslant \mathbb{F}_{q_0}^\times$. Now $|X_{\mathbf{0},i,j}^M|$ divides $2^4 \cdot 5^2$ or $2^5 \cdot 3^2$ for $r = 5$ and 4 respectively. By Lemma 8.1.5, $(q-1)^2 = (q_0-1)^2(q_0+1)^2$ must divide $2|K_{\mathbf{0}}||X_{\mathbf{0},i,j}^M|$, and so $(q_0-1)(q_0+1)^2$ divides $2|X_{\mathbf{0},i,j}^M|$, which implies that $r = 5$, $q_0 = 9$ and $K_{\mathbf{0}} \leqslant \mathbb{F}_9^\times$. By Lemma 8.1.5, $(q_0^2-1)^2 = 2^8 \cdot 5^2$ divides $2|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}|$. Consider the kernels $X_{\mathbf{0},(Q_i)}$,$X_{\mathbf{0},(Q_j)}$ and $X_{\mathbf{0},(Q_i),(Q_j)}$ of the actions of $X_{\mathbf{0},i}^{Q_i^\times}$, $X_{\mathbf{0},j}^{Q_j^\times}$ and $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$, respectively, on $Q_i^\times$, $Q_j^\times$ and $Q_i^\times \times Q_j^\times$, respectively. Now, $|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}| = |X_{\mathbf{0},i,j}|/|X_{\mathbf{0},(Q_i),(Q_j)}|$ divides $|K_{\mathbf{0}}||X_{\mathbf{0},i,j}^M|$ which divides $2^7 \cdot 5^2$. Thus $|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}| = 2^7 \cdot 5^2 = |X_{\mathbf{0},i,j}|$. Hence $X_{\mathbf{0},(Q_i),(Q_j)} = 1$, and $X_{\mathbf{0},(Q_i)} \cap X_{\mathbf{0},(Q_j)} = X_{\mathbf{0},(Q_i),(Q_j)} = 1$. Let $i = \langle e_1 \rangle$ and $j = \langle e_2 \rangle$. Then, $\mathrm{PSL}_3(5)_i \cong \mathrm{PSL}_3(5)_j \cong \mathrm{AGL}_2(5)$, each with minimal normal subgroup $\mathbb{Z}_5^2$, and the intersection of these minimal normal subgroups is $\mathbb{Z}_5$. As $K_{\mathbf{0}}X_{\mathbf{0},(Q_i)}/K_{\mathbf{0}}$ and $K_{\mathbf{0}}X_{\mathbf{0},(Q_j)}/K_{\mathbf{0}}$ are normal subgroups of $X_{\mathbf{0},i}/K_{\mathbf{0}} \cong \mathrm{PSL}_3(5)_i$ and $X_{\mathbf{0},j}/K_{\mathbf{0}} \cong \mathrm{PSL}_3(5)_j$, respectively, it fol-

lows that $X_{\mathbf{0},(Q_i)} = X_{\mathbf{0},(Q_j)} = 1$. However, the size of any finite transitive linear group having $\mathrm{PSL}_2(5)$ for a composition factor, divides $2^8 \cdot 3 \cdot 5$. This implies 5 divides $|X_{\mathbf{0},(Q_i)}|$, giving a contradiction. Consider $\mathrm{PSL}_2(13)$ as a composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$, $q = 3^6$ and $K_\mathbf{0} \leqslant \mathbb{F}_3^\times$. Hence $2|X_{\mathbf{0},i,j}| < (q-1)^2$, contradicting Lemma 8.1.5. Suppose $\mathrm{PSL}_2(9) \cong \mathrm{A}_6$ is a composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$, $q = 2^4$ and $K_\mathbf{0}$ is trivial. Then $|X_{\mathbf{0},i,j}|$ divides $2^7 \cdot 3^4$, contradicting Lemma 8.1.5, since $(q-1)^2 = 3^2 \cdot 5^2$. Consider $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$ as a composition factor of $X_{\mathbf{0},i}^{Q_i^\times}$ so that $q = 2^3$ and $K_\mathbf{0} = 1$. Any proper subgroup of $\mathrm{PSL}_3(2)$ with order divisible by 7 is isomorphic to $\mathbb{Z}_7$ and has index 24 in $\mathrm{PSL}_3(2)$ contradicting Lemma 8.1.5, since $m - 1 = 56$.

Suppose $r = 2$ or 3, $\mathrm{soc}(X_\mathbf{0}^M) \cong \mathrm{PSL}_4(r)$ and $m = (r^4-1)/(r-1)$. Then $\mathrm{PSL}_3(r)$ is a composition factor for $X_{\mathbf{0},i}^{Q_i^\times}$, so that $r = 2$, $q = 8$, and $K_\mathbf{0} = 1$; $r = 2$, $q = 7^2$, and $K_\mathbf{0} \leqslant \mathbb{F}_7^\times$; or $r = 3$, $q = 3^3$, and $K_\mathbf{0} \leqslant \mathbb{F}_3^\times$. Now, $X_{\mathbf{0},i,j}/K_\mathbf{0} \cong \mathbb{Z}_r^4(\mathrm{GL}_2(r) \times \mathbb{F}_r^\times)$ has order $r^5(r-1)^3(r+1)$, that is, $2^5 \cdot 3$ for $r = 2$, and $2^5 \cdot 3^5$ for $r = 3$. By Lemma 8.1.5, $(q-1)^2$ divides $2|K_\mathbf{0}||X_{\mathbf{0},i,j}^M|$. Thus $q \neq 8$ or 3^3, since then $(q-1)^2 = 7^2$ or $2^2 \cdot 13^2$, respectively. Also, $(r,q) \neq (2,7^2)$, since $(q-1)^2 = 2^8 \cdot 3^2$ and $2|K_\mathbf{0}||X_{\mathbf{0},i,j}^M| = 2^7 \cdot 3^2$.

Suppose $\mathrm{soc}(X_\mathbf{0}^M) \cong \mathrm{PSL}_t(r)$, $m = (r^t-1)/(r-1)$ and $t \geqslant 4$. Furthermore, suppose $q = p^d = r^{t-1}$, $X_{\mathbf{0},i}^{Q_i^\times}$ contains $\mathrm{SL}_{t-1}(r)$ as a normal subgroup, and $K_\mathbf{0}$ is a subgroup of $\mathbb{F}_r^\times$. Then $|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}|$ divides $|K_\mathbf{0}||A_{i,j}| = e(r-1)^3$, where e is the degree of the extension of $\mathbb{F}_r$ over its prime field. By Lemma 8.1.5, $(q-1)^2 = (r^{t-1}-1)^2$ must divide $|X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}|$, which gives a contradiction since $t - 1 \geqslant 3$. Otherwise, $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ provides the possibility that $X_{\mathbf{0},i,j}^M \cong 2^4 \rtimes \mathrm{SL}_2(2)$, $q = 7^2$ and $K_\mathbf{0} \leqslant \mathbb{F}_7^\times$. Now $|X_{\mathbf{0},i,j}|$ divides $2|K_\mathbf{0}||X_{\mathbf{0},i,j}^M| = 2^7 \cdot 3^2$, but $(q-1)^2 = 2^8 \cdot 3^2$ does not divide this.

Suppose $X_\mathbf{0}^M \cong \mathrm{PSL}_2(11)$ and $m = 11$. Here $X_{\mathbf{0},i}^M \cong \mathrm{PSL}_2(5)$, so $q = q_0^2$ where $q_0 = 4, 5, 9, 11, 19, 29$ or 59. By Lemma 8.1.5, $q - 1 = q_0^2 - 1$ must divide $12 = 2|X_{\mathbf{0},i,j}^M|$, a contradiction.

Suppose $X_\mathbf{0}^M \cong \mathrm{A}_7$ and $m = 15$. Now, $X_{\mathbf{0},i}^M \cong \mathrm{PSL}(2,7)$. Hence, $q = 7^2$ or 2^3. However $X_{\mathbf{0},i,j}^M \cong \mathrm{A}_4$ has order 12, and is thus not divisible by $q - 1$ or $(q-1)/2$, contradicting Lemma 8.1.5.

Suppose $X_\mathbf{0}^M \cong \mathrm{M}_{11}$ and $m = 11$. Here $X_{\mathbf{0},i}^M \cong \mathrm{A}_6.2$, so $q = 2^4$ or 9^2, by the isomorphism $\mathrm{A}_6 \cong \mathrm{PSL}_2(9)$. However $2|X_{\mathbf{0},i,j}^M| = 2^4 \cdot 3^2$, which is not divisible by $q - 1 = 15$ or 80.

Suppose $X_\mathbf{0}^M \cong \mathrm{M}_{11}$ and $m = 12$. Now, $X_{\mathbf{0},i}^M \cong \mathrm{PSL}_2(11)$, so $q = 11^2$. However $A_{i,j} = 1$, so $2|X_{\mathbf{0},i,j}^{Q_i^\times}/K_\mathbf{0}| = 2$ and is thus not divisible by $q - 1$.

Suppose $X_\mathbf{0}^M \cong \mathrm{M}_{22}$ and $m = 22$. Here $X_{\mathbf{0},i}^M \cong \mathrm{PSL}_3(4)$, so $q = 4^3$. Now, $A_{i,j} = \mathbb{Z}_2$ does not have order divisible by $q - 1$ or $(q-1)/2$. □

Proposition 8.4.8. *Suppose C is an X-alphabet-affine and $(X,2)$-neighbour-transitive code in $H(m,q)$, with $\delta \geqslant 5$, such that $X_\mathbf{0}^M$ is affine. Then $X_{\mathbf{0},i}^{Q_i^\times}$ is soluble.*

Proof. Suppose $X_{\mathbf{0},i}^{Q_i^\times}$ is insoluble. By Corollary 8.3.6 $m \geqslant 9$. By Lemma 8.4.4 we have that $X_{\mathbf{0},i,j}^{Q_i^\times}$ is soluble and $K_\mathbf{0}$ is soluble. Thus, by Lemma 8.1.7, any non-abelian composition

factor of $X_{\mathbf{0},i}^{Q_i^\times}$ must appear as a composition factor of $X_{\mathbf{0},i}^M$. By Lemma 8.4.2 we only need to consider for $X_{\mathbf{0},i}^M$ the infinite families of insoluble transitive linear groups acting on $M \setminus \{i\}$ in their natural action. Table 8.4.4 lists the largest possible soluble quotient of $X_{\mathbf{0},i,j}^M$, as in Lemma 8.4.6.

Suppose $X_{\mathbf{0},i}^{Q_i^\times}$ has non-abelian composition factor $\mathrm{PSL}_2(r)$, so that $m = r^2$ and $A_{i,j} = \mathrm{A\Gamma L}_1(r)$, where $r \neq 2$ or 3. If $q = r^2$, then $q-1$ does not divide $2|A_{i,j}|$, contradicting Lemma 8.1.5. Otherwise, $r = 4$ or 5 and $q = q_0^2$ where $q_0 = 4, 9, 11, 19, 29$ or 59; or $r = 13$ and $q = 3^6$. Again, $q-1$ does not divide $2|A_{i,j}| = 2^3 \cdot 3$, $2^3 \cdot 5$ or $2^3 \cdot 3 \cdot 13$, for $r = 4$, 5 or 13, respectively.

Suppose that $r = 2$ or 3, and $X_{\mathbf{0},i}^{Q_i^\times}$ has non-abelian composition factor $\mathrm{PSL}_3(r)$, so that $m = r^3$ and $A_{i,j} = \mathrm{AGL}_2(r)$. Now, $|A_{i,j}| = r^3(r+1)(r-1)^2 = 2^3 \cdot 3$ or $2^4 \cdot 3^3$, for $r = 2$ or 3, respectively. If $q = r^3$ then $q - 1 = 7$ or 26, which does not divide $2|A_{i,j}|$. Otherwise, $r = 2$ and $q = 7^2$, in which case a contradiction to Lemma 8.1.5 is reached, since $K_{\mathbf{0}} \leqslant \mathbb{F}_7^\times$ and $(q-1)^2$ does not divide $2|K_{\mathbf{0}}||A_{i,j}|$.

Suppose $m = r^t$, $q = r^t$, and $X_{\mathbf{0},i}^{Q_i^\times}$ has non-abelian composition factor $\mathrm{PSL}_t(r)$, where $t \geqslant 3$ and $(t,r) \neq (2,2), (2,3)$. Then $q - 1 = r^t - 1$ does not divide $2|A_{i,j}|$, contradicting Lemma 8.1.5.

Suppose $X_{\mathbf{0},i}^{Q_i^\times}$ has non-abelian composition factor $\mathrm{Sp}_4(2)'$, so that $m = q = 2^4$. Then 15 does not divide $2|A_{i,j}| = 2^5 \cdot 3$, contradicting Lemma 8.1.5.

Suppose $X_{\mathbf{0},i}^{Q_i^\times}$ has non-abelian composition factor $\mathrm{PSp}_t(r)$ with $m = r^t$, t even, $t \geqslant 2$, and $(t,r) \neq (2,2)$. Then $q = r^t$ and $q - 1$ does not divide $2|A_{i,j}|$, contradicting Lemma 8.1.5.

Suppose $X_{\mathbf{0},i}^{Q_i^\times}$ has non-abelian composition factor $\mathrm{G}_2(2)'$ and $m = q = 2^6$. Then $q - 1 = 63$ does not divide $2|A_{i,j}| = 2^5 \cdot 3$.

Thus $X_{\mathbf{0},i}^{Q_i^\times}$ has the sporadic group of Lie type $\mathrm{G}_2(r)'$ as a composition factor, $m = 2^t = r^6$. Then $q = r^6$ and $q - 1$ does not divide $2|A_{i,j}|$, contradicting Lemma 8.1.5. □

Constructions of 2-Neighbour-Transitive Codes

Chapters 6 and 8 have provided insight into the general structure of 2-neighbour-transitive codes, and their automorphism groups. This chapter begins by presenting constructions of several infinite families of 2-neighbour-transitive codes, as in Propositions 9.1.9, 9.2.3, 9.3.3, 9.4.6, 9.4.8 and 9.5.3. The Reed-Muller and projective Reed-Muller codes, Definitions 9.1.6 and 9.2.1, respectively, have been studied for decades (see [70, 72], for example). However, the author is not aware of any previous constructions of certain families, in particular, those in Definitions 9.3.1, 9.4.1, 9.4.2 and 9.4.3.

Theorems 6.1 and 8.1 imply that an $(X, 2)$-neighbour-transitive code C with minimum distance $\delta \geqslant 5$ is either as in Theorem 5.2, or C is X-alphabet-affine, C contains a block of imprimitivity that is an $X_{\mathbf{0}}$-module, and $X_{\mathbf{0},i}^{Q_i^\times}$ is soluble. For $q = 2$, Section 9.7 provides the following characterisation of 2-neighbour-transitive codes in $H(m, 2)$.

Theorem 9.1. *Let C be a binary code in $H(m, 2)$ with minimum distance $\delta \geqslant 5$. Then C is 2-neighbour-transitive if and only if one of the following holds*

1. *C is the binary repetition code with $\delta = m$;*
2. *C is one of the codes as in Definition 5.2.1, that is, the Hadamard code of length 12 with $\delta = 6$, its punctured code with $\delta = 5$, or the even weight subcode of its punctured code with $\delta = 6$; or,*
3. *there exists some $C' \subseteq C$ and $X \leqslant \mathrm{Aut}(C)$ such that C', $X_{\mathbf{0}}$ and m are as in Table 9.7.1, and X acts transitively on C.*

Note that in the line of Table 9.7.1 where $\mathrm{soc}(X_{\mathbf{0}}) = \mathrm{PSU}_3(r)$ and $r \equiv 1 \pmod 4$, it is possible that for certain values of r the corresponding code has $\delta = 4$.

Proposition 9.8.1 concerns linear-$(X, 2)$-neighbour-transitive codes in $H(m, q)$ with $q \geqslant 3$ and $\delta \geqslant 5$. In particular, Table 9.8.1 gives those parameter sets that are not ruled out in this chapter, with examples provided for many cases.

9.1 Polynomials and Reed-Muller codes

The main constructions in this chapter are in terms of polynomials. The key to these constructions is that, first, polynomials can be used to represent the vertices of the Hamming graph and, second, taking the subset of all polynomials of degree at most some fixed integer provides a simple way to define a subspace, and thus a (linear) code. None of the results on polynomials contained in this section are new, they can be found in either [33] or [94], for instance.

The *degree* of a monomial $x_1^{b_1} \cdots x_t^{b_t}$ is $b_1 + \cdots + b_t$ and the *degree* of a polynomial f is the largest degree of any monomial of f having a non-zero coefficient. An *indeterminate* x_i,

in a polynomial with coefficients from the field $\mathbb{F}_q$, can be considered to take possible values from an unspecified commutative ring containing $\mathbb{F}_q$. In particular, x_i and x_j commute, but x_i^a is not known to be equal to x_i for any choice of a. On the other hand, define a *variable* over $\mathbb{F}_q$ to take values only from the field $\mathbb{F}_q$. Hence, a variable x_i satisfies $x_i^q = x_i$. It is assumed throughout that if f is a polynomial, or monomial, in the variables $x_1, \ldots, x_t$ over $\mathbb{F}_q$, then f is reduced modulo $x_i^q - x_i = 0$, for each variable x_i, and that the degree of f refers to the degree after this reduction. Thus a polynomial in t variables will have degree at most $t(q-1)$. Some important classes of polynomials are defined below.

Definition 9.1.1. Denote by $\mathcal{P}_{q,t}$, $\mathcal{R}_{q,t}$, $\mathcal{H}_{q,t,k}$ and $\mathcal{S}_{q,t,\ell}$ the following $\mathbb{F}_q$-spaces of polynomials:

1. $\mathcal{P}_{q,t}$ - the set of polynomials in t indeterminates $x_1, \ldots, x_t$ with coefficients in $\mathbb{F}_q$,
2. $\mathcal{R}_{q,t}$ - the set of polynomials in t variables $x_1, \ldots, x_t$ over $\mathbb{F}_q$, with coefficients in $\mathbb{F}_q$,
3. $\mathcal{H}_{q,t,k}$ where $k \geqslant 0$ - the subset of all polynomials $f \in \mathcal{P}_{q,t}$ where all monomials of f have fixed degree k, and,
4. $\mathcal{S}_{q,t,\ell}$ where $\ell \in \{0, \ldots, q-1\}$ - the subset of all polynomials $f \in \mathcal{R}_{q,t}$ where the (possibly different) degree of each monomial of f lies in $\{\ell + d(q-1) \mid d = 0, \ldots, t-1\}$.

A polynomial in $\mathcal{R}_{q,t}$ or $\mathcal{H}_{q,t,k}$ is called *reduced* or *homogeneous*, respectively.

Whilst it is assumed here that a polynomial has finitely many terms, there is no bound on the possible degree of a polynomial in $\mathcal{P}_{q,t}$. However, a polynomial in $\mathcal{R}_{q,t}$, $\mathcal{H}_{q,t,k}$ or $\mathcal{S}_{q,t,\ell}$ can be considered to have bounded degree. In the case of $\mathcal{H}_{q,t,k}$ this bound is k and $\mathcal{S}_{q,t,\ell}$ it is $\ell + (t-1)(q-1)$, simply by definition, but the bound of $t(q-1)$ holds for $f \in \mathcal{R}_{q,t}$ as noted above. By 'forgetting' that the variables x_i are over $\mathbb{F}_q$, and, instead, taking them as indeterminates, $\mathcal{R}_{q,t}$ and $\mathcal{S}_{q,t,k}$ can be embedded as $\mathbb{F}_q$-subspaces of $\mathcal{P}_{q,t}$.

Lemma 9.1.2 shows that, when evaluated over $x = (x_1, \ldots, x_t) \in \mathbb{F}_q^t$, the spaces $\mathcal{P}_{q,t}$ and $\mathcal{H}_{q,t,k}$ give the same set of functions from $\mathbb{F}_q^t$ into $\mathbb{F}_q$ as $\mathcal{R}_{q,t}$ and $\mathcal{S}_{q,t,\ell}$, respectively, given appropriate conditions on k and ℓ. In particular, provided $\ell \neq 0$, a polynomial in $\mathcal{S}_{q,t,\ell}$ is equivalent, as a function from $\mathbb{F}_q^t$ into $\mathbb{F}_q$, to a polynomial in $\mathcal{H}_{q,t,k}$, for some $k \leqslant \ell + (t-1)(q-1)$. However, a polynomial in $\mathcal{S}_{q,t,0}$ having non-zero degree and non-zero constant term does not have such a functional equivalent in $\mathcal{H}_{q,t,k}$, for any k.

Lemma 9.1.2. *For any polynomial $f \in \mathcal{P}_{q,t}$ there exists a polynomial $f' \in \mathcal{R}_{q,t}$ such that $f(x) = f'(x)$ for all $x = (x_1, \ldots, x_t) \in \mathbb{F}_q^t$. Conversely, for any polynomial $f' \in \mathcal{R}_{q,t}$ there exists a polynomial $f \in \mathcal{P}_{q,t}$ such that $f(x) = f'(x)$ for all $x = (x_1, \ldots, x_t) \in \mathbb{F}_q^t$.*

Let $k \geqslant 0$ and $f \in \mathcal{H}_{q,t,k}$. If $k = 0$ then let $\ell = 0$, otherwise let $\ell \equiv k \pmod{q-1}$ with $1 \leqslant \ell \leqslant q-1$. Then there exists a polynomial $f' \in \mathcal{S}_{q,t,\ell}$ such that $f(x) = f'(x)$ for all $x = (x_1, \ldots, x_t) \in \mathbb{F}_q^t$. Conversely, let $\ell \in \{1, \ldots, q-1\}$, let $f' \in \mathcal{S}_{q,t,\ell}$ have degree $\ell + d(q-1)$, and let $k \in \{\ell + s(q-1) \mid s = d, \ldots, t-1\}$. Then there exists a polynomial $f \in \mathcal{H}_{q,t,k}$ such that $f(x) = f'(x)$ for all $x = (x_1, \ldots, x_t) \in \mathbb{F}_q^t$.

Proof. Let f be in $\mathcal{P}_{q,t}$ or $\mathcal{H}_{q,t,k}$. Then:

$$f(x) = \sum_{b_1 \geqslant 0} \cdots \sum_{b_t \geqslant 0} a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t},$$

for some $a_{b_1,\ldots,b_t} \in \mathbb{F}_q$, with the extra condition when $f \in \mathcal{H}_{q,t,k}$ that $a_{b_1,\ldots,b_t} = 0$ unless $b_1 + \cdots + b_t = k$. If $x \in \mathbb{F}_q^t$ then $x_i^q = x_i$ so that $a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t} = a_{b_1,\ldots,b_t} x_1^{b'_1} \cdots x_t^{b'_t}$, where $b'_i \equiv b_i \pmod{q-1}$ with $b'_i = 0$ if $b_i = 0$ and $1 \leqslant b'_i \leqslant q-1$ otherwise. In particular, if $b_1 + \cdots + b_t = k$ then $b'_1 + \cdots + b'_t \equiv k \pmod{q-1}$. The required polynomial f' in $\mathcal{R}_{q,t}$ or $\mathcal{S}_{q,t,\ell}$ is then:

$$f'(x) = \sum_{b_1 \geqslant 0}^{q-1} \cdots \sum_{b_t \geqslant 0}^{q-1} a'_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t},$$

where

$$a'_{b_1,\ldots,b_t} = \sum_{i_j \geqslant 0} a_{(b_1+i_1(q-1)),\ldots,(b_t+i_t(q-1))}.$$

Conversely, if $f' \in \mathcal{R}_{q,t}$ then, by considering $x_1, \ldots, x_t$ to be indeterminates, we have $f' \in \mathcal{P}_{q,t}$.

Finally, if $\ell \in \{1, \ldots, q-1\}$ and $f' \in \mathcal{S}_{q,t,\ell}$ has degree $\ell + d(q-1)$, for some $d \in \{0, \ldots, t-1\}$, then:

$$f'(x) = \sum_{b_1=0}^{q-1} \cdots \sum_{b_t=0}^{q-1} a'_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t},$$

for some $a'_{b_1,\ldots,b_t} \in \mathbb{F}_q$, where $a'_{b_1,\ldots,b_t} = 0$ unless $b_1 + \cdots + b_t \equiv \ell \pmod{q-1}$ and $a'_{0,\ldots,0} = 0$. Then, for $k \in \{\ell + s(q-1) \mid s = d, \ldots, t-1\}$, the following polynomial f is in $\mathcal{H}_{q,t,k}$:

$$f(x) = \sum_{b_1=0}^{q-1} \cdots \sum_{b_t=0}^{q-1} a'_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t} x_j^{k-(b_1+\cdots+b_t)},$$

where j depends on $b_1, \ldots, b_t$ and is taken to be the smallest value $j \in \{1, \ldots, t\}$ such that $b_j \neq 0$. The monomials in f and f' are then in one-to-one correspondence and, under this correspondence, each monomial takes the same value in $\mathbb{F}_q$ when evaluated over $\mathbb{F}_q^t$. □

The next result follows directly from Lemma 9.1.2 by noting that the maximum degree of a polynomial in $\mathcal{S}_{q,t,\ell}$ is $\ell + (t-1)(q-1)$.

Corollary 9.1.3. *Let $\ell \in \{1, \ldots, q-1\}$ and $k = \ell + d(q-1)$, for some $d \leqslant t-1$. Then $\mathcal{S}_{q,t,\ell}$ is the set of polynomials obtained by reducing all polynomials in $\mathcal{H}_{q,t,k}$ modulo $x_i^q - x_i = 0$, for each $i = 1, \ldots, t$.*

Lemma 9.1.4. *The set of functions from $\mathbb{F}_q^t$ into $\mathbb{F}_q$ is given by $\mathcal{R}_{q,t}$, with basis $\{x_1^{b_1} \cdots x_t^{b_t} \mid 0 \leqslant b_i \leqslant q-1\}$. Moreover, for each integer $\ell \in \{1, \ldots, q-1\}$, the set of all functions f from $\mathbb{F}_q^t$ into $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$, for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_q^t$, is given by $\mathcal{S}_{q,t,\ell}$.*

Proof. There are q^{q^t} functions from $\mathbb{F}_q^t$ into $\mathbb{F}_q$. Any polynomial in $\mathcal{R}_{q,t}$ is a function from $\mathbb{F}_q^t$ into $\mathbb{F}_q$. If $\mathbf{a} = (a_1, \ldots, a_t)$, then the polynomial

$$g_{\mathbf{a}}(x) = \prod_{i=1}^{t}(1 - (x_i - a_i)^{q-1}),$$

in $\mathcal{R}_{q,t}$ evaluates to 1 at $(a_1, \ldots, a_t) \in \mathbb{F}_q^t$ and 0 for $x \in \mathbb{F}_q^t$, $x \neq (a_1, \ldots, a_t)$. Thus, the set $\{g_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_q^t\}$ forms a basis in $\mathcal{R}_{q,t}$ for the set of functions from $\mathbb{F}_q^t$ into $\mathbb{F}_q$ and $|\mathcal{R}_{q,t}| \geqslant q^{q^t}$. Now, there are q^t possible monomial terms in any polynomial in $\mathcal{R}_{q,t}$, since there are q choices for each b_i in the term $x_1^{b_1} \cdots x_t^{b_t}$. There are q choices for the coefficient of each monomial in a polynomial, since each coefficient is in $\mathbb{F}_q$. Thus $|\mathcal{R}_{q,t}| = q^{q^t}$, and the first part of the result follows. This also shows that $\{x_1^{b_1} \cdots x_t^{b_t} \mid 0 \leqslant b_i \leqslant q-1\}$ is in fact a basis for $\mathcal{R}_{q,t}$.

Any function f from $\mathbb{F}_q^t$ into $\mathbb{F}_q$ satisfying $f(ax) = a^\ell f(x)$ is determined by knowing the value of f on a representative of each 1-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^t$. Note that $f(0) = 0$ since $f(0x) = 0f(x)$. The number of 1-dimensional subspaces is $m = (q^t - 1)/(q - 1)$, and f can take q possible values on a representative. Thus, there are q^m functions satisfying the required condition. Conversely, let $f \in \mathcal{S}_{q,t,\ell}$. Then:

$$f(x) = \sum_{b_1=0}^{q-1} \cdots \sum_{b_t=0}^{q-1} a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t},$$

where $a_{b_1,\ldots,b_t} \in \mathbb{F}_q$, $a_{0,\ldots,0} = 0$, and $a_{b_1,\ldots,b_t} = 0$ unless $b_1 + \cdots + b_t \equiv \ell \pmod{q-1}$. It is claimed that f satisfies $f(ax) = a^\ell f(x)$, for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_q^t$. To see this requires two observations. First, if $x_i = 0$, for some $i \in \{1, \ldots, t\}$ such that $b_i \neq 0$, the monomial $a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t} = 0 = a^\ell \cdot 0$. Next, if $x_i \neq 0$ for each value of i satisfying $b_i \neq 0$, where $i \in \{1, \ldots, t\}$, then:

$$a_{b_1,\ldots,b_t}(ax_1)^{b_1} \cdots (ax_t)^{b_t} = a^{b_1+\cdots+b_t} a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t} = a^\ell a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t}.$$

The only remaining case is where $b_i = 0$ for all $i = 1, \ldots, t$. Since $a_{0,\ldots,0} = 0$, the required property holds for all monomials comprising f. Thus f satisfies $f(ax) = a^\ell f(x)$, as claimed. Showing that $|\mathcal{S}_{q,t,\ell}| = q^m$ will complete the proof. Again, there are q choices for each b_i. However, setting $a_{0,\ldots,0} = 0$ leaves $q^t - 1$ choices for monomials with non-zero coefficients. For these $q^t - 1$ choices $b_1 + \cdots + b_t \equiv k \pmod{q-1}$ for some $k \in \{1, \ldots, q-1\}$. Since we must have $k = \ell$, there are $m = (q^t - 1)/(q - 1)$ possible monomials having non-zero coefficients in f. As each $a_{b_1,\ldots,b_t}$ is an element of $\mathbb{F}_q$, it follows that there are q^m polynomials in $\mathcal{S}_{q,t,\ell}$. □

Since the vertex set of a Hamming graph $H(m, q)$ is the set of functions from M into Q, by taking $M = \mathbb{F}_q^t$ and $Q = \mathbb{F}_q$, Lemma 9.1.4 means that the vertices of $H(q^t, q)$ can be represented by the polynomials $\mathcal{R}_{q,t}$. Thus, vertices α, β, μ, ν (and so on) will often be treated as polynomials.

Let $G \leqslant \mathrm{AGL}_t(q)$ act naturally on $\mathbb{F}_q^t$ and G_0 be the stabiliser of $0 \in \mathbb{F}_q^t$ in G. Then define an action of G and G_0, respectively, on $\mathcal{R}_{q,t}$ and $\mathcal{S}_{q,t,\ell}$, where $\ell \in \{1, \ldots, q-1\}$, via $\alpha^g(x) = \alpha(x^{g^{-1}})$, where $\alpha \in \mathcal{R}_{q,t}$ or $\mathcal{S}_{q,t,\ell}$, and $g \in G$ or G_0, respectively. The next result shows that G and G_0 indeed stabilise $\mathcal{R}_{q,t}$ and $\mathcal{S}_{q,t,\ell}$, respectively, and that the degree of a polynomial is preserved by these groups.

Lemma 9.1.5. *Let g be an element of $\mathrm{AGL}_t(q)$ or $\mathrm{GL}_t(q)$ and α be a polynomial in $\mathcal{R}_{q,t}$ or $\mathcal{S}_{q,t,\ell}$, respectively, where $\ell \in \{1, \ldots, q-1\}$. Then α^g is in $\mathcal{R}_{q,t}$ or $\mathcal{S}_{q,t,\ell}$, respectively, and α and α^g have the same degree.*

Proof. Consider the degree 1 polynomial $e_i^*(x) = x_i$. Let $g \in G$. Then,

$$e_i^{*g}(x) = (x^{g^{-1}})_i = d_i + \sum_{j=1}^{t} c_{ij} x_j,$$

for some $d_i, c_{ij} \in \mathbb{F}_q$. Next, consider a monomial $\mu(x) = a_{b_1,\ldots,b_t} x_1^{b_1} \cdots x_t^{b_t}$ of α. With g, d_i, c_{ij} as above:

$$\mu^g(x) = a_{b_1,\ldots,b_t}(d_1 + \sum_{j=1}^{t} c_{1j}x_j)^{b_1} \cdots (d_t + \sum_{j=1}^{t} c_{1j}x_j)^{b_t}.$$

It can be seen that, upon expanding this expression and reducing modulo $x_i^q - x_i = 0$ for each i, a polynomial of degree at most $b_1 + \cdots + b_t$ is returned. Thus α^g has degree at most that of the maximum degree of a monomial of α, and so at most the degree of α itself. Let $\beta = \alpha^g$ and suppose the degree of β were less than the degree of α. The same argument applied to g^{-1} and a monomial of β then implies that $\beta^{g^{-1}}$ has degree at most that of β. However, $\beta^{g^{-1}}(x) = \beta(x^g) = \alpha^g(x^g) = \alpha(x)$, giving a contradiction. It follows that g preserves the degree of α. Suppose $\alpha \in \mathcal{S}_{q,t,\ell}$. Then in the above monomials the coefficient $a_{0,\ldots,0} = 0$, and $a_{b_1,\ldots,b_t} = 0$ unless $b_1 + \cdots + b_t \equiv \ell \pmod{q-1}$. If $g \in \mathrm{GL}_t(q)$ then $d_i = 0$ for all $i \in \{1, \ldots, t\}$. Thus, each term in the monomial $\mu^g(x)$, above, has degree $b_1 + \cdots + b_t \equiv \ell \pmod{q-1}$, so that $\alpha^g \in \mathcal{S}_{q,t,\ell}$. □

The Reed-Muller codes are defined below.

Definition 9.1.6 (Reed-Muller codes)**.** Let $M = \mathbb{F}_q^t$, $Q = \mathbb{F}_q$ and $k \in \{0, \ldots, t(q-1)\}$. The *$k$-th order q-ary Reed-Muller code* of length $m = q^t$ in $H(m, q)$, denoted $\mathcal{RM}_q(k, t)$, is the $\mathbb{F}_q$-subspace of $\mathcal{R}_{q,t}$ consisting of all polynomials of degree at most k. That is,

$$\mathcal{RM}_q(k,t) = \left\langle x_1^{b_1} \cdots x_t^{b_t} \mid b_i \geqslant 0; b_1 + \cdots + b_t \leqslant k \right\rangle.$$

The following result (see [2, Theorem 5.4.1 and Corollary 5.5.4]) the parameters of the Reed-Muller codes.

Theorem 9.1.7. *Let C be the Reed-Muller code $\mathcal{RM}_q(k,t)$ and the integers s and ℓ satisfy $k = s(q-1)+\ell$ and $0 \leqslant \ell < q-1$. Then C has minimum distance $(q-\ell)q^{t-s-1}$ and dimension*

$$\sum_{i=0}^{k}\sum_{j=0}^{t}(-1)^j\binom{t}{j}\binom{i-jq+t-1}{i-jq}.$$

Proposition 9.1.8. *Let $C = \mathcal{RM}_2(k,t)$ in $H(2^t,2)$ with $k \leqslant t-2$, and G be a 2-transitive subgroup of $\mathrm{AGL}_t(2)$. Then C is $(X,2)$-neighbour-transitive, where $X_{\mathbf{0}} = G$, T_C is the group of translations by codewords in C and $X = T_C \rtimes X_{\mathbf{0}}$.*

Proof. The parameters ℓ and k in Theorem 9.1.7 satisfy $\ell = 0$ and $s = k \leqslant t-2$, and so C has minimum distance at least 4. By Lemma 9.1.5, G fixes C and, in particular, fixes the vertex $\mathbf{0} \in C$. Now C is $(X,2)$-neighbour-transitive, since T_C acts transitively on C and G acts 2-transitively on M, and thus transitively on both $\Gamma_1(\mathbf{0})$ and $\Gamma_2(\mathbf{0})$. □

In the next proposition, note that $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ corresponds to multiplication of a polynomial by a scalar in $\mathbb{F}_q^\times$ and that the 'repetition' codewords α such that $\alpha_i = \alpha_j$, for all $i,j \in M$, correspond to the constant polynomials $f(x) = a$, for some $a \in \mathbb{F}_q$. Also, here $\mathrm{AGL}_t(q)$ is, through the action defined immediately prior to Lemma 9.1.5, a subgroup of the top group of $\mathrm{Aut}(\Gamma)$. Moreover, Theorem 9.1.7 implies that there are non-trivial choices of q,t and k such that $\mathcal{RM}_q(k,t)$ has minimum distance $\delta \geqslant 5$.

Proposition 9.1.9. *Let $q \geqslant 3$, $m = q^t$, $C = \mathcal{RM}_q(k,t)$ in $H(m,q)$ have minimum distance $\delta \geqslant 5$, and G be a 2-homogeneous subgroup of $\mathrm{AGL}_t(q) \leqslant L \cong \mathrm{S}_m$ acting naturally on M. Then C is X-neighbour-transitive, but not $(X,2)$-neighbour-transitive, where $X_{\mathbf{0}} = \mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes G$, T_C is the group of translations by codewords in C and $X = T_C \rtimes X_{\mathbf{0}}$.*

Proof. Now T_C acts transitively on C. Also, G fixes C and the vertex $\mathbf{0} \in C$, by Lemma 9.1.5, and acts transitively on M. Moreover, for each $i \in M$, $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ acts transitively on the set of weight 1 vertices $\alpha \in V\Gamma$ such that $\alpha_i = a$, for some $a \in \mathbb{F}_q^\times$. It follows that C is X-neighbour-transitive.

Let α and β be weight two vertices of $H(m,q)$ and i,j be distinct elements of M such that

$$\alpha_i = \alpha_j = \beta_i = a \in \mathbb{F}_q^\times \quad \text{and} \quad a \neq \beta_j = b \in \mathbb{F}_q^\times.$$

Note that G fixes any constant function $f'(x) = c \in \mathbb{F}_q$, since $f'^g(x) = f'(x^{g^{-1}}) = c$. Thus $X_{\mathbf{0}}$ fixes the set of constant functions, setwise. It follows from this that no element of $X_{\mathbf{0}}$ maps the vertex α to β, since such an element would not map the constant function $f(x) = a$ to another constant function. □

9.2 Projective Reed-Muller codes

The projective Reed-Muller codes (see Definition 9.2.1) are normally defined in a Hamming graph where M is a set of representatives of the set of 1-dimensional subspaces of $\mathbb{F}_q^t$.

However, the definition below takes M to be the set of 1-dimensional subspaces of $\mathbb{F}_q^t$ themselves and, for each $i \in M$, the alphabet Q_i to be the set of functions from i to $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$ for all $a \in \mathbb{F}_q$ and $x \in i$, where $\ell \in \{1, \dots, q-1\}$ is a parameter of the code. By Lemma 9.1.4, the set $\mathcal{S}_{q,t,\ell}$ is in bijection with the vertex set of the Hamming graph $H(m, q)$ just described, where $m = (q^t - 1)/(q - 1)$. Note that if $\gcd(q-1, \ell) = 1$ then, with the exception of the zero function, an element of Q_i will be a bijection. This formulation allows the action of $\mathrm{GL}_t(q)$ on the Hamming graph, induced from the action on $\mathbb{F}_q^t$, to be more easily investigated.

Definition 9.2.1 (Projective Reed-Muller codes)**.** Let M be the set of all 1-dimensional subspaces of $\mathbb{F}_q^t$, so that $m = (q^t - 1)/(q - 1)$, let $k \in \{1, \dots, t(q-1)\}$, let $\ell \equiv k \pmod{q-1}$ with $1 \leqslant \ell \leqslant q - 1$, and, for each $i \in M$, let Q_i be the set of functions from i to $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$ for all $a \in \mathbb{F}_q$ and $x \in i$. Then the *k-th order projective Reed-Muller code*, denoted $\mathcal{PRM}_q(k, t)$, in $H(m, q)$ is the subspace of $\mathcal{S}_{q,t,\ell}$ consisting precisely of those polynomials of degree k or less. That is,

$$\mathcal{PRM}_q(k,t) = \left\langle x_1^{b_1} \cdots x_t^{b_t} \mid b_i \geqslant 0; b_1 + \cdots + b_t = b \equiv \ell \pmod{q-1}; \exists b \in \{1, \dots, k\} \right\rangle.$$

The following result is [94, Theorem 1].

Theorem 9.2.2. *Let C be the projective Reed-Muller code $\mathcal{PRM}_q(k, t)$ and the integers s and ℓ satisfy $k - 1 = s(q-1) + \ell$ and $0 \leqslant \ell < q - 1$. Then C has minimum distance $(q-\ell)q^{t-s-2}$ and dimension*

$$\sum_{\substack{1 \leqslant i \leqslant k \\ i \equiv k \pmod{q-1}}} \sum_{j=0}^{t} (-1)^j \binom{t}{j} \binom{i - jq + t - 1}{i - jq}.$$

Letting $\ell = 0$ in the definition of projective Reed-Muller codes, in which case it is required that $k \equiv 0 \pmod{q-1}$, produces codes which are not Reed-Muller codes, but lie in a class known as *polynomial codes* [70]. In fact, the polynomial codes defined in this way are a particular subset of the family defined in [70].

Note, in regards to the next result, the action on $\mathcal{S}_{q,t,\ell}$ given by multiplying each polynomial by an element of $\mathbb{F}_q^\times$, that is $f(x) \mapsto af(x)$ for $a \in \mathbb{F}_q^\times$, corresponds to an element of $\mathrm{Diag}_m(\mathbb{F}_q^\times)$, since this is the resulting action in the Hamming graph. The subgroup of $\mathrm{GL}_t(q)$ acting trivially on M is the group of scalar matrices of $\mathrm{GL}_t(q)$. Moreover, if $a \in \mathbb{F}_q^\times$ satisfies $a^\ell = 1$, then the element of $\mathrm{GL}_t(q)$ given by the scalar matrix aI, where I is the identity matrix, acts trivially on $\mathcal{S}_{q,t,\ell}$. Thus, in contrast to Proposition 9.1.9, the intersection of $\mathrm{GL}_t(q)$ with $K_{\mathbf{0}} = \mathrm{Diag}_m(\mathbb{F}_q^\times)$ is congruent to $\mathbb{Z}_{(q-1)/\gcd(\ell, q-1)}$. Also, Theorem 9.2.2 gives the minimum distance δ of $\mathcal{PRM}_q(k, t)$, from which it can be seen that, for certain choices of parameters, the hypotheses $\delta \geqslant 3$ or $\delta \geqslant 5$ hold.

Proposition 9.2.3. *Let $C = \mathcal{PRM}_q(k, t)$, where $t \geqslant 2$ and $k \in \{1, \dots, t(q-1)\}$. Let ℓ be the unique integer satisfying $\ell \equiv k \pmod{q-1}$ such that $1 \leqslant \ell \leqslant q - 1$. Moreover, let*

$G \leqslant \mathrm{GL}_t(q)$ act on $H(m,q)$ via the induced action as in Lemma 9.1.5, $X_{\mathbf{0}} = \mathrm{Diag}_m(\mathbb{F}_q^\times)G$, T_C be the group of translations by codewords in C, and $X = T_C \rtimes X_{\mathbf{0}}$. Then the following hold:

1. *If $\delta \geqslant 3$ and G acts transitively on the set of 1-dimensional subspaces of $\mathbb{F}_q^t$ then C is X-neighbour-transitive.*
2. *If $\delta \geqslant 5$, $\gcd(\ell, q-1) = 1$ and $G = \mathrm{GL}_t(q)$ then C is $(X,2)$-neighbour-transitive, where $X \cong T_C \rtimes \mathrm{GL}_t(q)$.*

Proof. Note that the vertex set of $H(m,q)$ is identified with $\mathcal{S}_{q,t,\ell}$. First, T_C acts transitively on C, since C forms an $\mathbb{F}_q$-subspace of $\mathcal{S}_{q,t,k}$. Let $\mu, \nu \in \Gamma_1(\mathbf{0})$ with $\mu(e_1) = 1$ and $\nu(v) = a$ for some $a \in \mathbb{F}_q^\times$ and non-zero $v \in \mathbb{F}_q^t$. Suppose $\delta \geqslant 3$ and G acts transitively on the set of 1-dimensional subspaces of $\mathbb{F}_q^t$. It follows that there exists some $g \in G$ such that $\langle v \rangle^g = \langle e_1 \rangle$. Thus $\nu^g(e_1) = \nu(bv) = b^\ell a$, for some $b \in \mathbb{F}_q^\times$. Hence $(b^\ell a)^{-1}\mu^g = \nu$ and $X_{\mathbf{0}}$ acts transitively on $\Gamma_1(\mathbf{0})$. This proves part 1.

Suppose $\delta \geqslant 5$, $G = \mathrm{GL}_t(q)$ and $\gcd(\ell, q-1) = 1$, so that the map $a \mapsto a^\ell$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. Let $\mu, \nu \in \Gamma_2(\mathbf{0})$ with $\mu(e_1) = \mu(e_2) = 1$, $\nu(u) = a$ and $\nu(v) = b$, for some $a, b \in \mathbb{F}_q^\times$ and distinct non-zero $u, v \in \mathbb{F}_q^t$. Then, for all $c, d \in \mathbb{F}_q^\times$, there exists $g \in G$ such that $cu^g = e_1$ and $dv^g = e_2$. Thus $\nu^g(e_1) = \nu(cu) = c^\ell a$ and $\nu^g(e_2) = \nu(dv) = d^\ell b$. Choosing $c^\ell = a^{-1}$ and $d^\ell = b^{-1}$, which is possible since $\gcd(q-1, \ell) = 1$, gives $\nu^g = \mu$. Hence $X_{\mathbf{0}}$ acts transitively on $\Gamma_2(\mathbf{0})$, as required. Note that, as $\gcd(\ell, q-1) = 1$, $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ is induced by the scalar matrices in $\mathrm{GL}_t(q)$, so $X_{\mathbf{0}} \cong \mathrm{GL}_t(q)$. □

9.3 Twisted Reed-Muller codes

Suitably restricting the domain of the polynomials defining projective Reed-Muller codes gives rise to codes similar in nature to Reed-Muller codes (in that $M \cong \mathbb{F}_q^t$ in the definition below, so that any action on entries must be affine; compare with Definition 9.1.6), but with a twisted action. Some of these codes turn out to be 2-neighbour-transitive.

Definition 9.3.1 (Twisted Reed-Muller codes)**.** Let $m = q^t$ and M be the set of 1-dimensional subspaces of $\mathbb{F}_q^{t+1}$ defined as

$$M = \{\langle (1, a_1, \ldots, a_t) \rangle \mid a_1, \ldots, a_t \in \mathbb{F}_q\}.$$

Let $k \in \{1, \ldots, (t+1)(q-1)\}$ and $\ell \equiv k \pmod{q-1}$ with $1 \leqslant \ell \leqslant q-1$. For each $i \in M$, let Q_i be the set of functions from i to $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$ for all $a \in \mathbb{F}_q$ and $x \in i$ and let $H(m,q)$ be the Hamming graph with entries M and alphabet Q_i in entry $i \in M$. The *k-th order twisted Reed-Muller code*, denoted $\mathcal{TRM}_q(k,t)$, is the subset of $\mathcal{S}_{q,t+1,\ell}$ consisting of those polynomials of degree at most k.

Remark 9.3.2. In the action of $\mathrm{GL}_{t+1}(q)$ on $\mathbb{F}_q^{t+1}$, the subgroup preserving M fixes the hyperplane of $\mathbb{F}_q^{t+1}$ consisting of points having first co-ordinate 0. Thus, if $C = \mathcal{TRM}_q(k,t)$

then $\mathbb{Z}_{q-1} \rtimes \mathrm{AGL}_t(q) \leqslant \mathrm{Aut}(C)_{\mathbf{0}}$. Also, if $k \equiv \ell \pmod{q-1}$ and $\gcd(\ell, q-1) = 1$ and $g \in Z(\mathrm{GL}_{t+1}(q))$ then there exists some $a \in \mathbb{F}_q^\times$ such that $f^g(x) = f(ax) = a^\ell f(x)$. Thus $Z(\mathrm{GL}_{t+1}(q)) \leqslant \mathbb{Z}_{q-1} \rtimes \mathrm{AGL}_t(q)$ induces $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ on the Hamming graph.

While there is no equivalent of Theorem 9.1.7 given here, the minimum distance of first order codes $\mathcal{TRM}_q(1,t)$ agrees with that of $\mathcal{RM}_q(1,t)$. To see this, note that $\mathcal{TRM}_q(1,t)$ consists of degree 1 polynomials, which are zero precisely on a hyperplane of $\mathbb{F}_q^{t+1}$, and so are zero on either no elements of M, or on

$$\frac{q^t-1}{q-1} - \frac{q^{t-1}-1}{q-1}$$

elements of M, since M is the complement of a hyperplane. Thus $\mathcal{TRM}_q(1,t)$ has minimum distance $q^t - q^{t-1}$, so that the following proposition gives infinitely many examples of $(X,2)$-neighbour-transitive codes. As far as the author is aware, these codes have not appeared in the literature before.

Proposition 9.3.3. *Let $C = \mathcal{TRM}_q(k,t)$ in $H(q^t,q)$, where $k \equiv \ell \pmod{q-1}$, for some $\ell \in \{1,\dots,q-1\}$ with $\gcd(\ell, q-1) = 1$, and C have minimum distance $\delta \geqslant 5$. Then C is $(X,2)$-neighbour-transitive, with $X = T_C \rtimes X_{\mathbf{0}}$ and $X_{\mathbf{0}} \cong \mathbb{Z}_{q-1} \rtimes \mathrm{AGL}_t(q)$.*

Proof. Now, X acts transitively on C, since $T_C \leqslant X$. Also, $X_{\mathbf{0}}^M \cong \mathrm{AGL}_t(q)$ acts 2-transitively on M. Since $K_{\mathbf{0}} \cong \mathbb{F}_q^\times$ it follows that $X_{\mathbf{0}}$ acts transitively on the set of weight 1 vertices. Thus, since $\delta \geqslant 5$, it remains to show that $X_{\mathbf{0}}$ acts transitively on the set of vertices that are non-zero on precisely two chosen, distinct, entries of M.

Let $e_1,\dots,e_{t+1}$ be the standard basis vectors of $\mathbb{F}_q^{t+1}$, $\langle e_1\rangle, \langle e_1+e_2\rangle \in M$, $a,b \in \mathbb{F}_q^\times$ and α be the weight two vertex of $H(m,q)$ such that $\alpha(e_1) = a$ and $\alpha(e_1+e_2) = b$. Now, for all $c,d \in \mathbb{F}_q^\times$ there exists some $g \in \mathrm{GL}_{t+1}(q)$ such that $e_1^g = ce_1$, $(e_1+e_2)^g = d(e_1+e_2)$ and $e_u^g = e_u$ if $u \neq 1,2$. Since g fixes $\langle e_1\rangle$, g also fixes M and so has an induced action on $H(m,q)$. Hence,

$$\alpha^g(e_1) = \alpha(e_1^{g^{-1}}) = \alpha(c^{-1}e_1) = c^{-\ell}\alpha(e_1) = c^{-\ell}a,$$

and,

$$\alpha^g(e_1+e_2) = \alpha((e_1+e_2)^{g^{-1}}) = \alpha(d^{-1}(e_1+e_2)) = d^{-\ell}\alpha(e_1+e_2) = d^{-\ell}b.$$

As $\gcd(\ell, q-1) = 1$, we may choose c and d so that $d^\ell = b$ and $c^\ell = a$, and hence $\alpha^g(e_1) = \alpha^g(e_1+e_1) = 1$, from which the result follows. □

9.4 Codes related to other 2-transitive groups

The Suzuki, Ree, and unitary groups each have 2-transitive actions on certain sets of 1-dimensional subspaces of $\mathbb{F}_q^t$, for appropriate choices of q and t. The Suzuki group $\mathrm{Sz}(q)$, where $q = 2^{2n+1}$ for some integer $n \geqslant 1$, acts 2-transitively on the *Suzuki-Tits ovoid*, consisting

of (q^2+1) 1-spaces. The Ree group $\mathrm{Ree}(q)$, where $\sigma = 3^{2n+1}$ for some integer $n \geqslant 1$, acts 2-transitively on the *Ree unital*, consisting of (q^3+1) 1-spaces. The unitary group $\mathrm{PGU}_3(q)$ acts 2-transitively on a set of q^3+1 points called a unital. This leads to the consideration of the codes in the next three definitions, constructed in a similar manner to the projective Reed-Muller codes. Note that in the Hamming graphs of interest, M is now taken to be one of the above ovoids or unitals, so that vertices are functions with a suitably restricted domain. In particular, the domain of the functions becomes a union of the set of 1-spaces comprising the corresponding ovoid or unital. As in the previous section, polynomials in $\mathcal{S}_{q,t,\ell}$ are used to represent these functions.

Definition 9.4.1. Let $q = 2^{2n+1}$ for some integer $n \geqslant 1$, $m = q^2+1$, $k \in \{1,\dots,4(q-1)\}$ and $\ell \in \{1,\dots,q-1\}$ such that $k \equiv \ell \pmod{q-1}$. Let $H(m,q)$ be the Hamming graph such that M is the Suzuki-Tits ovoid in $V = \mathbb{F}_q^4$ and, for each $i \in M$, Q_i is the set of functions from i to $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$, for all $a \in \mathbb{F}_q$ and $x \in i$. Define the *k-th order Suzuki code* $\mathcal{SC}_q(k)$ to be the subspace of $\mathcal{S}_{q,4,\ell}$ formed by the polynomials of degree at most k.

Definition 9.4.2. Let $q = 3^{2n+1}$ for some integer $n \geqslant 1$, $m = q^3+1$, $k \in \{1,\dots,7(q-1)\}$ and $\ell \in \{1,\dots,q-1\}$ such that $k \equiv \ell \pmod{q-1}$. Let $H(m,q)$ be the Hamming graph such that M is the Ree unital in $V = \mathbb{F}_q^7$ and, for each $i \in M$, Q_i is the set of functions from i to $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$, for all $a \in \mathbb{F}_q$ and $x \in i$. Define the *k-th order Ree code* $\mathcal{RC}_q(k)$ to be the subspace of $\mathcal{S}_{q,7,\ell}$ formed by the polynomials of degree at most k.

Definition 9.4.3. Let q be a prime power, $m = q^3+1$, $k \in \{1,\dots,3(q^2-1)\}$ and $\ell \in \{1,\dots,q-1\}$ such that $k \equiv \ell(q+1) \pmod{q^2-1}$. Let $H(m,q)$ be the Hamming graph such that M is the unital in $V = \mathbb{F}_{q^2}^3$ corresponding to the 2-transitive action of $\mathrm{PGU}_3(q)$ and, for each $i \in M$, Q_i is the set of functions from i to $\mathbb{F}_q$ such that $f(ax) = a^\ell f(x)$, for all $a \in \mathbb{F}_q$ and $x \in i$. Define the *k-th order unitary code* $\mathcal{UC}_q(k)$ to be the subspace formed by all $f \in \mathcal{S}_{q^2,3,\ell(q+1)}$ such that the degree of f is at most k and $f(x) \in \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^2}^3$.

If we consider the codes $\mathcal{SC}_q(1)$, consisting of the polynomials of degree 1, and $\mathcal{UC}_q(q+1)$, consisting of polynomials of degree 1 when reduced to a subfield, then we can calculate the minimum distance fairly easily.

Proposition 9.4.4. *The first order codes $\mathcal{SC}_q(1)$ and $\mathcal{UC}_q(1)$ have minimum distances q^2-q and q^6-2q, respectively.*

Proof. Since each code is linear, the minimum distance is equal to the minimum weight of a non-zero codeword. First, let $C = \mathcal{SC}_q(1)$. A degree 1 polynomial f in $\mathcal{S}_{q,4,1}$ will evaluate to zero on precisely the points of a hyperplane in $\mathcal{PG}_3(q)$. Any hyperplane is either tangent to an ovoid, or meets the ovoid in an 'oval' consisting of $q+1$ points. It follows that f is non-zero on either q^2 or q^2-q points of the ovoid. Thus, the minimum distance of $\mathcal{SC}_q(1)$ is q^2-q.

Let $C = \mathcal{UC}_q(q+1)$. Then a polynomial f of degree $q+1$ in $\mathcal{S}_{q^2,3,q+1}$ is zero precisely on a Baer subplane of $\mathcal{PG}_2(q^2)$, that is, f is linear upon reduction to the subfield $\mathbb{F}_q$. By [5,

Corollary 8], each Baer subplane meets a unital in either 1, $q+1$, or $2q+1$ points. Thus, since $m = q^3+1$, the minimum distance of $\mathcal{UC}_q(q+1)$ is q^3-2q. □

Remark 9.4.5. An equivalent of Theorem 9.2.2 for the codes $\mathcal{SC}_q(k)$, $\mathcal{RC}_q(k)$ and $\mathcal{UC}_q(k)$ is not presented here. Thus, in later results involving these codes, though not desirable, the condition that the minimum distance is at least 5 is required. However, Proposition 9.4.4 shows that there are infinitely many cases where each of $\mathcal{SC}_q(k)$ and $\mathcal{UC}_q(k)$ have minimum distance $\delta \geqslant 5$. To further illustrate that there are choices of k and q that give rise to non-trivial codes, it will be useful to estimate the dimensions of some small cases. Theorem 9.2.2 gives an upper bound for the dimension of $\mathcal{SC}_q(k)$ and $\mathcal{RC}_q(k)$, since setting $t = 4$ or 7, respectively, $\mathcal{PRM}_q(k,t)$ is generated by the same polynomials. Thus, it is seen that the dimension of $\mathcal{SC}_q(k)$ is at most 4, 10, 20 and 35, when $k = 1, 2, 3$ and 4 respectively, whilst the Hamming graph has dimension q^2+1. Similarly, $\mathcal{RC}_q(k)$ has dimension at most 7, 28, 84 and 210, for $k = 1, 2, 3$ and 4 respectively, whilst the Hamming graph has dimension q^3+1. Things are slightly more complicated for $\mathcal{UC}_q(k)$, since the codewords are polynomials in $\mathcal{S}_{q^2,3,\ell}$ where ℓ is a multiple of $q+1$. However, the $\mathbb{F}_q$-dimension of $\mathcal{PRM}_{q^2}(q+1,3)$ gives an upper bound for the dimension of $\mathcal{UC}_q(q+1)$ of at most twice the $\mathbb{F}_{q^2}$-dimension of $\mathcal{PRM}_{q^2}(q+1,3)$. So $\mathcal{UC}_q(q+1)$ has dimension at most $2(q^2+5q+6)$, whilst the Hamming graph has dimension q^3+1. Thus, there are non-trivial instances of these codes, provided q is large enough.

Following the discussion in Remark 9.4.5, in Propositions 9.4.6 and 9.4.8 it is left as an assumption that the minimum distance is at least 5 .

Proposition 9.4.6. *Suppose $C = \mathcal{SC}_q(k)$ in $H(q^2+1,q)$ has minimum distance $\delta \geqslant 5$ and $\gcd(k, q-1) = 1$. Then C is $(X,2)$-neighbour-transitive, where $X = T_C \rtimes (\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{Sz}(q))$ and T_C is the group of translations by codewords of C.*

Proof. Since T_C acts transitively on C, $\mathrm{Sz}(q)$ acts 2-transitively on M and $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ acts transitively on the set vertices of weight 1 that are non-zero in a specified entry, it suffices to show that $\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{Sz}(q)$ acts transitively on the vertices that are non-zero in two fixed entries. Recall, from Definition 9.4.1, that $k \in \{1, \ldots, 4(q-1)\}$ with $\ell \in \{1, \ldots, q-1\}$ such that $k \equiv \ell \pmod{q-1}$, and that if $\alpha \in C$ then $\alpha(ax) = a^\ell \alpha(x)$ for all $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_q^4$. The condition $\gcd(k, q-1) = 1$ thus implies $\gcd(\ell, q-1) = 1$.

Following [103, Section 4.2.2], elements of $\mathrm{Sz}(q)$ are 4×4 matrices with respect to the ordered basis $\{e_1, e_2, f_2, f_1\}$, and if $i = \langle e_1 \rangle$ and $j = \langle f_1 \rangle$ then $i, j \in M$. Then $X_{\mathbf{0},i,j} = \mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{Sz}(q)_{i,j}$, where $\mathrm{Sz}(q)_{i,j}$ is the group of diagonal 4×4 matrices with diagonal entries $(a, a^{2^{n+1}-1}, a^{-2^{n+1}+1}, a^{-1})$, for some $a \in \mathbb{F}_q^\times$. Let α be a weight two vertex of $H(m,q)$ such that $\alpha(e_1) = c$ and $\alpha(f_1) = d$, where $c, d \in \mathbb{F}_q^\times$. If $b \in \mathbb{F}_q^\times$ and $g \in \mathrm{Sz}(q)_{i,j}$ with $a \in \mathbb{F}_q^\times$ as above, then

$$b\alpha^g(e_1) = b\alpha(e_1^{g^{-1}}) = b\alpha(a^{-1}e_1) = ba^{-\ell}\alpha(e_1) = a^{-\ell}bc,$$

and

$$b\alpha^g(f_1) = b\alpha(f_1^{g^{-1}}) = b\alpha(af_1) = ba^\ell\alpha(f_1) = a^\ell bd.$$

If a and b exist such that $1 = a^{-\ell}bc = a^\ell bd$ then the result follows. This requires $a^{2\ell} = cd^{-1}$ and $b = a^\ell c^{-1}$. Since q is even and $\gcd(\ell, q-1) = 1$ it follows that $\gcd(2\ell, q-1) = 1$ and thus the required a and b exist. □

Remark 9.4.7. In the proof of Proposition 9.4.6, the last step required every element of $\mathbb{F}_q^\times$ to be a square of some other element. This occurs in fields of characteristic 2, but not in one of odd characteristic. Attempting the same argument for $\mathcal{RC}_q(k)$ culminates in the same requirement, and is thus fruitless. The situation is similar for $\mathcal{UC}_q(k)$, and hence the next result requires q to be a power of 2.

Proposition 9.4.8. *Let q be a power of 2 and $C = \mathcal{UC}_q(k)$ in $H(q^3+1, q)$, where $\gcd(k, q^2-1) = q+1$. If C has minimum distance $\delta \geqslant 5$ then C is $(X, 2)$-neighbour-transitive, where $X \cong T_C \rtimes (\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{PGU}_3(q))$ and T_C is the group of translations by codewords of C.*

Proof. The proof strategy is similar to that of Proposition 9.4.6. Since T_C acts transitively on C, $\mathrm{PGU}_3(q)$ acts 2-transitively on M and $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ acts transitively on the set vertices that are non-zero in a specified entry, it suffices to show that $\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{PGU}_3(q^s)$ acts transitively on the vertices that are non-zero in two fixed entries. Recall, from Definition 9.4.3, that $k \in \{1, \ldots, 3(q^2-1)\}$ with $\ell \in \{1, \ldots, q-1\}$ such that $k \equiv \ell(q+1) \pmod{q^2-1}$, and if $\alpha \in C$ then $\alpha(ax) = a^{\ell(q+1)}\alpha(x)$ for all $a \in \mathbb{F}_{q^2}$ and $x \in \mathbb{F}_{q^2}^3$. The condition $\gcd(k, q^2-1) = q+1$ thus implies $\gcd(\ell, q-1) = 1$.

Following [36, Section 7.7], elements of $\mathrm{PGU}_3(q)$ are 3×3 matrices with respect to the ordered basis $\{e_1, e_2, e_3\}$, and if $i = \langle e_1 \rangle$ and $j = \langle e_3 \rangle$ then $i, j \in M$. Then $X_{\mathbf{0},i,j} = \mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{PGU}_3(q)_{i,j}$, where $\mathrm{PGU}_3(q)_{i,j}$ is the group of 3×3 diagonal matrices with diagonal entries (a, b, a^{-q}), where $a \in \mathbb{F}_{q^2}^\times$ and $b \in \mathbb{F}_q^\times$. Let α be a weight two vertex of $\mathcal{H}(m, q)$ such that $\alpha(e_1) = c$ and $\alpha(e_3) = d$, where $c, d \in \mathbb{F}_q^\times$. If $b \in \mathbb{F}_q^\times$ and $g \in X_{\mathbf{0},i,j}$ for some $a \in \mathbb{F}_{q^2}^\times$ as above, then

$$b\alpha^g(e_1) = b\alpha(e_1^{g^{-1}}) = b\alpha(a^{-1}e_1) = ba^{-\ell(q+1)}\alpha(e_1) = a^{-\ell(q+1)}bc,$$

and

$$b\alpha^g(e_3) = b\alpha(e_3^{g^{-1}}) = b\alpha(a^{-q^s}e_3) = ba^{\ell q(q+1)}\alpha(e_3) = a^{\ell q(q+1)}bd.$$

If a and b can be chosen so that $1 = a^{-\ell(q+1)}bc = a^{\ell q(q+1)}bd$ then the result follows. This requires $a^{\ell(q+1)^2} = cd^{-1}$ and $b = a^{\ell(q+1)}c^{-1}$. Now, as a ranges over each element of $\mathbb{F}_{q^2}^\times$ the $(q+1)$-th power a^{q+1} ranges over each element of $\mathbb{F}_q^\times$, and as $\gcd(q+1, q-1) = 1 = \gcd(\ell, q-1)$ we have that $a^{\ell(q+1)^2}$ ranges over all elements of $\mathbb{F}_q^\times$. Thus there exists a such that $a^{\ell(q+1)^2} = cd^{-1}$ and taking $b = a^{\ell(q+1)}c^{-1}$ gives the required g and b. □

9.5 Subfield codes

Further examples of 2-neighbour-transitive codes can be constructed by restricting the polynomials making up the codes considered so far in this chapter, to those only taking values in a subfield. In particular, if $f \in \mathcal{S}_{q^s,t,\ell}$ then f has been considered to be a vertex in the Hamming graph $H(m, q^s)$ with entry set M some set of 1-dimensional subspaces of $\mathbb{F}_{q^s}^t$ and alphabet Q_i, for each $i \in M$, the set of all functions f_i from i to $\mathbb{F}_{q^s}$ satisfying $f_i(ax) = a^\ell f_i(x)$ for all $a \in \mathbb{F}_{q^s}$ and $x \in i$. If $(q^s - 1)/(q - 1)$ divides ℓ and $f(x) \in \mathbb{F}_q$, for all $x \in i$ and $i \in M$, then the polynomial f is a vertex in the Hamming graph $H(m, q)$ with the same entry set M and alphabet Q_i, for each $i \in M$, the set of all functions f_i from i to $\mathbb{F}_q$ satisfying $f_i(ax) = a^\ell f_i(x)$ for all $a \in \mathbb{F}_{q^s}$ and $x \in i$. Note that $a^\ell \in \mathbb{F}_q$ for all $a \in \mathbb{F}_{q^s}$, since $(q^s - 1)/(q - 1)$ divides ℓ.

Definition 9.5.1. Let k be a multiple of $(q^s - 1)/(q - 1)$. Then the *k-th order projective Reed-Muller, twisted Reed-Muller, Suzuki, Ree, and unitary subfield-codes* $\mathcal{PRM}_{q^s/q}(k, t)$, $\mathcal{TRM}_{q^s/q}(k, t)$, $\mathcal{SC}_{q^s/q}(k)$, $\mathcal{RC}_{q^s/q}(k)$, and $\mathcal{UC}_{q^s/q}(k)$, respectively, in $H(m, q)$ (with M as in the appropriate definition) are defined to be the sets of all vertices α of $\mathcal{PRM}_{q^s}(k, t)$, $\mathcal{TRM}_{q^s}(k, t)$, $\mathcal{SC}_{q^s}(k)$, $\mathcal{RC}_{q^s}(k)$, and $\mathcal{UC}_{q^s}(k)$, respectively, such that $\alpha(x) \in \mathbb{F}_q$ for all $x \in i$ and $i \in M$.

Note that as $\mathcal{PRM}_{q^s/q}(k, t)$ is linear and the codewords of $\mathcal{PRM}_{q^s/q}(k, t)$ are also codewords in $\mathcal{PRM}_{q^s}(k, t)$ the minimum distance of $\mathcal{PRM}_{q^s/q}(k, t)$ is at least $(q^s - \ell)q^{s(t-v-2)}$, by Theorem 9.2.2, where v and ℓ are such that $k - 1 = v(q^s - 1) + \ell$ and $0 \leqslant \ell < q - 1$.

Proposition 9.5.2. *Let $C = \mathcal{PRM}_{q^s/q}(k, t)$, where $\gcd(k, q^s - 1) = (q^s - 1)/(q - 1)$, have minimum distance $\delta \geqslant 5$. Then C is $(X, 2)$-neighbour-transitive, where $X \cong T_C \rtimes \mathrm{GL}_t(q^s)/\mathbb{Z}_{(q^s-1)/(q-1)}$ and T_C is the group of translations by codewords in C.*

Proof. To see that $\mathrm{GL}_t(q^s)$ fixes C, note that each vertex is a function from $\mathbb{F}_{q^s}^t$ into $\mathbb{F}_q$. As $\mathrm{GL}_t(q^s)$ acts on the domain of each function, and, by Lemma 9.1.5, preserves the degree of each polynomial, it also fixes C. By the definition of the projective Reed-Muller codes, k satisfies $k \in \{1, \ldots, t(q^s - 1)\}$. Let $\ell \equiv k \pmod{q^s - 1}$ where $1 \leqslant \ell \leqslant q^s - 1$, so that $\alpha \in C$ implies $\alpha(ax) = a^\ell \alpha(x)$, for all $a \in \mathbb{F}_{q^s}$ and $x \in \mathbb{F}_{q^s}^t$. The condition $\gcd(k, q^s - 1) = (q^s - 1)/(q - 1)$ is then equivalent to $\gcd(\ell, q^s - 1) = (q^s - 1)/(q - 1)$. As in the discussion immediately preceding Proposition 9.2.3, $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ is induced by the center of $\mathrm{GL}_t(q^s)$ in its action induced on $H(m, q)$, which corresponds to the group of scalar matrices aI, for $a \in \mathbb{F}_{q^s}$, the action of such an element being trivial when $a^\ell = 1$.

Since T_C acts transitively on C, $\mathrm{GL}_t(q^s)$ acts 2-transitively on M and $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ acts transitively on the set vertices that are non-zero in a specified entry, it suffices to show that $\mathrm{GL}_t(q^s)$ acts transitively on the vertices that are non-zero in two fixed entries.

Let $\{e_1, \ldots, e_t\}$ be a basis for $\mathbb{F}_{q^s}^t$ and $i = \langle e_1 \rangle, j = \langle e_2 \rangle \in M$. Furthermore, let $c, d \in \mathbb{F}_q^\times$ and α be the weight 2 vertex in $H(m, q)$ such that $\alpha(e_1) = c$ and $\alpha(e_2) = d$. Let $g \in \mathrm{GL}_t(q^s)$ and $a, b \in \mathbb{F}_{q^s}^\times$ such that $e_1^g = ae_1$, $e_2^g = be_2$ and $e_r^g = e_r$ for $r = 3, \ldots, t$. Then $\alpha^g(e_1) = a^{-\ell}c$

and $\alpha^g(e_2) = b^{-\ell}d$. The result follows upon choosing a and b such that $a^\ell = c$ and $b^\ell = d$, which is possible for all $c, d \in \mathbb{F}_q^\times$ since $\gcd(\ell, q^s - 1) = (q^s - 1)/(q - 1)$, as then $\alpha^g(e_1) = 1$ and $\alpha^g(e_2) = 1$. □

While the minimum distances of the codes in the next proposition are not calculated here in terms of their parameters, note that the minimum distance of the respective code from which they are derive gives a lower bound for their minimum distance. Remark 9.3.2 gives information about the group X in the case of $\mathcal{TRM}_{q^s/q}(k, t)$, while it should be noted that here $\gcd(k, q^s - 1) = (q^s - 1)/(q - 1)$ so that for $g \in Z(\mathbb{Z}_{q^s-1} \rtimes \mathrm{AGL}_t(q^s))$ there exists $a \in \mathbb{F}_{q^s}^\times$ such that, for a vertex f in $H(m, q)$, $f^g(x) = f(ax) = a^k f(x)$, where $a^k \in \mathbb{F}_q^\times$. Thus $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ is induced on $H(m, q)$ by $Z(\mathbb{Z}_{q^s-1} \rtimes \mathrm{AGL}_t(q^s))$.

Proposition 9.5.3. *The following codes C are $(X, 2)$-neighbour-transitive, for the given X and where T_C is the group of translations by codewords of C, provided C has minimum distance $\delta \geqslant 5$:*

1. $C = \mathcal{TRM}_{q^s/q}(k, t)$ *in* $H(q^{ts}, q)$, *where* $\gcd(k, q^s - 1) = (q^s - 1)/(q - 1)$ *and* $X = T_C \rtimes (\mathbb{Z}_{q^s-1} \rtimes \mathrm{AGL}_t(q^s)/\mathbb{Z}_{(q^s-1)/(q-1)})$.

2. $C = \mathcal{SC}_{q^s/q}(k)$ *in* $H(q^{2s} + 1, q)$, *where* $\gcd(k, q^s - 1) = (q^s - 1)/(q - 1)$ *and* $X = T_C \rtimes (\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{Sz}(q^s))$.

3. $C = \mathcal{UC}_{q^s/q}(k)$ *in* $H(q^{3s}+1, q)$, *where* q *is a power of* 2, $\gcd(k, q^{2s}-1) = (q^{2s}-1)/(q-1)$ *and* $X = T_C \rtimes (\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{PGU}_3(q^s))$.

Proof. To see that each group fixes C, note that each vertex is a polynomial function from $\mathbb{F}_{q^s}^t$ into $\mathbb{F}_q$. Also, $\mathrm{Diag}_m(\mathbb{F}_q^\times)$ fixes C. As each of $\mathbb{Z}_{q-1} \rtimes \mathrm{AGL}_t(q^s)/\mathbb{Z}_{(q^s-1)/(q-1)}$, $\mathrm{Sz}(q^s)$ and $\mathrm{PGU}_3(q^s)$, respectively, acts on the domain of each polynomial, fixes M, and, by Lemma 9.1.5, preserves the degree of each polynomial, $X_{\mathbf{0}}$, and thus X, fixes C.

Since T_C acts transitively on C, $\mathbb{Z}_{q-1} \rtimes \mathrm{AGL}_t(q^s)/\mathbb{Z}_{(q^s-1)/(q-1)}$, $\mathrm{Sz}(q^s)$ or $\mathrm{PGU}_3(q^s)$, respectively, acts 2-transitively on M and $\mathrm{Diag}_m(\mathbb{F}_q^\times) \leqslant X_{\mathbf{0}}$ (see Remark 9.3.2 in the case of $\mathcal{TRM}_{q^s/q}(k, t)$) acts transitively on the set vertices that are non-zero in a specified entry, it suffices to show that $\mathbb{Z}_{q^s-1} \rtimes \mathrm{AGL}_t(q^s)/\mathbb{Z}_{(q^s-1)/(q-1)}$, $\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{Sz}(q^s)$ or $\mathrm{Diag}_m(\mathbb{F}_q^\times) \rtimes \mathrm{PGU}_3(q^s)$, respectively, acts transitively on the vertices that are non-zero in two fixed entries. Let $\ell \equiv k \pmod{q^s - 1}$ so that $\alpha(ax) = a^\ell \alpha(x)$ for all $a \in \mathbb{F}_{q^s}$ and $x \in \mathbb{F}_q^{t'}$, where $t' = t + 1$, 4 or 3, respectively.

Let $C = \mathcal{TRM}_{q^s/q}(k, t)$. Let $a, b \in \mathbb{F}_q^\times$ and $\alpha \in C$ be the weight two vertex such that $\alpha(e_1) = a$ and $\alpha(e_1 + e_2) = b$. Now, for all $c, d \in \mathbb{F}_{q^s}^\times$ there exists some $g \in \mathrm{GL}_{t+1}(q^s)$ such that $e_1^g = ce_1$, $(e_1 + e_2)^g = d(e_1 + e_2)$ and $e_u^g = e_u$ if $u \neq 1, 2$. Since g fixes $\langle e_1 \rangle$, g also fixes M and so has an induced action on C. Hence,

$$\alpha^g(e_1) = \alpha(e_1^{g^{-1}}) = \alpha(c^{-1}e_1) = c^{-\ell}\alpha(e_1) = c^{-\ell}a,$$

and,

$$\alpha^g(e_1+e_2)=\alpha((e_1+e_2)^{g^{-1}})=\alpha(d^{-1}(e_1+e_2))=d^{-\ell}\alpha(e_1)=d^{-\ell}b.$$

Since $\gcd(\ell,q^s-1)=(q^s-1)/(q-1)$, both c and d may be chosen so that $d^\ell=b$ and $c^\ell=a$. Then $\alpha^g(e_1)=\alpha^g(e_1+e_1)=1$, proving part 1.

Next, let $C=\mathcal{SC}_{q^s/q}(k)$. Recall, from Definition 9.4.1, that $k\in\{1,\ldots,4(q^s-1)\}$ with $\ell\in\{1,\ldots,q^s-1\}$ such that $k\equiv\ell\pmod{q^s-1}$, and that if $\alpha\in C$ then $\alpha(ax)=a^\ell\alpha(x)$ for all $a\in\mathbb{F}_{q^s}$ and $x\in\mathbb{F}_{q^s}^4$. The condition $\gcd(k,q^s-1)=(q^s-1)/(q-1)$ thus implies $\gcd(\ell,q^s-1)=(q^s-1)/(q-1)$.

Again, following [103, Section 4.2.2], elements of $\mathrm{Sz}(q^s)$ are 4×4 matrices with respect to the ordered basis $\{e_1,e_2,f_2,f_1\}$. Let $i=\langle e_1\rangle$ and $j=\langle f_1\rangle$. Then $X_{\mathbf{0},i,j}=\mathrm{Diag}_m(\mathbb{F}_q^\times)\rtimes\mathrm{Sz}(q^s)_{i,j}$, where $\mathrm{Sz}(q^s)_{i,j}$ is the group of diagonal 4×4 matrices with diagonal entries

$$(a,a^{2^{n+1}-1},a^{-2^{n+1}+1},a^{-1}),$$

for some $a\in\mathbb{F}_{q^s}^\times$. Let α be a weight two vertex of $H(m,q)$ such that $\alpha(e_1)=c$ and $\alpha(f_1)=d$, where $c,d\in\mathbb{F}_q^\times$. If $b\in\mathbb{F}_q^\times$ and $g\in\mathrm{Sz}(q)_{i,j}$ with $a\in\mathbb{F}_{q^s}^\times$ as above, then

$$b\alpha^g(e_1)=b\alpha(e_1^{g^{-1}})=b\alpha(a^{-1}e_1)=ba^{-\ell}\alpha(e_1)=a^{-\ell}bc,$$

and

$$b\alpha^g(f_1)=b\alpha(f_1^{g^{-1}})=b\alpha(af_1)=ba^\ell\alpha(f_1)=a^\ell bd.$$

If a and b exist such that $1=a^{-\ell}bc=a^\ell bd$ then C is $(X,2)$-neighbour-transitive. This requires $a^{2\ell}=cd^{-1}$ and $b=a^\ell c^{-1}$. As a ranges over all elements of $\mathbb{F}_{q^s}^\times$, a^ℓ ranges over all elements of $\mathbb{F}_q^\times$, since $\gcd(\ell,q^s-1)=(q^s-1)/(q-1)$. Additionally, $\gcd(2,q-1)=1$, since q is even, and thus the required a and b exist.

Let $C=\mathcal{UC}_{q^s,q}(k)$. Recall, from Definition 9.4.3, that $k\in\{1,\ldots,3(q^{2s}-1)\}$ with $\ell\in\{1,\ldots,q^s-1\}$ such that $k\equiv\ell(q^s+1)\pmod{q^{2s}-1}$, and if $\alpha\in C$ then $\alpha(ax)=a^{\ell(q^s+1)}\alpha(x)$ for all $a\in\mathbb{F}_{q^{2s}}$ and $x\in\mathbb{F}_{q^{2s}}^3$. The condition $\gcd(k,q^{2s}-1)=(q^{2s}-1)/(q-1)$ thus implies $\gcd(\ell,q^{2s}-1)=(q^s-1)/(q-1)$.

Following [36, Section 7.7], elements of $\mathrm{PGU}_3(q^s)$ are 3×3 matrices with respect to the ordered basis $\{e_1,e_2,e_3\}$. Let $i=\langle e_1\rangle$ and $j=\langle e_3\rangle$. Then $X_{\mathbf{0},i,j}=\mathrm{Diag}_m(\mathbb{F}_q^\times)\rtimes\mathrm{PGU}_3(q^s)_{i,j}$, where $\mathrm{PGU}_3(q^s)_{i,j}$ is the group of 3×3 diagonal matrices with diagonal entries (a,b,a^{-q^s}), where $a\in\mathbb{F}_{q^{2s}}^\times$ and $b\in\mathbb{F}_{q^s}^\times$. Let α be a weight two vertex of $\mathcal{H}(m,q)$ such that $\alpha(e_1)=c$ and $\alpha(e_3)=d$, where $c,d\in\mathbb{F}_q^\times$. If $b\in\mathbb{F}_q^\times$ and $g\in X_{\mathbf{0},i,j}$ for some $a\in\mathbb{F}_{q^{2s}}^\times$ as above, then

$$b\alpha^g(e_1)=b\alpha(e_1^{g^{-1}})=b\alpha(a^{-1}e_1)=ba^{-\ell(q^s+1)}\alpha(e_1)=a^{-\ell(q^s+1)}bc,$$

and

$$b\alpha^g(e_3)=b\alpha(e_3^{g^{-1}})=b\alpha(a^{-q^s}e_3)=ba^{\ell q^s(q^s+1)}\alpha(e_3)=a^{\ell q^s(q^s+1)}bd.$$

If a and b can be chosen so that $1=a^{-\ell(q^s+1)}bc=a^{\ell q^s(q^s+1)}bd$ then the result follows. This requires $a^{\ell(q^s+1)^2}=cd^{-1}$ and $b=a^{\ell(q^s+1)}c^{-1}$. Now, as a ranges over each element of $\mathbb{F}_{q^{2s}}^\times$,

$a^{\ell(q^s+1)}$ ranges over each element of $\mathbb{F}_q^\times$, since $\gcd(\ell, q^{2s}-1) = (q^s-1)/(q-1)$. Also, $q^s+1 \equiv 2 \pmod{q-1}$ so that it is equivalent to find $a' \in \mathbb{F}_q^\times$ such that $(a')^2 = cd^{-1}$. Since q is even and $\gcd(\ell, q-1) = 1$, the required a and b exist. □

9.6 Linear-2-neighbour-transitive codes

Throughout this section, let the vector space $V \cong \mathbb{F}_q^m$ be the vertex set of the Hamming graph $H(m,q)$. If C is a subspace of V, then denote by T_C the group formed by the set of all translations by elements of C. Recall that $K = X \cap B$ is the kernel of the action of X on M. This section considers linear-$(X,2)$-neighbour-transitive codes, that is, codes that are $(X,2)$-neighbour-transitive, where $X_i^{Q_i} \cong \mathrm{AGL}_1(q)$ and $K_{\mathbf{0}} \cong \mathbb{F}_q^\times$, as in Definition 1.2.2. Whilst the standard definition of a linear code C only requires C to be fixed by the group T_C and $\mathrm{Diag}_m(\mathbb{F}_q^\times)$; in order to simplify the discussion here, the definition also requires that no field automorphisms of the alphabet be present in X.

Lemma 9.6.1. *Let C be a code in $H(m,q)$ and $T_C \leqslant X \leqslant \mathrm{Aut}(C)$ then $X = T_C \rtimes X_{\mathbf{0}}$.*

Proof. Let $x = h\sigma \in X$, with $h \in B$ and $\sigma \in L$, and $\alpha \in C$. Then $x^{-1}t_\alpha x = \sigma^{-1}t_\alpha\sigma = t_\beta$, for some $\beta \in C$. Thus T_C is normalised by X and, since T_C is transitive on C, it follows that $X = T_C \rtimes X_{\mathbf{0}}$. □

Lemma 9.6.1 shows, in particular, that if C is a linear-$(X,2)$-neighbour-transitive code in $H(m,q)$, then $X_{\mathbf{0}}^M \cong X^M$.

Lemma 9.6.2. *Let $q \geqslant 3$ and C be a linear-$(X,2)$-neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 5$. Then there is no 1-dimensional subspace of the vertex set of $H(m,q)$ fixed by X.*

Proof. Note that, since $m \geqslant \delta$, we have $m \geqslant 5$. Suppose U is such a subspace and let $\alpha \in U$ with $\alpha \neq \mathbf{0}$. Every non-zero vertex in U has the same support, since each vertex in U is a scalar multiple of α. First, α does not have weight 1, since $X_{\mathbf{0}}$ acts transitively on the set of weight 1 vertices and the $\mathbb{F}_q$-span of the weight 1 vertices is the entire vertex set. Let $\alpha_i = a$ and $\alpha_j = b$ for some $a, b \in \mathbb{F}_q^\times$ and distinct $i, j \in M$. Since $\delta \geqslant 5$, the stabiliser $X_{\mathbf{0},\{i,j\}}$ acts transitively on set of weight 2 vertices that are non-zero in entries i and j. Thus, the size of the orbit of α under $X_{\mathbf{0},\{i,j\}}$ is divisible by $(q-1)^2$, which contradicts $|U| = q$, since $q \geqslant 3$. □

Lemma 9.6.3. *Let C be a linear-$(X,2)$-neighbour-transitive code in $H(m,q)$, with $\delta \geqslant 5$. Then $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ or $\{(g,h) \mid |g||h| \text{ is even}\} \leqslant \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$. In particular, $X_{\mathbf{0},i,j}^M$ has a cyclic quotient of order $q-1$ or $(q-1)/2$.*

Proof. By definition $X_{\mathbf{0},i}^{Q_i^\times} \cong \mathbb{F}_q^\times$. Thus, $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \leqslant X_{\mathbf{0},i}^{Q_i^\times} \times X_{\mathbf{0},j}^{Q_j^\times} \cong \mathbb{F}_q^\times \times \mathbb{F}_q^\times$. By Lemma 8.1.5, it follows that $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times}$ has order $(q-1)^2$ or $(q-1)^2/2$. By Proposition 2.5.5, each of $X_{\mathbf{0},i}^{Q_i^\times}$ and $X_{\mathbf{0},j}^{Q_j^\times}$ act transitively on $Q_i^\times$ and $Q_j^\times$, respectively. It follows that $X_{\mathbf{0},i,j}^{Q_i^\times \times Q_j^\times} \cong \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ or the unique index 2 subdirect subgroup of this. Since $K_{\mathbf{0}} \cong \mathbb{F}_q^\times$, applying Lemma 8.1.4 gives the result. □

9.7 Binary linear codes

When $q = 2$ a code is called *binary* and, for any $X \leqslant \mathrm{Aut}(\Gamma)$ the groups $X_{\mathbf{0},i}^{Q_i^\times}$ and $K_{\mathbf{0}}$ are trivial. Thus, binary linear-$(X, 2)$-neighbour-transitive codes are linear in the usual sense. The next lemma shows that a binary linear-$(X, 2)$-neighbour-transitive code with $\delta \geqslant 5$ is a submodule of the $\mathbb{F}_2$-permutation module of a 2-homogeneous groups in its 2-homogeneous action.

Lemma 9.7.1. *Let C be a linear-$(X, 2)$-neighbour-transitive code, with minimum distance $\delta \geqslant 5$, in $H(m, 2)$ with vertex set $V \cong \mathbb{F}_2^m$. Then C is a submodule of V, regarded as the 2-homogeneous permutation module for the action of $X^M \cong X_{\mathbf{0}}$ on M.*

Proof. If C is linear-$(X, 2)$-neighbour-transitive then, by Lemma 9.6.1, $X = T_C \rtimes X_{\mathbf{0}}$. If $x = h\sigma \in X_{\mathbf{0}}$, with $h \in B$ and $\sigma \in L$, then $h = 1$, since h_i fixes 0, and thus also 1, in Q_i. Hence, $X_{\mathbf{0}} \cong X_{\mathbf{0}}^M \cong X^M$ acts as pure permutations on entries, so that V may be regarded as the permutation module for the action of $X_{\mathbf{0}}$ on M. Since $\delta \geqslant 5$, Proposition 2.5.3 implies that this action is 2-homogeneous. Thus, C is a submodule of the 2-homogeneous $\mathbb{F}_2 X_{\mathbf{0}}$-permutation module V. □

The next result is somewhat of a converse to Lemma 9.7.1. Note that if C has minimum distance $\delta = 3$ and C is perfect, then C has covering radius $\rho = 1$, and is thus *not* 2-neighbour-transitive, since C_2 is empty.

Lemma 9.7.2. *Let G act 2-homogeneously on a set M of size $m \geqslant 5$, $V \cong \mathbb{F}_2^m$ be the permutation module for the action of G on M, Y be the submodule of V consisting of the set of all constant functions, and C be a submodule of V. Then C is a code in $H(m, 2)$ with minimum distance δ, and precisely one of the following statements holds:*

1. *$C = \{\mathbf{0}\}$.*
2. *$\delta = 1$ and $C = V$.*
3. *$\delta = m$ and $C = Y$ and C is linear-$(X, 2)$-neighbour-transitive, where $X \cong \mathbb{Z}_2 \rtimes G$.*
4. *$\delta = 2$ and $C = Y^\perp$, the dual of Y under the standard inner product.*
5. *$\delta = 3$ and C is a perfect code in $H(m, 2)$.*
6. *$4 \leqslant \delta < m$ and C is linear-$(X, 2)$-neighbour-transitive, where $X = T_C \rtimes G$.*

Proof. First, the permutation module V may be regarded as the vertex set of $H(m, 2)$ in the natural way, so that C is a code in $H(m, 2)$ and $X = T_C \rtimes G \leqslant \mathrm{Aut}(C)$, so that $X_{\mathbf{0}} = G$. Part 1 holds if and only if $|C| = 1$. Assume $|C| \geqslant 2$ and let δ be the minimum distance of C. Since T_C acts transitively on C, and $\mathbf{0} \in C$, there exists a weight δ codeword in C. Note that the weight 1 vertices are the characteristic vectors of the subsets of M of size 1, and

the weight 2 vertices are the characteristic vectors of the subsets of M of size 2. Since G acts 2-homogeneously on M, it follows that $X_{\mathbf{0}}$ acts transitively on each of the sets $\Gamma_s(\mathbf{0})$, for $s = 1, 2$. Thus, $\Gamma_1(\mathbf{0})$ is a subset of either C or C_1, since any weight 1 vertex is distance 1 from $\mathbf{0} \in C$, and $\Gamma_2(\mathbf{0})$ is a subset of either C, C_1 or C_2, since any weight 2 vertex is distance 2 from $\mathbf{0} \in C$. If $\Gamma_2(\mathbf{0}) \subseteq C_2$ it immediately follows that C is $(X, 2)$-neighbour-transitive, as T_C acts transitively on C, and $X_{\mathbf{0}}$ acts transitively on $\Gamma_1(\mathbf{0})$ and $\Gamma_2(\mathbf{0})$.

Suppose $\delta = 1$. Then there exists some $\alpha, \beta \in C$ such that $d(\alpha, \beta) = 1$. Since T_C acts transitively on C, it can be assumed that $\beta = \mathbf{0}$. It then follows that α is in $\Gamma_1(\mathbf{0}) \cap C$, so that $\Gamma_1(\mathbf{0}) \subseteq C$. Thus, every weight 1 vertex ν is in C, and the translation t_ν by ν in X. Hence $C = V$, as in part 2.

Suppose $\delta = m$. If $\alpha \in V$ with $d(\mathbf{0}, \alpha) = m$ it follows that $\alpha_i = 1$ for all $i \in M$. As $\mathbf{0} \in C$, we have part 3, that is $C = Y$. Since $m \geqslant 5$, we deduce $\Gamma_2(\mathbf{0}) \subseteq C_2$, so that C is $(X, 2)$-neighbour-transitive, by the argument in the first paragraph of the proof.

Suppose $\delta = 2$. Then $\Gamma_1(\mathbf{0}) \subseteq C_1$. However, there exists a vertex $\alpha \in \Gamma_2(\mathbf{0}) \cap C$, so that $\Gamma_2(\mathbf{0}) \subseteq C$ and every weight 2 codeword is in C. Thus $C = Y^\perp$, and part 4 holds.

Suppose $\delta = 3$. Again, $\Gamma_1(\mathbf{0}) \subseteq C_1$. Now, there exists a weight 3 vertex $\alpha \in C$ and distinct $i, j, k \in M$ such that $\mathrm{supp}(\alpha) = \{i, j, k\}$. Let $\nu \in \Gamma_2(\mathbf{0})$ such that $\nu_i = \nu_j = 1$. Then $d(\alpha, \nu) = 1$, so that $\nu \in C_1$. Hence, $\Gamma_2(\mathbf{0}) \subseteq C_1$ and so $\Gamma_2(\mathbf{0}) \cap C_2 = \emptyset$. As T_C acts transitively on C, we have that $\Gamma_2(\beta) \cap C_2 = \emptyset$ for any $\beta \in C$. Hence $C_2 = \emptyset$ and C is perfect, giving part 5.

Finally, suppose $4 \leqslant \delta < m$. Since $\delta \geqslant 4$, every weight 1 and 2 vector is at least distance 2 from any non-zero codeword. Thus, $\Gamma_1(\mathbf{0}) \subseteq C_1$ and $\Gamma_2(\mathbf{0}) \subseteq C_2$ so that C is a linear-$(X, 2)$-neighbour-transitive code, completing the result. □

A lower bound for the minimum distance of the dual of a linear code generated by the blocks of certain designs is given in [2, Lemma 2.4.2]. This result is applied below, and will be used later to provide information about the minimum distance of some binary linear-$(X, 2)$-neighbour-transitive codes of interest.

Lemma 9.7.3. *Let C be binary linear code in $H(m, 2)$ with minimum distance δ satisfying $3 \leqslant \delta < m$, with $X \leqslant \mathrm{Aut}(C)$ such that $X_{\mathbf{0}}$ act 2-homogeneously on M, and let $C^\perp$ be the dual code of C with minimum distance $\delta^\perp$. Then $m - 1 \leqslant (\delta - 1)(\delta^\perp - 1)$. In particular, if $C \subseteq C^\perp$ then $\delta \geqslant \sqrt{m - 1} + 1$.*

Proof. First, as $3 \leqslant \delta < m$, neither C nor $C^\perp$ are either the repetition code, or its dual. As $X_{\mathbf{0}}$ acts transitively on the set of all 2-subsets of M, the set $\Gamma_\delta(\mathbf{0}) \cap C$ of all weight δ codewords of C forms a 2-(m, δ, λ) design $\mathcal{D}$ for some integer λ. Let $C_2(\mathcal{D})$ be the code spanned by the blocks of $\mathcal{D}$, considered as characteristic vectors. Now, $C_2(\mathcal{D})$ is fixed setwise by $X_{\mathbf{0}}$ and $C_2(\mathcal{D}) \neq \mathrm{Rep}(m, 2)$, since $\mathcal{D}$ contains at least 1 weight $\delta < m$ vertex. As $C_2(\mathcal{D})$ is contained in C, it follows that the minimum distance of $C_2(\mathcal{D})$ is also δ, and $C^\perp$ is contained in $(C_2(\mathcal{D}))^\perp$. Thus, $\delta^\perp$ is bounded below by the minimum distance of $(C_2(\mathcal{D}))^\perp$. Hence, by [2,

Lemma 2.4.2], $\delta^\perp \geqslant (r+\lambda)/\lambda$, where $r = (m-1)\lambda/(\delta-1)$. Thus, $\delta^\perp \geqslant (m-1)/(\delta-1)+1$, or $m-1 \leqslant (\delta-1)(\delta^\perp-1)$ as required. Suppose $C \subseteq C^\perp$. Then $\delta^\perp \leqslant \delta$ so that $m-1 \leqslant (\delta-1)^2$, that is, $\delta \geqslant \sqrt{m-1}+1$. □

Mortimer [82] investigated when proper submodules exist, other than those corresponding to the binary repetition code and its dual, inside permutation modules of 2-transitive groups. In the case of permutation modules over $\mathbb{F}_2$, a more thorough account is given in [64], where affine 2-arc transitive graphs are studied, including completion of most of the relevant cases left unanswered from [82]. Note that perfect linear codes over finite fields are classified (see [97]), and a code with minimum distance 100 and length 276 invariant under $X_{\mathbf{0}}^M \cong \mathrm{Co}_3$ is given in [53]. Also, the minimum distance δ of the codes corresponding to the line where $\mathrm{soc}(X_{\mathbf{0}}) = \mathrm{PSU}_3(r)$ with $r \equiv 1 \pmod 4$ in Table 9.7.1 has not been shown here to satisfy $\delta \geqslant 5$, though these codes are 2-neighbour-transitive with $\delta \geqslant 4$, by Lemma 9.7.2.

Theorem 9.7.4. *Let C' be a binary linear-$(X', 2)$-neighbour-transitive code in $H(m, 2)$ with minimum distance at least 5, and $C' \neq \mathrm{Rep}(m, 2)$. Then C' contains a binary linear-$(X, 2)$-neighbour-transitive code C, of dimension k with minimum distance δ, where $X_{\mathbf{0}} = X'_{\mathbf{0}}$ and $X = T_C \rtimes X_{\mathbf{0}}$, such that the values of $X_{\mathbf{0}}$, m, δ and k satisfy one of the lines of Table 9.7.1.*

Also, for $X_{\mathbf{0}}$, m and k as in each of the lines of Table 9.7.1, there exists a binary code C in $H(m, 2)$ of $\mathbb{F}_2$-dimension k, such that C is linear-$(X, 2)$-neighbour-transitive, where $X = T_C \rtimes X_{\mathbf{0}}$, for some δ satisfying the condition in that line of the table.

Proof. By Lemma 9.7.1, $X'_{\mathbf{0}}$ is 2-homogeneous on M and C' is a submodule of the vertex set $V \cong \mathbb{F}_2^m$ of $H(m, 2)$, regarded as the $\mathbb{F}_2$-permutation module for the action of $X'_{\mathbf{0}}$ on M. Every 2-homogeneous permutation module has (at least) two proper submodules, given by the repetition code Y and its dual $Y^\perp$, under the standard inner product. Since $Y^\perp$ has minimum distance 2, and $C' \neq Y$ by assumption, we require that the *heart*, defined to be $Y^\perp/(Y \cap Y^\perp)$, is reducible.

Lemma 9.7.2 implies that any submodule of V of dimension at least 1, other than V,Y and $Y^\perp$, gives a code C such that C is either perfect with $\delta = 3$, or C is linear-$(X, 2)$-neighbour-transitive with $\delta \geqslant 4$. As perfect linear codes over $\mathbb{F}_2$ have been classified (see [97], for instance), differentiating these cases is possible. In fact, if $\delta = 3$, $m \geqslant 5$ and C is perfect, then C is a Hamming code of length $2^t - 1$, where $t \geqslant 3$.

First, suppose $X_{\mathbf{0}}$ acts 2-transitively on M. The main result of [82] then implies that $X_{\mathbf{0}}$ and m are as in Table 9.7.1, so that we can restrict the discussion to those groups listed. Further details taken from [82] will be pointed out as they are used. The remaining information in Table 9.7.1 comes from explicit examples, with the help of [64], and Lemma 9.7.3 for some of the bounds on δ. A *preminimal* submodule of V is defined to be a submodule U containing Y such that U/Y is a minimal submodule of V/Y. Hence, we have that C' contains a module U that is either minimal or preminimal. If δ_U is the minimum distance of U, then $\delta \leqslant \delta_U$ and

$\mathrm{soc}(X_{\mathbf{0}})$	m	δ	k	conditions
$\mathbb{Z}_p^d$	$r = p^d$	$\geqslant \sqrt{r-1}+1$	$\frac{r-1}{2}$	$23 \leqslant r \equiv 7 \pmod 8$
				2-hom. not 2-trans.
$\mathbb{Z}_2^t$	2^t	2^{t-1}	$t+1$	$t \geqslant 4$, 2-trans.
$\mathrm{PSL}_t(2^k)$	$\frac{2^{kt}-1}{2^k-1}$	$\geqslant \frac{2^{k(t-1)}-1}{2^k-1}+1$	t^k	$t \geqslant 3$, $(k,t) \neq (1,3)$
A_7	15	8	4	-
$\mathrm{PSL}_2(r)$	$r+1$	$\geqslant \sqrt{r}+1$	$\frac{r+1}{2}$	$23 \leqslant r \equiv \pm 1 \pmod 8$
				not 3-trans.
$\mathrm{Sp}_{2t}(2)$	$2^{2t-1}-2^{t-1}$	$2^{2t-2}-2^{t-1}$	$2t+1$	$t \geqslant 3$
$\mathrm{Sp}_{2t}(2)$	$2^{2t-1}+2^{t-1}$	2^{2t-2}	$2t+1$	$t \geqslant 3$
$\mathrm{PSU}_3(r)$	r^3+1	$\geqslant r^2+1$	r^2-r+1	r is odd
$\mathrm{PSU}_3(r)$	r^3+1	$\geqslant 4$	r^3-r^2+r	$r \equiv 1 \pmod 4$
$\mathrm{Ree}(r)$	r^3+1	$\geqslant r^2+1$	r^2-r+1	$r \geqslant 3$
M_{22}	22	7	10	-
M_{23}	23	8	11	-
M_{24}	24	8	12	-
HS	176	$\geqslant 50$	21	-
Co_3	276	100	23	-

Table 9.7.1: Parameters for "minimal" binary linear-$(X,2)$-neighbour-transitive codes C (see Theorem 9.7.4) in $H(m,q)$ where k and is the dimension of C, $X = T_C \rtimes X_{\mathbf{0}}$, and the minimum distance δ of C satisfies $5 \leqslant \delta \leqslant m$. Note that when $\mathrm{soc}(X_{\mathbf{0}}) = \mathrm{PSU}_3(r)$, $k = r^3 - r^2 + r$ and $r \equiv 1 \pmod 4$ it is an open question as to precisely when $\delta \geqslant 5$, so it is possible $\delta = 4$ for certain r.

$\delta \geqslant 5$ implies $\delta_U \geqslant 5$. In the following, let $C = U$. In [64, Section 3] the faithful minimal and preminimal $X_{\mathbf{0}}$-submodules of the permutation module V for the 2-transitive group $X_{\mathbf{0}}$ are classified.

Let $X_{\mathbf{0}}$ be a 2-transitive subgroup of $\mathrm{AGL}_t(2)$ and $m = 2^t$, so that $t \geqslant 3$. By [64, Theorem 4.1], there is no minimal submodule and a unique preminimal submodule, spanned by the constant and linear functions, giving $\delta \leqslant 2^{t-1}$. Indeed this preminimal submodule is the Reed-Muller code $\mathcal{RM}_2(1,t)$, by [2, Theorem 5.3.3], with minimum distance 2^{t-1} and dimension $m+1$. Thus, $\delta \geqslant 5$ is satisfied when $t \geqslant 4$.

Let $\mathrm{soc}(X_{\mathbf{0}}) \cong \mathrm{PSL}_t(2^k)$ and $m = (2^{kt}-1)/(2^k-1)$, or $X_{\mathbf{0}} \cong \mathrm{A}_7 \leqslant \mathrm{PSL}_4(2)$ and $m = 15$. Note that $t \geqslant 3$, by [82]. By [64, Theorems 5.1 and 5.2], both a unique preminimal submodule, of dimension $m^k + 1$, and a unique minimal submodule, of dimension m^k, exist, and are generated by the characteristic functions of all hyperplanes, and the characteristic functions of all complements of hyperplanes, respectively. The subfield code $\mathcal{PRM}_{2/2^k}(2^k-1,t)$ has minimum distance $(2^{k(t-1)}-1)/(2^k-1)$, by [2, Proposition 5.7.1], and is generated by the characteristic functions of all hyperplanes, by [2, Theorem 5.7.9]. The code generated by the characteristic vectors of all complements of hyperplanes is the even weight subcode of $\mathcal{PRM}_{2/2^k}(2^k-1,t)$ which has minimum distance at least $(2^{k(t-1)}-1)/(2^k-1)+1$, by [2, Theorem 5.7.9]. If $(k,t) = (1,3)$ then the characteristic vector of the complement of a hyperplane has weight 4. Thus, $\delta \geqslant 5$ requires $(k,t) \neq (1,3)$.

Let $\mathrm{soc}(X_{\mathbf{0}}) \cong \mathrm{PSL}_2(r)$, where, by [82], $X_{\mathbf{0}}$ is not 3-transitive, $r \equiv \pm 1 \pmod 8$ and $m = r+1$. By [64, Lemma 5.4], there are no minimal submodules and exactly two preminimal submodules, both having dimension $(r+1)/2$ and producing codes with minimum distance at most $(r+1)/2$. Perfect codes must have odd length, by [97], which implies that $\delta \geqslant 4$, but to satisfy $\delta \geqslant 5$ requires $r \geqslant 9$. By [2, Theorem 2.10.1 and Corollary 2.10.2], the minimum distance of extended quadratic residue codes satisfy $(\delta-1)^2 \geqslant r$, so that, except for $r = 9$ (since 15 is not a prime power), we have that $\delta \geqslant 5$ holds. Suppose $r = 9$ and $\delta \geqslant 5$. Then, by [9, Table 1], $|C| \leqslant 12$. However, by [82, (F) Page 13], C has dimension at least 4, and thus $|C| \geqslant 2^4$, giving a contradiction. Thus $\delta \geqslant 5$ occurs only when $r \geqslant 23$.

Let $X_{\mathbf{0}} \cong \mathrm{Sp}_{2t}(2)$, $t \geqslant 2$ and $m = 2^{2t-1} - 2^{t-1}$ or $2^{2t-1} + 2^{t-1}$. By [64, Theorem 6.2], there are no minimal submodules, if $t = 2$ there are two preminimal submodules, each having dimension $2t+1$, and if $t \geqslant 3$ then there is a unique preminimal submodule, of dimension $2t+1$. From [64, Lemma 6.1] we have that δ is 2^{2t-2} and $2^{2t-2} - 2^{t-1}$ when $m = 2^{2t-1} - 2^{t-1}$ and $2^{2t-1} + 2^{t-1}$, respectively. Thus, $\delta \geqslant 5$ requires $t \geqslant 3$.

Let $\mathrm{soc}(X_{\mathbf{0}}) \cong \mathrm{PSU}_3(r)$ and $m = r^3 + 1$. Then, by [82], r is odd. Let D be the design submodule of the 2-$(r^3+1, r+1, 1)$ design invariant under $X_{\mathbf{0}}$. If $r \equiv 1 \pmod 4$ then, by [64, Theorem 7.2], there are no minimal submodules and two preminimal submodules, namely D and $D^\perp$, of dimensions $r^2 - r + 1$ and $r^3 - r^2 + r$, respectively. If $r \equiv 3 \pmod 4$ then, by [64, Theorem 7.3] and [58, Theorem 4.1], $D^\perp$ is the unique preminimal submodule of dimension $r^2 - r + 1$. By Lemma 9.7.3, $D^\perp$ has minimum distance at least $r^2 + 1$. Since m is even, and

hence D is not perfect, $\delta \geqslant 4$ is also satisfied for D, by Lemma 9.7.2.

Let $\mathrm{soc}(X_{\mathbf{0}}) \cong \mathrm{Ree}(r)$ and $m = r^3 + 1$. By [64, Theorem 7.4], a unique preminimal submodule exists, so that $C \subseteq C^{\perp}$. Thus, by Lemma 9.7.3, $\delta \geqslant r^{3/2} + 1$.

Let $X_{\mathbf{0}} \cong \mathrm{M}_m$, where $m = 22, 23$ or 24. For $m = 24$, the Golay code $\mathcal{G}_{24}$ has minimum distance 8. For $m = 23$ the Golay code $\mathcal{G}_{23}$ has minimum distance 7, and the even weight subcode of $\mathcal{G}_{23}$ has minimum distance 8. Puncturing each of these codes (see Proposition 4.2.9) results in two codes of length 22, which are invariant under M_{22}, with minimum distance 6 and 7, respectively. By the discussion in [64, Section 8] these are all the possibilities for C.

Let $X_{\mathbf{0}} = \mathrm{HS}$. Then [64, Section 8] states that there exists a unique preminimal submodule, which is a codimension 1 submodule of a 2-$(176, 50, 14)$ design. Hence C has minimum distance at least 50 and dimension 21. Let $X_{\mathbf{0}} \cong \mathrm{Co}_3$. Then [64, Section 8] states that there exists a unique preminimal submodule of dimension 23. A code C with length 276, dimension 23 and $\delta = 100$ is constructed in [53].

Suppose $X_{\mathbf{0}}$ is a 2-homogeneous, but not 2-transitive, subgroup of $\mathrm{A\Gamma L}_1(r)$ where $m = r$ is a prime power, so that $r \equiv 3 \pmod 4$. In the case that $r \equiv 7 \pmod 8$, then quadratic residue codes provide examples. By [25, Theorem 14.5], quadratic residue codes satisfy $\delta^2 - \delta + 1 \geqslant r$, so that $\delta \geqslant 5$ whenever $r \geqslant 23$. If $m = 7$, then the quadratic residue codes are the perfect Hamming code and its dual with minimum distances 3 and 4, and dimensions 4 and 3, respectively. Comparing dimensions tells us that these are all the possibilities for C here. The perfect Hamming code does not arise for larger r, since, for $t \geqslant 4$, $\mathrm{PSL}_t(2)$ does not have a subgroup that acts 2-homogeneously, but not 2-transitively, on $2^t - 1$ points. For $r \equiv 3 \pmod 8$, the argument in [82] for $\mathrm{PSL}_2(r) \leqslant G \leqslant \mathrm{P\Sigma L}_2(r)$ gives a contradiction. □

Theorem 9.1 may now be proved.

Proof of Theorem 9.1. Suppose C is an $(X, 2)$-neighbour-transitive code in $H(m, 2)$ with $\delta \geqslant 5$. It follows from Proposition 2.5.5 that $X_i^{Q_i} \cong \mathrm{S}_2$ and from Proposition 2.5.3 that X acts transitively on M. Thus, either $X \cap B$ is trivial, or C is X-alphabet-affine. If C is X-alphabet-affine then, Theorem 8.1 states that C is an $(X, 2)$-neighbour-transitive extension of an $\mathbb{F}_2 X_{\mathbf{0}}$-submodule W of the vertex set of $H(m, 2)$, viewed as the permutation module $\mathbb{F}_2^m$ for $X_{\mathbf{0}}$. If $X \cap B$ is trivial then C is as in Theorem 5.2, and if $W = \mathrm{Rep}(m, 2)$ then C is as in Theorem 7.2, which combined give the first and second cases of the result. If W is not the repetition code then the minimum distance of W is less than m, by Lemma 2.6.1. Thus, by Theorem 9.7.4, W, and hence C, contains a code with parameters as in Table 9.7.1, and the third part of the result holds.

Conversely, if C is a code in $H(m, 2)$ as in the first or second part of the result, then C is 2-neighbour-transitive by Theorem 5.2 or Theorem 7.2. Suppose C is a code in $H(m, 2)$ with $\delta \geqslant 5$, and there exists some $C' \subseteq C$ and $X \leqslant \mathrm{Aut}(C)$, with C', $X_{\mathbf{0}}$ and m as in Table 9.7.1, such that X acts transitively on C. Then C is 2-neighbour-transitive by Theorem 9.7.4, and the result follows. □

$\mathrm{soc}(X^M)$	m	q	conditions
$\mathbb{Z}_p^t$	p^t	$q-1 \mid 2(p^t-1)$ or $2t$	X^M is 2-homogeneous
$\mathrm{PSL}_2(r)$	$\frac{r^t-1}{r-1}$	$q=p^d$	$r=p^s$
		$q-1 \mid 2(r-1)$ or $2s$	$r=p^s$ is odd
$\mathrm{PSL}_t(r)$	$\frac{r^t-1}{r-1}$	$q=p^d$	$r=p^s$
		$3,5,7$	$t=3$, $r=4$
		3	$t=4$, $r=2$
		5	$t=4$, $r=3$
$\mathrm{Sp}_{2t}(2)$	$2^{2t-1} \pm 2^{d-1}$	3 or 5	
$\mathrm{Sz}(r)$	r^2+1	$q-1 \mid 2(r-1)$ or $2(2s+1)$	$r=2^{2s+1}$
$\mathrm{Ree}(r)$	r^3+1	$q-1 \mid 2(r-1)$ or $2(2s+1)$	$r=3^{2s+1}$
$\mathrm{PSU}_3(r)$	r^3+1	$q-1 \mid 2(r^2-1)$ or $4s$	$r=p^s$
$\mathrm{PSL}_2(11)$	11	3 or 5	
M_{11}	11	3	
M_{11}	12	3	
M_{12}	12	3	
M_{22}	22	3 or 5	
HS	176	3 or 5	
Co_3	276	3 or 5	

Table 9.8.1: Possible parameters of non-binary linear-$(X,2)$-neighbour-transitive codes.

9.8 Non-binary linear-2-neighbour-transitive codes

In this section a weaker analogue of Theorem 9.7.4, for $q \geqslant 3$, is given. In particular Proposition 9.8.1 and Table 9.8.1 give restrictions on the parameters of non-binary linear-2-neighbour-transitive codes with $\delta \geqslant 5$.

There are several entries in Table 9.8.1 for which it is not known if an $(X,2)$-neighbour-transitive code with listed $X_{\mathbf{0}}$, m and q exists. Examples have been given where $X_{\mathbf{0}}$ is $\mathrm{PSL}_t(q)$, $\mathrm{AGL}_t(q)$, $\mathrm{Sz}(q)$ and $\mathrm{PSU}_3(q)$ in Propositions 9.2.3, 9.3.3, 9.4.6 and 9.4.8, though a similar construction for the Ree groups failed to produce examples. Also, in those examples the characteristic of the field over which the modules are defined is the same as that of the defining characteristic of the group $X_{\mathbf{0}}^M$. The ternary Golay codes are examples of $(X,2)$-neighbour-transitive codes where $X_{\mathbf{0}}^M \cong \mathrm{M}_{11}$ or M_{12} (see [93]). The generalisations in [101] of *quadratic residue codes* may be examples in the cases of the symplectic groups $X_{\mathbf{0}}^M \leqslant \mathrm{Sp}_{2t}(2)$ and $\mathrm{PSL}_2(r)$, though this needs to be investigated more thoroughly.

Proposition 9.8.1. *Let $q \geqslant 3$ and C be a linear-$(X,2)$-neighbour-transitive code in $H(m,\mathbb{F}_2)$ with minimum distance $\delta \geqslant 5$. Then m, q and $\mathrm{soc}(X^M)$ satisfy one of the lines from Table 9.8.1.*

Proof. If $m \leqslant 8$ then, by Corollary 8.3.6, C is a projective Reed-Muller code. Let $m \geqslant 9$.

By Proposition 2.5.3, X^M is a 2-homogeneous group, as in Theorem 2.4.6. By Lemma 9.6.3, $X^M_{\mathbf{0},i,j}$ has a cyclic quotient of order $q-1$ or $(q-1)/2$. There are no 1-dimensional $\mathbb{F}_q X_{\mathbf{0}}$-submodules of $V\Gamma$, by Lemma 9.6.2. Thus, the composition factors of $V\Gamma$ all have dimension at least 2. Table 2.8.1 gives, in the cross characteristic case, bounds on the minimal dimension of such composition factors when $X^M_{\mathbf{0}}$ involves certain simple groups.

If $X^M_{\mathbf{0}}$ is an affine group, that is, a subgroup of $\mathrm{AGL}_t(p^s)$, then a cyclic quotient of $X^M_{\mathbf{0},i,j}$ has order dividing p^s-1 or s.

Suppose $X^M_{\mathbf{0}} \cong \mathrm{A}_m$ or S_m. Then $X^M_{\mathbf{0},i,j}$ has a cyclic quotient of size at most 2. Hence $q=3$ or 5. By Theorem 2.8.1, the dimension of a proper projective representation in characteristic not 2 is divisible by $k = 2^{\lfloor (m-s-1)/2 \rfloor}$, where s is the weight of the binary vector expressing m in base 2. Now, s is at most $\log_2(m)$, which implies that $k \geqslant \sqrt{m} \cdot 2^{\lfloor (m-1)/2 \rfloor}$. A contradiction, since $m \geqslant 9$.

Let $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{PSL}_2(r)$, where $r = p_0^s$ for some prime p_0 and integer s, and $m = r+1$. Then $X^M_{\mathbf{0},i,j} \leqslant \mathbb{Z}_{r-1} \rtimes \mathbb{Z}_s$, so that $q-1$ divides $2(r-1)$ or $2s$. Since r must be at least 8, the minimal dimension of a proper projective representation of $\mathrm{PSL}_2(r)$, in characteristic other than p_0, is $(r-1)/\gcd(2,r-1)$, as in Table 2.8.1. If r is even, then this cannot occur, since there are no dimension 1 representations in the composition series for $V\Gamma$. If r is odd, then the only possibility is that C has dimension $(r-1)/2$ and $C^\perp$ has dimension $(r+3)/2$.

Let $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{PSL}_t(r)$ and $m = (r^t-1)/(r-1)$, where $t \geqslant 3$, and $r = p_0^s$ for some prime p_0 and integer s. It follows that $X^M_{\mathbf{0},i,j} \leqslant \mathbb{Z}_{p_0}^{2s(t-2)} \rtimes ((\mathbb{Z}_{r-1}.\mathrm{GL}_{t-2}(r)) \rtimes \mathbb{Z}_s)$. The possible cyclic quotients of $X^M_{\mathbf{0},i,j}$ imply that $q-1$ divides $2(r-1)$ or $2s$. Suppose q and r are co-prime. If $t=3$ and $r=4$ then it follows that $q=3,5$ or 7. If $t=4$ then $r=2$ gives $q=3$ and $r=3$ gives $q=3$ or 5. Otherwise, the minimal dimension of a proper projective representation of $\mathrm{PSL}_t(r)$ is at least $(r^t-1)/(r-1)-t$, which gives a contradiction. Thus, in all other cases $q = p_0^d$ for some integer d.

Let $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{Sp}_{2t}(2)$ and $m = 2^{t-1}(2^t \pm 1)$, where $t \geqslant 2$. Then the only non-trivial cyclic quotient of $X^M_{\mathbf{0},i,j}$ is $\mathbb{Z}_2$. Thus $q=3$ or 5.

Let $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{Sz}(r)$, where $r = 2^{2n+1}$ for some integer n, and $m = r^2+1$. Then $X^M_{\mathbf{0},i,j} \leqslant \mathbb{Z}_{r-1} \rtimes \mathbb{Z}_{2n+1}$. Thus $q-1$ divides $2(r-1)$ or $2(2n+1)$.

Let $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{Ree}(r)$, where $r = 3^{2n+1}$ for some integer n, and $m = r^3+1$. Then $X^M_{\mathbf{0},i,j} \leqslant \mathbb{Z}_{r-1} \rtimes \mathbb{Z}_{2n+1}$. Thus $q-1$ divides $2(r-1)$ or $2(2n+1)$.

Let $\mathrm{soc}(X^M_{\mathbf{0}}) \cong \mathrm{PSU}(r)$, where r is a prime power, and $m = r^3+1$. Then $X^M_{\mathbf{0},i,j} \leqslant \mathbb{Z}_{r^2-1} \rtimes \mathbb{Z}_{4n+2}$. Thus $q-1$ divides $2(r^2-1)$ or $2(4n+2)$.

The cyclic quotients of $X_{\mathbf{0},i,j}$ when $X^M_{\mathbf{0}}$ is: $\mathrm{PSL}_2(11)$ and $m=11$, A_7 and $m=15$, M_{11} and $m=11$, M_{11} and $m=12$, M_{12} and $m=12$, M_{22} and $m=22$, M_{23} and $m=23$, M_{24} and $m=24$, HS and $m=176$, and Co_3 when $m=276$, have sizes dividing: 2, 2, 2, 1, 1, 2, 1, 1, 2, and 2, respectively. Thus, in each case q is: 3 or 5, 3 or 5, 3 or 5, 3, 3, 3 or 5, 3, 3, 3 or 5, and 3 or 5. By [28], the dimensions, less than $m=15$, of the irreducible representations of A_7 and 2.A_7 over $\mathbb{F}_3$ or $\mathbb{F}_5$ are $4, 6, 8, 10, 12$ and 13, which gives a contradiction, since there are no

dimension 1 representations in the composition series for $V\Gamma$. For the remaining groups [66] gives the minimal dimensions of the irreducible representations, which rule out the remaining cases not listed. □

Concluding Remarks and New Directions

The preceding chapters have provided some insights into the algebraic symmetries of error-correcting codes in Hamming graphs. Several areas of mathematics have made an appearance along the way, from design theory and finite geometry, to representation theory, hints of algebraic geometry, and, of course, group theory.

However, there is, as always, much work left to be done. First, the main concepts encountered throughout this thesis are discussed, and the open questions regarding each one. Then, the remaining sections consider the possible future directions of this work.

10.1 Towards a classification of 2-neighbour-transitive codes

Chapters 3 and 4 introduced s-elusive codes, a generalisation of a class of codes studied in [43] and [56]. The defining characteristic of an s-elusive code is that the automorphism group of the set of s-neighbours of the code, is larger than that of the code itself. The existence of an s-elusive code was shown to imply the existence of designs with certain parameters. Infinite families of s-elusive codes in $H(m,q)$ were produced, for $s=1$ with q arbitrary; and $(s,q)=(2,2)$. Moreover, a single example of a 3-elusive code was found in $H(22,2)$, by first observing that the Witt design W_{22} satisfied the required parameters. The design W_{22} can be extended, as in [81], to designs on a larger number of points, with parameters satisfying Lemma 4.2.6. This leads to the following questions.

Question 10.1.1. Do 2-elusive codes exist in $H(m,q)$ when $q \geqslant 3$? In particular, are any of the examples constructed in Chapter 9 2-elusive? Is there an infinite family of 3-elusive codes related the infinite families of Steiner 3-designs constructed in [81]?

From Chapter 5 onwards, the focus shifted to 2-neighbour-transitive codes. As it will be useful to compare similar types of results arising later, a summary of some results that have been useful in this thesis is given below. These results are Propositions 2.5.3 and 2.5.5, and Lemmas 8.1.2 and 8.1.3.

Theorem 10.1.2. *Let C be an $(X,2)$-neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 5$, $\mathbf{0} \in C$ and K be the kernel of the action of X on M. Then,*

1. *the quotient group $X_{\mathbf{0}}^{M} \cong X_{\mathbf{0}}/K_{\mathbf{0}}$ acts 2-homogeneously on M,*
2. *the subgroup $X_i \leqslant X$ stabilising the entry $i \in M$ acts 2-transitively on Q_i,*
3. *the subgroup $K_{\mathbf{0}} \leqslant K$ stabilising $\mathbf{0} \in C$ is diagonal and acts semi-regularly on $Q_i^{\times}$, and,*
4. *the subgroup $X_{\mathbf{0},i,j} \leqslant X$ stabilising the codeword $\mathbf{0}$ and the entries i and $j \in M$ acts transitively on $Q_i^{\times}$, and either transitively or with two equal-sized orbits on $Q_i^{\times} \times Q_j^{\times}$.*

Let C be an $(X, 2)$-neighbour-transitive code in $H(m, q)$ with minimum distance δ. Theorem 5.2 classified such C and X in the case that $\delta \geqslant 5$ and the kernel K of the action of X on the set of entries is trivial. Thus, K was assumed to be non-trivial in subsequent chapters. Part two of Theorem 10.1.2 is key in the subsequent investigation of K. Chapter 6 assumes $X_i^{Q_i}$ is an almost-simple group, and Theorem 6.1 showed that if C is X-alphabet-almost-simple and $(X, 2)$-neighbour-transitive then $\delta \leqslant 3$. The work in that chapter relied on the results of [45], which uses the structure of $\mathrm{soc}(K)$ to characterise X-alphabet-almost-simple and X-neighbour-transitive codes.

Moving to the case where $X_i^{Q_i}$ is an affine 2-transitive group, Chapter 7 classified $(X, 2)$-neighbour-transitive codes C having a module of particular small dimensions as a block of imprimitivity for the action of X on C. Chapter 8 then proves that for any X-alphabet-affine and $(X, 2)$-neighbour-transitive code C with minimum distance $\delta \geqslant 5$, the 2-transitive affine group $X_i^{Q_i}$ is soluble, and that C has a block of imprimitivity that is a submodule of the vertex set of $H(m, q)$, considered as an $X_{\mathbf{0}}$-module.

Chapter 9 then studies the blocks of imprimitivity shown to exist in Chapter 8, for the case that $X_i^{Q_i} \cong \mathrm{AGL}_1(q)$ and $K_{\mathbf{0}} \cong \mathbb{F}_q^\times$, where $K_{\mathbf{0}}$ is the kernel of the action of $X_{\mathbf{0}}$ on M; codes satisfying these conditions are called linear-$(X, 2)$-neighbour-transitive (see Definition 1.2.2). By considering linear-$(X, 2)$-neighbour-transitive codes in $H(m, 2)$, Theorem 9.1 characterises all binary $(X, 2)$-neighbour-transitive codes with minimum distance $\delta \geqslant 5$, via certain minimal submodules of the $\mathbb{F}_2$-permutation module for $X_{\mathbf{0}}$. Proposition 9.8.1 gives the possibilities for $X_{\mathbf{0}}$, m, and q, in the case that C is linear-$(X, 2)$-neighbour-transitive in $H(m, q)$ and $q \geqslant 3$. For many of the possible parameter sets in this case, examples are given.

Indeed, Chapter 9 gives a range of examples of linear-$(X, 2)$-neighbour-transitive codes, some infinite families of which appear to be new. These include the twisted Reed-Muller codes $\mathcal{TRM}_q(k, t)$, the Suzuki codes $\mathcal{SC}_q(k)$, and the unitary codes $\mathcal{UC}_q(k)$ (see Propositions 9.2.3, 9.3.3, 9.4.6 and 9.4.8). Note that a similar construction produced the Ree codes $\mathcal{RC}_q(k)$ (see Definition 9.4.2), though these were not shown to be 2-neighbour-transitive (see Remark 9.4.7).

This leads to a series of questions.

Question 10.1.3. Is it possible to give formulas for the dimension and minimum distance for each of the twisted Reed-Muller, Suzuki, Ree, and unitary codes, defined in Chapter 9, and their subfield codes?

Question 10.1.4. Is there a nicer description of the twisted Reed-Muller, Suzuki, Ree, and unitary codes, defined in Chapter 9, for instance, in terms of filtrations of a sub- or quotient algebra of the symmetric algebra? Can such a description lead to insights regarding the properties of these codes?

Theorem 9.7.4 finds all minimal binary linear-$(X, 2)$-neighbour-transitive codes with minimum distance $\delta \geqslant 5$, in the sense that any binary $(X, 2)$-neighbour-transitive code with $\delta \geqslant 5$

contains a subcode that is equivalent to one of these codes. Proposition 9.8.1 does not go so far as to find these in the case $q \geqslant 3$.

Question 10.1.5. Can all minimal linear-$(X, 2)$-neighbour-transitive codes in $H(m, q)$, with $q \geqslant 3$ and minimum distance $\delta \geqslant 5$, be found?

For some of the groups $X_{\mathbf{0}} = G$ involved in Theorem 9.7.4 giving rise to interesting linear-$(X, 2)$-neighbour-transitive codes, the entire submodule lattice of the permutation module of G is known (for instance $G = \mathrm{PSL}_t(2^k)$, see [4]), so that all binary linear-$(X, 2)$-neighbour-transitive codes with $X_{\mathbf{0}} = G$ and $\delta \geqslant 4$ are in fact known. This leads to the important, albeit ambitious, problem.

Question 10.1.6. Can the submodule lattice of the $\mathbb{F}_2$-permutation modules be determined for each of the 2-homogeneous groups in Theorem 9.7.4, and the parameters of the corresponding binary linear-$(X, 2)$-neighbour-transitive codes be calculated?

Theorem 7.2 classified the $(X, 2)$-neighbour-transitive extensions of 1-dimensional $X_{\mathbf{0}}$-submodules of the vertex set of the Hamming graph. In order to classify all 2-neighbour-transitive codes with $\delta \geqslant 5$ this would need to be done in general.

Question 10.1.7. Given a linear-$(X, 2)$-neighbour-transitive code C with $\delta \geqslant 5$, as in Theorem 9.7.4, can all $(X, 2)$-neighbour-transitive extensions of C be classified? If C is one of the codes $\mathcal{PRM}_q(k, t)$, $\mathcal{TRM}_q(k, t)$, $\mathcal{SC}_q(k)$ or $\mathcal{UC}_q(k)$ (see Chapter 9), can all $(X, 2)$-neighbour-transitive extensions of C be classified?

Moving away from linear-$(X, 2)$-neighbour-transitive codes, or their extensions, the next step is to consider the other possibilities for the transitive linear group $X_{\mathbf{0},i}^{Q_i^\times}$. In this case, Lemma 8.1.4 may greatly restrict the possible cases.

Question 10.1.8. Are there examples of $(X, 2)$-neighbour-transitive codes in $H(m, q)$, with minimum distance $\delta \geqslant 5$, where either $\mathrm{SL}_2(3) \trianglelefteq X_{\mathbf{0},i}^{Q_i}$ and $q = 3^4, 5^2, 7^2, 11^2, 23^2$, or $2_-^{1+4} \trianglelefteq X_{\mathbf{0},i}^{Q_i}$ and $q = 3^4$? Can such codes be characterised, or possibly even classified?

10.2 A discussion of algebraic symmetry and coding theory

Algebraic symmetries of graphs have been studied in some depth over the past 50 years or so (see, for instance, [26, 37, 50]). Often the group of interest acts transitively on the vertex set of the graph. Studying symmetries of codes can be viewed, in some sense, as studying the orbits of groups acting on graphs where the action on the vertex set is intransitive, which has received much less attention. Codes in the Hamming graphs have, of course, been studied a fair amount. However, this is often done without considering the full automorphism group of the Hamming graphs, making the above comparison less applicable. In some respects, this thesis also has somewhat of a narrow viewpoint, mainly concerning 2-neighbour-transitive codes in Hamming graphs. Indeed, the only families so far discussed, of codes defined via algebraic

symmetry, are s-neighbour-transitive codes and s-elusive codes, the latter in fact involving a group that does *not* fix the code. This section briefly considers some of the other possibilities.

As an immediate generalisation of the codes studied here, the definition of an s-neighbour-transitive code can be applied to codes in any graph Σ by simply replacing $H(m, q)$ with Σ in Definition 1.1.2. Indeed, neighbour-transitive codes have been studied in the Johnson graphs, with a classification all but complete, see [77, 84, 63]. Codes in Grassman graphs have been of recent interest due to applications in network coding [6].

Question 10.2.1. What can be said about (X, s)-neighbour-transitive codes in Grassman graphs?

Each of the Hamming, Johnson and Grassman graphs can be regarded as an association scheme[1], a structure which consists of an underlying set and a family of relations on the set that satisfies certain conditions. Of interest simply as a remark here, the definition of s-neighbour-transitive given above may also be modified to apply to codes defined via association schemes, by replacing the distance partition, obtained via the graph metric, with something similar obtained via the family of relations of the association scheme.

Whilst the benefit of a definition that applies so generally is obvious, considering the desired/inherent structure of a specific family of mathematical objects can also give rise to interesting symmetry conditions. The Hamming graph $\Gamma = H(m, q)$ is the Cartesian product of m disjoint copies of a complete graph K_q on q vertices. Moreover, as abstract groups, $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(mK_q)$, where mK_q is the union of these m disjoint copies of K_q. Section 10.3 briefly discusses codes related to a rank-3 group (defined in that section), via the action of $X \leqslant \mathrm{Aut}(\Gamma)$ on mK_q, relating these properties back to potentially desirable properties of codes. Below are some alternate symmetry conditions for codes in Hamming graphs, one of which is defined in terms of the action of $X \leqslant \mathrm{Aut}(C)$ on mK_q. These conditions are only momentarily discussed here.

Definition 10.2.2. Let C be a code in $H(m, q)$ containing a distinguished vertex $\mathbf{0}$, with $X \leqslant \mathrm{Aut}(C)$ such that X acts transitively on C, and $\Sigma \cong mK_q$ be the graph given by the union, over $i \in M$, of the set of the m disjoint complete graphs, each with vertex set the disjoint copy Q_i of the alphabet of $H(m, q)$. Then C is defined to be

1. (X, s)-*distance-transitive* if $X_{\mathbf{0}}$ acts transitively on the set $\Gamma_s(\mathbf{0})$ of vertices that are distance s from $\mathbf{0}$,

2. (X, s)-*homogeneous* if every isomorphism between induced subgraphs of Σ on at most s vertices lifts to an automorphism in X, and,

3. (X, s)-*locally-homogeneous* if every isomorphism between induced subgraphs on at most s vertices of the induced subgraph $[\Gamma_1(\mathbf{0})] \cong mK_{q-1}$ lifts to an automorphism in $X_{\mathbf{0}}$.

[1] See [32].

Though it will not be shown here, Propositions 2.5.3 and 2.5.5 can be used to show that a code C in $H(m,q)$ with minimum distance $\delta \geqslant 2s+1$ is (X,s)-distance-transitive if and only if it is (X,s)-neighbour-transitive. Thus, (X,s)-distance-transitive codes are only of separate interest when $\delta \leqslant 2s$; it is noted that the conclusions of Propositions 2.5.3 and 2.5.5 hold for (X,s)-distance-transitive codes regardless of δ, that is, $X_{\mathbf{0}}$ acts s-homogeneously on M and $X_i^{Q_i}$ acts 2-transitively on Q_i. The same two results can also be used to prove that a code C in $H(m,q)$ with $\delta \geqslant 3$ is X-neighbour-transitive if and only if it is $(X,1)$-locally-homogeneous. However, in general, the property (X,s)-locally-homogeneous is stricter than (X,s)-distance-transitivity, which is generally stronger again than (X,s)-neighbour-transitivity. In view of this, it is expected that achieving a classification of $(X,2)$-locally-homogeneous codes in Hamming graphs would be significantly easier than a similar result for $(X,2)$-neighbour-transitive codes.

Question 10.2.3. Is a classification of $(X,2)$-locally-homogeneous codes in Hamming graphs possible? Does Definition 10.2.2 give rise to interesting classes of codes in either the Johnson or Grassman graphs?

10.3 Rank-3 actions and codes

A group G acting on a set Ω has *rank*-3 if G acts transitively on Ω, and given some $\alpha \in \Omega$ the stabiliser G_α has three orbits on Ω, including the orbit $\{\alpha\}$. If C is a 2-neighbour-transitive code in $H(m,q)$, with $\delta \geqslant 5$, and we consider the action of X on the disjoint union $\bigcup_{i\in M} Q_i$, instead of the vertices of $H(m,q)$, then the next result shows that this action is an imprimitive rank-3 action, provided there is a 2-transitive action on entries and C is not the repetition code. Note that X almost always has a 2-transitive action on M, as this action is 2-homogeneous, by the first part of Theorem 10.1.2, and almost all 2-homogeneous groups are 2-transitive, by Theorem 2.4.6.

Lemma 10.3.1. *Let C be an $(X,2)$-neighbour-transitive code in $H(m,q)$ with minimum distance $\delta \geqslant 5$, and $C \neq \mathrm{Rep}(m,2)$ if $q=2$, such that X acts 2-transitively on M. Then the action of X on $\Omega = \bigcup_{i\in M} Q_i$ has rank-3.*

Proof. Let $i \in M$ and $a = 0 \in Q_i$. Then we must show that the stabiliser $X_{i,a}$ has three orbits on Ω. By the second part of Theorem 10.1.2, we have that $X_i^{Q_i}$ acts 2-transitively on Q_i. Thus $X_{i,a}$ has two orbits on Q_i. It remains to show that $X_{i,a}$ acts transitively on $\bigcup_{j\in M\setminus\{i\}} Q_j$. Since Definition 1.2.1 partitions the family of $(X,2)$-neighbour-transitive codes with $\delta \geqslant 5$ as either X-entry-faithful, X-alphabet-almost-simple or X-alphabet-affine, it follows from Theorem 6.1 that either $K=1$, or C is X-alphabet-affine.

If $K=1$ then, by Theorem5.2, C is the even weight subcode of the punctured Hadamard code of length 12 with $\delta = 6$, $X_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$ and $X \cong \mathrm{M}_{11}$. Since the weight 6 codewords of C form a $2\text{-}(11,6,3)$ design (see Definition 5.2.1), there exists, for all $j \in M \setminus \{i\}$ and $a \in Q_j$, a weight 6 codeword α such that $\alpha_i = 0$ and $\alpha_j = a$, by [2, Proposition 1.2.1]. As X acts transitively on C, there exists an $x = h\sigma \in X$, with $h \in B$ and $\sigma \in L$, such that

$\alpha^x = \mathbf{0}$. As $X_{\mathbf{0}} \cong \mathrm{PSL}_2(11)$ acts 2-transitively on M, there exists, for all $k \in M \setminus \{i\}$, a $y = (1, \ldots, 1)\sigma' \in X$, with $\sigma' \in L$, such that $i^{\sigma\sigma'} = 1$, $j^{\sigma\sigma'} = k$ and $\alpha^{xy} = \mathbf{0}$. Thus, $X_{i,a}$ acts transitively on $\bigcup_{j \in M\setminus\{i\}} Q_j$.

If C is X-alphabet-affine, then the first part of Theorem 8.1 allows Lemma 8.2.4 to be applied, from which it follows that $X_{i,a}$ acts transitively on $\bigcup_{j \in M\setminus\{i\}} Q_j$, since X acts 2-transitively on M. □

The study of finite rank-3 permutation groups was initiated, from a modern combinatorial point of view, by Higman in [57]. Primitive rank-3 actions are classified in [75]. The imprimitive case is studied in [35], where [35, Lemma 2.1] shows that both of the following actions are 2-transitive: the action of G on the set of blocks $\mathcal{B}$, and, for a block $B \in \mathcal{B}$, the action of the stabiliser G_B on B.

Suppose that X is a finite group acting faithfully and transitively on a set Ω with a system of imprimitivity $\{Q_i \mid i \in M\}$, where M is a set of size at least 2, so that $\Omega = \bigcup_{i \in M} Q_i$. Then X can also be considered to act on the Hamming graph $H(m, q)$ with vertex set $\prod_{i \in M} Q_i$. The orbits of X on the set of vertices of $H(m, q)$ can be regarded as a set $\mathcal{C}$ of codes in $H(m, q)$ such that $X \leqslant \mathrm{Aut}(C)$ and X acts transitively on C, for all $C \in \mathcal{C}$. In this way, a system of imprimitivity for a group X acting imprimitively on a set Ω gives rise to a set of codes in an associated Hamming graph, with X acting transitively on each code, and each code having some minimum distance. Higman proved [57, Corollaries, page 147] that an imprimitive rank-3 group has a unique system of imprimitivity. Thus, if the action of X on Ω is rank-3, then the set $\mathcal{C}$ of codes given by that action is unique.

Let Q and M be finite sets of size at least 2. For each $i \in M$, let Q_i be a disjoint copy of Q. Let $H(m, q)$ be the Hamming graph with vertex set $\prod_{i \in M} Q_i$ and let $\Omega = \bigcup_{i \in M} Q_i$. Then [35, Lemma 2.1] can be expressed as the following proposition.

Proposition 10.3.2. *Let C be a code in $H(m, q)$ and $X \leqslant \mathrm{Aut}(C)$ such that X acts transitively on C and has a rank-3 action on Ω. Then X acts 2-transitively on M, and X_i acts 2-transitively on Q_i, for all $i \in M$.*

Define a code C in $H(m, q)$ to be *rank-3* if the action of $X \leqslant \mathrm{Aut}(C)$ on $\Omega = \bigcup_{i \in M} Q_i$ is rank-3 and X is transitive on C. Although this may not immediately seem like a natural condition to put on a code, Lemma 10.3.1 shows that 2-neighbour-transitive codes often have this property. Also, in error-correcting coding theory it is often an assumption that interference affects equally any symbol in any position. A group theoretic formulation of this could be to ask that X acts transitively on Ω. Rank-3 may then be seen as asking that interference affect any pair of symbols in a given position independently, and any pair of symbols in a distinct pair of positions independently.

Another reason to consider such codes comes from permutation group theory. In the case that the action on the alphabet is almost simple, all rank-3 actions are effectively already clas-

sified, by [35, Theorem 1.1]. Studying rank-3 codes with an affine action on the alphabet may give a way to approach something close to a classification of imprimitive rank-3 groups.

Many of the results in Theorem 10.1.2, concerning 2-neighbour-transitive codes, do not carry over to rank-3 codes. Thus, it may be worth first considering an intermediate case. The results that hold for codes with minimum distance $\delta \geqslant 3$ that are rank-3 and neighbour-transitive are given below. Proposition 10.3.2 and Proposition 2.5.5 provide some of the these results, while the last is stated without proof, though it is similar to the relevant part of the proof of Lemma 8.1.1.

Theorem 10.3.3. *Let C be a rank-3 and neighbour-transitive code in $H(m,q)$ with $\delta \geqslant 3$, $G = \mathrm{Aut}(C)$, $\mathbf{0} \in C$ and K be the subgroup of G acting trivially on M. Then,*

1. *the group $X^M \cong X_{\mathbf{0}}/K$ acts 2-transitively on M,*
2. *the subgroup $X_i \leqslant X$ stabilising the entry $i \in M$ acts 2-transitively on Q_i,*
3. *the group $X_{\mathbf{0}}^M \cong X_{\mathbf{0}}/K_{\mathbf{0}}$ is a transitive subgroup of a 2-transitive group,*
4. *the subgroup $X_{\mathbf{0},i} \leqslant X$ stabilising the entry $i \in M$ acts transitively on $Q_i^\times$, and,*
5. *the subgroup $K_{\mathbf{0}} \leqslant K$ stabilising $\mathbf{0} \in C$ is diagonal.*

Hence, considering codes which are rank-3 and neighbour-transitive allows the retention of many of the important tools from the analysis of 2-neighbour-transitive codes. If we look at the blocks of imprimitivity for the action of G on the code, we no longer have that this is fixed by a 2-homogeneous group acting on the entries, though we do have that it is fixed by a transitive subgroup of a 2-transitive group. This leads to the final question.

Question 10.3.4. What characterisation or classification results can be made for rank-3 and neighbour-transitive codes with $\delta \geqslant 3$?

Bibliography

[1] K. S. Andrews, D. Divsalar, S. Dolinar, J. Hamkins, C. R. Jones, and F. Pollara, 'The development of turbo and ldpc codes for deep-space applications', *Proceedings of the IEEE* **95** (2007), no. 11, 2142–2156.

[2] E. F. Assmus and J. D. Key, *Designs and their codes*, in *Cambridge Tracts in Mathematics* **103** (Cambridge University Press, 1994).

[3] B. Bagchi and S. Inamdar, 'Projective geometric codes', *Journal of Combinatorial Theory, Series A* **99** (2002), no. 1, 128–142.

[4] M. Bardoe and P. Sin, 'The permutation modules for $GL(n+1,q)$ acting on $\mathbb{P}_n(q)$ and $\mathbb{F}_q^{n+1}$', *Journal of the London Mathematical Society* **61** (2000), no. 1, 58–80.

[5] S. G. Barwick, C. M. O'Keefe, and L. Storme, 'Unitals which meet Baer subplanes in 1 modulo q points', *Journal of Geometry* **68** (2000), no. 1, 16–22.

[6] R. Bassoli, H. Marques, J. Rodriguez, K. W. Shum, and R. Tafazolli, 'Network coding theory: A survey', *IEEE Communications Surveys Tutorials* **15** (2013), no. 4, 1950–1978.

[7] T. Berger and P. Charpin, 'The automorphism group of generalized Reed-Muller codes', *Discrete mathematics* **117** (1993), no. 1, 1–17.

[8] T. P. Berger, 'Automorphism groups of homogeneous and projective Reed-Muller codes', *IEEE Trans. Inf. Theor.* **48** (2006), no. 5, 1035–1045.

[9] 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* (1978), 81–93.

[10] N. Biggs, 'Perfect codes in graphs', *Journal of Combinatorial Theory, Series B* **15** (1973), no. 3, 289 – 296.

[11] I. F. Blake, G. Cohen, and M. Deza, 'Coding with permutations', *Inf. Control* **43** (1979), 1–19.

[12] A. Bochert, 'Ueber die zahl der verschiedenen werthe, die eine function gegebener buchstaben durch vertauschung derselben erlangen kann', *Mathematische Annalen* **33** (1889), no. 4, 584–590.

[13] J. Borges and J. Rifà, 'On the nonexistence of completely transitive codes', *Information Theory, IEEE Transactions on* **46** (2000), no. 1, 279–280.

[14] J. Borges, J. Rifà, and V. Zinoviev, 'Nonexistence of completely transitive codes with error-correcting capability $e > 3$', *Information Theory, IEEE Transactions on* **47** (2001), no. 4, 1619–1621.

[15] ———, 'On linear completely regular codes with covering radius $\rho = 1$. construction and classification', *arXiv preprint arXiv:0906.0550* (2009).

[16] ———, 'On q-ary linear completely regular codes with $\rho = 2$ and antipodal dual', *Advances in Mathematics of Communications (AMC)* **4** (2010), no. 4, 567–578.

[17] ———, 'New families of completely regular codes and their corresponding distance regular coset graphs', *Designs, Codes and Cryptography* (2012), 1–10.

[18] ———, 'Families of completely transitive codes and distance transitive graphs', *Discrete Mathematics* **324** (2014), 68–71.

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

[20] W. Burnside, *Theory of groups of finite order* (University, 1911).

[21] A. Calderbank and D. B. Wales, 'A global code invariant under the higman-sims group', *Journal of Algebra* **75** (1982), no. 1, 233 – 260.

[22] R. Calderbank, 'On uniformly packed [n, n–k, 4] codes over GF(q) and a class of caps in PG(k–1, q)', *Journal of the London Mathematical Society* **2** (1982), no. 2, 365–384.

[23] R. Calderbank and W. M. Kantor, 'The geometry of two-weight codes', *Bulletin of the London Mathematical Society* **18** (1986), no. 2, 97–122.

[24] P. J. Cameron, *Permutation groups*, in *London Mathematical Society Student Texts* (Cambridge University Press, 1999).

[25] P. J. Cameron and J. H. van Lint, *Designs, graphs, codes and their links*, in *London Mathematical Society Student Texts* (Cambridge University Press, 1991).

[26] P. J. Cameron et al., 'Automorphisms of graphs', *Topics in algebraic graph theory* **102** (2004), 137–155.

[27] C. Colbourn, *CRC handbook of combinatorial designs*, in *Discrete Mathematics and Its Applications* (Taylor & Francis, 1996).

[28] J. Conway, *Atlas of finite groups: Maximal subgroups and ordinary characters for simple groups* (Clarendon Press, 1985).

[29] J. Conway and N. Sloane, 'Soft decoding techniques for codes and lattices, including the golay code and the leech lattice', *IEEE Transactions on Information Theory* **32** (1986), no. 1, 41–50.

[30] D. Cvetkovic, P. Rowlinson, and S. Simic, *Eigenspaces of graphs*, in *Encyclopedia of Mathematics and its Applications* (Cambridge University Press, 2008).

[31] P. Delsarte, 'On cyclic codes that are invariant under the general linear group', *Information Theory, IEEE Transactions on* **16** (1970), no. 6, 760–769.

[32] ———, *An algebraic approach to the association schemes of coding theory*, in *Philips research reports: Supplements* (N. V. Philips' Gloeilampenfabrieken, 1973).

[33] P. Delsarte, J.-M. Goethals, and F. J. Mac Williams, 'On generalized Reed Ì Ţ-Muller codes and their relatives', *Information and control* **16** (1970), no. 5, 403–442.

[34] P. Delsarte and V. I. Levenshtein, 'Association schemes and coding theory', *IEEE Transactions on Information Theory* **44** (1998), no. 6, 2477–2504.

[35] A. Devillers, M. Giudici, C. H. Li, G. Pearce, and C. E. Praeger, 'On imprimitive rank 3 permutation groups', *Journal of the London Mathematical Society* **84** (2011), no. 3, 649–669.

[36] J. D. Dixon and B. Mortimer, *Permutation groups*, **163** (New York: Springer, 1996).

[37] A. Gardiner, 'Symmetry conditions in graphs', *Surveys in Combinatorics* (1979), 22–43.

[38] N. Gill, N. I. Gillespie, and J. Semeraro, 'Conway groupoids and completely transitive codes', *Combinatorica* (2017), 1–44.

[39] N. I. Gillespie, *Neighbour transitivity on codes in Hamming graphs* (Ph.D. thesis, The University of Western Australia, Perth, Australia, 2011).

[40] N. I. Gillespie, M. Giudici, D. R. Hawtin, and C. E. Praeger, 'Entry-faithful 2-neighbour transitive codes', *Designs, Codes and Cryptography* (2015), 1–16.

[41] N. I. Gillespie and D. R. Hawtin, 'Alphabet-almost-simple 2-neighbour-transitive codes', *Ars Mathematica Contemporanea (to appear)* (2017).

[42] N. I. Gillespie, D. R. Hawtin, and C. E. Praeger, 'The structure of elusive codes in Hamming graphs', *arXiv preprint arXiv:1404.0950* (2014).

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

[44] ———, 'Uniqueness of certain completely regular Hadamard codes', *Journal of Combinatorial Theory, Series A* **120** (2013), no. 7, 1394 – 1400.

[45] ———, 'Characterisation of a family of neighbour transitive codes', *arXiv preprint arXiv:1405.5427* (2014).

[46] ———, 'Diagonally neighbour transitive codes and frequency permutation arrays', *Journal of Algebraic Combinatorics* **39** (2014), no. 3, 733–747.

[47] ———, 'New characterisations of the Nordstrom-Robinson codes', *Bulletin of the London Mathematical Society* **49** (2017), no. 2, 320–330.

[48] M. Giudici, *Completely transitive codes in Hamming graphs* (Master's thesis, The University of Western Australia, Perth, Australia, 1998).

[49] M. Giudici and C. E. Praeger, 'Completely transitive codes in Hamming graphs', *European Journal of Combinatorics* **20** (1999), no. 7, 647 – 662.

[50] C. Godsil and G. F. Royle, *Algebraic graph theory*, **207** (Springer Science & Business Media, 2013).

[51] J. M. Goethals and S. L. Snover, 'Nearly perfect binary codes', *Discrete Mathematics* **3** (1972), no. 1, 65 – 88.

[52] V. D. Goppa, 'Algebraico-geometric codes', *Izvestiya: Mathematics* **21** (1983), no. 1, 75–91.

[53] W. H. Haemers, C. Parker, V. Pless, and V. D. Tonchev, 'A design and a code invariant under the simple group Co_3', *J. Comb. Theory, Ser. A* **62** (1993), 225–233.

[54] J. Hall, Marshall, 'Note on the Mathieu group M_12', *Archiv der Mathematik* **13** (1962), no. 1, 334–340.

[55] D. R. Hawtin, 'Elusive preparata codes', *Pre-print* (July, 2017).

[56] D. R. Hawtin, N. I. Gillespie, and C. E. Praeger, 'Elusive codes in Hamming graphs', *Bulletin of the Australian Mathematical Society* **88** (2013), 286–296.

[57] D. G. Higman, 'Finite permutation groups of rank 3', *Mathematische Zeitschrift* **86** (1964), no. 2, 145–156.

[58] G. Hiss, 'Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups', *Indagationes Mathematicae* **15** (2004), no. 2, 223 – 243.

[59] H. Hoeve, J. Timmermans, and L. Vries, 'Error correction and concealment in the compact disc system', *Origins and Successors of the Compact Disc* (1982), 82.

[60] Y. Hong, 'On the nonexistence of unknown perfect 6- and 8-codes in Hamming schemes $H(n, q)$ with q arbitrary', *Osaka J. Math.* **21** (1984), no. 3, 687–700.

[61] S. Huczynska and G. L. Mullen, 'Frequency permutation arrays', *Journal of Combinatorial Designs* **14** (2006), no. 6, 463–478.

[62] K. A. S. Immink, *Codes for mass data storage systems* (Shannon Foundation Publisher, 2004).

[63] M. Ioppolo, *Neighbour-transitive codes and configurations in Johnson and q-Johnson schemes* (Ph.D. thesis, The University of Western Australia, Perth, Australia, 2017).

[64] A. Ivanov and C. E. Praeger, 'On finite affine 2-arc transitive graphs', *Eur. J. Comb.* **14** (1993), no. 5, 421–444.

[65] G. James and M. W. Liebeck, *Representations and characters of groups*, in *Cambridge mathematical textbooks* (Cambridge University Press, 2001).

[66] C. Jansen, 'The minimal degrees of faithful representations of the sporadic simple groups and their covering groups', *LMS Journal of Computation and Mathematics* **8** (2005), 122–144.

[67] W. M. Kantor, 'Automorphism groups of designs', *Mathematische Zeitschrift* **109** (1969), no. 3, 246–252.

[68] ———, 'k-Homogeneous groups', *Mathematische Zeitschrift* **124** (1972), no. 4, 261–265.

[69] T. Kasami, S. Lin, and W. Peterson, 'New generalizations of the Reed-Muller codes–i: Primitive codes', *Information Theory, IEEE Transactions on* **14** (1968), no. 2, 189–199.

[70] ———, 'Polynomial codes', *IEEE Transactions on Information Theory* **14** (1968), no. 6, 807–814.

[71] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. Urbanke, 'Reed-Muller codes achieve capacity on erasure channels', in *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, *STOC '16* (ACM, 2016), 658–669.

[72] G. Lachaud, 'Projective Reed-Muller codes', in *International Colloquium on Coding Theory and Applications* (Springer, 1986), 125–129.

[73] ———, 'The parameters of projective Reed-Müller codes', *Discrete Mathematics* **81** (1990), no. 2, 217–221.

[74] C. H. Li, T. K. Lim, and C. E. Praeger, 'Homogeneous factorisations of complete graphs with edge-transitive factors', *Journal of Algebraic Combinatorics* **29** (2009), no. 1, 107–132.

[75] M. W. Liebeck, 'The affine permutation groups of rank three', *Proceedings of the London Mathematical Society* **3** (1987), no. 3, 477–516.

[76] M. W. Liebeck, C. E. Praeger, and J. Saxl, 'A classification of the maximal subgroups of the finite alternating and symmetric groups', *Journal of Algebra* **111** (1987), no. 2, 365 – 383.

[77] R. A. Liebler and C. E. Praeger, 'Neighbour-transitive codes in Johnson graphs', *Designs, codes and cryptography* **73** (2014), no. 1, 1–25.

[78] K. Lindström, 'All nearly perfect codes are known', *Information and Control* **35** (1977), no. 1, 40 – 47.

[79] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, in *North-Holland Mathematical Library* (North-Holland, 1978).

[80] R. J. McEliece, 'The reliability of computer memories', *Scientific American* **252** (1985), no. 1, 88–95.

[81] H. Mohácsy and D. K. Ray-Chaudhuri, 'A construction for infinite families of steiner 3-designs', *Journal of Combinatorial Theory, Series A* **94** (2001), no. 1, 127–141.

[82] B. Mortimer, 'The modular permutation representations of the known doubly transitive groups', *Proceedings of the London Mathematical Society* **3** (1980), no. 1, 1–20.

[83] A. Neumaier, 'Completely regular codes', *Discrete Mathematics* **106-107** (1992), no. 0, 353 – 360.

[84] M. Neunhöffer and C. E. Praeger, 'Sporadic neighbour-transitive codes in Johnson graphs', *Designs, codes and cryptography* **72** (2014), no. 1, 141–152.

[85] C. Perkins, *Rtp: Audio and video for the internet* (Addison-Wesley Professional, 2003).

[86] C. E. Praeger, 'The inclusion problem for finite primitive permutation groups', *Proceedings of the London Mathematical Society* **3** (1990), no. 1, 68–88.

[87] L. L. Scott, 'Representations in characteristic p', in *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, **37** (1980), 319–331.

[88] G. M. Seitz and A. E. Zalesskii, 'On the minimal degrees of projective representations of the finite Chevalley groups, II', *Journal of Algebra* **158** (1993), no. 1, 233–243.

[89] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev, 'Uniformly packed codes', *Problems Inform. Transmission* **7** (1971), 30–39.

[90] C. E. Shannon, 'A mathematical theory of communication', *Bell System Tech. J.* **27** (1948), 379–423,623–656.

[91] P. Sin, 'On codes that are invariant under the affine group', *The Electronic Journal of Combinatorics* **19** (2012), no. 4, P20.

[92] P. Solé, 'Completely regular codes and completely transitive codes', **RR-0727** (1987).

[93] _____, 'Completely regular codes and completely transitive codes', *Discrete Mathematics* **81** (1990), no. 2, 193–201.

[94] A. B. Sorensen, 'Projective Reed-Muller codes', *IEEE Transactions on Information Theory* **37** (1991), no. 6, 1567–1576.

[95] D. Stinson, *Combinatorial designs: Construction and analysis* (Springer, 2004).

[96] I. Tamo, D. S. Papailiopoulos, and A. G. Dimakis, 'Optimal locally repairable codes and connections to matroid theory', *IEEE Transactions on Information Theory* **62** (2016), no. 12, 6661–6671.

[97] A. Tietäväinen, 'On the nonexistence of perfect codes over finite fields', *SIAM Journal on Applied Mathematics* **24** (1973), no. 1, 88–96.

[98] J. Todd, 'A combinatorial problem', *J. Math. Phys.* **12** (1933), 321–333.

[99] H. van Tilborg, *Uniformly packed codes* (Technische Hogeschool, 1976).

[100] A. Wagner, 'An observation on the degrees of projective representations of the symmetric and alternating group over an arbitrary field', *Archiv der Mathematik* **29** (1977), no. 1, 583–589.

[101] H. N. Ward, 'Quadratic residue codes and symplectic groups', *Journal of Algebra* **29** (1974), no. 1, 150 – 171.

[102] E. Weiss, 'Generalized Reed-Muller codes', *Information and Control* **5** (1962), no. 3, 213–222.

[103] R. Wilson, *The finite simple groups*, **251** (Springer Science & Business Media, 2009).

[104] A. Zinoviev and V. K. Leontiev, 'The nonexistence of perfect codes over Galois fields', in *Problems of Control and Information 2* (1973), 123–132.