Codes in Johnson graphs associated with quadratic forms over $\mathbb{F}_2$

Mark Ioppolo

Supervised by John Bamberg, Alice Devillers and Cheryl Praeger

This thesis presented for the degree
of Doctor of Philosophy of the
University of Western Australia

Centre for the Mathematics of Symmetry and Computation
Department of Mathematics and Statistics
University of Western Australia

October 2019

Declaration

I, Mark Ioppolo, certify that:

- This thesis has been substantially accomplished during enrolment in this degree.
- This thesis does not contain material which has been submitted for the award of any other degree or diploma in my name, in any university or other tertiary institution.
- In the future, no part of this thesis will 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 and, where relevant, in the Authorship Declaration that follows.
- This thesis does not violate or infringe any copyright, trademark, patent, or other rights whatsoever of any person.
- This thesis does not contain work that I have published, nor work under review for publication.

Signature:
Date: 21 October 2019

Version

My thesis was passed on 12 February 2020. You are currently reading version 1.0, which includes some corrections and is to be submitted to UWA on 12 June 2020. I am maintaining my own copy which you can download from my homepage: `https://mioppolo.github.io/`

Abstract

A *code* in a graph is a proper subset of the graph's vertex set. The elements of a code are called the *codewords*, and the *automorphism group* of a code is the group of all graph automorphisms which leave invariant the set of codewords. Given a finite set $\mathcal{V}$ of v elements and an integer k which satisfies $1 \leqslant k \leqslant v-1$, we define the *Johnson graph* $J(\mathcal{V}, k)$ as follows: the vertices are the k-element subsets of $\mathcal{V}$, and vertices Δ_1 and Δ_2 are adjacent if and only if $|\Delta_1 \cap \Delta_2| = k-1$. A code Γ in $J(\mathcal{V}, k)$ is called $X-$*strongly incidence-transitive* if X is a subgroup of $\mathrm{Aut}(\Gamma)$ which acts transitively on Γ, and for each codeword $\Delta \in \Gamma$, the setwise stabiliser X_Δ acts transitively on $\Delta \times \overline{\Delta}$, where $\overline{\Delta} = \mathcal{V} \backslash \Delta$. The study of strongly incidence-transitive codes in Johnson graphs was initiated by Robert Liebler and Cheryl Praeger, in association with their investigations of neighbour-transitive codes in Johnson graphs. Their research led to the discovery of several new infinite families of strongly incidence-transitive codes, but also left several open problems. This thesis contributes towards the classification of strongly incidence-transitive codes in Johnson graphs by addressing problems posed by Liebler and Praeger connected with the following group actions:

(i) $X = \mathrm{Sp}_{2n}(2)$ and $\mathcal{V} = \mathcal{Q}^\epsilon$ is the set of all ϵ-type quadratic forms on $\mathbb{F}_2^{2n}$ which polarise to the nondegenerate alternating form preserved by X; and

(ii) $\mathcal{V} = \mathbb{F}_2^n$ and X is a 2-transitive subgroup of $\mathrm{AGL}_n(2)$ which contains the group of translations of $\mathcal{V}$.

In case (i) we classify all X-strongly incidence-transitive codes in $J(\mathcal{V}, k)$ under the condition that the stabiliser of a codeword lies in one of the *geometric Aschbacher classes* of subgroups of $\mathrm{Sp}_{2n}(2)$, denoted $\mathcal{C}_1$-$\mathcal{C}_8$. This produces several new infinite families of X-strongly incidence-transitive codes associated with the geometric Aschbacher classes, and in particular, we find that the stabiliser of a codeword always lies in $\mathcal{C}_1$. Additionally, we investigate the X-strongly incidence-transitive codes in case (i) related to the fully deleted permutation modules for the symmetric and alternating groups, and find a pair of complementary codes when $n = 4$ with codeword stabilisers isomorphic to S_{10}. There are no further examples associated with the fully deleted permutation modules for the symmetric and alternating groups. If the stabiliser of a codeword lies in the almost-simple Aschbacher class $\mathcal{C}_9$ then we are able to rule out the majority of possibilities, but leave some open cases. In particular, it is currently unknown whether there exists an X-strongly incidence-transitive code Γ in case (i) with $\Delta \in \Gamma$ and $\mathrm{soc}(X_\Delta)$ either an alternating group A_m with $m > 2n+2$ or a classical group of Lie type over $\mathbb{F}_4$.

In case (ii) we introduce *single-component* strongly incidence-transitive codes and show that every X-strongly incidence-transitive code can be expressed as a disjoint union of single-component codes. Additionally, we construct a projection from an arbitrary single-component code Γ in $J(2^n, k)$ onto a *translation-free* code in $J(2^{n-m}, k/2^m)$, where the number of translations fixing a given codeword setwise is 2^m. For $r \geqslant 4$, it is demonstrated that the translation-free X-strongly incidence-transitive codes in $J(2^r, k)$ are the block sets of known families of point 2-transitive symmetric designs with automorphism group $\mathrm{ASp}_r(2)$, with r even and $k = 2^{r-1} \pm 2^{r/2-1}$. We provide a process for lifting a translation-free code to a single-component code, though it is currently unknown whether there are alternative methods for achieving this.

Acknowledgements

To my supervisors: John Bamberg, Alice Devillers and Cheryl Praeger; it feels impossible to express the gratitude I feel towards you. Your guidance, patience, encouragement and enthusiasm were everything. Thank you for sharing your knowledge with me.

Thank you to Dimitri Leemans and Rebecca Waldecker for reading my thesis, providing valuable feedback and asking stimulating questions.

Thank you to Michael Giudici and Thomas Stemler for answering PhD related questions and signing far too much paperwork.

To CMSC staff and students, past and present - you made UWA an interesting and enjoyable place to spend my time. Thank you for the interesting conversations, fun times and always making me feel welcome.

To Heather, Emma, Attilio, Zoe, Shane, Aidan, Gemma, Magdalena and all my other lovely friends and family; thank you for being the people I needed as I progressed through my studies.

Shannon, Kristin, Brian, Adrian, Daniel, Jesse, Melissa, Sylvia, David, Phil and Jon; you made my experience at UWA something wonderful.

Thank you to Simeon Ball, Jan de Beul, Philippe Cara, Marcel Fernandez and John Sheeky for the opportunity to visit your institutions, for the conversations, hospitality and speaking with me about research.

Thank you to the UWA School of Mathematics, the Australian Mathematical Sciences Institute and the Combinatorial Mathematics Society of Australasia for travel allowances.

Finally, to everybody I forgot; *thank you.*

This research is supported by an Australian Postgraduate Award and an Australian Government Research Training Program (RTP) Scholarship.

My dissertation is dedicated to my mum, Heather Ioppolo. I am eternally greatful for your never ending support and for you being my personal cheer squad.

Contents

CHAPTER 1

Introduction

The birth of information theory is generally attributed to the publication of Claude Shannon's article 'A Mathematical Theory of Communication' [**2**] in 1948. In the two years following, Hamming introduced the perfect 1-error-correcting codes which now bear his name [**3**], and Golay published a one page article [**4**] which provided generator matrices for the perfect binary and ternary Golay codes. Early coding theory was largely motivated by the possibility of detecting and correcting errors which occur while communicating over a noisy channel. However, the underlying mathematical structures are deeply connected with finite geometry, combinatorics and group theory. As an example, the automorphism groups of the Golay codes and their extensions are closely related the the Mathieu groups [**5**, Chapter 5]. The relationships between codes, combinatorics and algebra are explored in [**6**], and further information of the sort can be found in [**7, 8, 9, 10, 5**].

Hamming [**3**] defines a *code* of length n over an alphabet $\mathcal{A}$ of size q to be a subset of vectors in the n-fold cartesian product $\mathcal{A}^n$, and calls the elements of a given code the *codewords*. If $\mathcal{A}$ is a finite field then $\mathcal{A}^n$ is a finite vector space. In this situation, a (n, k)-*linear code* is defined to be a k-dimensional subspace of $\mathcal{A}^n$. Whether or not the code is linear, $\mathcal{A}^n$ comes equipped with a metric d_H, commonly called the *Hamming metric*, which is defined as follows: for any codewords x and y, $d_H(x, y)$ is the number of indices such that $x_i \neq y_i$. It is the Hamming metric which enables one to quantify the 'error correcting capabilities' of a particular code. Indeed, suppose $\Gamma \subset \mathcal{A}^n$ is a code, and let δ denote the minimum Hamming distance between any distinct pair of codewords. Imagine Alice wishes to communicate with Bob over a digital channel using the code Γ. Alice encodes a message as a codeword x, and upon transmission, the string received by Bob is y. To decode y, Bob attempts to identify a unique codeword z which minimises $d_H(z, y)$. Of course, if z is not unique then Bob cannot decode y, but provided that $d_H(x, y) \leqslant \lfloor \frac{\delta-1}{2} \rfloor$, y will be correctly decoded to x. This type of decoding is called *nearest-neighbour decoding*. Further details can be found in [**9**, Chapter 3].

Hamming's definition of a code admits a natural generalisation. Indeed, let $(\mathcal{X}, d)$ be a metric space, where $|\mathcal{X}| < \infty$. A *code* is simply a subset of $\mathcal{X}$. For the entirety of this dissertation, we restrict this definition slightly by specifying that $\mathcal{X}$ is the vertex set of a connected undirected graph $\mathscr{G}$ with a finite number of vertices and without loops or multiple edges. Graphs come equipped with a *path length metric*, which computes the length of the shortest path between any given pair of vertices in $\mathscr{G}$. Codes of this type are generally referred to as *codes in graphs*. It should be noted that Hamming's definition of a code fits within the framework of codes in graphs since we may choose the vertex set of $\mathscr{G}$ to be $\mathcal{A}^n$ and define vertices x and y to be adjacent if and only if their Hamming distance is one. Examples from this important family of graphs are appropriately named *Hamming graphs*, and denoted $H(n, q)$ with $n \geqslant 1$ and $q = |\mathcal{A}| \geqslant 2$. The study of codes in graphs was introduced in the PhD thesis of Phillipe Delsarte [**11**], wherin he comments that '(the Hamming and Johnson graphs) appear to provide a natural framework for a combinatorial theory of codes'. We have met the former of these families, now we introduce the latter.

Let $\mathcal{V}$ be a finite set of cardinality v and let k be an integer which satisfies $1 \leqslant k \leqslant v-1$. We denote by $\binom{\mathcal{V}}{k}$ the set of all k-element subsets of $\mathcal{V}$. The *Johnson graphs*, denoted $J(\mathcal{V},k)$, are a family of distance-regular graphs with vertex set $\binom{\mathcal{V}}{k}$. A pair of k-sets $\Delta_1, \Delta_2 \in \binom{\mathcal{V}}{k}$ are adjacent in $J(\mathcal{V},k)$ if and only if $|\Delta_1 \cap \Delta_2| = k-1$. The *Johnson metric* on $J(v,k)$ is defined by the equation $d(\Delta_1,\Delta_2) = v - |\Delta_1 \cap \Delta_2|$. This corresponds to the length of the shortest path between Δ_1 and Δ_2. When convenient to do so, we write $J(v,k)$ instead of $J(\mathcal{V},k)$. Note that if $k=1$ or $v-1$ then $J(v,k)$ is a complete graph on v vertices. We therefore assume $2 \leqslant k \leqslant v-2$ for the remainder of the thesis.

We note that Norman Biggs introduces the concept of codes in distance-transitive graphs in [**12**], independently of Delsarte.

1.1. Codes in graphs

Let $\mathscr{G}$ be a simple connected regular graph with vertex set $V(\mathscr{G})$, and let $\Gamma \subset V(\mathscr{G})$ be a code. Denote by d the path length metric defined on the vertex set of $\mathscr{G}$. The *minimum distance* of Γ is defined as $\delta = \min\{d(x,y) \mid x,y \in \Gamma, x \neq y\}$. If $e = \lfloor \frac{\delta-1}{2} \rfloor$ then for any vertex $y \in V(\mathscr{G})$ which has a distance at most e from a codeword $x \in \Gamma$, the distance from y to x is strictly less than the distance from y to any other codeword. For this reason, Γ is called an *e-error correcting code*, where $e = \lfloor \frac{\delta-1}{2} \rfloor$. For each $x \in V(\mathscr{G})$ we define the *distance* from x to Γ by $d(x,\Gamma) = \min\{d(x,y) \mid y \in \Gamma\}$, and the *covering radius* of Γ by $\rho = \max\{d(x,\Gamma) \mid x \in V(\mathscr{G}) \backslash \Gamma\}$. For each $r \in \mathbb{N}$ we define the *sphere* of radius r centred on Γ by $\Gamma_r = \{x \in V(\mathscr{G}) \mid d(x,\Gamma) = r\}$. In particular, elements of Γ_1 are called the *neighbours* of Γ. Note that $\Gamma = \Gamma_0$. Similarly, we define the *disk* of radius r centered on Γ by $D_r(\Gamma) = \{x \in V(\mathscr{G}) \mid d(x,\Gamma) \leqslant r\}$. Note that ρ is the smallest integer such that $V(\mathscr{G}) = \cup_{x\in\Gamma} D_\rho(x)$.

The *sphere packing bound* is a fundamental inequality in coding theory. For a code Γ in a graph $\mathscr{G}$ with minimum distance δ and $e = \lfloor \frac{\delta-1}{2} \rfloor$, the sphere packing bound can be expressed as

$$|\Gamma| \sum_{x\in\Gamma} |D_e(x)| \leqslant |V(\mathscr{G})| \tag{1.1}$$

where $D_e(x)$ is a disk of radius e centred on a codeword x. Equality holds in Equation (1.1) if and only if the vertices of $\mathscr{G}$ can be partitioned into non-intersecting disks of radius ρ. In this case, Γ is called a *perfect code*. If Γ is a perfect code then it is always possible to decode using nearest-neighbour decoding. Of course, if too many errors occur then it is possible to decode incorrectly, but for every string z received by the decoder there exists a unique codeword x which minimises $d_H(x,z)$. We have already met some examples of perfect codes in Hamming graphs $H(n,q)$; the Hamming codes constructed in [**3**] and the Golay codes [**4**] are perfect. Disappointingly, perfect codes are quite rare. Indeed, if $\mathscr{G}$ is a Hamming graph over a finite field of order q then the only nontrivial perfect codes in $\mathscr{G}$ are the Hamming codes and the Golay codes (see [**13, 14**]). There are no known nontrivial examples of perfect codes in Johnson graphs, and Delsarte [**11**] conjectures that no examples exist. Delsarte's conjecture is open, though bounds and necessary conditions have led to non-existence proofs in special cases. Chapter 1 of [**15**] provides an excellent overview of the problem.

An alternative approach is to weaken the conditions placed upon perfect codes. To this end, Delsarte [**11**] introduced a family of codes called *completely regular codes*. Completely regular codes share many of the combinatorial properties associated with perfect codes [**16**], and if $\mathscr{G}$ is a distance regular graph then every perfect code in $\mathscr{G}$ is completely regular [**17**]. The classes of codes described thus far are defined in terms of a combinatorial restriction, but this is certainly not the only way to construct codes.

Definition 1.1
Let Γ be a code in $\mathscr{G}$. The *automorphism group* of Γ is the subgroup of elements in $\mathrm{Aut}(\mathscr{G})$ which stabilise Γ setwise. The full automorphism group of a code Γ is denoted $\mathrm{Aut}(\Gamma)$.

A code Γ induces a partition of $V(\mathscr{G})$ with parts $\Gamma_i = \{x \in V(\mathscr{G}) \mid d(x,\Gamma) = i\}$, where i is an integer ranging from 0 to ρ. Since $\mathrm{Aut}(\Gamma)$ preserves adjacency and fixes Γ setwise, the parts Γ_i are necessarily invariant under the action of $\mathrm{Aut}(\Gamma)$. The majority of our work is dedicated to the construction and classification of families of codes using automorphism groups and the distance partition.

1.2. Codes in Hamming graphs

Let $\mathcal{A}$ be set of size q. Recall that the *Hamming graph* $H(n,q)$ is the graph with vertex set $\mathcal{A}^n$, and for any vertices x and y, x is adjacent to y if and only if $d_H(x,y) = 1$. For any vertex x, the *weight* of x is defined to be the number indices i with $1 \leqslant i \leqslant n$ and $x_i \neq 0$. The weight is denoted by $\mathrm{wt}(x)$. If Γ is a linear code then $\mathrm{wt}(x)$ is the distance from x to the zero vector.

The symmetric group S_n acts on the vertices of $H(n,q)$ as the group of $n \times n$ permutation matrices which permute the coordinates of vectors in $\mathcal{A}^n$. If Γ is a code in $H(n,q)$, we call the group of $n \times n$ permutation matrices which fix Γ setwise the *permutational automorphism group* of Γ. The permutational automorphism group is denoted $\mathrm{PAut}(\Gamma)$. The full automorphism group of $H(m,q)$ is the wreath product $S_q \wr S_n$ [**18**, Theorem 9.2.1], where S_q is the symmetric group on $\mathcal{A}$. In accordance with Definition 1.1, we consider the full automorphism group of Γ to be the setwise stabiliser of Γ in $S_q \wr S_n$. This is denoted $\mathrm{Aut}(\Gamma)$. As explained in [**19**, Section 2.3.5], the definition of the automorphism group of a code differs slightly throughout the coding theory literature. While $S_q \wr S_n$ preserves Hamming distance, coding theorists are often interested specifically in the weight preserving automorphisms of codes, and usually refer to $\mathrm{PAut}(\Gamma)$ as the 'automorphism group of Γ'. In addition, when $\mathcal{A}$ is a finite field of order q, there are two other automorphism groups which we mention. A *monomial matrix* with entries in $\mathbb{F}_q$ is a square matrix with exactly one nonzero entry in every row and column. The *monomial automorphism group*, $\mathrm{MAut}(\Gamma)$ is the group of $n \times n$ monomial matrices which fix Γ setwise. If $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, then for $x = (x_1, x_2, \ldots, x_n) \in H(n,q)$ we define $x^\sigma = (x_1^\sigma, x_2^\sigma, \ldots, x_n^\sigma)$. The *coding automorphism group*, denoted $\mathrm{CAut}(\Gamma)$, is the group generated by the $n \times n$ monomial matrices and field automorphisms. It is shown in [**19**, Section 2.3.5] that the automorphism groups discussed above can be identified with subgroups of $\mathrm{Aut}(\Gamma)$ such that $\mathrm{PAut}(\Gamma) \leqslant \mathrm{MAut}(\Gamma) \leqslant \mathrm{CAut}(\Gamma) \leqslant \mathrm{Aut}(\Gamma)$, and that each containment can be strict.

Definition 1.2
Let $\mathscr{G} = H(n,q)$. Let $\Gamma \subset V(\mathscr{G})$ be a code with covering radius ρ and let X be a subgroup of $\mathrm{Aut}(\Gamma)$.

For $r \leqslant \rho$, we call Γ an (X, r)-*neighbour-transitive code* if $X \leqslant \mathrm{Aut}(\Gamma)$ acts transitively on Γ_i for all i with $0 \leqslant i \leqslant r$. In particular, if Γ is $(X, 1)$-neighbour-transitive then we call Γ a *neighbour-transitive code*, and if Γ is (X, ρ)-neighbour-transitive then we call Γ a *completely-transitive code*. If Γ is linear and $X \leqslant \mathrm{MAut}(\Gamma)$ acts transitively on the set of cosets of Γ then we call Γ X-*coset completely-transitive*.

The phrase 'completely-transitive code' was introduced by Solé in [**20**], specifically for codes in $H(n, 2)$. We call the codes discussed in [**20**] *coset completely-transitive codes*, as in Definition 1.2, to distinguish them from the more general notion of complete transitivity. Note that $\mathrm{PAut}(\Gamma) = \mathrm{MAut}(\Gamma)$ when $q = 2$. Solé demonstrates that every binary coset completely-transitive code is completely regular and shows that if Γ is a linear code in $H(n, 2)$ with covering radius $\rho \leqslant n/2$ and the group of $n \times n$ permutation matrices which fix Γ setwise is r-homogeneous, then Γ is coset completely transitive. As an application of the latter result, Solé provides the following examples of linear binary coset completely-transitive codes: the perfect Hamming codes over $\mathbb{F}_2$, the extended Hamming codes over $\mathbb{F}_2$ and the binary Golay codes in $H(23, 2)$ and $H(24, 2)$.

Giudici and Praeger [**21**] generalise the notion of coset complete-transitivity to codes in $H(n, q)$ and introduce X-completely transitive-codes in $H(n, q)$ as a subclass of completely regular codes. They prove that a linear code in $H(m, q)$ is coset completely-transitive if and only if it is $T_\Gamma\, \mathrm{MAut}(\Gamma)$-completely-transitive, where T_Γ denotes the group of translations of $\mathbb{F}_q^n$ which fix Γ setwise. Since $T_\Gamma\, \mathrm{MAut}(\Gamma)$ fixes Γ setwise, it follows that coset complete-transitivity is a special case of complete-transitivity. In particular, a binary or ternary linear code is coset completely-transitive if and only if it is completely-transitive [**21**, Theorem 1.2]. However, there exist completely transitive codes which are not coset completely transitive. Completely-transitive codes, neighbour-transitive codes and 2-neighbour-transitive codes in Hamming graphs are further studied in [**22, 19, 23, 24, 25**].

1.3. Codes in Johnson graphs

Let $\mathcal{V}$ be a finite set of cardinality $v \geqslant 4$ and let k be an integer which satisfies $2 \leqslant k \leqslant v - 2$. Recall that the Johnson graph $J(\mathcal{V}, k)$ is the graph with vertex set $\binom{\mathcal{V}}{k}$, where k-sets $\Delta_1, \Delta_2 \in \binom{\mathcal{V}}{k}$ are adjacent if and only if $|\Delta_1 \cap \Delta_2| = k - 1$. If $\Delta \in \binom{\mathcal{V}}{k}$ then we write $\overline{\Delta} := \mathcal{V} \backslash \Delta$.

Every element of $\mathrm{Sym}(\mathcal{V})$ induces a permutation on $\binom{\mathcal{V}}{k}$. Indeed, for each vertex $\beta \in \binom{\mathcal{V}}{k}$ and each permutation $g \in \mathrm{Sym}(\mathcal{V})$ we define $\beta^g = \{\omega^g \mid \omega \in \beta\}$. It turns out that $\mathrm{Sym}(\mathcal{V})$ is an automorphism group of $J(v, k)$ and, provided that $k \neq \frac{1}{2}v$, $\mathrm{Sym}(\mathcal{V})$ is the full automorphism group of $J(v, k)$ (see [**18**, Theorem 9.1.2]). We define a bijection $c : \binom{\mathcal{V}}{k} \to \binom{\mathcal{V}}{v-k}$ which maps each vertex β to its complement $\beta^c = \overline{\beta} = \mathcal{V} \backslash \beta$. In fact, c is a graph isomorphism between $J(v, k)$ and $J(v, v-k)$ and $c^2 = 1$. If $v = 2k$ then c generates a subgroup of order two in $\mathrm{Aut}(J(2k, k))$ and the full automorphism group of $J(2k, k)$ is $\mathrm{Sym}(\mathcal{V}) \times \langle c \rangle \cong \mathrm{Sym}(\mathcal{V}) \times C_2$. To summarise, the full automorphism group of the Johnson graphs are given by

$$\mathrm{Aut}(J(\mathcal{V}, k)) \cong \begin{cases} \mathrm{Sym}(\mathcal{V}) \times C_2 & \text{if } v = 2k \geqslant 4 \\ \mathrm{Sym}(\mathcal{V}) & \text{otherwise.} \end{cases} \tag{1.2}$$

The details are available in [**18**, Theorem 9.1.2].

Let $\Gamma \subset \binom{\mathcal{V}}{k}$ be a code and X a subgroup of the automorphism group of $J(\mathcal{V}, k)$. For the remainder of the thesis, we assume that $X \leqslant \mathrm{Sym}(\mathcal{V})$, unless we explicitly state otherwise. Definition 1.2 can be generalised to an arbitrary simple connected graph, though we are interested mainly in the case $\mathscr{G} = J(v, k)$.

Definition 1.3
Let $\mathscr{G}$ be a simple connected graph. Let $\Gamma \subset V(\mathscr{G})$ be a code with covering radius ρ and let X be a subgroup of $\mathrm{Aut}(\Gamma)$. For $r \leqslant \rho$, we call Γ an (X, r)-*neighbour-transitive code* if $X \leqslant \mathrm{Aut}(\Gamma)$ acts transitively Γ_i for all i with $0 \leqslant i \leqslant r$. If Γ is an (X, ρ)-neighbour-transitive code then we call Γ a *completely-transitive code.* If Γ is an $(X, 1)$-neighbour-transitive code then we call Γ a *neighbour-transitive code.*

Definition 1.4
Let Γ be a code in $J(\mathcal{V}, k)$. The *complementary code* is the code in $J(\mathcal{V}, v-k)$ defined by $\Gamma^c = \{\mathcal{V}\backslash\Delta \mid \Delta \in \Gamma\}$. If $\Gamma = \Gamma^c$ then we call Γ a *self-complementary code.*

Remark 1.5
By [**1**, Remark 1.4(d)], Γ is neighbour-transitive if and only if Γ^c is neighbour-transitive, and both codes have the same minimum distance.

Completely-transitive codes in Johnson graphs were introduced by Godsil and Praeger in [**26**]. Neighbour-transitive codes are introduced in [**1**] and further explored in [**27**] and [**28**]. Neighbour-transitive codes in Johnson graphs play a central role in this thesis.

Let $\Gamma \subset \binom{\mathcal{V}}{k}$ be a code, and let Δ be a codeword. By definition, a vertex $\Delta_1 \in \binom{\mathcal{V}}{k}$ lies adjacent to Δ if and only if $|\Delta \cap \Delta_1| = k-1$. We view the pair (Γ, Γ_1) as an incidence structure, where $\Delta \in \Gamma$ is incident with $\Delta_1 \in \Gamma_1$ if and only if $|\Delta \cap \Delta_1| = k-1$. This leads to the following definition.

Definition 1.6 ([**1**])
Let Γ be a code in $J(\mathcal{V}, k)$ and X a subgroup of $\mathrm{Aut}(J(\mathcal{V}, k))$. We call Γ an X-*incidence-transitive code* if X acts transitively on pairs $(\Delta, \Delta_1) \in \Gamma \times \Gamma_1$ with $|\Delta \cap \Delta_1| = k-1$.

It is possible to further strengthen the notion of incidence-transitivity by identifying the neighbours of a codeword Δ with the elements of the cartesian product $\Delta \times \overline{\Delta}$ in the following manner.

Lemma 1.7
Let $\mathscr{G} = J(\mathcal{V}, k)$ with $1 < k < |\mathcal{V}| - 1$. Let Δ be a vertex of $\mathscr{G}$ and denote by $\Gamma_1(\Delta)$ the set of vertices of $\mathscr{G}$ adjacent to Δ. Then the function $f : \Delta \times \overline{\Delta} \to \Gamma_1(\Delta)$ defined by $f(\omega, \omega_1) = (\Delta\backslash\{\omega\}) \cup \{\omega_1\}$ is a bijection.

PROOF. By definition, $\Delta_1 \in \Gamma_1$ if and only if $|\Delta \cap \Delta_1| = k - 1$, which holds if and only if there exist unique elements $\omega, \omega_1 \in \mathcal{V}$ such that $\Delta \backslash (\Delta \cap \Delta_1) = \{\omega\}$ and $\Delta_1 \backslash (\Delta \cap \Delta_1) = \{\omega_1\}$. It follows that f is a bijection. □

Definition 1.8 ([**1**])
Let Γ be a code in $J(\mathcal{V}, k)$ and X a subgroup of $\mathrm{Aut}(J(\mathcal{V}, k))$. We call Γ an *X-strongly incidence-transitive code* if X acts transitively on Γ and, for all $\Delta \in \Gamma$, the setwise stabiliser X_Δ acts transitively on the cartesian product $\Delta \times \overline{\Delta}$.

Since X is required to act transitively on Γ in Definition 1.8, it follows that X_Δ acts transitively on $\Delta \times \overline{\Delta}$ for all $\Delta \in \Gamma$ if and only if there exists a codeword $\Delta \in \Gamma$ such that X_Δ acts transitively on $\Delta \times \overline{\Delta}$. If Γ is X-incidence-transitive then clearly Γ is neighbour-transitive also. If $\delta \leqslant 2$, then [**1**, Example 2.2] shows that there exist neighbour-transitive codes which are not incidence-transitive. In addition, every strongly incidence-transitive code is incidence-transitive, but there exist incidence-transitive codes, necessarily with $\delta = 1$, which are not strongly incidence-transitive; examples of these can be found in [**1**, Examples 3.1 and 4.4].

This thesis is a contribution towards the classification of X-strongly incidence-transitive codes in Johnson graphs $J(\mathcal{V}, k)$ with $X \leqslant \mathrm{Sym}(\mathcal{V})$. The classification is divided into three subcases determined by the action of X on the point set $\mathcal{V}$: X is *intransitive* on $\mathcal{V}$, X is transitive and *imprimitive* on $\mathcal{V}$, or X is *primitive* on $\mathcal{V}$ (see Section 2.2 for definitions). In the two former cases, a complete classification of X-neighbour-transitive codes is achieved in [**1**]. The authors note that while some of the constructed codes are new, others correspond to codes previously studied (see [**29, 30, 31, 26**]). If X acts primitively on $\mathcal{V}$ then the following theorem suggests that a complete classification is possible.

Theorem 1.9 ([**1**])
Let $\Gamma \subset \binom{\mathcal{V}}{k}$ and $X \leqslant \mathrm{Aut}(\Gamma) \cap \mathrm{Sym}(\mathcal{V})$, where $2 \leqslant k \leqslant |\mathcal{V}| - 2$.

(a) Γ is X-strongly incidence-transitive if and only if Γ is X-incidence-transitive and $\delta \geqslant 2$.
(b) If $\delta \geqslant 3$ and Γ is X-neighbour-transitive, then Γ is X-strongly incidence-transitive.
(c) If X is primitive on $\mathcal{V}$ and Γ is incidence-transitive, then X is 2-transitive on $\mathcal{V}$.

If X acts primitively on $\mathcal{V}$ then Theorem 1.9(c) allows us to make use of the classification of the finite 2-transitive permutation groups (see [**32, 33**]; a statement is available in Section 2.2). The finite 2-transitive permutation groups can be further subdivided into two families: those which lie in an infinite family of group actions, and those which do not. The latter subfamily, referred to as the *sporadic* case, are considered in [**27**] and a classification of the associated X-strongly incidence-transitive codes with minimum distance at least 2 is obtained. There are 27 examples in total, including 5 examples of self-complementary codes.

In combination with Durante [**28**], Liebler and Praeger [**1**] classified all the neighbour-transitive codes in $J(\mathcal{V}, k)$ admitting a group of automorphisms which acts 2-transitively on $\mathcal{V}$ and lies in an infinite family of 2-transitive actions, excluding the natural action of $\mathrm{AGL}_n(2)$ on $\mathbb{F}_2^n$ and the *Jordan-Steiner actions* of $\mathrm{Sp}_{2n}(2)$. We describe these cases below.

Jordan-Steiner case: *For each integer $n \in [1:\infty)$ and each $\varepsilon \in \{+,-\}$ we let $\mathcal{V} = \mathcal{Q}_n^\varepsilon$ denote the set of all $2^{n-1}(2^n+\varepsilon)$ quadratic forms of type ε which polarise to a given nondegenerate alternating bilinear form B. The symplectic group $X = \mathrm{Sp}_{2n}(2)$ preserving B admits a faithful and 2-transitive action on $\mathcal{Q}^\varepsilon$ as follows: for all $\varphi \in \mathcal{Q}^\varepsilon$ and $g \in X$ we define φ^g by the equation $\varphi^g(x) = \varphi(xg^{-1})$, for all $x \in V$.*

Binary affine case: *For each integer $n \in [1:\infty)$ we let V denote the set of all n-tuples over $\mathbb{F}_2$. The affine group $\mathrm{AGL}_n(2)$ acts naturally on V by a combination of translations and matrix multiplication. The action is faithful and 2-transitive on $\mathcal{V}$. Denote by X any 2-transitive subgroup of $\mathrm{AGL}_n(2)$ which contains the full subgroup of translations of $\mathcal{V}$.*

When reading the literature it appears that the binary affine case is classified using a combination of results in [**1, 28**]. During the course of my PhD we discovered a small gap in [**1**, Proposition 6.6] for affine type codes over $\mathbb{F}_2$. We show in Appendix A that the results of Liebler and Praeger remain valid in the affine case for $q > 2$.

Problem 1.10 (Main Problem)
Let $\mathcal{V}$ be a set of $v \geqslant 4$ points and suppose $3 \leqslant k \leqslant v-3$. Classify the X-strongly incidence-transitive codes $\Gamma \subset \binom{\mathcal{V}}{k}$ with $X \leqslant \mathrm{Sym}(\mathcal{V}) \cap \mathrm{Aut}(\Gamma)$, where the action of X on $\mathcal{V}$ is as described above in the Jordan-Steiner case or the binary affine case.

The Jordan-Steiner actions are described in Chapter 3. A summary of our results and the open cases which remain is available in Chapter 8. We may assume $3 \leqslant k \leqslant v-3$ in Problem 1.10 because X acts 2-transitively on $\mathcal{V}$ and therefore X acts transitively on the vertices of $J(v,2)$ and $J(v,v-2)$. As mentioned previously, $J(v,1)$ and $J(v,v-1)$ are complete graphs.

Remark 1.11
When ε appears in numerical formulas, we commit a slight abuse of notation and identify $+$ with $+1$ and $-$ with -1. This convention is followed throughout the thesis in order to simplify formulas which involve ε.

1.4. Related concepts and preliminary results

In Section 1.4 we introduce some concepts linked with strongly incidence-transitive codes in Johnson graphs, outline our methods of investigation in the Jordan-Steiner case, and prove some basic results which are used throughout the thesis.

1.4.1. Block designs

An *incidence structure* is a triple $\mathscr{D} = (\mathfrak{p}, \mathfrak{b}, \mathfrak{i})$ which consists of a finite set $\mathfrak{p}$ of v *points*, a finite set $\mathfrak{b}$ of blocks, each of size k, and an incidence relation $\mathfrak{i} \subseteq \mathfrak{p} \times \mathfrak{b}$. An incidence structure is called a t-(v, k, λ) design if for every t-subset $\mathfrak{t} \subset \mathfrak{p}$, there are precisely λ blocks incident with every element of $\mathfrak{t}$. If the block set of $\mathscr{D}$ is $\{\mathfrak{p}\}$ or $\binom{\mathfrak{p}}{k}$ then $\mathscr{D}$ is a t-design for all $t \leqslant k$. These are referred to as *trivial designs*. The number of blocks of $\mathscr{D}$ is denoted b, and the number of blocks incident with any given point is denoted r. The latter of these parameters called the *replication number*. The parameters of $\mathscr{D}$ are related by the equations

$$bk = vr \text{ and } r(k-1) = \lambda(v-1). \tag{1.3}$$

We view each block as a k-subset of points and we do not allow repeated blocks. We therefore identify $\mathfrak{b}$ with a collection of k-element subsets of $\mathfrak{p}$, and write $p \in \beta$ if and only if $(p, \beta) \in \mathfrak{i}$. The elements of $\mathfrak{i}$ are called *flags* and the elements of $(\mathfrak{p} \times \mathfrak{b})\backslash\mathfrak{i}$ are called *antiflags*. Let $\mathscr{D}$ be a t-(v, k, λ) design. An *automorphism* of $\mathscr{D}$ is a pair (σ, μ), where σ is a permutation on the point set, μ is a permutation on the block set, and for every $(p, \beta) \in \mathfrak{p} \times \mathfrak{b}$ we have $p \in \beta$ if and only if $p^\sigma \in \beta^\mu$.

The blocks of a t-(v, k, λ) design define a code in $J(v, k)$, although an arbitrary code in $J(v, k)$ does not necessarily correspond to the block set of a design. However, if Γ is an X-strongly incidence-transitive code in $J(\mathcal{V}, k)$ and X acts primitively on $\mathcal{V}$, then by [**1**, Theorem 1.2(c)], X acts 2-transitively on $\mathcal{V}$. This implies $(\mathcal{V}, \Gamma)$ is a 2-(v, k, λ) design. Moreover, the set of codewords of each of the 27 strongly incidence-transitive codes constructed in [**27**] is a t-(v, k, λ) design with $t \geqslant 2$.

Definition 1.12
Let $\mathscr{D}$ be a t-(v, k, λ) design and X an automorphism group of $\mathscr{D}$. We call $\mathscr{D}$ an X-*strongly incidence-transitive design* if X acts transitively on the set

$$\mathcal{T} = \{(p_1, p_2, \beta) \in \mathfrak{p} \times \mathfrak{p} \times \mathfrak{b} \mid p_1 \in \beta \text{ and } p_2 \notin \beta\}$$

under the natural action on cartesian products.

Anne Delandtsheer classified the strongly incidence-transitive 2-$(v, k, 1)$ designs as a Corollary to her classification of antiflag-transitive linear spaces [**34**].

Theorem 1.13 ([**34**])
Let $\mathscr{L}$ be a 2-$(v, k, 1)$ design and suppose X is an automorphism group of $\mathscr{L}$ which acts transitively on the set of antiflags of $\mathscr{L}$. Then $\mathscr{L}$ corresponds to one of the following designs:

(a) a Desarguesian projective or affine space of dimension at least 2,
(b) a Hermitian unital,
(c) Hering's plane of order 27, or
(d) the nearfield plane of order 9.

In particular, $\mathscr{L}$ is strongly incidence-transitive if and only if $\mathscr{L}$ is as in item (a) or (b).

1.4.2. Group factorisations

Let G be a finite group and let A and B be proper nontrivial subgroups of G. If G can be expressed as a product $AB = \{ab \mid a \in A, b \in B\}$ of subgroups A and B, then we say the expression $G = AB$ is a *factorisation* of G. If A and B are maximal subgroups of G then we say the factorisation is *maximal.* If neither A nor B contain T, then we call the factorisation a *core-free factorisation.* The maximal factorisations of the simple groups of Lie type are classified in [**35**]. The factorisations of the sporadic simple groups are classified in [**36**]. These classification results will be used in Chapter 6.

Lemma 1.14 ([**35**], pg. 41)
Let G be a finite group and let A and B be subgroups of G. The following statements are equivalent:
(a) $G = AB$
(b) A is transitive on the cosets of B in G
(c) B is transitive on the cosets of A in G
(d) $|G : A| = |B : A \cap B|$
(e) $|G : B| = |A : A \cap B|$

Lemma 1.15
Let Γ be a strongly incidence-transitive code in $J(\mathcal{V}, k)$ for $2 \leqslant k \leqslant v - 2$. For all $\Delta \in \Gamma$ and for all $(\varphi, \psi) \in \Delta \times \overline{\Delta}$, the expression $X_\Delta = X_{\Delta,\varphi} X_{\Delta,\psi}$ is a group factorisation.

Proof. Let $\Delta \in \Gamma$ and $G = X_\Delta$. If Γ is strongly incidence-transitive then G_φ acts transitively on the elements of $\overline{\Delta}$. Then the Orbit-Stabiliser Theorem implies the action of G_φ on $\overline{\Delta}$ is permutationally isomorphic to the action of G_φ on the coset space G/G_ψ. Similarly, the transitive action of G_ψ on Δ is permutationally isomorphic to the transitive action of G_ψ on the coset space G/G_φ. Therefore Theorem 1.14 implies G is transitive on $\Delta \times \overline{\Delta}$ if and only if $G = G_\varphi G_\psi$. □

Lemma 1.16 ([**35**], pg. 41)
Let G be a finite group and let A and B be subgroups of G. Then

$$|A \cap B| \geqslant \frac{|A||B|}{|G|}.$$

Equality holds if and only $G = AB$ is a factorisation.

1.4.3. Plan of attack

The following observation provides a starting point for our analysis of the Jordan-Steiner actions.

Lemma 1.17 ([**27**])
Let $\mathcal{V}$ be a set of v elements and let $\Gamma \subset \binom{\mathcal{V}}{k}$ be an X-strongly incidence-transitive code, where X is a transitive subgroup of $\mathrm{Sym}(\mathcal{V})$ and $2 \leqslant k \leqslant v - 2$. Then there exists an integer $\ell \geqslant 1$ and a chain of

Class	Associated Geometric Structure
$\mathcal{C}_1$	Subspace
$\mathcal{C}_2$	Direct sum decomposition
$\mathcal{C}_3$	Field extension
$\mathcal{C}_4$	Tensor product
$\mathcal{C}_5$	Subfield
$\mathcal{C}_6$	Extraspecial structure
$\mathcal{C}_7$	Tensor power
$\mathcal{C}_8$	Classical form

TABLE 1.1. Geometric Aschbacher classes and associated structures

subgroups

$$X_\Delta = H_0 < H_1 < \cdots < H_\ell = X$$

such that each H_i is a maximal subgroup in H_{i+1} for $0 \leqslant i < \ell$, all H_i with $1 \leqslant i \leqslant \ell$ are transitive on $\mathcal{V}$, H_0 has exactly two orbits Δ and $\mathcal{V}\backslash\Delta$, and X_Δ is transitive on $\Delta \times (\mathcal{V}\backslash\Delta)$.

Aschbacher [**37**] introduced nine classes of subgroups in classical groups which have come to be known as *Aschbacher classes*. The first eight Aschbacher classes $\mathcal{C}_1 - \mathcal{C}_8$ are said to be of *geometric type*, since they are associated with geometric structures in vector spaces. The geometric classes are roughly described in Table 1.4.3. The ninth Aschbacher class $\mathcal{C}_9$ is called the *almost simple* class, since taking the quotient of an element of $\mathcal{C}_9$ by its centre yields an almost simple group.

Aschbacher demonstrated that the maximal subgroups of a classical group must lie in at least one of $\mathcal{C}_i$ for $1 \leqslant i \leqslant 9$, though the elements of these classes are not necessarily maximal. Kleidman and Liebeck extended Aschbacher's theorem in [**38**] by providing necessary and sufficient conditions to determine maximality of a geometric subgroup of a classical group, provided that the dimension of the natural module is at least 13. Bray, Holt and Roney-Dougal's book [**39**] contains a full analysis of the geometric and almost simple maximal subgroups of classical groups where the dimension of the natural module is between 2 and 12, inclusive. Knowledge of the maximal subgroups of classical groups will be an invaluable tool for the construction and analysis of strongly incidence-transitive codes with automorphism group $\mathrm{Sp}_{2n}(2)$. Detailed descriptions of the geometric Aschbacher classes can be found in [**39**]. We describe below the maximal subgroups of $\mathrm{Sp}_{2n}(2)$.

Theorem 1.18 ([**5**], pg. 92)
Let $V = \mathbb{F}_2^{2n}$ and let M be a maximal subgroup of $\mathrm{Sp}_{2n}(2)$ which lies in one of the classes $\mathcal{C}_1 - \mathcal{C}_8$. Then one of the following holds:

(a) $M \cong \mathrm{Sp}_{2d}(2) \times \mathrm{Sp}_{2(n-d)}(2)$ is a $\mathcal{C}_1$-subgroup fixing a $2d$-dimensional nondegenerate subspace of V, where $1 \leqslant d \leqslant n/2 - 1$.
(b) $M \cong 2^{d(d+1)/2}.2^{2d(n-d)} \rtimes \mathrm{Sp}_{2(n-d)}(2)$ is a $\mathcal{C}_1$-subgroup fixing a d-dimensional totally isotropic subspace of V, where $1 \leqslant d \leqslant n$.
(c) $M \cong \mathrm{Sp}_{2m}(2) \wr S_t$ is a $\mathcal{C}_2$-subgroup fixing a decomposition $V = \oplus_{i=1}^t V_i$ of V into nondegenerate subspaces, each of dimension $2m = 2n/t$.
(d) $M \cong \mathrm{Sp}_{2m}(2^b) \rtimes C_b$ is a $\mathcal{C}_3$-subgroup where b is prime and $n = mb$.

(e) $M \cong \mathrm{GO}^{\varepsilon}_{2n}(2)$ is a $\mathcal{C}_8$-subgroup corresponding to a point stabiliser in the Jordan-Steiner actions.

Remark 1.19

We reflect on the geometric Achbacher classes which do not appear in Theorem 1.18. Further information may be obtained by studying the tables in [**38**] and [**39**].

(a) The $\mathcal{C}_1$-subgroup $\mathrm{Sp}_{2d}(2) \times \mathrm{Sp}_{2(n-d)}(2)$ is not maximal for $d = n/2$ since it lies inside the maximal $\mathcal{C}_2$ subgroup $\mathrm{Sp}_n(2) \times \mathrm{Sp}_n(2) \times \mathbb{Z}_2$.
(b) The $\mathcal{C}_4$-subgroups of $\mathrm{Sp}_{2n}(2)$ are of the form $H \cong \mathrm{Sp}_{n_1}(2) \otimes \mathrm{GO}^{\varepsilon}_{n_2}(2)$ where $n_2 \geqslant 3$. However, $H < \mathrm{GO}^{\varepsilon}_{2n}(2) < \mathrm{Sp}_{2n}(2)$, so H is not maximal in $\mathrm{Sp}_{2n}(2)$.
(c) The $\mathcal{C}_5$-subgroups of $\mathrm{Sp}_{2n}(q)$ are isomorphic to $\mathrm{Sp}_{2n}(q_0).(2, q-1, r)$ where $q = q_0^r$ and r is prime. This case does not arise since $\mathbb{F}_2$ has no proper subfields.
(d) The $\mathcal{C}_6$-subgroups of $\mathrm{Sp}_{2n}(q)$ are of the form $2^{1+2m}.\,\mathrm{GO}^{-}_{2m}(2)$ with $2n = 2^m$. By [**38**, Table 3.5.C] these do not need to be considered when $q = 2$.
(e) The $\mathcal{C}_7$-subgroups of $\mathrm{Sp}_{2n}(2)$ are of the form $H \cong 2.\,\mathrm{PSp}_n(q)^t.2^{t-1}.S_t$. Such groups are maximal if and only if mq is odd and $(m, q) \neq (2, 3)$. If mq is even then groups of this type are maximal in the hyperbolic orthogonal groups and are therefore not maximal in $\mathrm{Sp}_{2m}(2)$.

We finish our introduction with a number of basic results which are referenced throughout the thesis.

Corollary 1.20

Let Γ be a code in $J(\mathcal{V}, k)$ with $2 \leqslant k \leqslant |\mathcal{V}| - 2$ and let $X \leqslant \mathrm{Sym}(\mathcal{V}) \cap \mathrm{Aut}(\Gamma)$. Then Γ is X-strongly incidence-transitive if and only if X acts transitively on $\mathcal{V}$, there exists $\omega \in \mathcal{V}$ such that X_ω acts transitively on the set of codewords which contain ω, and there exists $\Delta \in \Gamma$ with $\omega \in \Delta$ such that $X_{\omega,\Delta}$ acts transitively on $\overline{\Delta}$.

Lemma 1.21

Let Γ be a strongly incidence-transitive code in $J(\mathcal{V}, k)$ with $\Delta \in \Gamma$. Let M be a subgroup of $X = \mathrm{Aut}(\Gamma)$ which acts transitively on $\mathcal{V}$ while preserving a system of imprimitivity $\mathcal{I}$. If $X_\Delta < M \leqslant X$ then Δ is a union of blocks in $\mathcal{I}$.

Proof. Let $\Delta \in \Gamma$. Since Γ is strongly incidence-transitive, X_Δ has two orbits in $\mathcal{V}$, namely Δ and $\overline{\Delta}$. We assume without loss of generality that $|\Delta| \leqslant |\overline{\Delta}|$. Suppose that Δ is not a union of blocks. Naturally, this implies $\overline{\Delta}$ is not a union of blocks either. Therefore there exists a block $\Sigma \in \mathcal{I}$ such that $\Sigma \cap \Delta$ and $\Sigma \cap \overline{\Delta}$ are non-empty, and since $|\Delta| \leqslant \frac{1}{2}|\mathcal{V}|$ there exists $\Sigma' \in \mathcal{I}$ such that $\Sigma' \neq \Sigma$ and $\Sigma' \nsubseteq \Delta$. Choose $\omega_0, \omega, \omega' \in \mathcal{V}$ as follows: $\omega_0 \in \Sigma \cap \Delta, \omega \in \Sigma \cap \overline{\Delta}$ and $\omega' \in \Sigma' \cap \overline{\Delta}$. Since Γ is X-strongly incidence-transitive, there exists a permutation $h \in X_{\Delta,\omega_0}$ such that $\omega^h = \omega'$. However, ω_0 is fixed by h and therefore Σ is fixed setwise by h. On the other hand h moves $\omega \in \Sigma$ to $\omega' \in \Sigma'$, a contradiction. Therefore Δ and $\overline{\Delta}$ are unions of blocks. $\square$

Remark 1.22

Suppose Γ is a strongly incidence-transitive code in $J(\mathcal{V},k)$ for some $2 \leqslant k \leqslant \frac{1}{2}|\mathcal{V}|$. Let $\Delta \in \Gamma$ and M be a maximal subgroup of $\mathrm{Aut}(\Gamma)$ such that $X_\Delta \leqslant M$. Then by definition, for all $\omega \in \Delta$ the point stabiliser $X_{\Delta,\omega}$ acts transitively on $\overline{\Delta}$. Since $X_\Delta \leqslant M$, for each $\omega \in \Delta$ there exists a unique M_ω-orbit in $\mathcal{V}$ containing $\overline{\Delta}$. We will denote this orbit by $\Theta(\omega)$. In particular, for any subset $A \subseteq \Delta$ we must have $\overline{\Delta} \subseteq \cap_{\omega \in A}\Theta(\omega)$.

CHAPTER 2

Group theoretic background

Chapter 2 contains a brief review of selected topics in finite group theory. Further details can be found in [**40, 41, 42, 33, 5**].

2.1. Finite simple groups

Let G be a group. The *commutator* $[\cdot,\cdot] : G \times G \to G$ is defined by

$$[g,h] = g^{-1}h^{-1}gh$$

for all $g, h \in G$. The *derived subgroup* of G is defined by

$$G' = \langle [g,h] \mid g, h \in G \rangle.$$

If $G = G'$ then G is called a *perfect group*. The *exponent* of a finite group is the least common multiple of its element orders. The *Frattini subgroup* $\Phi(G)$ is the intersection of all maximal subgroups of G. A subgroup $H \leqslant G$ is called a *characteristic subgroup* of G if it is fixed setwise by the natural action of $\mathrm{Aut}(G)$. For example, the Frattini subgroup $\Phi(G)$ and the derived subgroup G' are characteristic subgroups of $\mathrm{Aut}(G)$.

Definition 2.1
Let G be a nontrivial group. We say G is *simple* if it contains no proper non-trivial normal subgroups. We say G is *almost simple* if there exists a nonabelian simple group T such that $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$. We say G is *quasisimple* if G is perfect and $G/Z(G)$ is almost simple.

Theorem 2.2 (CFSG. See [**5**], pg. 3)
Every finite simple group is isomorphic to one of the following groups:

(a) A cyclic group C_p of prime order;
(b) An alternating group A_n with $n \geqslant 5$;
(c) A simple group of Lie type
  (i) $\mathrm{PSL}_n(q)$, $n \geqslant 2$, except $\mathrm{PSL}_2(2)$ and $\mathrm{PSL}_2(3)$;
  (ii) $\mathrm{PSU}_n(q)$, $n \geqslant 3$, except $\mathrm{PSU}_3(2)$;
  (iii) $\mathrm{PSp}_{2n}(q)$, $n \geqslant 2$, except $\mathrm{PSp}_4(2)$;
  (iv) $\mathrm{P}\Omega_{2n+1}(q)$, $n \geqslant 3$, q odd;
  (v) $\mathrm{P}\Omega^+_{2n}(q)$, $n \geqslant 4$;
  (vi) $\mathrm{P}\Omega^-_{2n}(q)$, $n \geqslant 4$;
  (vii) $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$;

(viii) $G_2(q)$, $q \geqslant 3$;
(ix) $F_4(q)$;
(x) ${}^2B_2(2^{2n+1})$, $n \geqslant 1$;
(xi) ${}^2G_2(3^{2n+1})$, $n \geqslant 1$;
(xii) ${}^2F_4(2^{2n+1})$, $n \geqslant 1$;
(xiii) ${}^2F_4(2)'$

where q is a prime power; or

(d) one of 26 sporadic simple groups
(i) a Mathieu group $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$;
(ii) a Leech lattice group $Co_1, Co_2, Co_3, McL, HS, Suz, J_2$;
(iii) a Fischer group $Fi_{22}, Fi_{23}, Fi_{24}'$
(iv) a Monstrous group $\mathbb{M}, \mathbb{B}, Th, HN, He$;
(v) a pariah $J_1, J_3, J_4, O'N, Ly, Ru$.

Conversely, every group listed above is simple, and the only repetitions are $\mathrm{PSL}_2(4) \cong \mathrm{PSL}(2,5) \cong A_5$, $\mathrm{PSL}_2(7) \cong \mathrm{PSL}(3,2)$, $\mathrm{PSL}_2(9) \cong A_6$, $\mathrm{PSL}_4(2) \cong A_8$ and $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$.

2.2. Permutation Groups

Section 2.2 is a review of selected results related to finite permutation groups. For further details we suggest consulting [**33**], [**32**], or the classic text [**43**].

A permutation on a set Ω is a bijection from Ω to itself. The symmetric group is denoted by $\mathrm{Sym}(\Omega)$ and consists of all permutations on Ω, with multiplication defined by composition of permutations. A *permutation group* is a subgroup of $\mathrm{Sym}(\Omega)$. The cardinality of Ω is referred to as the *permutation degree* of G. If $|\Omega| = n < \infty$ then we write $S_n = \mathrm{Sym}(\Omega)$.

A *group action* of G on a set Ω is a group homomorphism $\lambda : G \to \mathrm{Sym}(\Omega)$. The homomorphism λ is sometimes called a *permutation representation* of G. The *kernel* of λ is the subgroup of all elements of G which fix every point of Ω. If $\ker(\lambda) = \{1\}$ then we say that G acts *faithfully* on Ω, otherwise the action is *unfaithful*. A group with a faithful permutation representation is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$.

When there is no risk of ambiguity we will suppress the function λ and denote the image of ω under $\lambda(g)$ by ω^g. If Ω is a set of vectors and G is a matrix group acting by right multiplication we will instead denote the image of v under $\lambda(g)$ by vg. A *G-space* is a set Ω together with a function $\Omega \times G \to \Omega$ which satisfies

(a) $\omega^1 = \omega$ for all $\omega \in \Omega$, and
(b) $(\omega^g)^h = \omega^{gh}$ for all $\omega \in \Omega$ and $g, h \in G$.

As one might expect, a group action may be used to define a G-space and a G-space may always be derived from a group action.

Example 2.3
Let $G = \mathrm{GL}_n(q)$ dnote the group of invertible $n \times n$ matrices over $\mathbb{F}_q$, and let Ω denote the set of all 1-dimensional subspaces of the vector space $\mathbb{F}_q^n$. Then G acts on Ω by right multiplication. The action

is faithful if and only if $q = 2$; the kernel is the subgroup of scalar matrices with nonzero determinant, $K = \{\alpha I \mid \alpha \in \mathbb{F}_q \backslash \{0\}\}$. The quotient group $\mathrm{PGL}_n(q) = \mathrm{GL}_n(q)/K$ acts faithfully on Ω.

Definition 2.4
Let G be a permutation group on Ω and let $\omega \in \Omega$. The *orbit* of ω under G is the subset of Ω

$$\omega^G = \{\omega^g \mid g \in G\}$$

which consists of all images of ω under an element of G. The *stabiliser* of ω in G is the subgroup of G

$$G_\omega = \{g \in G \mid \omega^g = \omega\}$$

which consists of all elements of G which fix ω. Similarly, for any subset S of Ω, the *setwise stabiliser* of S in G is the subgroup of G

$$G_S = \{g \in G \mid \omega^g \in S, \forall s \in S\}$$

which consists of all elements of G which leave S invariant. We define

$$G_{\omega,S} = G_\omega \cap G_S.$$

Definition 2.5
Suppose $G \leqslant \mathrm{Sym}(\Omega)$ and $H \leqslant \mathrm{Sym}(\Sigma)$. A *permutational isomorphism* from G to H consists of a bijection $f : \Omega \to \Sigma$ and a group isomorphism $\theta : G \to H$ such that $f(\omega)^{\theta(g)} = f(\omega^g)$ for all $\omega \in \Omega$ and $g \in G$. If $G = H$ and there exists a permutational isomorphism between the action of G on Ω and the action of G on Σ then we say the actions are *equivalent*.

Theorem 2.6 (The Orbit-Stabiliser Theorem [**33**], pg. 5)
Let G be a permutation group on Ω. For all $\omega \in \Omega$ there exists a bijection between ω^G and the set $\cos(G : G_\omega)$ of right cosets of G_ω in G. In particular, if Ω is finite then $|G| = |\omega^G||G_\omega|$.

Example 2.7
Let $G = \mathrm{GL}_n(q)$, $V = \mathbb{F}_q^n$ and let Ω_k denote the set of k-dimensional subspaces of V. Then G acts on Ω_k and Ω_{n-k} for each integer k satisfying $1 \leqslant k \leqslant n$. The function $\perp$: $\Omega_1 \to \Omega_{n-1}$ defined by $\langle u \rangle^\perp = \{x \in V \mid ux^T = 0\}$ is a bijection and the mapping $\iota : g \mapsto (g^{-1})^T$ is an automorphism of G. Moreover, for all $g \in G$ we have

$$\begin{aligned}\left(u^\perp\right)^{\iota(g)} &= \{x \in V \mid ux^T = 0\}^{g^{-T}} \\ &= \{xg^{-T} \in V \mid ux^T = 0\}.\end{aligned}$$

Setting $y = xg^{-T}$ we have $x = yg^T$ and therefore

$$\begin{aligned}\{xg^{-T} \in V \mid ux^T = 0\} &= \{y \in V \mid u(yg^T)^T = 0\} \\ &= \{y \in V \mid (ug)y^T = 0\} \\ &= \langle ug \rangle^\perp.\end{aligned}$$

We have shown $\left(u^{\perp}\right)^{\iota(g)} = \langle ug\rangle^{\perp}$ and therefore the pair $(\iota, \perp)$ is a permutational isomorphism between the action of G on Ω_1 and the action of G on Ω_{n-1}.

Definition 2.8
Let N be a group and let H be a subgroup of $\mathrm{Aut}(N)$. The *semidirect product* of N by H is the group $N \rtimes H$ which has underlying set $N \times H$ and defined as follows:

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 n_2^{h_1^{-1}}, h_1 h_2)$$

for all $n_1, n_2 \in N$ and $h_1, h_2 \in H$.

Example 2.9
The affine group $G = \mathrm{AGL}_n(q)$ consists of all affine transformations of a vector space $V = \mathbb{F}_q^n$. We may express G as a semidirect product $G = V \rtimes G_0$, where V acts on itself by translation and $G_0 \cong \mathrm{GL}_n(q)$ acts on V by matrix multiplication.

Definition 2.10
Let G and H be finite groups and let $H \leqslant S_n$. The *wreath product* $G \wr H$ is the group

$$G \wr H = G^n \rtimes H$$

where the action of H on G^n, which allows us to identify H with a subgroup of $\mathrm{Aut}(G^n)$, is defined by

$$(g_1, g_2, \cdots, g_n)^{h^{-1}} = (g_{1^h}, g_{2^h}, \cdots, g_{n^h})$$

for all $(g_1, g_2, \cdots, g_n) \in G^n$ and $h \in H$.

Definition 2.11
A permutation group G on Ω is called *transitive* if for all $\omega_1, \omega_2 \in \Omega$, there exists $g \in G$ such that $\omega_1^g = \omega_2$. In other words, G has a single orbit in Ω. We say G acts *intransitively* on Ω if it has more than one orbit in Ω. If G is transitive on Ω and $|G| = |\Omega|$ then G is called a *regular* permutation group.

A permutation group $G \leqslant \mathrm{Sym}(\Omega)$ acts on the set Ω^k of k-tuples by

$$(\omega_1, \omega_2, \ldots, \omega_k)\sigma = (\omega_1\sigma, \omega_2\sigma, \ldots, \omega_k\sigma)$$

for $\sigma \in G$ and $\omega_i \in \Omega$. This action leaves invariant the set of k-tuples of pairwise distinct elements of Ω. We say G is *k-transitive* if it acts transitively on the set of k-tuples of pairwise distinct elements of Ω.

Lemma 2.12 ([**33**], pg. 10)
Let G be a permutation group. Then G is k-transitive if and only if G is transitive and G_ω is $(k-1)$-transitive on $\Omega\backslash\{\omega\}$.

The only k-transitive permutation groups with $k \geqslant 6$ are the alternating and symmetric groups (see [**32**], Chapter 7). The k-transitive groups with $2 \leqslant k \leqslant 5$ are known explicitly. The only known proofs of these results depend on the classification of finite simple groups (see Theorem 2.2). Theorem 2.13 below lists the 2-transitive group actions. A description of each of the actions is available in [**32**], Section 7.7.

Theorem 2.13 ([**44**])
Let G be a finite 2-transitive group acting on a finite set Ω. Then one of the following holds:

(a) G is of almost simple type with unique minimal normal subgroup T, and T is one of the following non-abelian simple groups:
   (i) $T = A_n$, of degree $n \geqslant 5$;
   (ii) $T = \mathrm{PSL}_n(q)$, of degree $(q^n - 1)/(q - 1)$ with $n \geqslant 2$ and $(n, q) \neq (2, 2), (2, 3)$;
   (iii) $T = \mathrm{Sp}_{2n}(2)$, of degree $2^{n-1}(2^n \pm 1)$, with $n \geqslant 3$;
   (iv) $T = \mathrm{PSU}_3(q)$, of degree $q^3 + 1$ with $q \geqslant 3$;
   (v) $T = \mathrm{Sz}(q)$, of degree $q^2 + 1$, with $q = 2^{2n+1} > 2$;
   (vi) $T = \mathrm{Ree}(q)$, of degree $q^3 + 1$, with $q = 3^{2n+1} > 3$;
   (vii) $T = M_n$, a Mathieu group of degree n, with $n \in \{11, 12, 22, 23, 24\}$;
   (viii) $T = \mathrm{PSL}_2(11)$ of degree 11; $T = M_{11}$ of degree 12; $T = A_7$ of degree 15; $T = \mathrm{PSL}_2(8)$ of degree 28; $T = \mathrm{HS}$ of degree 176; $T = \mathrm{Co}_3$ of degree 276.

(b) G is of affine type, and Ω may be identified with a vector space V of dimension n over $\mathbb{F}_q$, for some prime power q. Moreover, one of the following holds for $G_{\mathbf{0}}$, the stabiliser of the zero vector in V:
   (i) $\mathrm{SL}_n(q) \leqslant G_{\mathbf{0}} \leqslant \Gamma\mathrm{L}_n(q)$;
   (ii) $\mathrm{Sp}_{2n}(q) \trianglelefteqslant G_{\mathbf{0}}$;
   (iii) $n = 6$, q even and $G_2(q) \trianglelefteqslant G_{\mathbf{0}}$;
   (iv) $\mathrm{SL}_2(3) = 2^{1+2} \rtimes 3 \trianglelefteqslant G_{\mathbf{0}}$;
   (v) $2^{1+4} \trianglelefteqslant G_{\mathbf{0}}$;
   (vi) $\mathrm{SL}_2(5) \trianglelefteqslant G_{\mathbf{0}}$;
   (vii) $n = 4$, $q = 2$ and $G_{\mathbf{0}} = A_6$ or A_7;
   (viii) $n = 6, q = 2$ and $G_{\mathbf{0}} = \mathrm{PSU}_3(3)$;
   (ix) $n = 6, q = 3$ and $G_{\mathbf{0}} = \mathrm{SL}_2(13)$.

Definition 2.14
Let G be a transitive permutation group. A *block* for G is a subset $\Sigma \subseteq \Omega$ such that for all $g \in G$, $\Sigma^g = \Sigma$ or $\Sigma \cap \Sigma^g = \varnothing$. Note that if Σ is a block for G then Σ^g is also a block for all $g \in G$. A *system of imprimitivity* for G is a G-invariant partition of Ω into blocks. Every permutation group admits at least two systems of imprimitivity: a partition of Ω into single element sets and a partition of Ω with a single block. Such partitions are considered trivial. A transitive permutation group which preserves no nontrivial system of imprimitivity is called a *primitive* group. Now, let M be a proper subgroup of G.

We say M is a *maximal subgroup* of G if there are no groups H such that $M < H < G$. The maximality of point stabilisers in G are directly related to the primitive actions of G.

Lemma 2.15 ([**32**], pg. 14)
Let G be a transitive permutation group on a non-empty set Ω. Then G is primitive if and only if there exists $\omega \in \Omega$ such that the point stabiliser G_ω is a maximal subgroup of G.

Lemma 2.16 ([**32**], pg. 18)
Let G be a transitive subgroup of $\mathrm{Sym}(\Omega)$ and let $N \lhd G$ be an intransitive normal subgroup. Then the N-orbits in Ω form a system of imprimitivity preserved by G. In particular, if G is primitive then every normal subgroup is transitive.

Definition 2.17
A permutation group on a set Ω is called *k-homogeneous* if it acts transitively on the set $\binom{\Omega}{k}$ of k-subsets of Ω.

A k-transitive group is necessarily k-homogeneous. However, the converse is not true. The next theorem classifies the k-homogeneous groups which are not k-transitive.

Theorem 2.18 ([**45**])
Let G be a permutation group which is k-homogeneous on a finite set Ω but not k-transitive, where $2 \leqslant k \leqslant \frac{1}{2}|\Omega|$. Then up to permutational isomorphism, one of the following holds:
(a) $k = 2$ and $G \leqslant \mathrm{A\Gamma L}_1(q)$ with $n = q \equiv 3 \mod 4$;
(b) $k = 3$ and $\mathrm{PSL}_2(q) \leqslant G \leqslant \mathrm{P\Gamma L}_2(q)$, where $n - 1 = q \equiv 3 \mod 4$;
(c) $k = 3$ and $G = \mathrm{AGL}_1(8), \mathrm{A\Gamma L}_1(8)$ or $\mathrm{A\Gamma L}_1(32)$; or
(d) $k = 4$ and $G = \mathrm{PSL}_2(8), \mathrm{P\Gamma L}_2(8)$ or $\mathrm{P\Gamma L}_2(32)$.
Conversely, each group listed above is a k-homogeneous group which is not k-transitive.

2.3. Classical groups

Section 2.3 provides an introduction to classical forms and their isometry groups. Further details are available from [**42, 46, 39, 38**].

Definition 2.19
Let V be a vector space over $\mathbb{F}$ and let $\sigma \in \mathrm{Aut}(\mathbb{F})$. A function $B : V \times V \to \mathbb{F}$ is called a *$\sigma-$sesquilinear form* if for all $u, v, w \in V$ and $\alpha, \beta \in \mathbb{F}$, B satisfies:
(a) $B(\alpha u + \beta v, w) = \alpha B(u, w) + \beta B(v, w)$; and
(b) $B(u, \alpha v + \beta w) = \alpha^\sigma B(u, v) + \beta^\sigma B(u, w)$.

If σ is the identity mapping then we say B is a *bilinear form*. We call B *symmetric* if $B(u, v) = B(v, u)$ for all $u, v \in V$. We call B *alternating* if $B(v, v) = 0$ for all $v \in V$.

A bilinear form B is called *reflexive* if for all $u, v \in V$ we have $B(u, v) = 0$ if and only if $B(v, u) = 0$. We assume bilinear forms are reflexive unless otherwise stated.

Definition 2.20
A *quadratic form* on V is a function $\varphi : V \to \mathbb{F}$ such that the following hold:
(a) $\varphi(\alpha v) = \alpha^2\varphi(v)$ for all $\alpha \in \mathbb{F}$ and $v \in V$; and
(b) the function $B : V \times V \to \mathbb{F}$ defined by the equation

$$B(u, v) = \varphi(u + v) - \varphi(u) - \varphi(v) \tag{2.1}$$

is a symmetric bilinear form.

The bilinear form obtained from a quadratic form φ by Equation (2.1) is called the *polar form* of φ. We say φ *polarises* to B. If $\mathrm{char}(\mathbb{F})$ is odd then Equation (2.1) implies $\varphi(v) = \frac{1}{2}B(v, v)$ for all $v \in V$ and therefore there is a unique correspondence between each quadratic form and its polar form. If $\mathrm{char}(F) = 2$, however, this does not hold; there are generally multiple quadratic forms which polarise to the same symmetric bilinear form. The eccentricities of quadratic forms in characteristic two are discussed further in Chapter 3.

A pair of vectors $u, v \in V$ satisfying $B(u, v) = 0$ is said to be *orthogonal*. Let U be a subspace of V. The subset of V defined by

$$U^\perp = \{v \in V \mid B(u, v) = 0 \text{ for all } u \in U\}$$

is called the *orthogonal complement* of U with respect to B.

Lemma 2.21 ([**42**], pg. 52)
Let V be an $n-$dimensional vector space over a field $\mathbb{F}$ and let U b3 a $k-$dimensional subspace of V. Then $U^\perp$ is an $(n - k)$-dimensional subspace of V.

Definition 2.22
Let V be a vector space equipped with a bilinear form B. Then B is *nondegenerate* if $V^\perp = \{0\}$.

Definition 2.23
Let V be a vector space equipped with a sesquilinear form B. A *similarity* of B is an invertible linear transformation $g \in \mathrm{GL}(V)$ for which there exists a scalar $\lambda_g \in \mathbb{F}\backslash\{0\}$ such that $B(ug, vg) = \lambda_g B(u, v)$ for all $u, v \in V$. A *similarity* of φ is an invertible linear transformation $g \in \mathrm{GL}(V)$ for which there exists a scalar $\lambda_g \in \mathbb{F}\backslash\{0\}$ such that $\varphi(vg) = \lambda_g\varphi(v)$ for all $v \in V$. A similarity with $\lambda = 1$ is called an *isometry* of B (or φ).

If there exists an isometry between a pair of quadratic or sesquilinear forms then we will say they are *isometric*. The following theorem characterises nondegenerate reflexive sesquilinear forms. It is sometimes referred to as the 'Birkhoff-von Neumann Theorem', though it was published by Richard Brauer in 1936 [**47**].

Theorem 2.24 ([**47**])
Let V be a vector space with $\dim(V) \geqslant 3$ and let B be a nondegenerate and reflexive σ-sesquilinear form on V. Then one of the following holds:

(a) B is alternating: $\sigma = 1$ and $B(v, v) = 0$ for all $v \in V$;
(b) B is symmetric: $\sigma = 1$ and $B(u, v) = B(v, u)$ for all $u, v \in V$; or
(c) B is Hermitian: $\sigma^2 = 1$, $\sigma \neq 1$ and $B(u, v) = B(v, u)^\sigma$ for all $u, v \in V$.

Definition 2.25
Let J be an $n \times n$ matrix with entries in $\mathbb{F}$. The function $V \times V \to \mathbb{F}$ defined by $B(u, v) = uJv^T$ is a bilinear form on $V = \mathbb{F}^n$. Conversely, for any bilinear form B defined on a vector space with basis $\mathscr{B} = \{e_1, \ldots, e_n\}$, the matrix J defined by $J_{ij} = B(e_i, e_j)$ satisfies $B(u, v) = uJv^T$. The matrix J is called the *Gram matrix* for B with respect to $\mathscr{B}$.

Definition 2.26
Let V be a vector space equipped with either a bilinear form B or quadratic form φ.

(a) A vector $v \in V$ is $\varphi-$*singular* if $\varphi(v) = 0$.
(b) A subspace $U \leqslant V$ is $\varphi-$*totally singular* if $\varphi(v) = 0$ for all $v \in U$.
(c) A subspace $U \leqslant V$ is $B-$*totally isotropic* if $U \leqslant U^\perp$.
(d) A pair of nonzero vectors $u, v \in V \backslash \{0\}$ is called a *hyperbolic pair* if $B(u, v) = 1$ and $B(u, u) = B(v, v) = 0$.

Totally isotropic subspaces are sometimes called totally singular in the literature. When working with fields of even characteristic it is necessary to differentiate between singular and isotropic spaces as a subspace might be totally isotropic with respect to B but not totally singular with respect to a polar form φ. On the other hand, Equation (2.1) implies that a totally-singular subspace is also totally-isotropic.

Lemma 2.27 ([**48**], pg. 46)
Let $V = \mathbb{F}_q^m$. We have the following:

(a) The number of d-dimensional subspaces in V is

$$N_d(m, q) = \prod_{i=0}^{d-1} \frac{q^{m-i} - 1}{q^{i+1} - 1} \tag{2.2}$$

(b) If V is equipped with a nondegenerate symplectic form then $m = 2n$ and the number of d-dimensional totally isotropic subspaces in V is

$$\prod_{i=0}^{d-1} \frac{q^{2(n-i)} - 1}{q^{i+1} - 1} \tag{2.3}$$

(c) If V is equipped with a nonsingular ε-type quadratic form and $m = 2n$, then the number of d-dimensional totally singular subspaces in V is

$$\begin{array}{rl} N_d(n,q)\prod_{n-d}^{n-1}(q^i+1) & \text{if } \varepsilon = + \\ N_d(n-1,q)\prod_{n-d+1}^{n}(q^i+1) & \text{if } \varepsilon = - \end{array} \tag{2.4}$$

Theorem 2.28 (Witt's Theorem [**42**], pg. 57)
Let V be a vector space equipped with a bilinear form B. If U is a subspace of V and $g : U \to V$ is a linear isometry then g can be extended to an isometry $\overline{g} : V \to V$ such that $\overline{g}|_U = g$ if and only if $(U \cap V^{\perp})^g = U^g \cap V^{\perp}$. In particular, if U and W are subspaces of V and $g : U \to W$ is an isometry then g may be extended to an isometry of V.

Witt's Theorem implies that the maximally totally isotropic (and totally singular) subspaces with respect to a particular form have the same dimension. This dimension is called the *Witt index* of the form. Note that the Witt index is at most $\dim(V)/2$, since Lemma 2.21 implies $\dim(V) = \dim(W) + \dim(W^{\perp})$ for any subspace W.

Theorem 2.29 ([**38**], pg. 24)
Let V be a $2n$-dimensional vector space over $\mathbb{F}_q$ equipped with a symplectic form B. Then there exists a basis $\mathscr{B} = \{e_1, f_{,1}, e_2, f_2, \ldots, e_n, f_n\}$ for V such that $B(e_i, e_i) = B(f_i, f_i) = 0$ and $B(e_i, f_j) = \delta_{ij}$ for all integers i, j satisfying $1 \leqslant i, j \leqslant n$. Moreover, there is a unique isometry class of such forms on V.

Theorem 2.30 ([**38**], pg. 22)
Let V be a m-dimensional vector space over $\mathbb{F}_q$ equipped with a nondegenerate Hermitian form B. Then q is a square and there exists a basis

$$\mathscr{B} = \begin{cases} \{e_1, f_1, \ldots, e_n, f_n\} & \text{if } m = 2n \\ \{e_1, f_1, \ldots, e_n, f_n, v\} & \text{if } m = 2n+1 \end{cases} \tag{2.5}$$

for V such that $B(e_i, f_j) = \delta_{ij}, B(e_i, e_j) = B(f_i, f_j) = B(e_i, v) = B(f_i, v) = 0$ and $B(v, v) = 1$.

Theorem 2.31 ([**38**], pg. 27)
Let V be a m-dimensional vector space over $\mathbb{F}_q$ equipped with a nonsingular quadratic form φ. Let B denote the polar form of φ. Then there exists a basis $\mathscr{B}$ for V satisfying

(a) $\mathscr{B} = \{e_i, f_i \mid 1 \leqslant i \leqslant n\}$, where $\varphi(e_i) = \varphi(f_i) = 0$ for $1 \leqslant i \leqslant n-1$, $B(e_i, f_j) = \delta_{ij}$ and one of the following holds:
   (i) Hyperbolic type $(+)$: $\varphi(e_n) = \varphi(f_n) = 0$, giving Witt index n;

Type	Condition	Example
Zero Bilinear		$B(v,v') = 0$
Symplectic Bilinear	$\dim(v) = 2n$	$B(v,v') = \sum_{i=1}^{n}(x_i y_i' - y_i x_i')$
Hyperbolic Quadratic	$\dim(V) = 2n$	$\varphi(v) = \sum_{i=1}^{n} x_i y_i$
Elliptic Quadratic	$\dim(V) = 2n, \lambda \in \mathbb{F}_q^\times$	$\varphi(v) = \sum_{i=1}^{n-1} x_i y_i + x_n^2 + \lambda y_n^2$
Parabolic Quadratic	$\dim(V) = 2n+1, \lambda \in \mathbb{F}_q^\times$	$\varphi(v) = \sum_{i=1}^{n} x_i y_i + \lambda x_{n+1}$
Hermitian Sesquilinear	$\dim(V) = 2n, q$ square	$B(v,v') = \sum_{i=1}^{n}(x_i x_i'^{\sqrt{q}} + y_i y_i'^{\sqrt{q}})$
	$\dim(V) = 2n+1, q$ square	$B(v,v') = \sum_{i=1}^{n}(x_i x_i'^{\sqrt{q}} + y_i y_i'^{\sqrt{q}}) + x_{n+1} x_{n+1}'^{\sqrt{q}}$

Table 2.1. Representatives for the isometry classes of classical forms

(ii) Elliptic type $(-)$: $\varphi(e_n) = 1$ and $\varphi(f_n) = \mu$ where $x^2 + x + \mu$ is irreducible over $\mathbb{F}$, giving Witt index $n-1$.

(b) Parabolic type $(\circ)$: $\mathscr{B} = \{e_i, f_i, w \mid 1 \leqslant i \leqslant n\}$, where $\varphi(e_i) = \varphi(f_i) = 0$ for $1 \leqslant i \leqslant n-1$, $B(e_i, f_j) = \delta_{ij}$ and $\varphi(w) = 1$.

Let $v = \sum_{i=1}^{n}(x_i e_i + y_i f_i)$ or $\sum_{i=1}^{n}(x_i e_i + y_i f_i) + x_{n+1} e_{n+1}$ depending on whether $\dim(V)$ is even or odd, and define $v' \in V$ similarly. Examples of the forms introduced in this section are provided in Table 2.3 using the bases from Theorems 2.29, 2.30 and 2.31.

Lemma 2.32
Let V be a vector space equipped with a nondegenerate symplectic form B. Suppose $V = \oplus_{i=1}^{t} V_i$ where each V_i is nondegenerate with respect to B. For each integer i such that $1 \leqslant i \leqslant t$, let φ_i denote a quadratic form on V_i polarising to $B|_{V_i}$. Then there exists a unique quadratic form φ on V such that $\varphi|_{V_i} = \varphi_i$ for all $1 \leqslant i \leqslant t$.

Proof. We proceed by induction on t. If $t = 1$ then the result is obvious. Suppose $t > 1$ and the result is true for $t-1$. Let $W = \oplus_{i=1}^{t-1} V_i$ and $V = W \oplus V_t$. By induction there exists a unique form φ' on W polarising to $B|_W$ such that for all $1 \leqslant i \leqslant t-1$ we have $\varphi'|_{V_i} = \varphi_i$. Suppose $\varphi|_W = \varphi'$, $\varphi|_{V_t} = \varphi_t$ and φ polarises to B. For all $x \in V = W \oplus V_t$ we have $x = w + v$ for unique $w \in W$ and $v \in V_t$ and

$$\varphi(x) = \varphi(w+v) = \varphi(w) + \varphi(v) + B(w,v) = \varphi'(w) + \varphi_t(v) + B(w,v). \tag{2.6}$$

Therefore we define φ uniquely by Equation (2.6), for all $x = w + v \in V$. We check that φ has the desired properties:

$$\varphi|_W(w) = \varphi(w+0) = \varphi'(w)$$
$$\varphi|_{V_t}(v) = \varphi(0+v) = \varphi_t(v).$$

Form	Isometry Group	Name
Zero Bilinear	$\mathrm{GL}_n(q)$	Linear
Symplectic Bilinear	$\mathrm{Sp}_{2n}(q)$	Symplectic
Hermitian Sesquilinear	$\mathrm{GU}_n(q)$	Unitary
Hyperbolic Quadratic	$\mathrm{GO}^+_{2n}(q)$	Hyperbolic orthogonal
Elliptic Quadratic	$\mathrm{GO}^-_{2n}(q)$	Elliptic orthogonal
Parabolic Quadratic	$\mathrm{GO}^\circ_{2n+1}(q)$	Parabolic orthogonal

Table 2.2. Isometry groups of the classical forms

Finally, we show that φ polarises to B. For $i = 1, 2$ let $x_i = w_i + v_i$, where $w_i \in W$ and $v_i \in V_t$

$$\begin{aligned}\varphi(x_1 + x_2) + \varphi(x_1) + \varphi(x_2) =& \varphi(w_1 + v_1 + w_2 + v_2) + \varphi(w_1 + v_1) + \varphi(w_2 + v_2)\\ =& \varphi'(w_1 + w_2) + \varphi_t(v_1 + v_2) + B(w_1 + w_2, v_1 + v_2)\\ &+ \varphi'(w_1) + \varphi_t(v_1) + B(w_1, v_1) + \varphi'(w_2) + \varphi_t(v_2) + B(w_2, v_2)\\ =& B|_W(w_1, w_2) + B|_{V_t}(v_1, v_2) + B(w_1 + w_2, v_1 + v_2)\\ &+ B(w_1, v_1) + B(w_2, v_2)\\ =& B(w_1, w_2) + B(v_1, v_2) + B(w_1, v_2) + B(w_2, v_1)\\ =& B(w_1 + v_1, w_2 + v_2)\\ =& B(x_1, x_2).\end{aligned}$$

Therefore φ is the unique quadratic form on V which polarises to B. □

The majority of this thesis is concerned with actions of the so called *classical groups*.

Definition 2.33

Let f be a σ-sesquilinear or quadratic form. The *isometry group* of f is the set of isometries under composition.

The isometry groups of the classical forms appearing in Table 2.3 and the related classical groups are summarised below in Table 2.3.

Of course, the 'zero form' defined by $B(u, v) = 0$ for all $u, v \in V$ is degenerate. Consider the following chain of groups

$$\Omega \leqslant S \leqslant G \leqslant \Gamma \leqslant A. \tag{2.7}$$

Here, G denotes the isometry group of a nondegenerate reflexive sesquilinear form. The *special group* S is the subgroup of G consisting of determinant 1 matrices. The group Ω generally corresponds to the derived subgroup of S, though if $G = \mathrm{GO}(m, 2^e)$ then Ω related to the *spinor norm* (see [**42**], Chapter 11 for more details). The *conformal group* C is the group of *similarities* and the semilinear group Γ is the group of *semi-similarities*. Finally, A generally corresponds to the automorphism group of Ω; exceptions are noted in [**39**], Theorem 1.6.21. A *classical group* is a group H satisfying $\Omega \leqslant H \leqslant A$ for a nondegenerate reflexive sesquilinear form. We follow [**39**] and refer informally to any group H satisfying $\Omega \trianglelefteqslant H \leqslant A$ with respect to Equation (2.7) as a *classical group*. Table 2.3 appears in [**39**] and provides a useful summary of notation.

Case	Ω	S	G	C	Γ	A
L	$\mathrm{SL}_n(q)$	$\mathrm{SL}_n(q)$	$\mathrm{GL}_n(q)$	$\mathrm{GL}_n(q)$	$\Gamma\mathrm{L}_n(q)$	$\Gamma\mathrm{L}_n(q) \rtimes \langle\tau\rangle$
U	$\mathrm{SU}_n(q)$	$\mathrm{SU}_n(q)$	$\mathrm{GU}_n(q)$	$\mathrm{CGU}_n(q)$	$\mathrm{C}\Gamma\mathrm{U}_n(q)$	$\mathrm{C}\Gamma\mathrm{U}_n(q)$
S	$\mathrm{Sp}_n(q)$	$\mathrm{Sp}_n(q)$	$\mathrm{Sp}_n(q)$	$\mathrm{CSp}_n(q)$	$\mathrm{C}\Gamma\mathrm{Sp}_n(q)$	$\mathrm{C}\Gamma\mathrm{Sp}_n(q)$
O	$\Omega_n^\varepsilon(q)$	$\mathrm{SO}_n^\varepsilon(q)$	$\mathrm{GO}_n^\varepsilon(q)$	$\mathrm{CGO}_n^\varepsilon(q)$	$\mathrm{C}\Gamma\mathrm{O}_n^\varepsilon(q)$	$\mathrm{C}\Gamma\mathrm{O}_n^\varepsilon(q)$

TABLE 2.3. Notation for the classical groups

The associated *projective groups* are obtained as the quotient of a given group by its subgroup of scalar matrices. The projective notation is obtained by appending P to the beginning of the notation appearing in Table 2.3.

CHAPTER 3

The Jordan-Steiner actions

The symplectic group $\mathrm{Sp}_{2n}(2)$ has a pair of 2-transitive actions of degrees $2^{n-1}(2^n \pm 1)$, which we refer to as the Jordan-Steiner actions. Chapter 3 provides an introduction to the Jordan-Steiner actions. We refer the reader to Section 7.7 of [**32**] for further details on the Jordan-Steiner actions and to [**49, 50, 51**] for some applications to coding and design theory. The submodule structure of the associated permutation modules is studied in [**52**].

3.1. The Jordan–Steiner Actions

Let V be a $2n$-dimensional vector space over $\mathbb{F}_2$. Denote by $\mathscr{B}$ the set of alternating bilinear forms on V and by $\mathscr{Q}$ the set of quadratic forms on V. It is shown in [**53**, Proposition 1] that $\mathscr{B}$ and $\mathscr{Q}$ are vector spaces over $\mathbb{F}_2$ of respective dimensions $2n^2 + n$ and $2n^2 - n$, with addition defined pointwise. The mapping $\theta : \mathscr{Q} \to \mathscr{B}$ associates with each $\varphi \in \mathscr{Q}$ an alternating bilinear form $B \in \mathscr{B}$ defined by

$$B(x, y) = \varphi(x + y) - \varphi(x) - \varphi(y). \tag{3.1}$$

Equation (3.1) is called the *polarisation equation.* As discussed in [**53**], θ is a surjective linear transformation and $\ker(\theta)$ is the vector space of of all linear transformations from V to $\mathbb{F}_2$. We now fix a particular nondegenerate alternating form, which we denoted by $B : V \times V \to \mathbb{F}_2$. For brevity we shorten the phrase 'nondegenerate alternating bilinear form' to 'symplectic form'. Let $\mathcal{Q}$ denote the set of all quadratic forms on V which satisfy Equation (3.1). Denote by $X = \mathrm{Sp}_{2n}(2)$ the full isometry group of B. Given $\varphi \in \mathcal{Q}$ and $g \in X$, we define a function $\varphi^g : V \to \mathbb{F}_2$ by

$$\varphi^g(x) = \varphi(xg^{-1}). \tag{3.2}$$

It is routine to verify that (3.2) defines a group action of X on $\mathcal{Q}$. For each $\varepsilon \in \{\pm\}$ we denote by $\mathcal{Q}^\varepsilon$ the set of all ε-type quadratic forms on V which polarise to B.

Theorem 3.1 ([**32**], Section 7.7)
Let V be a $2n$-dimensional vector space over $\mathbb{F}_2$ equipped with a symplectic form B. For each $\varepsilon \in \{\pm\}$ the group $X = \mathrm{Sp}_{2n}(2)$ acts 2-transitively on $\mathcal{Q}^\varepsilon$.

The 2-transitive actions of X on $\mathcal{Q}^+$ and $\mathcal{Q}^-$ are called the *Jordan-Steiner actions.*

Lemma 3.2
Let $\varphi \in \mathcal{Q}$ and $g \in X$. If J is a Gram matrix for φ with respect to some ordered basis for V, then $g^{-1}Jg^{-T}$ is a Gram matrix for φ^g with respect to the same basis.

PROOF. By definition we have

$$\varphi^g(x) = \varphi(xg^{-1}) = \left(xg^{-1}\right) J \left(xg^{-1}\right)^T = x\left(g^{-1}Jg^{-T}\right)x^T$$

therefore $g^{-1}Jg^{-T}$ is a Gram matrix for φ^g. □

3.2. Relative coordinates for the Jordan-Steiner actions

The symplectic group $\mathrm{Sp}_{2n}(2)$ is isomorphic to the orthogonal group $\mathrm{GO}_{2n+1}(2)$ [**42**]. In Section 3.2 we construct a permutational isomorphism between the Jordan-Steiner actions of $\mathrm{Sp}_{2n}(2)$ and an action of $\mathrm{GO}_{2n+1}(2)$ on a subset of $2n$-dimensional subspaces of $\mathbb{F}_2^{2n+1}$. Let $\widetilde{V} = \mathbb{F}_2^{2n+1}$ equipped with basis $\mathscr{B} = \{e_1, \dots, e_n, f_1, \dots, f_n, e_{n+1}\}$. Consider the quadratic form $\Phi : \widetilde{V} \to \mathbb{F}_2$ defined by

$$\Phi(x) = \sum_{i=1}^{n} x_i y_i + x_{n+1} \tag{3.3}$$

for all $x = \sum_{i=1}^{n}(x_ie_i + y_if_i) + x_{n+1}e_{n+1} \in \widetilde{V}$. Denote the polar form of Φ by $\widetilde{B}$. Note that $B(e_i, f_j) = \delta_{ij}$, $\Phi(e_i) = \Phi(f_i) = 0$ for $1 \leqslant i \leqslant n$ and $\Phi(e_{n+1}) = 1$. The alternating form $\widetilde{B}(x, y)$ is degenerate with radical $\widetilde{V}^\perp = \langle e_{n+1}\rangle$.

Lemma 3.3
Let $\widetilde{V}$ be a vector space over $\mathbb{F}_q$ equipped with a bilinear form $\widetilde{B} : \widetilde{V} \times \widetilde{V} \to \mathbb{F}_q$. Let $V = \widetilde{V}/\widetilde{V}^\perp$. Then the mapping $B : V \times V \to \mathbb{F}_q$ defined by

$$B(u + \widetilde{V}^\perp, v + \widetilde{V}^\perp) = \widetilde{B}(u, v) \tag{3.4}$$

is a nondegenerate bilinear form on V.

PROOF. If $\widetilde{V}^\perp = \{0\}$ then the statement is trivial. Suppose $\widetilde{B}$ is degenerate. First we show that B is well defined. Let $u, u', v, v' \in \widetilde{V}$ such that $u' = u + \widetilde{V}^\perp$ and $v' = v + \widetilde{V}^\perp$. Then there exists $c, d \in \widetilde{V}^\perp$ such that $u' = u + c$ and $v' = v + d$. Since $c, d \in \widetilde{V}^\perp$, we have

$$\begin{aligned} B(u' + \widetilde{V}^\perp, v' + \widetilde{V}^\perp) &= \widetilde{B}(u', v') \\ &= \widetilde{B}(u + c, v + d) \\ &= \widetilde{B}(u, v) + \widetilde{B}(u, d) + \widetilde{B}(c, v) + B(c, d) \\ &= \widetilde{B}(u, v) \\ &= B(u + \widetilde{V}^\perp, v + \widetilde{V}^\perp). \end{aligned}$$

In particular, B is well defined. Bilinearity of B follows directly from bilinearity of $\widetilde{B}$. Finally, let $w \in \widetilde{V}$. Then $B(w + \widetilde{V}^\perp, v + \widetilde{V}^\perp) = 0$ for all $v \in \widetilde{V}$ if and only if $\widetilde{B}(w, v) = 0$ for all $v \in \widetilde{V}$, that is, if and only if $w \in \widetilde{V}^\perp$. Therefore B is nondegenerate. □

Definition 3.4
Consider the vector space $\widetilde{V} = \mathbb{F}_2^{2n+1}$ equipped with the quadratic form Φ as defined in Equation (3.3).

Let $\widetilde{B}$ denote the polar form of Φ. A hyperplane $H < \widetilde{V}$ is called *complementary* if $H \cap \widetilde{V}^{\perp} = \{0\}$. We denote by $\widetilde{\mathcal{Q}}$ the set of all 2^{2n} complementary hyperplanes in $\widetilde{V}$.

Lemma 3.5
For all $H \in \widetilde{\mathcal{Q}}$, the restriction $\pi|_H : H \to V$ is an isomorphism of vector spaces, with inverse defined by

$$\pi|_H^{-1}(v + \widetilde{V}^{\perp}) = \begin{cases} v & \text{if } v \in H \\ v + \widetilde{e}_{n+1} & \text{if } v \notin H \end{cases} \tag{3.5}$$

Proof. For all $v \in \widetilde{V}$, exactly one of v and $v + \widetilde{e}_{n+1}$ lies in H. Therefore Equation (3.5) is a well defined inverse for $\pi|_H$. Linearity of $\pi|_H$ follows from the fact that π is linear. Therefore $\pi|_H$ is a vector space isomorphism. □

Lemma 3.6
For all $H \in \widetilde{\mathcal{Q}}$, the mapping $\varphi : V \to \mathbb{F}_2$ defined by

$$\varphi = \Phi \circ \pi|_H^{-1} \tag{3.6}$$

is a quadratic form on V which polarises to B.

Proof. For convenience we rewrite equation (3.3) as $B(x, y) = \widetilde{B}(\pi|_H^{-1}(x), \pi|_H^{-1}(y))$, where $x, y \in V$. Then for all $x, y \in V$

$$\begin{aligned} \varphi(x + y) &= \Phi \circ \pi|_H^{-1}(x + y) \\ &= \Phi(\pi|_H^{-1}(x + y)) \\ &= \Phi(\pi|_H^{-1}(x) + \pi|_H^{-1}(y)) \text{ since } \pi|_H^{-1} \text{ is linear} \\ &= \Phi(\pi|_H^{-1}(x)) + \Phi(\pi|_H^{-1}(y)) + \widetilde{B}(\pi|_H^{-1}(x), \pi|_H^{-1}(y)) \text{ by Equation (3.1)} \\ &= \Phi \circ \pi|_H^{-1}(x) + \Phi \circ \pi|_H^{-1}(y) + B(x, y) \\ &= \varphi(x) + \varphi(y) + B(x, y). \end{aligned}$$

Therefore φ is a quadratic form on V which polarises to B. □

Lemma 3.7
The map $\mu : \widetilde{\mathcal{Q}} \to \mathcal{Q}$ defined by $\mu(H) = \Phi \circ \pi|_H^{-1}$ is a bijection.

Proof. Let $H, H' \in \widetilde{\mathcal{Q}}$. Then $\mu(H) = \mu(H')$ if and only if

$$\Phi(\pi|_H^{-1}(x)) = \Phi(\pi|_{H'}^{-1}(x)) \text{ for all } x \in V. \tag{3.7}$$

Let $x = v + \widetilde{V}^{\perp}$ for some $v \in \widetilde{V}$. Let χ_H be the indicator function defined by

$$\chi_H(v) = \begin{cases} 1 & \text{if } v \notin H \\ 0 & \text{if } v \in H \end{cases}$$

for $v \in \widetilde{V}$. Recall that $\widetilde{V}^{\perp} = \langle e_{n+1} \rangle$. Then we have $\pi|_H^{-1}(x) = v + \chi_H(v)e_{n+1}$. Expanding the left hand side of equation (3.7), we have

$$\begin{aligned}\Phi(\pi|_H^{-1}(x)) &= \Phi(v + \chi_H(v)e_{n+1}) \\ &= \Phi(v) + \Phi(\chi_H(v)e_{n+1}) + \widetilde{B}(v, \chi_H(v)e_{n+1}) \\ &= \Phi(v) + \chi_H(v)\Phi(e_{n+1}) + \chi_H(v)\widetilde{B}(v, e_{n+1})\end{aligned}$$

and therefore

$$\begin{aligned}\Phi(\pi|_H^{-1}(x)) + \Phi(\pi|_{H'}^{-1}(x)) =& \Phi(v) + \chi_H(v)\Phi(e_{n+1}) + \chi_H(v)\widetilde{B}(v, e_{n+1}) + \\ & \Phi(v) + \chi_{H'}(v)\Phi(e_{n+1}) + \chi_{H'}(v)\widetilde{B}(v, e_{n+1}) \\ =& \left(\chi_H(v) + \chi_{H'}(v)\right)\Big(\Phi(e_{n+1}) + \widetilde{B}(v, e_{n+1})\Big) \\ =& \chi_H(v) + \chi_{H'}(v),\end{aligned}$$

where the last equality follows from the fact that $\Phi(e_{n+1}) = 1$ and $e_{n+1} \in \widetilde{V}^{\perp}$. Combining the equation $\Phi(\pi|_H^{-1}(x)) + \Phi(\pi|_{H'}^{-1}(x)) = \chi_H(v) + \chi_{H'}(v)$ with Equation (3.7), we deduce that $\Phi(\pi|_H^{-1}(x)) = \Phi(\pi|_{H'}^{-1}(x))$ if and only if v lies in both H and H', or v lies in neither. Therefore $\Phi(\pi|_H^{-1}(x)) = \Phi(\pi|_{H'}^{-1}(x))$ for all $x \in V$ if and only if $\pi|_H^{-1}(x) = \pi|_{H'}^{-1}(x)$ for all $x \in V$. But $\pi|_H^{-1}(x) = \pi|_{H'}^{-1}(x)$ for all $x \in V$ if and only if $H = H'$, therefore μ is injective. Since $|\mathcal{Q}| = |\widetilde{\mathcal{Q}}|$, it follows that μ is a bijection. □

Lemma 3.8
Let $\mu : \widetilde{\mathcal{Q}} \to \mathcal{Q}$ denote the bijection defined in Lemma 3.7 and let $G = \mathrm{Isom}(\Phi)$. Then μ induces a permutational isomorphism between the subspace action of G on $\widetilde{\mathcal{Q}}$ and the induced action of G on $\mathcal{Q}$.

Proof. In view of Lemmas 3.6 and 3.7, it is sufficient to prove that the equation

$$(\Phi \circ \pi_H^{-1})^g(x) = \Phi \circ \pi|_{H^g}^{-1}(x) \tag{3.8}$$

holds for all $H \in \widetilde{Q}$, $x = v + \widetilde{V}^{\perp} \in V$ and $g \in \mathrm{Isom}(\Phi)$. Beginning with the left hand side of Equation (3.8) we have

$$\begin{aligned}(\Phi \circ \pi_H^{-1})^g(x) =& \Phi(\pi_H^{-1}(xg^{-1})) \\ =& \Phi(\pi_H^{-1}(vg^{-1} + \widetilde{V}^{\perp})).\end{aligned}$$

By Equation (3.5) we have

$$\Phi \circ \pi|_H^{-1}(vg^{-1} + \widetilde{V}^{\perp}) = \begin{cases} \Phi(vg^{-1}) & \text{if } vg^{-1} \in H \\ \Phi(vg^{-1} + e_{n+1}) & \text{if } vg^{-1} \notin H \end{cases}$$

We now use the facts: $e_{n+1}g = e_{n+1}$, $vg^{-1} \in H$ if and only if $v \in H^g$, and $\Phi(vg) = \Phi(v)$ for all $v \in \widetilde{V}$. From these we deduce

$$\Phi \circ \pi|_H^{-1}(vg^{-1} + \widetilde{V}^{\perp}) = \begin{cases} \Phi(v) & \text{if } v \in H^g \\ \Phi(v + e_{n+1}) & \text{if } v \notin H^g \end{cases} \tag{3.9}$$

The right hand side of Equation (3.9) is equal to $\Phi \circ \pi|_{H^g}^{-1}(v + \widetilde{V}^{\perp})$, and therefore Equation (3.8) holds. ☐

Recall the following notation from Definition 2.26: for $\varphi \in \mathcal{Q}$ we denote by $\mathrm{sing}(\varphi)$ the set of $\varphi-$singular vectors of V. Note that $\varphi(0) = 0$ for all $\varphi \in \mathcal{Q}$ and therefore, according to Definition 2.26, $\mathrm{sing}(\varphi)$ contains the zero vector for all $\varphi \in \mathcal{Q}$. We denote by $\mathrm{sing}(\varphi)^{\#}$ the set of nonzero φ-singular vectors in V. Lemma 3.8 allows us to derive useful relationships between elements of $\mathcal{Q}$ and their singular vectors.

Lemma 3.9
For every $\varphi_0, \varphi \in \mathcal{Q}$ there exists a unique vector $c \in V$ such that the following equation holds for all $x \in V$

$$\varphi(x) = \varphi_0(x) + B(x, c). \tag{3.10}$$

Conversely, for all $c \in V$ and $\varphi_0 \in \mathcal{Q}$, equation (3.10) defines an element of $\mathcal{Q}$. Moreover,

$$\mathrm{sing}(\varphi) = \begin{cases} \mathrm{sing}(\varphi_0) + c & \text{if } c \in \mathrm{sing}(\varphi_0) \\ V \backslash (\mathrm{sing}(\varphi_0) + c) & \text{if } c \notin \mathrm{sing}(\varphi_0) \end{cases} \tag{3.11}$$

Proof. If $\varphi = \varphi_0$ then, since B is nondegenerate, $c = 0$ is the unique vector for which Equation (3.10) holds. Suppose that $\varphi \neq \varphi_0$ and let $H_0 = \mu^{-1}(\varphi_0)$ and $H = \mu^{-1}(\varphi)$ denote the corresponding complementary hyperplanes in $\widetilde{V}$, where $\mu : H \mapsto \Phi \circ \pi|_H^{-1}$. Lemma 3.7 implies $H_0 \neq H$. The intersection $S = H_0 \cap H$ is a $(2n-1)-$dimensional subspace in $\widetilde{V}$ which avoids $\widetilde{V}^{\perp}$, and thus $\pi(S)$ is a hyperplane in V. Therefore, $\pi(S) = \langle c \rangle^{\perp}$ for a unique non-zero $c \in V$, and φ_0, φ coincide precisely on $\pi(S)$. Therefore $\varphi(x) \neq \varphi_0(x)$ if and only if $x \notin \langle c \rangle^{\perp}$, in which case $B(x, c) = 1$ and $\varphi(x) = \varphi_0(x) + B(x, c)$. Thus for all x, $\varphi_0(x)$ and $\varphi(x)$ differ by $B(x, c)$ and hence Equation (3.10) holds.

Conversely, let $c \in V$, $\phi_0 \in \mathcal{Q}$ and let φ be defined by Equation (3.10). Noting that $-1 = 1$ in $\mathbb{F}_2$, for all $x, y \in V$ we have

$$\begin{aligned} \phi(x+y) - \phi(x) - \phi(y) =& \phi_0(x+y) + B(x+y, c) + \phi_0(x) + B(x, c) + \phi_0(y) + B(y, c) \\ =& \phi_0(x+y) + \phi_0(x) + \phi_0(y) \\ =& B(x, y). \end{aligned}$$

Thus ϕ defines a quadratic form which polarises to B, that is, $\phi \in \mathcal{Q}$. Finally, consider $\mathrm{sing}(\phi) = \{y \in V \mid \phi_0(y) + B(y, c) = 0\}$. Suppose $c \in \mathrm{sing}(\phi_0)$. Let $y \in \mathrm{sing}(\phi_0) + c$, so $y = x + c$ for some $x \in \mathrm{sing}(\phi_0)$.

Then by Equation (3.10)

$$\begin{aligned}\phi(y) =&\phi_0(x+c)+B(x+c,c)\\ =&\phi_0(x)+\phi_0(c)+B(x,c)+B(x,c)+B(c,c)\\ =&0\end{aligned}$$

so $\operatorname{sing}(\phi_0)+c \subseteq \operatorname{sing}(\phi)$. Similarly, if $y \in \operatorname{sing}(\phi)$ then

$$\begin{aligned}\phi_0(y+c) =&\phi_0(y)+\phi_0(c)+B(y,c)\\ =&\phi_0(y)+B(y,c)\\ =&\phi(y)\\ =&0,\end{aligned}$$

and hence $y=(y+c)+c \in \operatorname{sing}(\phi_0)+c$. Thus Equation (3.11) holds in this case. A similar argument yields Equation (3.11) when $c \notin \operatorname{sing}(\phi_0)$. $\square$

If ϕ_0 is fixed and $\varphi(x)=\varphi_0(x)+B(x,c)$ for for all $x \in V$ then we will write $\varphi=\varphi_c$. Note that φ_c and φ_0 agree on $\langle c\rangle^\perp$, since $x \in \langle c\rangle^\perp$ precisely when $B(x,c)=0$.

Lemma 3.10

For each $\varphi_0 \in \mathcal{Q}^\varepsilon$ the function $\lambda_{\varphi_0} : V \to \mathcal{Q}$ defined by $\lambda_{\varphi_0}(c)=\varphi_c$ induces a permutational isomorphism between the actions of X_{φ_0} on V and $\mathcal{Q}$. In particular, the image of $\operatorname{sing}(\varphi_0)$ under λ_{φ_0} is $\mathcal{Q}^\varepsilon$.

Proof. Lemma 3.9 implies that λ_{φ_0} is a bijection. Let $\phi_0 \in \mathcal{Q}$, $c \in V$ and $g \in X_{\varphi_0}$. Then for all $x \in V$ we have

$$\begin{aligned}\varphi_c^g(x) =&\varphi_c(xg^{-1})=\varphi_0(xg^{-1})+B(xg^{-1},c)=\varphi_0^g(x)+B(x,cg)\\ =&\varphi_0(x)+B(x,cg)=\varphi_{cg}(x).\end{aligned}$$

Thus $(\varphi_c)^g=\varphi_{cg}$. Therefore, for all $c \in V$, we have $\lambda_{\varphi_0}(c)^g=(\varphi_c)^g=\varphi_{cg}=\lambda_{\varphi_0}(cg)$. By Lemma 3.9, λ_{φ_0} maps elements of $\operatorname{sing}(\varphi_0)$ into $\mathcal{Q}^\varepsilon$ and since [**54**, Theorem 1.41] gives $|\operatorname{sing}(\varphi_0)|=|\mathcal{Q}^\varepsilon|$, it follows that λ_{φ_0} induces a bijection from $\operatorname{sing}(\varphi_0)$ to $\mathcal{Q}^\varepsilon$. $\square$

Corollary 3.11

The action of X on $\mathcal{Q}$ is permutationally isomorphic to the action of X on the collection $\{\operatorname{sing}(\varphi) \subset V \mid \varphi \in \mathcal{Q}\}$.

Proof. This should not be surprising since each quadratic form in $\mathcal{Q}$ is uniquely determined by its singular vectors. However, we show directly that for all $g \in X$ we have

$$\begin{aligned}\operatorname{sing}(\varphi^g) &= \{x \in V \mid \varphi^g(x)=0\}=\{x \in V \mid \varphi(xg^{-1})=0\}\\ &= \{xg \in V \mid \varphi(x)=0\}=\operatorname{sing}(\varphi)^g.\end{aligned}$$

□

Corollary 3.12
Let $\varphi_0, \varphi_d \in \mathcal{Q}$ with $d \in V$. Let $c \in V$. For all $g \in X$, if $\varphi_0^g = \varphi_d$ then $\varphi_c^g = \varphi_{cg+d}$.

Proof. For all $\varphi_c \in \mathcal{Q}$ and $g \in X$ satisfying $\varphi_0^g = \varphi_d$ we have

$$\begin{aligned}\varphi_c^g(x) =& \varphi_0(xg^{-1}) + B(xg^{-1}, c) \\ =& \varphi_d(x) + B(x, cg) \\ =& \varphi_0(x) + B(x, cg + d)\end{aligned}$$

so $\varphi_c^g = \varphi_{cg+d}$ as claimed. □

Note that if $g \in X_{\varphi_0}$ then Corollary 3.12 reduces to $\varphi_c^g = \varphi_{cg}$, as in Lemma 3.10.

Lemma 3.13
For all $\varphi_0, \varphi_c \in \mathcal{Q}$ we have $\mathrm{sing}(\varphi_0) \cap \mathrm{sing}(\varphi_c) = \mathrm{sing}(\varphi_0) \cap \langle c\rangle^\perp$, and if $\phi_0 \in \mathcal{Q}^\epsilon$ with $\epsilon \in \{+,-\}$ then

$$|\mathrm{sing}(\varphi_0) \cap \mathrm{sing}(\varphi_c)| = \begin{cases} 2^{n-1}(2^{n-1} + \varepsilon) & \text{if } c \in \mathrm{sing}(\varphi_0) \\ 2^{2n-2} & \text{if } c \notin \mathrm{sing}(\varphi_0) \end{cases}$$

Proof. If $x \in \mathrm{sing}(\varphi_0)$ then $\varphi_c(x) = \varphi_0(x) + B(x,c) = B(x,c)$. Therefore $x \in \mathrm{sing}(\varphi_0) \cap \mathrm{sing}(\varphi_c)$ if and only $x \in \mathrm{sing}(\varphi_0) \cap \langle c\rangle^\perp$. Let $\varphi \in \mathcal{Q}$ and $c \in V$. Then for all $g \in X$ we have

$$\begin{aligned}(\mathrm{sing}(\varphi) \cap \langle c\rangle^\perp)^g &= \{xg \in V \mid \varphi(x) = 0 \text{ and } B(x,c) = 0\} \\ &= \{x \in V \mid \varphi(xg^{-1}) = 0 \text{ and } B(xg^{-1}, c) = 0\} \\ &= \{x \in V \mid \varphi^g(x) = 0 \text{ and } B(x, cg) = 0\} \\ &= \mathrm{sing}(\varphi^g) \cap \langle cg\rangle^\perp. \end{aligned} \tag{3.12}$$

Since X acts transitively on $\mathcal{Q}^\varepsilon$, Equation (3.12) implies that in order to determine the cardinality of $\mathrm{sing}(\varphi_0) \cap \langle c\rangle^\perp$, we may choose the most convenient form $\phi_0 \in \mathcal{Q}^\epsilon$ for our computations. Further, X_{φ_0} acts transitively on $\mathcal{Q}^\varepsilon \backslash \{\varphi_0\}$ and [**35**, subcase 3.2.4e] implies X_{φ_0} acts transitively on $\mathcal{Q}^{-\varepsilon}$, therefore the cardinality of $|\mathrm{sing}(\varphi_0) \cap \langle c\rangle^\perp|$ depends only on whether or not $c \in \mathrm{sing}(\varphi_0)$. Therefore, we let $\{e_i, f_i \mid 1 \leqslant i \leqslant n\}$ be a symplectic basis for V and, without loss of generality, for all $x = \sum_{i=1}^n (x_i e_i + y_i f_i) \in V$ we define $\phi_0 \in \mathcal{Q}^\epsilon$ by

$$\varphi_0(x) = \begin{cases} \sum_{i=1}^n x_i y_i & \text{if } \varepsilon = + \\ x_n + y_n + \sum_{i=1}^n x_i y_i & \text{if } \varepsilon = - \end{cases}$$

With $x = \sum_{i=1}^n (x_i e_i + y_i f_i)$, consider the following subcases:

(a) If $c = e_1$ then $\varphi_0(c) = 0$ and $\langle c\rangle^\perp = \langle e_i, f_j \mid 1 \leqslant i \leqslant n, 2 \leqslant j \leqslant n\rangle$. If $x \in \langle c\rangle^\perp$ then $y_1 = 0$ and therefore $|\operatorname{sing}(\varphi_0) \cap \langle c\rangle^\perp|$ is the number of vectors in $\langle c\rangle^\perp$ for which

$$\sum_{i=2}^{n} x_i y_i = 0, \text{ if } \epsilon = +$$

$$\sum_{i=2}^{n} x_i y_i + x_n + y_n = 0, \text{ if } \epsilon = -.$$

In particular, since $x_1 \in \mathbb{F}_2$, $|\operatorname{sing}(\varphi_0) \cap \langle c\rangle^\perp|$ is twice the number of ε-type quadratic forms which polarise to a symplectic form on a $(2n-2)$-dimensional vector space over $\mathbb{F}_2$. That is, $|\operatorname{sing}(\varphi_0) \cap \langle c\rangle^\perp| = 2^{n-1}(2^{n-1} + \varepsilon)$.

(b) If $c = e_1 + f_1$ then $\varphi_0(c) = 1$ and $\langle c\rangle^\perp = \langle e_1 + f_1, e_i, f_i \mid 2 \leqslant i \leqslant n\rangle$. If $x \in \langle c\rangle^\perp$ then $x_1 = y_1 = \lambda$ and $|\operatorname{sing}(\varphi_0) \cap \langle c\rangle^\perp|$ is the number of vectors for which

$$\sum_{i=2}^{n} x_i y_i + \lambda = 0, \text{ if } \epsilon = + \tag{3.13}$$

$$\sum_{i=2}^{n} x_i y_i + x_n + y_n + \lambda = 0, \text{ if } \epsilon = -. \tag{3.14}$$

If $\lambda = 0$ then equations (3.13) and (3.14) have $2^{n-2}(2^{n-1} + \epsilon)$ solutions. If $\lambda = 1$ then equations (3.13) and (3.14) have $2^{2(n-1)} - 2^{n-2}(2^{n-1} + \epsilon)$ solutions. Upon summing these values, we find $|\operatorname{sing}(\varphi_0) \cap \langle c\rangle^\perp| = 2^{2n-2}$.

This completes the proof. $\square$

CHAPTER 4

Reducible codeword stabilisers

Problem: Let G be a reducible subgroup of $X = \mathrm{Sp}_{2n}(2)$. Classify the X-strongly incidence transitive codes $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ with $X_{\Delta} \cong G$ for all $\Delta \in \Gamma$.

4.1. Introduction

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic vector space and let $X \cong \mathrm{Sp}_{2n}(2)$ be the isometry group of the symplectic form B. We denote by $\mathcal{Q}^{\varepsilon}$ the set of all ε-type quadratic forms on V which polarise to B. In Chapter 4 we classify the strongly incidence-transitive codes with point set $\mathcal{Q}^{\varepsilon}$ under the assumption that the stabiliser G of a codeword fixes a nontrivial proper subspace of V. By Theorem 2.31, we may choose a basis $\{e_1, f_1, \ldots, e_n, f_n\}$ for V such that if $x, x' \in V$ with $x = \sum_{i=1}^{n}(x_i e_i + y_i f_i)$ and $x' = \sum_{i=1}^{n}(x'_i e_i + y'_i f_i)$ then
$$B(x, x') = \sum_{i=1}^{n} x_i y'_i + y_i x'_i.$$
In particular, $B(e_i, e_j) = B(f_i, f_j) = 0$ for all $i, j \in [1:n]$, and $B(e_i, f_j) = 1$ if $i = j$ and 0 otherwise. We refer to $\{e_1, f_1, \ldots, e_n, f_n\}$ as a *symplectic basis*. We open with some descriptions of codes whose codeword stabilisers act reducibly on V.

Construction 4.1
Choose $\epsilon, \epsilon' \in \{+, -\}$ and $n, d \in \mathbb{Z}$, with $n \geqslant 2$ and $1 \leqslant d \leqslant n-1$. We construct a family of codes $\Gamma(n, d, \epsilon, \epsilon')$ in $J(\mathcal{Q}^{\epsilon}, k)$ as follows. Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space. For each $2d$-dimensional nondegenerate subspace U, define a codeword $\Delta(U)$ whose elements are all quadratic forms $\phi \in \mathcal{Q}^{\epsilon}$ such that $\varphi|_U$ is of type ε' and $\varphi|_{U^{\perp}}$ is of type $\varepsilon\varepsilon'$. We have, $k = |X : X_U| = 2^n(2^d + \epsilon')(2^{n-d} + \epsilon\epsilon')$.

Construction 4.2
Choose $\epsilon \in \{+, -\}$, $c = 0$ or 1 and $n, d \in \mathbb{Z}$ with $n \geqslant 2$, $1 \leqslant d \leqslant n$ and $(d, \varepsilon) \neq (n, -)$. We construct a family of codes $\Gamma(n, d, \epsilon, c)$ in $J(\mathcal{Q}^{\epsilon}, k)$ as follows. Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space. For each d-dimensional totally-isotropic subspace U we define a codeword $\Delta(U) = \{\phi \in \mathcal{Q}^{\epsilon} \mid \dim(\mathrm{sing}(\phi) \cap U) = d - c\}$. We have $k = |X : X_U| = 2^{n-1}(2^{n-d} + \varepsilon)$.

Our main theorem for Chapter 4 is as follows.

Theorem 4.3 (Main Theorem)
Let Γ be a code in $J(\mathcal{Q}^{\epsilon}, k)$, where $|\mathcal{Q}^{\epsilon}| \geqslant 4$ and $3 \leqslant k \leqslant |\mathcal{Q}^{\varepsilon}| - 3$. Suppose that $X = \mathrm{Sp}_{2n}(2) =$

$\mathrm{Aut}(\Gamma) \cap \mathrm{Sym}(\mathcal{Q}^{\varepsilon})$. Let Δ be a codeword and suppose that the stabiliser of Δ is a geometric subgroup of $\mathrm{Sp}_{2n}(2)$. Then Γ is X-strongly incidence-transitive if and only if it arises from Construction 4.1 or 4.2.

Remark 4.4
If Γ is a nonempty subset of $\binom{\mathcal{Q}^{\epsilon}}{k}$ with $k \in \{1, 2, |\mathcal{Q}^{\epsilon}| - 1, |\mathcal{Q}^{\epsilon}| - 2\}$ then we may deduce from the fact that X acts 2-transitively on $\mathcal{Q}^{\epsilon}$ that $\Gamma = \binom{\mathcal{Q}^{\epsilon}}{k}$. We consider these examples trivial and therefore we set $3 \leqslant k \leqslant |\mathcal{Q}^{\epsilon}| - 3$ in Theorem 4.3.

4.2. Stabiliser of a nondegenerate subspace

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic vector space and let U be a nontrivial proper nondegenerate subspace of V of dimension $2d$. Note that U is nondegenerate if and only if $U^{\perp}$ is nondegenerate, so without loss of generality we may assume that $\dim(U) \leqslant n$. We denote the setwise stabiliser of U by X_U. By [**38**, pg. 84], we have $X_U \cong \mathrm{Sp}(U) \times \mathrm{Sp}(U^{\perp})$. Theorem 1.18 states that X_U is a maximal subgroup of X unless $\dim(U) = n$; for if $\dim(U) = n$ then $\mathrm{Sp}(U) \times \mathrm{Sp}(U^{\perp}) < (\mathrm{Sp}(U) \times \mathrm{Sp}(U^{\perp})) \times \mathbb{Z}_2 < \mathrm{Sp}_{2n}(2)$, where the order 2 element in $\mathbb{Z}_2$ swaps U and $U^{\perp}$. The subgroup $(\mathrm{Sp}(U) \times \mathrm{Sp}(U^{\perp})) \times \mathbb{Z}_2$ is maximal in $\mathrm{Sp}_{2n}(2)$. Recall that a subspace $U \leqslant V$ is nondegenerate if and only if $V = U \oplus U^{\perp}$. If U is nondegenerate then $\dim(U)$ is even and we usually write $\dim(U) = 2d$ for some $1 \leqslant d \leqslant n-1$. If U is a nondegenerate subspace of V then B_U denotes the restriction of B to $U \times U$. If $\phi \in \mathcal{Q}^{\epsilon}$ then ϕ_U denotes the restriction of ϕ to U. We denote by $\mathcal{Q}_U^{\epsilon}$ the set of all Boolean quadratic forms on U which polarise to B_U.

Definition 4.5
Let U and W be nondegenerate subspaces of V with $U \cap W = \{0\}$.

(a) For each $v, v' \in U \oplus W$ with $v = u + w$ and $v' = u' + w'$ we define $B = B_U \oplus B_W$ by
$$B(v, v') = B_U(u, u') + B_W(w, w').$$
(b) For each $v \in U \oplus W$ with $v = u + w$ we define $\phi = \phi_U \oplus \phi_W$ by
$$\phi(v) = \phi_U(u) + \phi_W(w).$$

Lemma 4.6
Let U and W be nondegenerate subspaces of U with $U \cap W = \{0\}$. Let $(\phi_U, \phi_W) \in \mathcal{Q}_U^{\epsilon} \times \mathcal{Q}_W^{\epsilon'}$ and let B_U and B_W denote the polar forms of ϕ_U and ϕ_W. Then $\phi_U \oplus \phi_W$ is a quadratic form of type $\epsilon\epsilon'$ on $U \oplus W$ which polarises to $B_U \oplus B_W$.

PROOF. Follows from [**38**, Proposition 2.5.11]. $\square$

Lemma 4.7
The setwise stabiliser X_U consists of all block diagonal matrices with diagonal $(A, B) \in \mathrm{Sp}(U) \times \mathrm{Sp}(U^\perp)$.

PROOF. Let $\{e_1, f_1, \ldots, e_d, f_d\}$ be an ordered basis for U and let $\{e_{d+1}, f_{d+1}, \ldots, e_n, f_n\}$ be an ordered basis for $U^\perp$. When written with respect to the bases above, the elements of $\mathrm{GL}\, 2n(2)$ which stabilise U setwise are block diagonal with blocks $(R, S) \in \mathrm{GL}_{2d}(2) \times \mathrm{GL}_{2(n-d)}(2)$. The Gram matrix $\mathcal{J}$ for B is block diagonal with n blocks of the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Let $\mathcal{J}_U$ denote the Gram matrix for the restriction B_U, and similarly for $U^\perp$. Invoking the requirement that $M = (R, S) \in \mathrm{Sp}_{2n}(2)$, which can be written as $M\mathcal{J}M^T = \mathcal{J}$, we have

$$\begin{pmatrix} R & O \\ O & S \end{pmatrix} \begin{pmatrix} \mathcal{J}_U & O \\ O & \mathcal{J}_{U^\perp} \end{pmatrix} \begin{pmatrix} R^T & O \\ O & S^T \end{pmatrix} = \begin{pmatrix} R\mathcal{J}_U R^T & O \\ O & S\mathcal{J}_{U^\perp} S^T \end{pmatrix} = \begin{pmatrix} \mathcal{J}_U & O \\ O & \mathcal{J}_{U^\perp} \end{pmatrix}. \tag{4.1}$$

Equation (4.1) holds if and only if $(R, S) \in \mathrm{Sp}_{2d}(2) \times \mathrm{Sp}_{2(n-d)}(2)$. $\square$

Proposition 4.8
Choose $\epsilon, \epsilon' \in \{+, -\}$, $n \geqslant 2$ and let U be a $2d$-dimensional nondegenerate subspace of $V = \mathbb{F}_2^{2n}$ with $1 \leqslant d \leqslant n-1$. Let $\Delta = \{\varphi \in \mathcal{Q}^\varepsilon(V) \mid \varphi_U \in \mathcal{Q}_U^{\varepsilon'}\}$. Then X_U is transitive on $\Delta \times \overline{\Delta}$ and thus the output of Construction 4.1 is an X-strongly incidence-transitive code in $J(\mathcal{Q}^\epsilon, k)$ with $k = 2^{n-2}(2^d + \epsilon')(2^{n-d} + \epsilon\epsilon')$.

PROOF. Let U be a non-degenerate subspace of V so that $V = U \oplus U^\perp$ and $X_U \cong \mathrm{Sp}(U) \times \mathrm{Sp}(U^\perp)$. Lemmas 4.6 and 2.32 imply that for all $\varphi \in \mathcal{Q}^\varepsilon$ there exist unique $(\varphi_U, \varphi_{U^\perp}) \in \mathcal{Q}_U^{\epsilon'} \times \mathcal{Q}_{U^\perp}^{\epsilon\epsilon'}$ such that $\varphi = \varphi_U \oplus \varphi_{U^\perp}$. Since $\mathrm{Sp}(U)$ and $\mathrm{Sp}(U^\perp)$ act transitively in their respective Jordan-Steiner actions on $\mathcal{Q}_U^{\varepsilon'}$ and $\mathcal{Q}_{U^\perp}^{\varepsilon\varepsilon'}$, it is immediate that X_U acts transitively on $\Delta \times \overline{\Delta}$ for each $\varepsilon' \in \{+, -\}$. Moreover, Lemma 1.17 implies that $X_\Delta = X_U$. Witt's Lemma implies X is transitive on the set of nondegenerate subspaces of V of a given dimension, and therefore taking the orbit of Δ under the action of X yields the output of Construction 4.1. Finally, applying the Orbit-Stabiliser Theorem we have

$$\begin{aligned} k = |X_U : X_{U,\varphi}| &= \frac{|\mathrm{Sp}_{2d}(2)|}{|\mathrm{GO}_{2d}^{\epsilon'}(2)|} \frac{|\mathrm{Sp}_{2(n-d)}(2)|}{|\mathrm{GO}_{2(n-d)}^{\epsilon\epsilon'}(2)|} \\ &= 2^{d-1}(2^d + \epsilon') \cdot 2^{n-d-1}(2^{n-d} + \epsilon\epsilon') \\ &= 2^{n-2}(2^d + \epsilon')(2^{n-d} + \epsilon\epsilon'). \end{aligned}$$

Therefore the output of Construction 4.1 is an X-strongly incidence-transitive code in $J(\mathcal{Q}^\epsilon, k)$ with $k = 2^{n-2}(2^d + \epsilon')(2^{n-d} + \epsilon\epsilon')$. $\square$

4.3. Stabiliser of a totally isotropic subspace

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic vector space and let $X = \mathrm{Sp}_{2n}(2)$. Let U be a totally isotropic d-dimensional subspace of V, where $1 \leqslant d \leqslant n$, and let X_U denote the setwise stabiliser of U in X. By Witt's Theorem, X acts transitively on the set of totally isotropic d-dimensional subspaces of V and therefore the stabilisers of the d-dimensional totally isotropic subspace of V lie in a single conjugacy class of X. Without loss of generality we may choose a symplectic basis $\{e_i, f_i \mid 1 \leqslant i \leqslant n\}$ for V and then set $U = \langle e_i \mid 1 \leqslant i \leqslant d\rangle$. In particular, if $x, x' \in V$ are given by $x = \sum_{i=1}^{n}(x_i e_i + y_i f_i)$ and $x' = \sum_{i=1}^{n}(x'_i e_i + y'_i f_i)$, then

$$B(x, x') = \sum_{i=1}^{n} x_i y'_i + y_i x'_i.$$

In order to prove Theorem 4.3 we will need to investigate the structure of X_U and some subgroups in detail. We begin by calculating the setwise stabiliser of U in coordinates. It is convenient to order our basis as follows:

$$\mathscr{B} = \{e_1, \ldots, e_d, e_{d+1}, f_{d+1}, \ldots, e_n, f_n, f_1, \ldots, f_d\}. \tag{4.2}$$

Lemma 4.9

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space and $X = \mathrm{Sp}_{2n}(2)$. Choose $d \in [1 : n]$ and set $U = \langle e_1, \cdots, e_d\rangle$. Then the setwise stabiliser X_U consists of all $2n \times 2n$ matrices M of the form

$$M = \begin{pmatrix} A & 0 & 0 \\ Y & B & 0 \\ X & Z & C \end{pmatrix}$$

which satisfy the following conditions:

(i) $A \in \mathrm{GL}_d(2)$,
(ii) $B \in \mathrm{Sp}_{2(n-d)}(2)$,
(iii) $C = A^{-T}$,
(iv) $XC^T + CX^T = ZJZ^T$, and
(v) $CY^T = ZJB^T$.

where J is the $2(n-d) \times 2(n-d)$ block-diagonal matrix with blocks $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. In particular, C and Y are determined uniquely by Z, B and A.

Proof. We work with respect to the basis $\mathscr{B}$ defined in Equation (4.2). Any matrix $M \in \mathrm{Sp}_{2n}(2)$ which fixes U necessarily fixes $U^\perp = \langle e_1, \cdots, e_d, e_{d+1}, f_{d+1}, \cdots, e_n, f_n\rangle$. Therefore M must be of the form

$$M = \begin{pmatrix} A & 0 & 0 \\ Y & B & 0 \\ X & Z & C \end{pmatrix}$$

where A and C lie in $\mathrm{GL}_d(2)$, B lies in $\mathrm{GL}_{2(n-d)}(2)$, and X, Y and Z are respectively $d \times d$, $2(n-d) \times d$ and $d \times 2(n-d)$ matrices. The Gram matrix of B with respect to $\mathscr{B}$ is

$$\mathcal{J} = \begin{pmatrix} 0 & 0 & I_d \\ 0 & J & 0 \\ I_d & 0 & 0 \end{pmatrix}$$

where I_d is a $d \times d$ identity matrix and J is the $2(n-d) \times 2(n-d)$ block-diagonal matrix with blocks $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. By definition, $M \in \mathrm{Sp}_{2n}(2)$ if and only if $M\mathcal{J}M^T = \mathcal{J}$. We have

$$\begin{aligned} M\mathcal{J}M^T &= \begin{pmatrix} A & 0 & 0 \\ Y & B & 0 \\ X & Z & C \end{pmatrix} \begin{pmatrix} 0 & 0 & I_d \\ 0 & J & 0 \\ I_d & 0 & 0 \end{pmatrix} \begin{pmatrix} A^T & Y^T & X^T \\ 0 & B^T & Z^T \\ 0 & 0 & C^T \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & A \\ 0 & BJ & Y \\ C & ZJ & X \end{pmatrix} \begin{pmatrix} A^T & Y^T & X^T \\ 0 & B^T & Z^T \\ 0 & 0 & C^T \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & AC^T \\ 0 & BJB^T & BJZ^T + YC^T \\ CA^T & CY^T + ZJB^T & CX^T + XC^T + ZJZ^T \end{pmatrix}. \end{aligned}$$

Invoking the condition $\mathcal{J} = M\mathcal{J}M^T$, we have

$$\begin{pmatrix} 0 & 0 & I_d \\ 0 & J & 0 \\ I_d & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & AC^T \\ 0 & BJB^T & BJZ^T + YC^T \\ CA^T & CY^T + ZJB^T & CX^T + XC^T + ZJZ^T \end{pmatrix}.$$

Therefore $M \in \mathrm{Sp}_{2n}(2)$ if and only if conditions (i)-(v) hold. □

Lemma 4.10 below describes the structure of X_U as a semidirect product $X_U = R \rtimes L$. This is called a *Levi decomposition* with *Levi component* L and *unipotent radical* R.

Lemma 4.10 ([**38**], pg. 93)
Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space with basis $\mathscr{B}$ and U a totally isotropic d-dimensional subspace of V. Then there exist subspaces U' and W of V such that the following hold:

(a) U' is totally isotropic of dimension d, $U \oplus U'$ is nondegenerate, $W = (U \oplus U')^{\perp}$ and $V = (U \oplus U') \oplus W$,
(b) $X_U = R \rtimes L$, where L fixes setwise each of the subspaces U, U' and W, and R acts trivially on the spaces U, $U^{\perp}/U$ and $V/U^{\perp}$,
(c) $L \cong \mathrm{GL}(U) \times \mathrm{Sp}(W)$.

It is sometimes helpful to view the subspaces W and U' as embeddings of the quotient spaces $V/(U \oplus U')$ and $V/U^{\perp}$ inside V. Working with respect to $\mathscr{B}$, if $U = \langle e_i \mid 1 \leqslant i \leqslant d \rangle$ then we set $U' = \langle f_i \mid 1 \leqslant i \leqslant d \rangle$ and $W = \langle e_i, f_i \mid d+1 \leqslant i \leqslant n \rangle$.

Corollary 4.11
Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space with basis $\mathscr{B}$ and $X = \mathrm{Sp}_{2n}(2)$. Choose $d \in [1 : n]$ and set

$U = \langle e_1, \cdots, e_d \rangle$. The Levi component L and the unipotent radical R of X_U are given by

$$L = \left\{ \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & A^{-T} \end{pmatrix} \mid A \in \mathrm{GL}_d(2), B \in \mathrm{Sp}_{2(n-d)}(2) \right\}$$

$$R = \left\{ \begin{pmatrix} I_d & 0 & 0 \\ Y & I_{2(n-d)} & 0 \\ X & Z & I_d \end{pmatrix} \mid X + X^T = ZJZ^T, Y = JZ^T \right\}.$$

Proof. We have $U = \langle e_1, \ldots, e_d \rangle$. Let $U' = \langle f_1, \cdots, f_d \rangle$ and $W = \langle e_{d+1}, f_{d+1}, \cdots, e_n, f_n \rangle$. It is clear that property (a) of Lemma 4.10 holds. Suppose $M \in X_U$. Then Lemma 4.9 implies

$$M = \begin{pmatrix} A & 0 & 0 \\ Y & B & 0 \\ X & Z & C \end{pmatrix} = \begin{pmatrix} I_d & 0 & 0 \\ YA^{-1} & I_{2(n-d)} & 0 \\ XA^{-1} & ZB^{-1} & I_d \end{pmatrix} \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & A^{-T} \end{pmatrix} \tag{4.3}$$

so $X_U = RL$ and $R \cap L = \{I_{2n}\}$. Finally $R \lhd X_U$, so $X_U \cong R \rtimes L$. $\square$

4.3.1. The X_Δ orbits in $\mathcal{Q}^\varepsilon$ for U totally-isotropic

Lemma 4.12
Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space with basis $\mathscr{B}$ and U a totally isotropic d-dimensional subspace of V with $1 \leqslant d \leqslant n$. Then:

(a) For all $\varphi \in \mathcal{Q}^\varepsilon$ the intersection $\mathrm{sing}(\varphi) \cap U$ is a subspace of U. Moreover, $\dim(\mathrm{sing}(\varphi) \cap U) = d$ if U is φ-singular and $\dim(\mathrm{sing}(\varphi) \cap U) = d - 1$ otherwise.
(b) Define $\mathcal{Q}^\varepsilon_d := \{\varphi \in \mathcal{Q}^\varepsilon \mid U \subseteq \mathrm{sing}(\varphi)\}$ and $\mathcal{Q}^\varepsilon_{d-1} := \{\varphi \in \mathcal{Q}^\varepsilon \mid U \nsubseteq \mathrm{sing}(\varphi)\}$. Fix $\varphi_0 \in \mathcal{Q}^\varepsilon_d$ and let $c \in V$. Then $\varphi_c \in \mathcal{Q}^\varepsilon_d$ if and only if $c \in \mathrm{sing}(\varphi_0) \cap U^\perp$.
(c) X_U acts transitively on $\mathcal{Q}^\varepsilon_d$.

Proof. We have the following:

(a) Let $u, v \in U$. Since $U \leqslant U^\perp$ we have

$$\varphi(u + v) = \varphi(u) + \varphi(v) + B(u, v) = \varphi(u) + \varphi(v). \tag{4.4}$$

In particular, if $u, v \in \mathrm{sing}(\varphi) \cap U$ then Equation (4.4) implies $\varphi(u+v) = 0$ and therefore $\mathrm{sing}(\varphi) \cap U$ is a subspace. Moreover, Equation (4.4) implies that the restriction $\varphi|_U : U \to \mathbb{F}_2$ is a linear transformation and therefore $\dim(\varphi(U)) = 0$ or 1, depending on whether or not U is totally φ-singular. In particular, the Rank-Nullity Theorem implies $\dim(\mathrm{sing}(\varphi) \cap U) = d$ or $d - 1$.

(b) Lemma 3.9 implies $c \in \mathrm{sing}(\varphi_0)$. By definition we have

$$\varphi_c \in \mathcal{Q}^\varepsilon_d \Leftrightarrow U \subseteq \mathrm{sing}(\varphi_c) \Leftrightarrow U \subseteq \mathrm{sing}(\varphi_0) + c \Leftrightarrow U + c \subseteq \mathrm{sing}(\varphi_0).$$

But $U + c \subseteq \mathrm{sing}(\varphi_0)$ if and only if

$$\varphi_0(u + c) = 0 \text{ for all } u \in U. \tag{4.5}$$

Expanding Equation (4.5) using the polarisation identity and using the fact that $\varphi_0(u) = \varphi_0(c) = 0$, we have $\varphi(u + c) = B(u, c) = 0$. Therefore $\varphi_c \in \mathcal{Q}_d^\varepsilon$ if and only if $c \in \mathrm{sing}(\varphi_0) \cap U^\perp$.

(c) For each $c \in V$, the involution $\tau_c : V \to V$ defined by $x\tau_c = x + B(x, c)c$ is an element of X (see [**32**, Section 7.7]). If $c \in U^\perp$ then for all $u \in U$ we have $u\tau_c = u + B(u, c)c = u$, so τ_c fixes U pointwise. Calculating φ^{τ_c} we have

$$\varphi_0^{\tau_c}(x) = \varphi_0(x + B(x, c)c) = \varphi_0(x) + B(x, c)\varphi_0(c) + B(x, c)^2 = \varphi_0(x) + B(x, c) = \varphi(x). \tag{4.6}$$

Therefore X_U is transitive on $\mathcal{Q}_d^\varepsilon$.

□

Lemma 4.12 implies $\mathcal{Q}^\varepsilon$ is the disjoint union of $\mathcal{Q}_d^\varepsilon$ and $\mathcal{Q}_{d-1}^\varepsilon$. If $(d, \varepsilon) = (n, -)$ then $\mathcal{Q}_d^-$ is empty; this case is given extra attention in Section 4.4. Otherwise both $\mathcal{Q}_d^\varepsilon$ and $\mathcal{Q}_{d-1}^\varepsilon$ are nonempty. We will see in Lemma 4.21 that X_U also acts transitively on $\mathcal{Q}_{d-1}^\varepsilon$.

4.3.2. Maximal parabolic subgroups of orthogonal groups

By [**5**, Theorem 3.11 and Theorem 3.12], the maximal $\mathcal{C}_1$ subgroups of the orthogonal group $\mathrm{GO}^\varepsilon(\varphi) \cong \mathrm{GO}_{2n}^\varepsilon(2)$ which stabilise a totally-singular d-subspace U of V have shape $X_{\varphi,U} \cong 2^{d(d-1)/2}.2^{2d(n-d)}(\mathrm{GL}_d(2) \times \mathrm{GO}_{2(n-k)}^\varepsilon(2))$. In Section 4.3.2 we describe a subgroup of the maximal parabolic subgroups of X_φ which assists in the proof of Lemma 4.22.

Let x be a vector in V with coordinates defined by $x = \sum_{i=1}^n (x_i e_i + y_i f_i)$. We denote by φ_0^ε the quadratic form

$$\varphi_0^\varepsilon(x) = \begin{cases} \sum_{i=1}^n x_i y_i & \text{if } \varepsilon = +, \\ \sum_{i=1}^n x_i y_i + x_n^2 + y_n^2 & \text{if } \varepsilon = -. \end{cases} \tag{4.7}$$

The Gram matrix of φ_0^ε with respect to the ordered basis $\mathscr{B}$ is a $2n \times 2n$ matrix

$$K = \begin{pmatrix} 0 & 0 & I_d \\ 0 & K^\varepsilon & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{4.8}$$

where K^ε is the $2(n-d) \times 2(n-d)$ matrix

$$K^+ = \begin{pmatrix} 0 & 1 & & & \\ 0 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 0 & 0 \end{pmatrix} \quad \text{or} \quad K^- = \begin{pmatrix} 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 0 & 0 & & \\ & & & & & 1 & 1 \\ & & & & & 0 & 1 \end{pmatrix}. \tag{4.9}$$

Provided that $(d, \varepsilon) \neq (n, -)$, we have $\varphi_0^\varepsilon \in \mathcal{Q}_d^\varepsilon$.

Lemma 4.13
Let $H = \{M \in L \mid BK^\varepsilon B^T = K^\varepsilon\}$ where K^ε is the matrix defined by Equation (4.9) and

$$M = \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & A^{-T} \end{pmatrix}.$$

Then H is a subgroup of $L \cap \mathrm{GO}(\varphi_0^\varepsilon)$, where L denotes the Levi factor of X_U.

Proof. Consider the quadratic forms φ_0^ε defined by Equation (4.7) and their associated Gram matrices K, as defined in Equation (4.8). First we will show that every $M \in H$ fixes φ_0^ε by checking the sufficient condition $MKM^T = K$. We find

$$\begin{aligned} MKM^T &= \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & A^{-T} \end{pmatrix} \begin{pmatrix} 0 & 0 & I_d \\ 0 & K^\varepsilon & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} A^T & 0 & 0 \\ 0 & B^T & 0 \\ 0 & 0 & A^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & A \\ 0 & BK^\varepsilon & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} A^T & 0 & 0 \\ 0 & B^T & 0 \\ 0 & 0 & A^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & I_d \\ 0 & BK^\varepsilon B^T & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & I_d \\ 0 & K^\varepsilon & 0 \\ 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Therefore $MKM^T = K$ if and only if $BK^\varepsilon B^T = K^\varepsilon$ if and only if $M \in H$. In particular, $H \subseteq L \cap \mathrm{GO}(\varphi_0^\varepsilon)$. If $M, M' \in L \cap \mathrm{GO}(\varphi_0^\varepsilon)$ then

$$MM'^{-1} = \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & A^{-T} \end{pmatrix} \begin{pmatrix} A'^{-1} & 0 & 0 \\ 0 & B'^{-1} & 0 \\ 0 & 0 & A'^{T} \end{pmatrix} = \begin{pmatrix} AA'^{-1} & 0 & 0 \\ 0 & BB'^{-1} & 0 \\ 0 & 0 & A^{-T}A'^{T} \end{pmatrix}.$$

We have $(BB'^{-1})K^\varepsilon(BB'^{-1})^T = BB'^{-1}K^\varepsilon B'^{-T}B = K^\varepsilon$. Therefore $MM'^{-1} \in L \cap \mathrm{GO}(\varphi_0^\varepsilon)$ and $H \leqslant L \cap \mathrm{GO}(\varphi_0^\varepsilon)$. ∎

Note that this condition $MKM^T = K$ in the proof of Lemma 4.13 is sufficient but certainly not necessary; each quadratic form $\varphi \in \mathcal{Q}$ has a unique *lower-triangular* Gram matrix, but despite fixing φ in the Jordan-Steiner actions, the action of $\mathrm{GO}(\varphi)$ does not preserve this matrix in general.

4.3.3. A subgroup of X_U which acts regularly on the nonzero elements of $V/U^\perp$

In this section we use the multiplicative group of a finite field of order 2^d to construct a cyclic subgroup of X_U of order $2^d - 1$. To this end, we construct an element of $\mathrm{GL}_d(2)$ of order $2^d - 1$ and embed the cyclic group it generates in the Levi component of X_U. We show in Corollary 4.20 that this subgroup acts regularly on the non-zero elements of the quotient vector space $V/U^{\perp}$. Let us first recall some basic facts about finite fields.

Theorem 4.14 ([**55**], Theorem 2.1.63)
Let $\mathbb{F}$ be a field and $\mathbb{K}$ be a subfield with $\alpha \in \mathbb{F}$ algebraic of degree d over $\mathbb{K}$ and let h be the minimal polynomial of α over $\mathbb{K}$. Then

(a) The field $\mathbb{K}[\alpha]$ is isomorphic to the factor ring $\mathbb{K}[x]/\langle h\rangle$.
(b) The dimension of $\mathbb{K}[\alpha]$ over $\mathbb{K}$ is d.
(c) The set $\{\alpha^i \mid 0 \leqslant i \leqslant d-1\}$ is a basis for $\mathbb{K}[\alpha]$ over $\mathbb{K}$.
(d) Every element of $\mathbb{K}[\alpha]$ is algebraic over $\mathbb{K}$ with degree dividing d.

Definition 4.15 ([**55**], Definition 4.1.1)
An element $\alpha \in \mathbb{F}_q$ is a *primitive element* if α generates the multiplicative group $\mathbb{F}_q^{\times}$ of nonzero elements in $\mathbb{F}_{q^d}$.

Definition 4.16 ([**55**], Definition 4.1.2)
A polynomial $f \in \mathbb{F}_q[x]$ of degree $d \geqslant 1$ is a *primitive polynomial* if it is the minimal polynomial of a primitive element of $\mathbb{F}_q$.

Construction 4.17
Let α be a primitive element in $\mathbb{F}_{2^d}$ and let $h(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$ be the minimal polynomial of α. As a vector space over $\mathbb{F}_2$, we have $\mathbb{F}_{2^d} = \left\{\sum_{i=0}^{d-1} c_i\alpha^i \mid c_i \in \mathbb{F}_2\right\}$. Define an invertible linear transformation $f : \mathbb{F}_{2^d} \to \mathbb{F}_2^d$ by

$$f : \sum_{i=0}^{d-1} c_i\alpha^i \mapsto (c_0, ..., c_{d-1}). \tag{4.10}$$

The multiplicative group $\mathbb{F}_{2^d}^{\times}$ acts on $\mathbb{F}_{2^d}$ by multiplication modulo $h(x)$. Therefore, we obtain a faithful linear representation $\rho : \mathbb{F}_{2^d}^{\times} \to \mathrm{SL}_d(2)$ by setting

$$\rho(\alpha) = \begin{pmatrix} f(\alpha^1) \\ f(\alpha^2) \\ \vdots \\ f(\alpha^d) \end{pmatrix} = \begin{pmatrix} 0 & & & \\ \vdots & & I_{d-1} & \\ 0 & & & \\ a_0 & a_1 & \dots & a_{d-1} \end{pmatrix} \tag{4.11}$$

where a_i are the coefficients of the minimal polynomial for α. The subgroup $\langle\rho(\alpha)\rangle < \mathrm{SL}_d(2)$ is called a *Singer subgroup* and its generator $\rho(\alpha)$ is called a *Singer cycle*.

Lemma 4.18
Let s be the $2n \times 2n$ matrix defined by

$$s = \begin{pmatrix} \rho(\alpha)^{-T} & 0 & 0 \\ 0 & I_{2(n-d)} & 0 \\ 0 & 0 & \rho(\alpha) \end{pmatrix}.$$

and set $S = \langle s \rangle$. Then S is a subgroup of the Levi factor of X_U, S fixes a quadratic form and $|S| = 2^d - 1$.

Proof. Let $S = \langle s \rangle$. Since α is a primitive element of $\mathbb{F}_{2^d}^{\times} \cong C_{2^d-1}$, it follows from Construction 4.17 that S is cyclic of order $2^d - 1$. By Corollary 4.11, $S \leqslant X_U$ and by Lemma 4.13, $S \leqslant \mathrm{GO}(\varphi_0^{\varepsilon})$. $\square$

4.3.4. Proof of strong incidence-transitivity in the totally-isotropic case

Lemma 4.19
Let $S = \langle s \rangle$ denote the subgroup of X_U defined in Lemma 4.18. The action of S on $V/U^{\perp}$ is permutationally isomorphic to the action of $\mathbb{F}_{2^d}^{\times}$ on $\mathbb{F}_{2^d}$ by multiplication.

Proof. Let x denote a primitive element of $\mathbb{F}_{2^d}^{\times}$ and let $r(x) = \sum_{i=0}^{d-1} a_i x^i$ be its minimal polynomial. We choose bases $\{x^i \mid 0 \leqslant i \leqslant d-1\}$ and $\{f_j + U^{\perp} \mid 1 \leqslant j \leqslant d\}$ for $\mathbb{F}_{2^d}^{\times}$ and $V/U^{\perp}$, respectively. Define a mapping $\widetilde{f} : \mathbb{F}_{2^d} \to V/U^{\perp}$ by setting $\widetilde{f}(x^i) = f_{i+1} + U^{\perp}$ for $0 \leqslant i \leqslant d-1$ and extending linearly to $\mathbb{F}_{2^d}^{\times}$. Then $\widetilde{\rho}$ is an isomorphism between $\mathbb{F}_2$-vector spaces by construction. Similarly, we define $\widetilde{\rho} : \mathbb{F}_{2^d}^{\times} \to S$ by $\widetilde{\rho}(x^i) = s^i$. Then $\widetilde{\rho}$ is a group isomorphism by construction. We consider now the natural action of $\mathbb{F}_{2^d}^{\times}$ on $\mathbb{F}_{2^d}$ by multiplication modulo $r(x)$. For all $\sum_{i=0}^{d-1} c_i x^i \in \mathbb{F}_{2^d}$ we have

$$\begin{aligned} \left(\sum_{i=0}^{d-1} c_i x^i\right)^{x\widetilde{f}} &= \left(\sum_{i=0}^{d-2} c_i x^{i+1} + c_{d-1} \sum_{i=0}^{d-1} a_i x^i\right)^{\widetilde{f}} \\ &= \left(\sum_{i=0}^{d-2} c_i f_{i+2} + c_{d-1} \sum_{i=0}^{d-1} a_i f_{i+1}\right) + U^{\perp} \\ &= \left(\sum_{i=0}^{d-1} c_i f_{i+1} + U^{\perp}\right)^{s} \\ &= \left(\sum_{i=0}^{d-1} c_i x^i\right)^{\widetilde{f}s}. \end{aligned}$$

Suppose $g \in \mathbb{F}_{2^d}^{\times}$. Then $g = x^j$ where $0 \leqslant j \leqslant 2^d - 1$. Successively applying the equality $x\widetilde{f} = \widetilde{f}s$ we have $g\widetilde{f} = x^{j-1}\widetilde{f}s = \cdots = \widetilde{f}s^j = \widetilde{f}g^{\widetilde{\rho}}$ as required. $\square$

Corollary 4.20
The Singer subgroup $S = \langle s \rangle$ acts regularly on the nontrivial cosets of $V/U^{\perp}$.

Proof. The group $\mathbb{F}_{2^d}^{\times}$ acts regularly on itself by multiplication so the permutational isomorphism constructed in Lemma 4.19 implies S regularly on the nontrivial cosets of $V/U^{\perp}$. $\square$

Lemma 4.21
If $\varepsilon = +$ and $1 \leqslant d \leqslant n$, or $\varepsilon = -$ and $1 \leqslant d \leqslant n-1$, then X_U is transitive on the set $\mathcal{Q}^{\varepsilon}_{d-1} = \{\varphi \in \mathcal{Q}^{\varepsilon} \mid U \nsubseteq \operatorname{sing}(\varphi)\}$.

Proof. Let $\varphi_0 \in \mathcal{Q}^{\varepsilon}_{d}$ and $\psi, \psi' \in \mathcal{Q}^{\varepsilon}_{d-1}$. By Lemma 3.9 there exist $c, c' \in V$ such that for all $x \in V$

$$\psi(x) = \varphi(x) + B(x,c), \quad \psi'(x) = \varphi(x) + B(x,c'). \tag{4.12}$$

Corollary 4.20 says $\langle s \rangle \leqslant X_{U,\varphi_0}$ acts transitively on $V/U^{\perp}$. Therefore, we may assume that c and c' lie in the same coset of $V/U^{\perp}$. In this case $c + c' \in U^{\perp}$ so the symplectic transvection $\tau_{c+c'}$ maps ψ to ψ' and stabilises U. $\square$

The possibility that $d = n$ and $\varepsilon = -$ was excluded from Lemma 4.21. In this case $\mathcal{Q}^{-}_{n-1} = \mathcal{Q}^{-}$ and $\mathcal{Q}^{-}_{n} = \varnothing$ since the maximum dimension of a subspace which is totally singular with respect to an elliptic quadratic form is $n-1$. We study this exception in Section 4.4, demonstrating that X_U acts transitively on $\mathcal{Q}^{-}$ and performing further analysis.

In order to demonstrate transitivity 'inside' the nontrivial cosets of $V/U^{\perp}$ it is necessary to examine the unipotent radical. Recall that, by Lemma 4.22, $G = X_U$ is transitive on $\mathcal{Q}^{\varepsilon}_{d}$, and by Lemma 4.19 and Corollary 4.20, G_{φ_0} is transitive on $(V/U^{\perp})^{\#}$.

For $w \in V$ we set $[w] := w + U^{\perp}$, the image of w under the natural projection map $\pi : V \to V/U^{\perp}$.

Lemma 4.22
Fix $\varphi_0 \in \mathcal{Q}^{\varepsilon}_{d}$ and let $G = X_U$, $w \in \operatorname{sing}(\varphi_0) \cap (V \backslash U^{\perp})$. Then the stabiliser $G_{\varphi_0,[w]}$ acts transitively on $\operatorname{sing}(\varphi_0) \cap [w]$.

Proof. Let $w \in \operatorname{sing}(\varphi_0) \cap (V \backslash U^{\perp})$. The goal is to map w to an arbitrary element $u + w \in \operatorname{sing}(\varphi_0) \cap [w]$. Let $x = \sum_{i=1}^{n} (x_i e_i + y_i f_i) \in V$. By Lemma 4.12, X_U is transitive on $\mathcal{Q}^{\varepsilon}_{d}$ so without loss of generality we choose $\varphi_0 = \varphi^{\varepsilon}_{0}$ as defined in Equation (4.7). By Lemma 4.18 and Corollary 4.20, G_{φ_0} acts transitively on $\left(V/U^{\perp}\right)^{\#}$ so without loss of generality we choose $w = f_1$. Let $u = \sum_{i=1}^{n} u_i e_i + \sum_{i=d+1}^{n} v_i \in U^{\perp}$ and consider the matrix

$$g = \begin{pmatrix} I & 0 & 0 \\ Y & I & 0 \\ X & Z & I \end{pmatrix}$$

where X, Y, Z are defined by

$$X = \begin{pmatrix} u_1 & u_2 & \dots & u_d \\ u_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ u_d & 0 & \dots & 0 \end{pmatrix}, Z = \begin{pmatrix} u_{d+1} & v_{d+1} & \cdots & u_n & v_n \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, Y = JZ^T.$$

and J is the $2(n-d) \times 2(n-d)$ block-diagonal matrix with blocks $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

By Lemma 4.11, $g \in R$ if and only if $X + X^T = ZJZ^T$. Since the matrix X is symmetric, $X + X^T$ is the $d \times d$ matrix of zeroes, $\mathbf{0}_{d\times d}$. Computing ZJZ^T, we have

$$ZJZ^T = \begin{pmatrix} u_{d+1} & v_{d+1} & \cdots & u_n & v_n \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{pmatrix} \begin{pmatrix} u_{d+1} & 0 & \cdots & 0 \\ v_{d+1} & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ u_n & 0 & \cdots & 0 \\ v_n & 0 & \cdots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} v_{d+1} & u_{d+1} & \cdots & v_n & u_n \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} u_{d+1} & 0 & \cdots & 0 \\ v_{d+1} & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ u_n & 0 & \cdots & 0 \\ v_n & 0 & \cdots & 0 \end{pmatrix} = \mathbf{0}_{d\times d}.$$

Therefore $g \in R$. In particular, g is symplectic, stabilises both U and $[w]$, and maps $w = f_1$ to $u + w$. Thus $g \in X_{U,[w]}$. It remains to confirm that g fixes φ_0 in each case $\varepsilon = \pm$. With respect to the basis $\mathscr{B}$ in Equation (4.2), x^g is given by

$$x^g = \left(x_1 + \sum_{i=1}^{n} u_i y_i + \sum_{i=d+1}^{n} v_i x_i \right) e_1 + \sum_{i=1}^{d} y_i f_i + \sum_{i=d+1}^{n} (y_i + y_1 v_i) f_i + \sum_{i=2}^{n} (x_i + y_1 u_i) e_i.$$

Evaluating $\varphi_0^+(x^g)$ and noting that $y^2 = y$ for $y \in \mathbb{F}_2$, we get

$$\begin{aligned} \varphi_0^+(x^g) =& x_1 y_1 + y_1 \left(\sum_{i=1}^{n} u_i y_i + \sum_{i=d+1}^{n} v_i x_i \right) + \sum_{i=2}^{d} (x_i y_i + y_1 u_i y_i) \\ &+ \sum_{i=d+1}^{n} x_i y_i + y_1 \sum_{i=d+1}^{n} (v_i x_i + u_i y_i + y_1 u_i v_i) \\ =& \varphi_0^+(x) + y_1 \left(u_1 + \sum_{i=d+1}^{n} u_i v_i \right) \\ =& \varphi_0^+(x) + y_1 \varphi_0^+(u + f_1) \end{aligned}$$

Similarly, evaluating $\varphi_0^-(x^g)$ we get

$$\begin{aligned}\varphi_0^-(x^g) =& x_1y_1 + y_1\left(\sum_{i=1}^{n} u_iy_i + \sum_{i=d+1}^{n} v_ix_i\right) + \sum_{i=2}^{d}(x_iy_i + y_1u_iy_i)\\ &+ \sum_{i=d+1}^{n} x_iy_i + y_1\sum_{i=d+1}^{n}(v_ix_i + u_iy_i + u_iv_i) + x_n + y_n + y_1(u_n + v_n)\\ =& \varphi_0^-(x) + y_1\left(u_1 + \sum_{i=d+1}^{n} u_iv_i + u_n + v_n\right)\\ =& \varphi_0^-(x) + y_1\varphi_0^-(u + f_1)\end{aligned}$$

For both values of ε we have assumed $u + f_1 \in \mathrm{sing}(\varphi_0^\varepsilon)$, so $y_1\varphi_0^\varepsilon(u + f_1) = 0$. Therefore $\varphi_0^\varepsilon(x^g) = \varphi_0^\varepsilon(x)$ for all $x \in V$, so $\varphi_0^g = \varphi_0$. $\square$

Theorem 4.23

Let $V = (\mathbb{F}_2^n, B)$ be a symplectic space with symplectic basis $\mathscr{B}$ and $U = \langle e_i \mid 1 \leqslant i \leqslant d\rangle$ with $1 \leqslant d \leqslant n$ and $(d, \varepsilon) \neq (n, -)$. Let $\Delta = \mathcal{Q}_d^\varepsilon$ and $\Gamma := \Delta^X$. Then Γ is an X-strongly incidence-transitive code with $X = \mathrm{Sp}_{2n}(2)$.

Proof. By Lemma 4.9, X_U acts transitively on Δ, so it is sufficient to choose any $\varphi_0 \in \Delta$ and show that X_{Δ,φ_0} acts transitively on $\overline{\Delta}$. Let $\psi, \psi' \in \overline{\Delta}$. By Lemma 3.9, there exists unique $c, c' \in \mathrm{sing}(\varphi_0) \cap \left(V \backslash U^\perp\right)$ such that $\psi(x) = \varphi_c(x) = \varphi_0(x) + B(x, c)$ and $\psi'(x) = \varphi_{c'} = \varphi_0(x) + B(x, c')$. Further, Lemma 3.10 implies it is sufficient to show that there exists an element of X_{φ_0} which maps c to c'. Indeed, by Lemma 4.20, $X_{U,\varphi'}$ acts transitively on $\left(V/U^\perp\right)^\#$, so there exists $g \in X_{\Delta,\varphi_0}$ such that $cg \in \mathrm{sing}(\varphi_0) \cap [c']$. Since $cg, c' \in \mathrm{sing}(\varphi_0) \cap [c']$, Lemma 4.22 implies there exists $h \in X_{U,\varphi_0,[c']}$ such that $cgh = c'$. Therefore gh fixes φ_0 and maps φ_c to $\varphi_{c'}$, that is, Γ is X-strongly incidence-transitive. $\square$

Remark 4.24

If Γ is an X-strongly incidence-transitive code in $J(\mathcal{Q}^\varepsilon, k)$ with $\Delta \in \Gamma$ and X_Δ reducible on V, [**38**] shows that X_Δ is contained in the full setwise stabiliser of a nondegenerate or totally-isotropic subspace of V. In particular, Γ corresponds to one of the codes described in Theorem 4.3, or X_Δ is contained in the full setwise stabiliser of a totally isotropic subspace of dimension n and $\varepsilon = -$. We show in Section 4.4 that no further examples arise in the latter case.

4.4. Parabolic subgroups acting transitively on elliptic forms

We now consider the case $(d, \varepsilon) = (n, -)$. Fix the following notation throughout Section 4.4. Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space, let U be an n-dimensional totally isotropic subspace of V and let X_U be the stabiliser of U in $X = \mathrm{Sp}_{2n}(2)$. Note that since $\dim(U) = n$ we have $U = U^\perp$. For $\varphi \in \mathcal{Q}^-$ the maximum dimension of a totally φ-singular subspace is $n - 1$, and therefore Lemma 4.12 implies $\mathrm{sing}(\varphi) \cap U$ is an $(n-1)$-dimensional subspace of V for all $\varphi \in \mathcal{Q}^-$.

By [**35**], there is a factorisation $X = X_U\,\mathrm{GO}_{2n}^-(2)$ and therefore Lemma 1.14 implies that X_U acts transitively on $\mathcal{Q}^-$. In Section 4.4 we show that if $\Gamma \subset \binom{\mathcal{Q}^-}{k}$ is an X-strongly incidence-transitive code with $\Delta \in \Gamma$ and $X_\Delta \leqslant X_U$, then X_Δ leaves invariant a subspace of V of dimension less than n, and therefore Γ corresponds to one of the codes described in Theorem 4.3.

Recall from Lemma 4.11 that $X_U \cong R \rtimes L$, where R is the unipotent radical and $L \cong \mathrm{GL}_n(2)$ is the Levi factor. In particular, setting $n = d$ in Corollary 4.11 we have

$$R = \left\{ \begin{pmatrix} I_d & 0 \\ X & I_d \end{pmatrix} \mid X + X^T = 0 \right\}$$

so $R \cong \mathbb{F}_2^{n(n+1)/2}$ and $|R| = 2^{n(n+1)/2}$.

Lemma 4.25

Let U be a totally-isotropic n-dimensional subspace of V and let $\mathcal{H}$ denote the set of all $(n-1)$-dimensional subspaces of U. For each $H \in \mathcal{H}$ we define $P_H := \{\varphi \in \mathcal{Q}^- \mid \mathrm{sing}(\varphi) \cap U = H\}$. Then:

(a) If $H \in \mathcal{H}$ and $\varphi_0 \in P_H$ then $\varphi_c \in P_H$ if and only if $c \in \mathrm{sing}(\varphi_0) \cap U$. In particular, $|P_H| = 2^{n-1}$.

(b) The collection $\mathcal{P} = \{P_H \mid H \in \mathcal{H}\}$ is a system of imprimitivity for the action of X_U on $\mathcal{Q}^-$.

(c) P_H is an R-orbit for each $P_H \in \mathcal{P}$.

(d) The action of L on $\mathcal{P}$ is permutationally isomorphic to the transitive action of $\mathrm{GL}(U)$ on $\mathcal{H}$.

Proof. We proceed as follows:

(a) Let $H \in \mathcal{H}$, $\varphi_0 \in P_H$ and $\varphi_c \in \mathcal{Q}^-$. Then

$$\varphi_c \in P_H \Leftrightarrow H = \mathrm{sing}(\varphi_c) \cap U \Leftrightarrow \mathrm{sing}(\varphi_0) \cap U = \mathrm{sing}(\varphi_c) \cap U \tag{4.13}$$

$$\Leftrightarrow \mathrm{sing}(\varphi_0) \cap U = \mathrm{sing}(\varphi_0) \cap \mathrm{sing}(\varphi_c) \cap U. \tag{4.14}$$

By Lemma 3.13, $\mathrm{sing}(\varphi_0) \cap \mathrm{sing}(\varphi_c) = \mathrm{sing}(\varphi_0) \cap \langle c\rangle^\perp$, so using Equation (4.14) we deduce

$$\varphi_c \in P_H \Leftrightarrow \mathrm{sing}(\varphi_0) \cap U = \mathrm{sing}(\varphi_0) \cap U \cap \langle c\rangle^\perp \Leftrightarrow \mathrm{sing}(\varphi_0) \cap U \leqslant \langle c\rangle^\perp \Leftrightarrow c \in \mathrm{sing}(\varphi_0) \cap U. \tag{4.15}$$

Therefore $\varphi_c \in P_H$ if and only if $c \in \mathrm{sing}(\varphi_0) \cap U$. In particular, $|P_H| = |\mathrm{sing}(\varphi_0) \cap U| = 2^{n-1}$.

(b) Lemma 4.12 implies that $\mathcal{P}$ is a partition of $\mathcal{Q}^-$ and part (a) implies $|P_H| = 2^{n-1}$ for each $H \in \mathcal{H}$. Therefore $|\mathcal{P}| = |\mathcal{Q}^-|/|P_H| = 2^n - 1$. In particular, $\mathcal{P}$ is a partition of $\mathcal{Q}^-$ into equally sized parts. For all $H \in \mathcal{H}$ and for all $g \in X_U$ we have

$$\begin{aligned}(P_H)^g &= \{\varphi^g \in \mathcal{Q}^- \mid \mathrm{sing}(\varphi) \cap U = H\} = \{\varphi \in \mathcal{Q}^- \mid \mathrm{sing}(\varphi^{g^{-1}}) \cap U = H\} \\ &= \{\varphi \in \mathcal{Q}^- \mid \mathrm{sing}(\varphi)^{g^{-1}} \cap U = H\}\end{aligned}$$

where the last equality follows from Corollary 3.11. Since $g \in X_U$ we have

$$\mathrm{sing}(\varphi)^{g^{-1}} \cap U = H \Leftrightarrow (\mathrm{sing}(\varphi) \cap U)^{g^{-1}} = H \Leftrightarrow \mathrm{sing}(\varphi) \cap U = H^g$$

from which we deduce

$$(P_H)^g = P_{H^g} \tag{4.16}$$

Since X_U is transitive on $\mathcal{Q}^-$, it follows that $\mathcal{P}$ is a system of imprimitivity preserved by X_U.

(c) By Lemma 4.12, for all $c \in \operatorname{sing}(\varphi_0) \cap U$ the symplectic transvection $\tau_c : V \to V$ defined by $x^{\tau_c} = x + B(x,c)c$ lies in X_U. Moreover, for all cosets $x + U \in V/U$ we have $(x+U)^{\tau_c} = x + B(x,c)c + U = x + U$, since $c \in U$. In particular, τ_c fixes U and V/U pointwise, so Lemma 4.10 implies that if $c \in \operatorname{sing}(\varphi_0) \cap U$ then $\tau_c \in R$.

Consider an arbitrary $H \in \mathcal{H}$ with $\varphi_0, \varphi_c \in P_H$. Then part (a) implies $c \in \operatorname{sing}(\varphi_0) \cap U$. Computing $\varphi_0^{\tau_c}$ and expanding using the polarisation equation, we have

$$\varphi_0^{\tau_c}(x) = \varphi_0(x + B(x,c)c) = \varphi_0(x) + B(x,c)\phi(c) + B(x, B(x,c)c) \tag{4.17}$$

$$= \varphi_0(x) + B(x,c) = \varphi_c(x). \tag{4.18}$$

Since $|\operatorname{sing}(\varphi_0) \cap U| = 2^{n-1}$, Equation (4.17) implies that the length of an R-orbit in $\mathcal{Q}^-$ is at least 2^{n-1}. On the other hand, X_U is transitive on $\mathcal{Q}^-$ and $R \lhd X_U$ so R the R-orbits in $\mathcal{Q}^-$ all have the same length. Therefore $|\varphi_0^R|$ divides both $|R| = 2^{n(n+1)/2}$ and $|\mathcal{Q}^-| = 2^{n-1}(2^n - 1)$, so the length of an R-orbit is at most 2^{n-1}. Therefore P_H is an R-orbit for each $H \in \mathcal{H}$.

(d) Let $\{e_i, f_i \mid 1 \leqslant i \leqslant n\}$ be a symplectic basis for V. Without loss of generality we assume $U = \langle e_i \mid 1 \leqslant i \leqslant n\rangle$. Let $W = \langle f_i \mid 1 \leqslant i \leqslant n\rangle$ and note that $V = U \oplus W$. We identify $v \in V$ with an ordered pair (u,w) with $u \in U$ and $w \in W$. By Corollary 4.11, for all $\ell \in L$ there exists $a \in \mathrm{GL}_n(2)$ such that $\ell = \begin{pmatrix} a & 0 \\ 0 & a^{-T} \end{pmatrix}$. Therefore for all $\ell \in L$ and $v \in V$ we have $v^\ell = (u,w)^\ell = (ua, wa^{-T})$ and therefore for $H \in \mathcal{H}$ we have

$$H^\ell = \{(u,0)^\ell \in U \mid u \in H\} = \{(ua,0) \in U \mid u \in H\} = H^a. \tag{4.19}$$

Define $F : \mathrm{GL}_n(2) \to L$ by $F(a) = \ell$ and $f : \mathcal{H} \to \mathcal{P}$ by $f(H) = P_H$. Clearly F is a group isomorphism and f is a bijection. Using equations (4.19) and (4.16), for all $H \in \mathcal{H}$ and $\ell \in L$ we have

$$f(H^a) = P_{H^a} = P_{(Ha, 0a^{-T})} = P_{H^\ell} = (P_H)^\ell = f(H)^{F(a)}.$$

Therefore the pair (F,f) is a permutational isomorphism.

□

Lemma 4.26
Let $\Gamma \subset \binom{\mathcal{Q}^-}{k}$ be a strongly incidence-transitive code with $\Delta \in \Gamma$ and let U be a totally isotropic n-dimensional subspace of V. If $X_\Delta < X_U$ then Γ corresponds to one of the codes constructed in Theorem 4.3.

Proof. Suppose $\Gamma \subset \binom{\mathcal{Q}^-}{k}$ is an X-strongly incidence-transitive code, $\Delta \in \Gamma$ and $X_\Delta < X_U$. We show that there exists a nontrivial proper X_Δ-invariant subspace of U. By Lemma 4.25 the R-orbits in $\mathcal{Q}^-$ form a system of imprimitivity preserved by X_U so Lemma 1.21 implies that Δ and $\overline{\Delta}$ are unions of R-orbits and $R < X_\Delta$. Therefore there exists $\mathcal{S} \subset \mathcal{H}$ such that $\Delta = \cup_{H \in \mathcal{S}} P_H$. We define $\check{\Gamma} \subset \binom{\mathcal{P}}{k/2^{n-1}}$ as follows. Let $\check{\Delta} = \{P_H \mid H \in \mathcal{S}\}$ and define $\check{\Gamma} = \check{\Delta}^L$. We claim that $\check{\Gamma}$ is L-strongly incidence-transitive. Indeed, since Γ is X-strongly incidence-transitive, X_Δ acts transitively on Δ and preserves $\mathcal{P}$, therefore L_Δ permutes the elements of $\check{\Delta}$ transitively. Similarly, L_Δ is transitive on $\mathcal{P} \backslash \check{\Delta}$. Now suppose $\Sigma_0 \in \check{\Delta}$ and $\Sigma, \Sigma' \in \mathcal{P} \backslash \check{\Delta}$. Choose any $\varphi_0, \varphi, \varphi' \in \mathcal{Q}^-$ such that $\varphi_0 \in \Sigma_0, \varphi \in \Sigma$ and

$\varphi' \in \Sigma'$. Since Γ is X-strongly incidence-transitive there exists $h \in X_{\Delta,\varphi_0}$ such that $\varphi' = \varphi^h$. But $X_\Delta < X_U$ so X_Δ preserves $\mathcal{P}$ and $X_{\Delta,\varphi_0} < X_{\Delta,\Sigma_0}$. Therefore there exists $\ell \in Rh \cap L_\Delta$ such that $\Sigma' = \Sigma^\ell$ and $\breve{\Gamma}$. By definition, L is transitive on $\breve{\Gamma}$ and therefore $\breve{\Gamma}$ is L-strongly incidence-transitive as claimed.

However, by Lemma 4.25, the action of L on $\mathcal{P}$ is permutationally isomorphic to the action of $\mathrm{GL}_n(2)$ on the $(n-1)$-dimensional subspaces of U and Example 2.7 shows that the action of $\mathrm{GL}_n(2)$ on the $(n-1)$-subspaces of U is permutationally isomorphic to the action of $\mathrm{GL}_n(2)$ on the 1-dimensional subspaces of U. Therefore $\breve{\Gamma}$ is equivalent to a 'projective type code' as described in [**1**, Section 7]; the details are included in Section B.1. Since $q = 2$ does not have a square root in $\mathbb{Z}$, $\breve{\Gamma}$ does not correspond to one of the Baer subline codes constructed in Example B.2. Moreover, if Δ is a $[0,2,3]_1$-set as in part (ii) of Theorem B.4 then, since each line of $\mathrm{PG}_n(2)$ is incident with three points, $k \in \{1,2\}$ and Γ is trivial. The only other possibility is that $\breve{\Gamma}$ is equivalent to a subspace code as in case (i) of Theorem B.4. Therefore $L_\Delta < L_W$ for some proper nontrivial subspace $W < U$. By Lemma 4.10, R fixes U pointwise and therefore $R < X_W$, so $X_\Delta \leqslant X_W$ and therefore Γ corresponds to one of the codes described in Theorem 4.3. □

4.5. Design and code parameters

Let $V = (\mathbb{F}_2^n, B)$ be a symplectic space and $X = \mathrm{Sp}_{2n}(2)$ the associated isometry group. Let Γ be an X-strongly incidence-transitive code in $J(\mathcal{Q}^\varepsilon, k)$. Since X acts transitively on Γ and 2-transitively on $\mathcal{Q}^\varepsilon$, the codewords of Γ form a 2-design with $v = 2^{n-1}(2^n + \varepsilon)$ points. We compute some parameters associated with the designs constructed throughout Chapter 4.

Definition 4.27
Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space where $n \geqslant 2$. We denote by $\mathscr{T} = \mathscr{T}^\varepsilon(n,d)$ a 2-design with point set $\mathcal{V} = \mathcal{Q}^\varepsilon$. For each totally-isotropic d-dimensional subspace of V which satisfies $1 \leqslant d \leqslant n$ and $d \neq n$ if $\varepsilon = -$, we define a block $\Delta^\varepsilon(U)$ of $\mathscr{T}$ by

$$\Delta^\varepsilon(U) = \{\varphi \in \mathcal{Q}^\varepsilon \mid \varphi(u) = 0 \ \ \forall u \in U\}. \tag{4.20}$$

We compute the parameters (v,k,λ,r,b) associated with the designs $\mathscr{T}^\varepsilon(n,d)$.

Lemma 4.28
Consider the 2-design $\mathscr{T} = \mathscr{T}^\varepsilon(n,d)$ defined in Definition 4.27. The parameters of $\mathscr{T}$ are given by

$$\begin{aligned}
v &= 2^{n-1}(2^n + \varepsilon)\\
b &= \prod_{i=0}^{d-1} \frac{2^{2(n-i)} - 1}{2^{i+1} - 1}\\
k &= 2^{n-1}(2^{n-d} + \varepsilon)\\
r &= \begin{cases} \left(\prod_{i=0}^{n-1} \frac{2^{n-i}-1}{2^{i+1}-1}\right)\left(\prod_{j=n-d}^{n-1}(2^j+1)\right) & \text{if } \varepsilon = +\\ \left(\prod_{i=0}^{n-2} \frac{2^{n-i-1}-1}{2^{i+1}-1}\right)\left(\prod_{j=n-d+1}^{n}(2^j+1)\right) & \text{if } \varepsilon = - \end{cases}
\end{aligned}$$

PROOF. By Definition 4.27 we have $v = |\mathcal{Q}^\varepsilon| = 2^{n-1}(2^n+\varepsilon)$ and b is the number of totally-isotropic d-dimensional subspaces of V. Using equation (2.3), we have $b = \prod_{i=0}^{d-1} \frac{2^{2(n-i)}-1}{2^{i+1}-1}$. By Theorem 4.23, $\mathscr{T}$ is strongly incidence-transitive, and therefore X_Δ acts transitively on the points of Δ. If $\varphi \in \Delta$ then the Orbit-Stabiliser Theorem implies $k = |X_\Delta : X_{\Delta,\varphi}|$. We use Theorem 1.18 to compute the orders of X_Δ and $X_{\Delta,\varphi}$. If $\varphi \in \Delta \cap \mathcal{Q}^\varepsilon$ then

$$\begin{aligned}
k &= |X_U : X_{U,\varphi}| \\
&= \frac{q^{d(d+1)/2} q^{2d(n-d)} |\operatorname{GL}_d(2) \times \operatorname{Sp}_{2(n-d)}(2)|}{q^{d(d-1)/2} q^{2d(n-d)} |\operatorname{GL}_d(2) \times \operatorname{GO}^\varepsilon_{2(n-d)}(2)|} \\
&= \frac{q^{d(d+1)/2} |\operatorname{Sp}_{2(n-d)}(2)|}{q^{d(d-1)/2} |\operatorname{GO}^\varepsilon_{2(n-d)}(2)|} \\
&= 2^d \cdot 2^{n-d-1}(2^{n-d} + \varepsilon) \\
&= 2^{n-1}(2^{n-d} + \varepsilon).
\end{aligned}$$

Now, if $\varphi \in \mathcal{V}$ then φ is incident with $\Delta^\varepsilon(U)$ if and only if U is φ-singular. Therefore the replication number is given by the number of ε-type d-dimensional singular subspaces in V. Using equations (2.2) and (2.4) we have

$$r = \begin{cases} \left(\prod_{i=0}^{n-1} \frac{2^{n-i}-1}{2^{i+1}-1}\right)\left(\prod_{j=n-d}^{n-1} (2^j+1)\right) & \text{if } \varepsilon = + \\ \left(\prod_{i=0}^{n-2} \frac{2^{n-i-1}-1}{2^{i+1}-1}\right)\left(\prod_{j=n-d+1}^{n} (2^j+1)\right) & \text{if } \varepsilon = -. \end{cases} \tag{4.21}$$

□

Note that equation (1.3) can be used to calculate λ from the parameters of Lemma 4.28.

Lemma 4.29

Let $\epsilon \in \{\pm\}$ and for each totally-isotropic d-space in V define $\Delta(U) = \{\varphi \in \mathcal{Q}^\varepsilon \mid U \text{ is } \varphi\text{-singular}\}$. If U and W are totally isotropic d-spaces in V with $\dim(U \cap W) = d-1$ then $|\ \Delta(U)\ \cap\ \Delta(W)\ | = 2^{n-2}\left(2^{n-d}+\varepsilon\right)$. Moreover, the minimum distance of the code from Theorem 4.23 constructed from the totally-isotropic d-spaces in V has minimum distance $\delta = 2^{n-2}(2^{n-d}+\varepsilon)$

PROOF. By Witt's Theorem we choose a symplectic basis $\{e_i, f_i \mid 1 \leqslant i \leqslant n\}$ for V and set, without loss of generality,

$$\begin{aligned}
U &= \langle e_i, e_d \mid 1 \leqslant i \leqslant d-1 \rangle & \dim(U) &= d \\
W &= \langle e_i, f_d \mid 1 \leqslant i \leqslant d-1 \rangle & \dim(W) &= d \\
H &= \langle e_i, f_i \mid d+1 \leqslant i \leqslant n \rangle & \dim(H) &= 2(n-d).
\end{aligned}$$

Then we have

$$\begin{aligned}
U^\perp &= U \oplus H & \dim(U^\perp) &= 2n-d \\
W^\perp &= W \oplus H & \dim(W^\perp) &= 2n-d \\
U \cap W &= \langle e_i \mid 1 \leqslant i \leqslant d-1 \rangle & \dim(U \cap W) &= d-1.
\end{aligned}$$

Suppose $\varphi_0 \in \Delta(U) \cap \Delta(W)$ and $c \in V$. Then $\varphi_c \in \Delta(U) \cap \Delta(W)$ if and only if $c \in \mathrm{sing}(\varphi_0) \cap U^\perp \cap W^\perp$. Note that $U^\perp \cap W^\perp = (U \cap W) \oplus H$. Therefore if $c \in U^\perp \cap W^\perp$ then there exist $x \in U \cap W$ and $y \in H$ such that $c = x + y$. Using the fact that $x \in U \cap W$, $\varphi_0 \in \Delta(U) \cap \Delta(W)$ and $B(x, y) = 0$ we have

$$\varphi_0(c) = \varphi_0(x) + \varphi_0(y) + B(x, y) = \varphi_0(y).$$

Therefore we have $|U \cap W| = 2^{d-1}$ possible choices for x and, imposing the condition $\varphi_0|_H = 0$ on the $2(n-1)$-dimensional nondegenerate subspace U, $2^{n-d-1}(2^{n-d} + \varepsilon)$ possible choices for y. Therefore we have $|\Delta(U) \cap \Delta(W)| = 2^{d-1}2^{n-d-1}(2^{n-d} + \varepsilon) = 2^{n-2}(2^{n-d} + \varepsilon)$. Therefore $\delta = k - 2^{n-2}(2^{n-d} + \varepsilon) = 2^{n-1}(2^{n-d} + \varepsilon) - 2^{n-2}(2^{n-d} + \varepsilon) = (2^{n-1} - 2^{n-2})(2^{n-d} + \varepsilon) = 2^{n-2}(2^{n-d} + \varepsilon)$. $\square$

CHAPTER 5

Irreducible geometric codeword stabilisers

Problem: Let G be an irreducible subgroup of $X = \mathrm{Sp}_{2n}(2)$ of geometric Aschbacher type. Classify the X-strongly incidence transitive codes $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ with $X_{\Delta} = G$ for $\Delta \in \Gamma$.

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic vector space and let $X \cong \mathrm{Sp}_{2n}(2)$ be the isometry group of the symplectic form B. We denote by $\mathcal{Q}^{\varepsilon}$ the set of all ε-type quadratic forms on V which polarise to B. In Chapter 5 we demonstrate that there are no X-strongly incidence-transitive codes $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ with $\Delta \in \Gamma$ and X_{Δ} irreducible on V and of geometric Aschbacher type. In particular, by Theorem 1.18 we assume X_{Δ} lies in $\mathcal{C}_2, \mathcal{C}_3$ or $\mathcal{C}_8$. These classes are considered in Sections 5.1, 5.2 and 5.3 respectively.

Lemma 5.1
Let $X = \mathrm{Sp}_{2n}(2)$ and let $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ be an X-strongly incidence-transitive code with $2 \leqslant k \leqslant \frac{1}{2}|\mathcal{Q}^{\epsilon}|$. If X_{Δ} acts irreducibly on $V = \mathbb{F}_2^{2n}$ for some $\Delta \in \Gamma$ then $|\Delta| \geqslant 2n+1$ and $n \geqslant 3$.

Proof. Suppose $\varphi_0 \in \Delta$ and let $C = \{c \in V \mid \varphi_c \in \Delta\}$. Let U denote the intersection of all subspaces in V which contain C. Since X_{Δ} fixes Δ and U is the unique subspace of minimal dimension containing C, it follows that X_{Δ} fixes U. But X_{Δ} acts irreducibly on V and $|C| \geqslant 2$, so $U = V$ and $\langle C \rangle = V$. Therefore C contains the zero vector and a spanning set for V, which implies $|C| = |\Delta| \geqslant 2n+1$. In particular, the assumption $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^{\varepsilon}|$ gives $2n+1 \leqslant |\Delta| \leqslant 2^{n-2}(2^n + \varepsilon)$. If $n = 1$, or $(n, \varepsilon) = (2, -)$ then this condition is impossible to satisfy. If $(n, \varepsilon) = (2, +)$ then $2n+1 = 5 = 2^{n-2}(2^n+1)$ so $|\Delta| = 5$ and $|\Delta \times \overline{\Delta}| = 155$. However, $|\mathrm{Sp}_4(2)|$ is not divisible by 155 so this case must also be excluded. Therefore $n \geqslant 3$ and $|\Delta| \geqslant 2n+1$. □

5.1. Imprimitive subgroups

Let $\mathcal{D}$ denote a direct sum decomposition $V = \bigoplus_{i=1}^{t} V_i$ of V into nondegenerate subspaces V_i of dimension $\dim(V_i) = \frac{2n}{t}$ with V_i orthogonal to V_j for all $i \neq j$. The $\mathcal{C}_2$-subgroups of $\mathrm{Sp}_{2n}(2)$ are the stabilisers $X_{\mathcal{D}}$. It is demonstrated in [**38**] that such groups are maximal in $\mathrm{Sp}_{2n}(2)$ and have structure $X_{\mathcal{D}} = \mathrm{Sp}\left(\frac{2n}{t}, 2\right) \wr S_t$. In this section we compute the $X_{\mathcal{D}}$-orbits in $\mathcal{Q}^{\varepsilon}$ and apply the results to the classification of strongly incidence-transitive codes. We begin with some notation.

Definition 5.2
Let $\mathcal{D}$ denote a decomposition $V = \oplus_{i=1}^{t} V_i$ and let $\varphi : V \to \mathbb{F}_2$ be a quadratic form of type ε on V. Denote by $\varepsilon_i = sgn(V_i)$ the type of $\varphi|_{V_i}$, and write $\varepsilon_{\mathcal{D}} = (\varepsilon_1, \ldots, \varepsilon_t)$. Let $\mathcal{E}(\varphi)$ denote the number of i such that $\varepsilon_i = -$.

Lemma 5.3
The $X_{\mathcal{D}}-$orbits in $\mathcal{Q}^{\varepsilon}$ are the subsets $\mathcal{O}_m = \{\varphi \in \mathcal{Q}^{\varepsilon} \mid \mathcal{E}(\varphi) = m\}$ for all integers $0 \leqslant m \leqslant t$ such that $(-1)^m = \varepsilon$.

Proof. For every $\varphi \in \mathcal{Q}^{\varepsilon}$, Theorem 3.1 implies the groups $\mathrm{Sp}(V_i) \cong \mathrm{Sp}(\frac{2n}{t}, 2)$ preserve the types ε_i of the restrictions $\varphi_i = \varphi|_{V_i}$ for all $1 \leqslant i \leqslant t$. Moreover, the S_t component of $X_{\mathcal{D}}$ permutes the components V_i of the decomposition $\mathcal{D}$ and therefore permutes the entries of the vector $(\varepsilon_1, \ldots, \varepsilon_t)$ while preserving $\mathcal{E}(\varphi)$. This implies the subsets $\mathcal{O}_m$ are $X_{\mathcal{D}}-$invariant. It remains to show that $X_{\mathcal{D}}$ acts transitively on each non-empty subset $\mathcal{O}_m$. Let $\varphi, \varphi' \in \mathcal{O}_m$ have types $\varepsilon = \Pi_{i=1}^{t} \varepsilon_i$ and $\varepsilon' = \Pi_{i=1}^{t} \varepsilon_i'$ respectively. Since $\mathcal{E}(\varphi) = \mathcal{E}(\varphi')$ and S_t acts transitively on the m-subsets of $\{1, \ldots, t\}$, there exists $\sigma \in S_t$ such that $\varepsilon_{i^{\sigma^{-1}}} = \varepsilon_i'$ for all $1 \leqslant i \leqslant t$, and by Lemma 2.32, we can represent φ^{σ} uniquely as $\varphi_{1^{\sigma^{-1}}} \oplus \cdots \oplus \varphi_{t^{\sigma^{-1}}}$. Further, Theorem 3.1 implies that $\mathrm{Sp}(V_i)$ acts transitively on the quadratic forms on V_i of type $\varepsilon_i' = \varepsilon_{i^{\sigma^{-1}}}$ for each i, so there exists $g_i \in \mathrm{Sp}(V_i)$ such that $\varphi_{i^{\sigma^{-1}}}^{g_i} = \varphi_i'$. Therefore $\sigma(g_1, \ldots, g_t) \in X_{\mathcal{D}}$ maps φ to φ' and the non-empty $\mathcal{O}_m$ are the $X_{\mathcal{D}}$-orbits in $\mathcal{Q}^{\varepsilon}$. Finally $\mathcal{O}_m \neq \varnothing$ if and only if $(-1)^m = \varepsilon$. □

Corollary 5.4
Consider the direct sum decomposition $\mathcal{D}$ of $V = \oplus_{i=1}^{t} V_i$ and let $X_{\mathcal{D}}$ denote the stabiliser of $\mathcal{D}$ in $\mathrm{Sp}_{2n}(2)$.
(a) If $t \geqslant 4$ then $X_{\mathcal{D}}$ has at least three orbits in $\mathcal{Q}^{+}$.
(b) If $t \geqslant 5$ then $X_{\mathcal{D}}$ has at least three orbits in $\mathcal{Q}^{-}$.

Proof. By Lemma 5.3 we need only to check the number of integers m satisfying $(-1)^m = \varepsilon$ with $0 \leqslant m \leqslant t$. If $\varepsilon = +$ and $t \geqslant 4$ then $\mathcal{O}_m$ are non-empty orbits for $m \in \{0, 2, 4\}$. If $\varepsilon = -$ and $t \geqslant 5$ then $\mathcal{O}_m$ are non-empty orbits for $m \in \{1, 3, 5\}$. Therefore $X_{\mathcal{D}}$ has three or more orbits in $\mathcal{Q}^{\varepsilon}$ in either case. □

Remark 5.5
Lemma 5.3 implies that $X_{\mathcal{D}}$ has two orbits in $\mathcal{Q}^{\varepsilon}$ only in the following cases:
(i) $t = 2$ and $\varepsilon = +$, namely $\mathcal{O}_0$ and $\mathcal{O}_2$,
(ii) $t = 3$ and $\varepsilon = \pm$, namely $\mathcal{O}_0$ and $\mathcal{O}_2$ for $\varepsilon = +$, and $\mathcal{O}_1$ and $\mathcal{O}_3$ for $\varepsilon = -$,
(iii) $t = 4$ and $\varepsilon = -$, namely $\mathcal{O}_1$ and $\mathcal{O}_3$
while $X_{\mathcal{D}}$ acts transitively, that is, $\mathcal{O}_1 = \mathcal{Q}^{-}$, in the case
(iv) $t = 2$ and $\varepsilon = -$.

Lemma 5.6
Suppose that $X_{\Delta} \leqslant X_{\mathcal{D}}$ and X_{Δ} acts transitively on $\Delta \times \overline{\Delta}$. Then case (i) or (iv) of Remark 5.5 holds and moreover, X_{Δ} contains a reducible subgroup which acts transitively on $\Delta \times \overline{\Delta}$.

Proof. In case (i) we have $V = V_1 \oplus V_2$ with V_1 and V_2 both nondegenerate. By the definition of the Aschbacher class $\mathcal{C}_2$, $V_2 = V_1^{\perp}$. Since $X_{\mathcal{D}}$ has two orbits in $\mathcal{Q}^+$, $X_\Delta = X_{\mathcal{D}}$ and Remark 1.5 implies we may choose Δ to be either orbit. Thus we may assume $\Delta = \mathcal{O}_0$ and $\overline{\Delta} = \mathcal{O}_2$. Then by Lemma 5.3, $X_\Delta \cong X_{\mathcal{D}}$. Let $\varphi_0 \in \Delta$. Then $X_{\Delta,\varphi_0} \cong \mathrm{GO}^+(n,2) \times \mathrm{GO}^+(n,2)$. For all $\mu \in \overline{\Delta}$, Lemma 2.32 implies that there exist elliptic forms μ_1 and μ_2, on V_1 and V_2 respectively, such that $\mu = \mu_1 \oplus \mu_2$. By [**35**, Table 1], the expression $\mathrm{Sp}_{2m}(2) = \mathrm{GO}_{2m}^+ \, \mathrm{GO}_{2m}^-(2)$ is a group factorisation for all $m \geqslant 2$, and therefore Lemma 1.14 implies the orthogonal group acts transitively on quadratic forms of opposite type. Therefore Lemma 2.32 implies that for all $\mu, \nu \in \overline{\Delta}$, there exists $(g_1, g_2) \in X_{\Delta,\varphi_0}$ such that $\mu_i^{g_i} = \nu_i$ and therefore, Δ^X is indeed a strongly incidence transitive code. However, we note that Δ corresponds precisely to the codeword used to construct Γ in Lemma 4.8. In particular, the subgroup $X_{V_1} \cong \mathrm{Sp}(n,2) \times \mathrm{Sp}(n,2)$ of $X_{\mathcal{D}}$ is reducible and has the same orbits in $\mathcal{Q}^+$ as $X_{\mathcal{D}}$. Although the full stabiliser in $X_\Delta = X_{\mathcal{D}}$ gives us an example in this case, the subgroup $H = X_{\Delta,V_1}$ is reducible and by Lemma 4.8 is strongly incidence-transitive on $\mathcal{Q}^+$.

In case (ii) we have $V = V_1 \oplus V_2 \oplus V_3$ and $\varepsilon \in \{+,-\}$. By Remark 1.5 may assume that $\Delta \subset \mathcal{Q}^\varepsilon$ consists of quadratic forms satisfying $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon$, while $\overline{\Delta}$ consists of forms satisfying $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\} = \{\varepsilon, -\varepsilon, -\varepsilon\}$. Note that if $\varepsilon = -$ and $\dim(V_i) = 2$ then $|\overline{\Delta}| = 1$, so the corresponding code is degenerate. Since both $|\Delta|$ and $|\overline{\Delta}| > 1$, $\dim(V_i) \geqslant 3$ in the case $\varepsilon = -$. Let $\varphi \in \Delta$, $\mu \in \overline{\Delta}$ such that μ has type $(\varepsilon, -\varepsilon, -\varepsilon)$ and $\varphi|_{V_1} \neq \mu|_{V_1}$. Since $X_\Delta = X_{\mathcal{D}}$ acts transitively on $\Delta \times \overline{\Delta}$, Lemma 2.32 allows us to define uniquely a third form $\nu \in \overline{\Delta}$ such that $\nu|_{V_1} = \varphi|_{V_1}, \nu|_{V_2} = \mu|_{V_2}$ and $\nu|_{V_3} = \mu|_{V_3}$. If $X_{\mathcal{D}}$ acts transitively on $\Delta \times \overline{\Delta}$ then there exists $g \in X_{\mathcal{D},\varphi}$ such that $\mu^g = \nu$, in particular, $\mu^g|_{V_1} = \varphi|_{V_1}$. But g fixes φ and therefore g fixes V_1 so $(\varphi|_{V_1}) = \varphi|_{V_1}$. Therefore we have a contradiction.

Case (iii) is dealt with in a similar manner to case (ii): by Remark 1.5 we may assume $\Delta = \mathcal{O}_1$, $\overline{\Delta} = \mathcal{O}_3$ and $X_\Delta = X_{\mathcal{D}}$. Select $\varphi \in \Delta$ and $\mu \in \overline{\Delta}$ with respective types $(+,+,+,-)_{\mathcal{D}}$ and $(+,-,-,-)_{\mathcal{D}}$ such that $\varphi|_{V_1} \neq \mu|_{V_1}$. Using Lemma 2.32 we define a unique quadratic form $\nu \in \mathcal{Q}^-$ by $\nu = \varphi_1 \oplus \mu_2 \oplus \mu_3 \oplus \mu_4$, where ν_1 is not isometric to φ_1. By definition, $\nu \in \overline{\Delta}$. Suppose there exists $g \in X_{\mathcal{D},\varphi}$ such that $\mu^g = \nu$. Since elements of X preserve type, we must have $(\mu^g)|_{V_1} = \varphi|_{V_1}$. But g fixes φ and must therefore fix φ_1, a contradiction.

In case (iv) we have $X_{\mathcal{D}} \cong \mathrm{Sp}(n,2) \wr C_2$ acting transitively on $\mathcal{Q}^-$. The subgroup $X_{V_1} = \mathrm{Sp}(n,2) \times \mathrm{Sp}(n,2)$ is normal in $X_{\mathcal{D}}$ by definition of the wreath product. Lemma 4.8 implies X_{V_1} has two orbits in $\mathcal{Q}^-$, namely the forms of type $(+,-)_{\mathcal{D}}$ and forms of type $(-,+)_{\mathcal{D}}$. Since X_{V_1} is an intransitive normal subgroup of $X_{\mathcal{D}}$ the X_{V_1}-orbits in $\mathcal{Q}^-$ form a system of imprimitivity. Then Lemma 1.21 implies that Δ must be a union of blocks, but Δ is properly contained in $\mathcal{Q}^-$ so this implies Δ is an X_{V_1}-orbit. Therefore $X_\Delta = X_{V_1}$ is reducible. $\square$

Combining the results of Corollary 5.4 and Lemma 5.6 we conclude that the only examples of strongly-incidence transitive codes with $X_\Delta \leqslant X_{\mathcal{D}}$ for some decomposition $\mathcal{D}$ correspond to the reducible examples constructed in Section 4.

5.2. Field reduction subgroups

Let α denote a primitive element of $\mathbb{F}_{2^b}$. In Construction 4.17 we viewed $\mathbb{F}_{2^b}$ and $\mathbb{F}_2^b$ as b-dimensional vector spaces over $\mathbb{F}_2$ and constructed an $\mathbb{F}_2$-linear isomorphism $f : \mathbb{F}_{2^b} \to \mathbb{F}_2^b$ defined by

$$f : \sum_{i=0}^{b-1} \beta_i \alpha^i \mapsto (\beta_0, \beta_1, \ldots, \beta_{b-1}).$$

Let $W = \mathbb{F}_{2^b}^{2m}$ and $V = \mathbb{F}_2^{2mb}$. Define an invertible linear transformation $L : W \to V$ by

$$L : (w_1, w_2, \ldots, w_{2m}) \mapsto (f(w_1); f(w_2); \ldots; f(w_{2m})) \tag{5.1}$$

where the ';' symbol in Equation (5.1) represents vector concatenation.

For $v \in V$ and $g \in \Gamma\mathrm{L}_{2m}(2^b)$ we define an action of $\Gamma\mathrm{L}_{2m}(2^b)$ on V by

$$vg = L((L^{-1}(v)g). \tag{5.2}$$

The image of $\Gamma\mathrm{L}_{2m}(2^b)$ in $\mathrm{GL}_{2mb}(2)$ is a $\mathcal{C}_3$-subgroup and it is maximal if and only if b is prime [**38**]. We denote the image $X_{\mathcal{S}}$ since it can be viewed as the setwise stabiliser of the regular b-spread $\mathcal{S}$ in V (see [**56**]). By [**35**, Table 1], the expression $X = X_{\mathcal{S}}\,\mathrm{GO}_{2mb}^{\varepsilon}(2)$ is a maximal factorisation for each $\epsilon \in \{+,-\}$. It follows from [**35**, Section 1.1] that $X_{\mathcal{S}}$ acts transitively on $\mathcal{Q}^{\epsilon}$.

Remark 5.7
We review some facts about automorphisms of finite fields; see [**55**] for further details. Let $q = 2^b$ with b prime and $\lambda \in \mathbb{F}_q$. The automorphism group of $\mathbb{F}_q$ is a cyclic group of order b generated by the Frobenius automorphism $f(\lambda) = \lambda^2$. The elements of $\mathbb{F}_q$ lying in the orbit $\lambda^{\mathrm{Aut}(\mathbb{F}_q)}$ are called the *conjugates* of λ in $\mathbb{F}_q$. Lemma 2.1.75 in [**55**] implies $\mathrm{Aut}(\mathbb{F}_q)$ fixes $\mathbb{F}_2$ pointwise while $|\lambda^{\mathrm{Aut}(\mathbb{F}_q)}| = b$ when $\lambda \in \mathbb{F}_q \backslash \mathbb{F}_2$. The field trace $\mathrm{Tr} : \mathbb{F}_{2^b} \to \mathbb{F}_2$ is defined by $\mathrm{Tr}(\alpha) = \sum_{i=1}^{2^{b-1}} \alpha^i$. Let $K = \ker(\mathrm{Tr})$ and $K^{\#} = K \backslash \{0\}$. Note that $\mathrm{Tr}(1) = 0$ if and only if $b = 2$, in which case $K = \{0, 1\}$ and $\mathrm{Aut}(\mathbb{F}_q)$ acts trivially on K. If $b \geqslant 3$ then $|K| = 2^{b-1}$ and apart from the trivial orbit $\{0\}$, $\mathrm{Aut}(\mathbb{F}_q)$ has $(2^{b-1}-1)/b$ orbits in K, each of which has length b. Since $\mathbb{F}_q$ has characteristic two, every $\lambda \in \mathbb{F}_q^{\times}$ is a square. For all $\lambda \in \mathbb{F}_q^{\times}$ we denote by $\sqrt{\lambda}$ the unique element in $\mathbb{F}_q^{\times}$ satisfying $\sqrt{\lambda}^2 = \lambda$.

If W is equipped with a bilinear or quadratic form then the trace may be used to define a bilinear or quadratic form on V. The following theorem is a special case of Theorem C from [**57**].

Theorem 5.8 ([**57**])
Let Φ be a quadratic form of type $\epsilon \in \{+,-\}$ on $W = \mathbb{F}_{2^b}^{2m}$ which polarises to a symplectic form $\widetilde{B}$. Then $B = Tr \circ \widetilde{B} \circ L^{-1}$ defines a non-degenerate alternating form on $V = \mathbb{F}_2^{2mb}$ and $\varphi = \mathrm{Tr} \circ \Phi \circ L^{-1}$ defines a type ε quadratic form on V which polarises to B.

Let $g\sigma \in \mathrm{Sp}_{2m}(2^b) \rtimes C_b$. Since g is an isometry of $\widetilde{B}$ and the trace of a field element is preserved by the field automorphism σ, for all $x, y \in V$ we have

$$\begin{aligned} B(xg, yg) &= \mathrm{Tr}(\widetilde{B}(L^{-1}(x)g\sigma, L^{-1}(y)g\sigma)) \\ &= \mathrm{Tr}(\widetilde{B}(L^{-1}(x)g, L^{-1}(y)g)\sigma) \\ &= \mathrm{Tr}(\widetilde{B}(L^{-1}(x), L^{-1}(y)) \\ &= B(x, y). \end{aligned}$$

Therefore, there exists an injective homomorphism from similarity group $\Gamma\mathrm{Sp}_{2m}(2^b)$ of $\widetilde{B}$ into the isometry group $\mathrm{Sp}_{2mb}(2)$ preserving B. Such subgroups form the class of $\mathcal{C}_3$ subgroups in $\mathrm{Sp}_{2mb}(2)$. It is shown in [**38**] that $\mathrm{Sp}_{2m}(2^b) \rtimes C_b$ is maximal if and only if b is prime. For the remainder of Section 5.2 we denote by T the mapping $T : \mathcal{Q}(W) \to \mathcal{Q}(V)$ defined for all $x \in V$ by

$$[T(\Phi)](x) = \mathrm{Tr} \circ \Phi \circ L^{-1}(x) = \mathrm{Tr}(\Phi(L^{-1}(x))). \tag{5.3}$$

We also set $K = \ker(\mathrm{Tr})$ and $K^{\#} = K \backslash \{0\}$.

Lemma 5.9
Let $\Phi_0 \in \mathcal{Q}(W)$ and set $\varphi_0 = T(\Phi_0)$ as defined in Equation (5.3). For each $c \in W$ define a function $\Phi_c : W \to \mathbb{F}_{2^b}$ by

$$\Phi_c(w) = \Phi_0(w) + \widetilde{B}(w, c)^2. \tag{5.4}$$

Then $\Phi_c \in \mathcal{Q}(W)$ and $T(\Phi_c) = \varphi_{L(c)}$.

Proof. Let $\Phi_0 \in \mathcal{Q}(W)$. Then for any $c \in W$ we define $\Phi_c(x) = \Phi_0(x) + \widetilde{B}(x, c)^2$. Then for all $\lambda \in \mathbb{F}_{2^b}$ and $x, y \in W$ we have

$$\begin{aligned} \Phi_c(\lambda x) &= \Phi_0(\lambda x) + \widetilde{B}(\lambda x, c)^2 \\ &= \lambda^2 \Phi_0(x) + \lambda^2 \widetilde{B}(x, c)^2 \\ &= \lambda^2 (\Phi_0(x) + \widetilde{B}(x, c)^2) \\ &= \lambda^2 \Phi_c(x) \end{aligned}$$

and

$$\begin{aligned} \Phi_c(x + y) &= \Phi_0(x + y) + \widetilde{B}(x + y, c)^2 \\ &= \Phi_0(x) + \Phi_0(y) + \widetilde{B}(x, y) + (\widetilde{B}(x, c) + \widetilde{B}(y, c))^2 \\ &= \Phi_0(x) + \widetilde{B}(x, c)^2 + \Phi_0(y) + \widetilde{B}(y, c)^2 + \widetilde{B}(x, y) \\ &= \Phi_c(x) + \Phi_c(y) + \widetilde{B}(x, y). \end{aligned}$$

In other words, Φ_c is a quadratic form on V which polarises to $\widetilde{B}$. Moreover, for all $x \in V$ we have

$$\begin{aligned} T[\Phi_c](x) &= \mathrm{Tr}(\Phi_c(L^{-1}(x))) \\ &= \mathrm{Tr}(\Phi_0(L^{-1}(x)) + \widetilde{B}(L^{-1}(x), c)^2) \\ &= \mathrm{Tr}(\Phi_0(L^{-1}(x))) + \mathrm{Tr}(\widetilde{B}(L^{-1}(x), c)^2) \\ &= \mathrm{Tr}(\Phi_0(L^{-1}(x))) + \mathrm{Tr}(\widetilde{B}(L^{-1}(x), c))^2 \\ &= T[\Phi_0](x) + B(x, L(c)) \\ &= \varphi_{L(c)}(x). \end{aligned}$$

Therefore $T[\Phi_c] = \varphi_{L(c)}$. □

Lemma 5.10

The mapping $T : \mathcal{Q}(W) \to \mathcal{Q}(V)$ defined in Equation (5.3) is a bijection.

Proof. Fix $\Phi_0 \in \mathcal{Q}(W)$ and let $\varphi_0 = T(\Phi_0)$. For all $\varphi \in \mathcal{Q}(V)$ there exists a unique $c \in V$ such that $\varphi = \varphi_c$. Since L is a bijection, $L^{-1}(c)$ is well defined and Lemma 5.9 implies $T(\Phi_{L^{-1}(c)}) = \varphi_c$. Therefore T is surjective.

We now show that T is injective. Suppose there exists $\Phi_0, \Phi \in \mathcal{Q}(W)$ such that $\Phi_0 \neq \Phi$ and $T(\Phi_0) = T(\Phi)$. Then for all $w \in W$ we have

$$\mathrm{Tr}(\Phi_0(w)) + \mathrm{Tr}(\Phi(w)) = 0. \tag{5.5}$$

Let $S = \mathrm{sing}(\Phi_0) \cap (W \backslash \mathrm{sing}(\Phi))$. Then $S = \varnothing$ if and only if $\mathrm{sing}(\Phi_0) = \mathrm{sing}(\Phi)$ if and only if $\Phi = \alpha\Phi_0$ for some $\alpha \in \mathbb{F}_q^\times$. If $\Phi = \alpha\Phi_0$ then Φ polarises to $\alpha\widetilde{B}$ and since $\Phi \in \mathcal{Q}(W)$, we must have $\alpha = 1$. Therefore S is non-empty. Now let $u \in S$, $\lambda \in \mathbb{F}_q \backslash K$ and $v = \sqrt{\frac{\lambda}{\Phi(u)}}u$. Then

$$\Phi_0(v) = \Phi_0\left(\sqrt{\frac{\lambda}{\Phi(u)}}u\right) = \frac{\lambda}{\Phi(u)}\Phi_0(u) = 0$$

and

$$\Phi(v) = \Phi\left(\sqrt{\frac{\lambda}{\Phi(u)}}u\right) = \frac{\lambda}{\Phi(u)}\Phi(u) = \lambda.$$

It follows that $\mathrm{Tr}(\Phi_0(v)) + \mathrm{Tr}(\Phi(v)) = 1$, which contradicts Equation (5.5). Therefore T is injective, and T is a bijection. □

Corollary 5.11

Let $\Phi_0, \Phi \in \mathcal{Q}(W)$ and set $\varphi_0 = T(\Phi_0)$ and $\varphi = T(\Phi)$ as defined in Equation (5.3). Then the following hold:

(a) There exists $c \in W$ such that $\Phi = \Phi_c$ as in Equation (5.4), and $\varphi = \varphi_{L(c)}$.
(b) Φ_0 and Φ are of the same type if and only if $\Phi_0(c) \in \ker(\mathrm{Tr})$.
(c) If $\Phi(x) = \Phi_0(x) + \widetilde{B}(x, c)^2$ and $\Phi'(x) = \Phi_0(x) + \widetilde{B}(x, d)^2$ then $\Phi'(x) = \Phi(x) + \widetilde{B}(x, c + d)^2$.

PROOF.

(a) Follows from Lemmas 5.9 and 5.10.
(b) By Theorem 5.8, Φ_0 and Φ_c are of the same type if and only if φ_0 and $\varphi_{L(c)}$ are of the same type. Therefore by Lemma 3.9, Φ_0 and Φ_c are of the same type if and only if $\varphi_0(L(c)) = \mathrm{Tr}(\Phi_0(c)) = 0$, that is $\Phi_0(c) \in K$.
(c) If $\Phi(x) = \Phi_0(x) + \widetilde{B}(x,c)^2$ and $\Phi'(x) = \Phi_0(x) + \widetilde{B}(x,d)^2$ then we add both equations together to get $\Phi(x) + \Phi'(x) = \widetilde{B}(x,c)^2 + \widetilde{B}(x,d)^2$, so $\Phi'(x) = \Phi(x) + \widetilde{B}(x,c+d)^2$.

□

Lemma 5.12
The bijection $T : \mathcal{Q}^\varepsilon(W) \to \mathcal{Q}^\varepsilon(V)$ and the isomorphism $f : \Gamma\mathrm{Sp}_{2m}(2^b) \to X_{\mathcal{S}}$ resulting from Equation (5.2) together form a permutational isomorphism between the action of $\Gamma\mathrm{Sp}_{2m}(2^b)$ on $\mathcal{Q}^\varepsilon(W)$ and $X_{\mathcal{S}}$ on $\mathcal{Q}^\varepsilon(V)$.

PROOF. By Lemma 5.10 T is a bijection and by Equation (5.2), $f : \Gamma\mathrm{Sp}_{2m}(2^b) \to X_{\mathcal{S}}$ is a isomorphism. Let $\Phi \in \mathcal{Q}^\varepsilon(W)$ and $g \in \Gamma\mathrm{Sp}_{2m}(2^b)$. For all $x \in V$ we have

$$\begin{aligned}[T(\Phi)]^{f(g)}(x) &= (\mathrm{Tr} \circ \Phi \circ L^{-1})^{f(g)}(x) = \mathrm{Tr}(\Phi(L^{-1}(xf(g)^{-1}))) \\ &= \mathrm{Tr}(\Phi(L^{-1}(x)g^{-1})) = \mathrm{Tr}(\Phi^g(L^{-1}(x))) \\ &= \mathrm{Tr} \circ \Phi^g \circ L^{-1}(x) = [T(\Phi^g)](x).\end{aligned}$$

Therefore $T(\Phi^g) = T(\Phi)^{f(g)}$. □

Remark 5.13
We will usually avoid writing the isomorphism $L : W \to V$ explicitly in our equations for the rest of the section. For example, if $c \in V$ then we will write $\Phi(c)$ for $\Phi(L^{-1}(c))$ and Φ_c for $\Phi_{L^{-1}(c)}$. In other words, we imagine the quadratic forms in $\mathcal{Q}(W)$ and $\mathcal{Q}(V)$ are able to switch between vectors in W and vectors in V as needed. The intent is to minimise clutter.

Lemma 5.14
Let $V = \mathbb{F}_2^{2mb}$ with b prime and let $G = X_{\mathcal{S}}$, where $\mathcal{S}$ denotes the regular b-spread in V. For all $\varphi \in \mathcal{Q}^\varepsilon(V)$ the group G_φ is a maximal $\mathcal{C}_3$ subgroup in $X_\varphi = \mathrm{GO}^\varepsilon_{2mb}(2)$. In particular, $G_\varphi \cong \mathrm{GO}^\varepsilon_{2m}(2^b) \rtimes C_b$.

PROOF. By Lemma 5.10 there exists a unique quadratic form $\Phi \in \mathcal{Q}^\varepsilon(W)$ such that $\varphi = \mathrm{Tr} \circ \Phi \circ L^{-1}$. Let $f : \Gamma\mathrm{Sp}_{2m}(2^b) \to X_{\mathcal{S}}$ denote the group isomorphism derived from Equation (5.2). Then $g \in G_\varphi$ if and only if $\mathrm{Tr}(\Phi(x^{f^{-1}(g)})) = \mathrm{Tr}(\Phi(x))$ for all $x \in W$. In particular, $f^{-1}(g) \in \Gamma\mathrm{O}^\varepsilon_{2m}(2^b)$. Since b is prime and $\Gamma\mathrm{O}^\epsilon_{2m}(2^b) \leqslant \Gamma\mathrm{Sp}_{2m}(2^b)$, [**38**] and [**39**] imply the image of $\Gamma\mathrm{O}^\varepsilon_{2m}(2^b)$ in X_φ is a type $\mathcal{C}_3$ maximal subgroup isomorphic to $\mathrm{GO}^\varepsilon_{2m}(2^b) \rtimes C_b$. □

Lemma 5.15

Let U be a non-singular 1-dimensional subspace of W and $q = 2^b$. For each $\lambda \in \mathbb{F}_q$ there exists a unique element $u \in U$ such that $\varphi(u) = \lambda$.

PROOF. Clearly $\varphi(0) = 0$. Let $w \in U\backslash\{0\}$. If $\varphi(w) = 0$ then for all $\lambda \in \mathbb{F}_q$ we have $\varphi(\lambda w) = \lambda^2\varphi(w) = 0$, a contradiction to the assumption that U is non-singular. Therefore $\varphi(w) \in \mathbb{F}_q^\times$. Since $\mathbb{F}_q$ has characteristic two, every $\lambda \in \mathbb{F}_q^\times$ is a square. For all $\lambda \in \mathbb{F}_q^\times$ we denote by $\sqrt{\lambda}$ the unique element in $\mathbb{F}_q^\times$ satisfying $\sqrt{\lambda}^2 = \lambda$. Let $u = \sqrt{\lambda\varphi(w)^{-1}}w$. Then $\varphi(u) = \varphi(\sqrt{\lambda\varphi(w)^{-1}}w) = \lambda\varphi(u)^{-1}\varphi(w) = \lambda$. Since $|U| = |\mathbb{F}_q|$, u is the unique element such that $\varphi(u) = \lambda$. □

Lemma 5.16

Let $q = 2^b$ with b prime, $\varphi_0 \in \mathcal{Q}^\epsilon(V)$ and $\Phi_0 = T^{-1}(\phi_0)$. For $\lambda \in K = \ker(\mathrm{Tr})$ we write

$$\theta_\lambda = \{\varphi_c \in \mathcal{Q}^\varepsilon \mid \Phi_0(c) = \lambda\}$$
$$\theta_{[\lambda]} = \left\{\varphi_c \in \mathcal{Q}^\varepsilon \mid c \neq 0 \text{ and } \Phi_0(c) \in \lambda^{\mathrm{Aut}(\mathbb{F}_{2^b})}\right\}.$$

Let G denote the image of $\Gamma\mathrm{Sp}_{2m}(2^b)$ in $\mathrm{Sp}_{2mb}(2)$. The non-trivial G_{φ_0}-orbits in $\mathcal{Q}^\varepsilon$ are of the form $\theta_{[\lambda]}$ where $\lambda \in K$. If $b \geqslant 3$ then, including the trivial orbit $\{\varphi_0\}$, there are $2 + \frac{2^{b-1}-1}{b}$ distinct G_{φ_0}-orbits in $\mathcal{Q}^\varepsilon$. If $b = 2$ then, including the trivial orbit $\{\varphi_0\}$, there are 3 distinct G_{φ_0}-orbits in $\mathcal{Q}^\varepsilon$. Moreover,

$$|\theta_{[0]}| = |\theta_0| = (q^{m-1} + \varepsilon)(q^m - \varepsilon), \tag{5.6}$$
$$|\theta_{[1]}| = |\theta_1| = q^{m-1}(q^n - \varepsilon), \text{ and} \tag{5.7}$$
$$|\theta_{[\lambda]}| = q^{m-1}b(q^m - \varepsilon) \text{ for all } \lambda \in K\backslash\mathbb{F}_2. \tag{5.8}$$

PROOF. By Lemma 5.14, every $g \in G_{\varphi_0}$ can be written as a product $g = g_0\sigma$ where $g_0 \in \mathrm{GO}^\varepsilon_{2m}(2^b) < G_{\varphi_0}$ and $\sigma \in C_b < G_{\varphi_0}$. For all $c \in K$ and $g_0\sigma \in G_{\varphi_0}$ we have

$$\Phi_0(cg_0\sigma) = \Phi_0(cg_0)\sigma = \Phi_0(c)\sigma$$

so the sets $\theta_{[\lambda]}$ are G_{φ_0}-invariant. Note that any $\sigma \in C_b$ fixes $\mathbb{F}_2$ so $\theta_{[0]} = \theta_0$ and $\theta_{[1]} = \theta_1$. We now apply Lemma 3.10. Let $u, v \in \mathrm{sing}(\varphi_0)$ with $\Phi_0(u), \Phi_0(v) \in K$. If $\Phi_0(u) = \Phi_0(v) = 0$ then by Witt's Lemma, there exists $g_0 \in \mathrm{GO}^\varepsilon_{2m}(2^b)$ such that $u^{g_0} = v$. Therefore G_{φ_0} is transitive on $\theta_{[0]}$. Let $\varphi_u, \varphi_v \in \theta_{[\lambda]}$ where $\lambda \in K^\#$. Then by definition there exists a field automorphism $\sigma \in C_b$ such that $\Phi_0(u)^\sigma = \Phi_0(v)$. Let $u' = \sqrt{\frac{\Phi_0(u)}{\Phi_0(v)}}v$. Since

$$\begin{aligned}
\Phi_0(u') &= \Phi_0\left(\sqrt{\frac{\Phi_0(u)}{\Phi_0(v)}}v\right) \\
&= \frac{\Phi_0(u)}{\Phi_0(v)}\Phi_0(v) \\
&= \Phi_0(u),
\end{aligned}$$

there exists $g_0 \in \mathrm{GO}^{\varepsilon}_{2m}(2^b)$ such that $u^{g_0} = u'$. Let $g = g_0\sigma$. We have $u^{g_0\sigma} \in \langle v\rangle$ and $\Phi_0(u^{g_0\sigma}) = \Phi_0(u')^{\sigma} = \Phi_0(v)$. Therefore Lemma 3.10 implies $u^g = v$. It follows that $\varphi_u^{g^{-1}} = \varphi_v$. Therefore G_{φ_0} is transitive on $\theta_{[\lambda]}$ for all $\lambda \in K^{\#}$.

The orbit θ_0 is parametrised by the non-zero Φ_0-singular vectors in W. Therefore $|\theta_0|$ is determined by multiplying the number of totally singular 1-spaces in W by $|\mathbb{F}_{2^b}^{\times}| = q-1$. Therefore $|\theta_0| = (q^{m-1}+\varepsilon)(q^m-\varepsilon)$. By Lemma 5.15, the number of vectors in V such that $\Phi(v) = \lambda$ for some fixed $\lambda \in \mathbb{F}_q^{\times}$ does not depend on λ, so

$$|\theta_\lambda| = \frac{q^{2m} - (q^{m-1}+\varepsilon)(q^m-\varepsilon) - 1}{q-1} = q^{m-1}(q^m - \varepsilon).$$

By Remark 5.7, C_b fixes $\mathbb{F}_2$ pointwise and therefore $\theta_{[0]} = \theta_0$ and $\theta_{[1]} = \theta_1$. In particular, if $b = 2$ then the G_{φ_0}-orbits in $\mathcal{Q}^{\varepsilon}$ are $\{\varphi_0\}, \theta_{[0]}$, and $\theta_{[1]}$. If $b \geqslant 3$ then for all $\lambda \in K^{\#}$ the orbit $\lambda^{\mathrm{Aut}(\mathbb{F}_q)}$ contains b distinct elements, so $|\theta_{[\lambda]}| = |\theta_\lambda| b = q^{n-1}(q^n - \varepsilon)b$. Since b is prime, Fermat's little theorem states that $2^{b-1} \equiv 1 \mod b$ and therefore there are $2 + \frac{2^{b-1}-1}{b}$ distinct G_{φ_0}-orbits in $\mathcal{Q}^{\varepsilon}$, namely $\{\{\varphi_0\}, \theta_{[0]}, \theta_{[\lambda_i]} | 1 \leqslant i \leqslant \frac{2^{b-1}-1}{b}\}$, where the λ_i lie in separate $\mathrm{Aut}(\mathbb{F}_q)$-orbits in $\mathbb{F}_q$. □

Lemma 5.17
Let $q = 2^b$. If $b \geqslant 3$ or $(\varepsilon, b) = (-, 2)$ then $|\theta_0| < \frac{1}{2}|\mathcal{Q}^{\varepsilon}|$. If $(\varepsilon, b) = (+, 2)$ then $|\theta_0| \geqslant \frac{1}{2}|\mathcal{Q}^{\varepsilon}|$ with equality holding if and only if $m = 1$.

Proof. To begin with we consider the case $b \geqslant 3$. Note that by Corollary 5.16 $|\theta_0| = (q^{m-1} + \varepsilon)(q^m - \varepsilon)$ and $\frac{1}{2}|\mathcal{Q}^{\varepsilon}| = \frac{1}{4}q^m(q^m+\varepsilon)$. If $\varepsilon = +$ we have

$$\begin{aligned}\frac{1}{2}|\mathcal{Q}^+| - |\theta_0| &= \frac{1}{4}q^m(q^m+1) - (q^{m-1}+1)(q^m-1)\\ &\geqslant \frac{1}{4}q^m(q^m+1) - q^m(q^{m-1}+1)\\ &= \frac{1}{4}q^m(q^{m-1}(q-4)-3)\\ &\geqslant \frac{1}{4}q^m(q-7).\end{aligned}$$

But $b \geqslant 3$ implies $q \geqslant 8$ so $\frac{1}{4}q^m(q-7) > 0$. Thus $|\theta_0| < \frac{1}{2}|\mathcal{Q}^+|$. If $\varepsilon = -$ we have

$$\begin{aligned}\frac{1}{2}|\mathcal{Q}^-| - |\theta_0| &= \frac{1}{4}q^m(q^m-1) - (q^{m-1}-1)(q^m+1)\\ &\geqslant \frac{1}{4}q^m(q^m-1) - q^{m-1}(q^m+1)\\ &= \frac{1}{4}q^{m-1}(q^m(q-4)-q-4)\\ &\geqslant \frac{1}{4}q^{m-1}(q(q-4)-q-4)\\ &= \frac{1}{4}q^{m-1}(q^2-5q-4).\end{aligned}$$

ε	b	m	Non-trivial suborbits	$\overline{\Delta} \subseteq$	Reference
$+$	2	$\geqslant 1$	θ_0, θ_1	θ_0	Lemma 5.20
	3	$\geqslant 1$	$\theta_0, \theta_{[\alpha]}$	$\theta_{[\alpha]}$	Lemma 5.21
-	2	1	$\theta_1 = \mathcal{Q}^- \backslash \{\varphi_0\}$	θ_1	Lemma 5.22
	3	1	$\theta_{[\alpha]} = \mathcal{Q}^- \backslash \{\varphi_0\}$	$\theta_{[\alpha]}$	Lemma 5.22
	2	$\geqslant 2$	θ_0, θ_1	θ_1	Lemma 5.19
	3	$\geqslant 2$	$\theta_0, \theta_{[\alpha]}$	$\theta_{[\alpha]}$	Lemma 5.21

TABLE 5.1. $\mathcal{C}_3$ suborbits

By elementary algebra, the roots of the quadratic $q^2 - 5q - 4$ are $\frac{1}{2}(5 \pm \sqrt{41})$ (approximately -0.7 and 5.7). Since $q \geqslant 8$, we have $\frac{1}{4}q^{m-1}(q^2 - 5q - 4) > 0$ therefore $|\theta_0| < \frac{1}{2}|\mathcal{Q}^-|$.

On the other hand if $b = 2$ then we have $|\theta_0| = (4^{m-1} + \varepsilon)(4^m - \varepsilon)$ and $\frac{1}{2}|\mathcal{Q}^\varepsilon| = 4^{m-1}(4^m + \varepsilon)$. Therefore

$$\begin{aligned} |\theta_0| - \frac{1}{2}|\mathcal{Q}^\varepsilon| &= (4^{m-1} + \varepsilon)(4^m - \varepsilon) - 4^{m-1}(4^m + \varepsilon) \\ &= 4^{2m-1} + \varepsilon 4^m - \varepsilon 4^{m-1} - 1 - 4^{m-1}(4^m + \varepsilon) \\ &= \frac{1}{2}\varepsilon 4^m - 1. \end{aligned}$$

Since m is a positive integer we see that $\varepsilon = +$ implies $|\theta_0| \geqslant \frac{1}{2}|\mathcal{Q}^+|$ with equality holding if and only if $m = 1$, while $\varepsilon = -$ implies $|\theta_0| < \frac{1}{2}|\mathcal{Q}^+|$ for all m. □

Lemma 5.18

Let Γ be a strongly incidence-transitive code in $J(\mathcal{Q}^\varepsilon, |\Delta|)$ such that $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^\varepsilon|$ and $X_\Delta \leqslant X_{\mathcal{S}} \cong \mathrm{Sp}_{2m}(2^b) \rtimes C_b$ for some prime b. Then $b = 2$ or 3. Moreover, the sub-orbits of $X_{\mathcal{S}}$ which may contain $\overline{\Delta}$ are summarised in Table 5.2, where α denotes a primitive element of $\mathbb{F}_{2^b}$.

PROOF. Recall that $X_\Delta \leqslant G$ and X_{Δ,φ_0} acts transitively on $\overline{\Delta}$, therefore $\overline{\Delta}$ is contained in a G_{φ_0}-orbit. We assume as usual that $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^\varepsilon|$. If $b \geqslant 3$ then Lemma 5.17 implies $\overline{\Delta} \nsubseteq \theta_{[0]}$. But there are $\frac{2^{b-1}-1}{b}$ distinct G_{φ_0}-orbits of the form $\theta_{[\lambda]}$ with $\lambda \in K^\#$. In order to satisfy the assumption $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^\varepsilon|$ we must have $b \leqslant 3$. The information contained in Table 5.2 now follows directly from Lemma 5.17. □

Thanks to Lemma 5.18 we now know that if Δ^X is a strongly incidence-transitive code and $X_\Delta \leqslant G = \mathrm{Sp}_{2m}(2^b) \rtimes C_b$ then $b = 2$ or 3. Moreover, for $m \geqslant 2$ we know precisely which G_{φ_0}-orbits may contain the complement $\overline{\Delta}$ of a potential codeword Δ.

Recall Remark 1.22 in which we argued that for any subset A of Δ we have $\overline{\Delta} \subseteq \cap_{\varphi \in A}\Theta(\varphi)$, where $\Theta(\varphi)$ denotes the G_φ-orbit in $\mathcal{Q}^\varepsilon$ containing $\overline{\Delta}$. For the rest of this section we will use Remark 1.22 to demonstrate the non-existence of strongly incidence-transitive codes with $X_\Delta \leqslant X_{\mathcal{S}}$ for $m \geqslant 2$, before turning our attention to some special cases in which X_Δ is reducible and $m = 1$.

Lemma 5.19
Let $V = \mathbb{F}_2^{4m}$ with $m \geqslant 2$, $X = \mathrm{Sp}_{4m}(2)$ and $G = \mathrm{Sp}_{2m}(4) \rtimes C_2$. If $\Delta \subset \mathcal{Q}^-$ and $X_\Delta \leqslant G$ then X_Δ is intransitive on $\Delta \times \overline{\Delta}$.

Proof. We proceed by contradiction. Suppose $\Delta \subset \mathcal{Q}^-$, $X_\Delta \leqslant G$ and X_Δ acts transitively on $\Delta \times \overline{\Delta}$. Without loss of generality assume $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^-|$.

Let $\varphi_0 \in \Delta$. Since X acts transitively on $\mathcal{Q}^-$ we may assume that

$$\Phi_0(x) = \sum_{i=1}^{m} x_i y_i + x_m^2 + \alpha y_m^2$$

where α is a primitive element of $\mathbb{F}_4$.

For any $A \subseteq \Delta$ we have $\overline{\Delta} \subseteq \cap_{\varphi \in A} \Theta(\varphi)$.

By Lemma 5.18, for all $a \in \mathrm{sing}(\Phi_0)$ we have $\mathrm{Tr} \circ \Phi_a \in \Delta$. If $\varphi_c \in \overline{\Delta}$ then $\Phi_c \in \Theta(\varphi_a)$ and therefore by Lemma 5.9 we must have $\Phi_a(a + c) = 1$. Note that Lemma 5.18 implies $\Phi_0(a) = 0$ and $\Phi_0(c) = 1$. Expanding the left hand side using equations (3.1) and (3.10) (the polarisation equation and parametrisation equation) we have

$$\begin{aligned}
\Phi_a(a + c) &= \Phi_0(a + c) + \widetilde{B}(a + c, a)^2 \\
&= \Phi_0(a) + \Phi_0(c) + \widetilde{B}(a, c) + (\widetilde{B}(a, a) + \widetilde{B}(a, c))^2 \\
&= 0 + 1 + \widetilde{B}(a, c) + (0 + \widetilde{B}(a, c))^2 \\
&= 1 + \widetilde{B}(a, c) + \widetilde{B}(a, c)^2 \\
&= 1 + \mathrm{Tr}(\widetilde{B}(a, c)).
\end{aligned}$$

Therefore we have $\mathrm{Tr}(\widetilde{B}(a, c)) = 0$, that is, $\widetilde{B}(a, c) \in \mathbb{F}_2$. However, if $a \in \mathrm{sing}(\Phi_0)$ then $\Phi_0(\lambda a) = \lambda^2 \Phi_0(a) = 0$, so $\lambda a \in \mathrm{sing}(\Phi_0)$ for all $\lambda \in \mathbb{F}_4$. This implies $\widetilde{B}(a, c) = 0$. Note that $A := \{e_i, f_i\}_{i=1}^{m-1} \subset \mathrm{sing}(\Phi_0)$. Therefore if $c = \sum_{i=1}^{m} (c_i e_i + d_i f_i)$ then $\widetilde{B}(e_i, c) = d_i = 0$ and $\widetilde{B}(f_i, c) = c_i = 0$ for all i such that $1 \leqslant i \leqslant m - 1$. Applying Lemma 5.18 again, we have $\Phi_0(c) = c_m d_m + c_m^2 + \alpha d_m^2 = 1$. Using Equation (5.8) from Corollary 5.16 to count the solutions to this equation, we find $|\cap_{a \in A \cup \{0\}} \Theta(\varphi_a)| = 4^{1-1}(4^1 + 1) = 5$. But $|\overline{\Delta}| \geqslant \frac{1}{2}|\mathcal{Q}^-(\mathbb{F}^{4m})| = 4^{m-1}(4^m - 1) > 5$ for all $m \geqslant 2$, a contradiction. Therefore no such Δ exists. □

Lemma 5.20
Let $V = \mathbb{F}_2^{4m}$. There are no subsets $\Delta \subset \mathcal{Q}^+(V)$ such that $X_\Delta \leqslant \mathrm{Sp}_{2m}(4) \rtimes C_2$ with X_Δ acting transitively on $\Delta \times \overline{\Delta}$.

Proof. Suppose for the sake of contradiction that Δ is such a subset. Without loss of generality assume $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^+|$. Since X acts transitively on $\mathcal{Q}^+$ we may assume $\varphi_0 = \mathrm{Tr} \circ \Phi_0 \in \Delta$ where

$$\Phi_0(x) = \sum_{i=1}^{m} x_i y_i.$$

We consider first the case $m > 1$ with $\overline{\Delta} \subseteq \theta_0$. Let α denote a primitive element of $\mathbb{F}_4$ and $A = \{e_m + f_m, \alpha e_m + \alpha^2 f_m, \alpha^2 e_m + \alpha f_m\}$. Note that $\Phi_0(a) = 1$ for all $a \in A$, therefore Lemma 5.18 tells us $\{\varphi_a | a \in A\} \subset \Delta$. If $\varphi_c \in \overline{\Delta}$ then necessarily $\varphi_c \in \Theta(\varphi_a)$ for all $a \in A$, so $\Phi_a(a + c) = 0$ by Lemma 5.9. Note that Lemma 5.18 implies $\Phi_0(a) = 1$ and $\Phi_0(c) = 0$. Expanding the left hand side with equations (3.1) and (3.10) we have

$$\begin{aligned}
\Phi_a(a + c) &= \Phi_0(a + c) + \widetilde{B}(a + c, a)^2 \\
&= \Phi_0(a) + \Phi_0(c) + \widetilde{B}(a + c, a) + \widetilde{B}(a, c)^2 \\
&= 1 + \mathrm{Tr}(\widetilde{B}(a, c)))
\end{aligned}$$

therefore we require $\mathrm{Tr}(\widetilde{B}(a, c)) = 1$, that is, $\widetilde{B}(a, c) \in \mathbb{F}_4 \backslash \mathbb{F}_2$. For our particular choice of A, this implies

(i) $\widetilde{B}(e_m + f_m, c) = c_m + d_m \in \mathbb{F}_4 \backslash \mathbb{F}_2$,
(ii) $\widetilde{B}(\alpha e_m + \alpha^2 f_m, c) = \alpha^2 c_m + \alpha d_m \in \mathbb{F}_4 \backslash \mathbb{F}_2$, and
(iii) $\widetilde{B}(\alpha^2 e_m + \alpha f_m, c) = \alpha c_m + \alpha^2 d_m \in \mathbb{F}_4 \backslash \mathbb{F}_2$.

Note that $\{\mu + \nu | \mu, \nu \in \mathbb{F}_4 \backslash \mathbb{F}_2\} = \mathbb{F}_2$. Adding requirements (i) and (ii) together we have $c_m + d_m + \alpha^2 c_m + \alpha d_m = \alpha c_m + \alpha^2 d_m \in \mathbb{F}_2$, which clearly contradicts requirement (iii). Therefore $\cap_{a \in A} \Theta(\varphi_a) = \varnothing$, contradicting $\overline{\Delta} \subseteq \cap_{a \in A} \Theta(\varphi_a)$. Therefore no such Δ exists.

Suppose now that $m = 1$ and $\overline{\Delta} \subset \theta_1$. Remark 1.22 implies for any $a \in \mathrm{sing}(\Phi_0)$ we have $\Phi_a(a + c) = 1$. Expanding the left hand side as with the previous case we find $\widetilde{B}(a, c) \in \mathbb{F}_2$. But if $a \in \mathrm{sing}(\Phi_0)$ then $\lambda a \in \mathrm{sing}(\varphi_0)$ for all $\lambda \in \mathbb{F}_4$, so $\widetilde{B}(a, c) = 0$. Let $c = c_1 e_1 + d_1 f_1$. Since $A = \{e_1, f_1\} \subset \mathrm{sing}(\Phi_0)$, we have $\widetilde{B}(e_1, c) = d_1 = 0$ and $\widetilde{B}(f_1, c) = c_1 = 0$, a contradiction. Therefore no such Δ exists in this case. □

Let us briefly recall some facts about the field $\mathbb{F}_8$. Let $P(\alpha) = \alpha^3 + \alpha + 1$ and recall that $\mathbb{F}_8 = \mathbb{F}_2[\alpha]/\langle P(\alpha)\rangle$. Let $K = \ker(\mathrm{Tr})$ and note that with respect to our choice of characteristic polynomial, $K = \{0, \alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha\}$. Since $\mathrm{Tr} : \mathbb{F}_8 \to \mathbb{F}_2$ is a homomorphism of $\mathbb{F}_2$-vector spaces, K is the kernel of a homomorphism and is therefore closed under addition. It is not closed under scalar multiplication over $\mathbb{F}_8$. The next Lemma demonstrates shows that no strongly incidence-transitive codes with $X_\Delta \leqslant \mathrm{Sp}_{2m}(8) \rtimes C_3$ exist for $m \geqslant 2$.

Lemma 5.21
Let $V = \mathbb{F}_2^{6m}$ with $m \geqslant 2$. There is no subset $\Delta \subset \mathcal{Q}^\varepsilon(V)$ such that $X_\Delta \leqslant \mathrm{Sp}_{2m}(8) \rtimes C_3$ with X_Δ acting transitively on $\Delta \times \overline{\Delta}$.

Proof. Suppose for the sake of contradiction that Δ is such a subset and let $\varphi_0 \in \Delta$. Further, we may assume that $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^\varepsilon|$. By Remark 1.22, for any subset $A \subseteq \Delta$ we have $\overline{\Delta} \subseteq \cap_{\varphi \in A} \Theta(\varphi)$. Since X acts transitively on $\mathcal{Q}^\varepsilon$ we may assume without loss of generality that $\varphi_0 = \mathrm{Tr} \circ \Phi_0^\varepsilon$, where

$$\Phi_0^+(x) = \sum_{i=1}^{m} x_i y_i$$
$$\Phi_0^-(x) = \sum_{i=1}^{m} x_i y_i + x_m^2 + \alpha y_m^2.$$

If $a \in \operatorname{sing}(\Phi_0)$ then $\lambda a \in \operatorname{sing}(\Phi_0)$ for all $\lambda \in \mathbb{F}_8$. By Remark 1.22 and Lemma 5.18, if $\operatorname{Tr} \circ \Phi_c \in \overline{\Delta}$ then $\Phi_{\lambda a}(\lambda a + c) \in K$ for all $\lambda \in \mathbb{F}_8$. Note that Lemma 5.18 implies $\Phi_0(a) = 0$ and $\Phi_0(c) = 1$. Expanding the left hand side using equations (3.1) and (3.10) we have

$$\begin{aligned}\Phi_{\lambda a}(\lambda a + c) &= \Phi_0(\lambda a + c) + \widetilde{B}(\lambda a + c, \lambda a)^2 \\ &= \lambda^2 \Phi_0(a) + \Phi_0(c) + \widetilde{B}(\lambda a + c, \lambda a) + \widetilde{B}(a, \lambda c)^2 \\ &= \Phi_0(c) + \lambda \widetilde{B}(a, c) + \lambda^2 \widetilde{B}(a, c)^2\end{aligned}$$

and therefore we arrive at the following condition

$$\Phi_0(c) + \lambda \widetilde{B}(a, c) + \lambda^2 \widetilde{B}(\lambda a, c)^2 \in K \text{ for all } \lambda \in \mathbb{F}_8. \tag{5.9}$$

Note that $K = \{0, \alpha, \alpha^2, \alpha^2 + \alpha\}$ is closed under addition. Since $\Phi_0(c) \in K$, Equation (5.9) implies the weaker condition

$$\lambda \widetilde{B}(a, c) + \lambda^2 \widetilde{B}(a, c)^2 \in K \text{ for all } \lambda \in \mathbb{F}_8. \tag{5.10}$$

Taking $\lambda = 1$ in Equation (5.10) we see that $\widetilde{B}(a, c) + \widetilde{B}(a, c)^2 \in K$. Since K is closed under addition we see that either $\widetilde{B}(a, c) \in K$ or $\widetilde{B}(a, c) = 1$. If $\widetilde{B}(a, c) = 1$ then choosing $\lambda \notin K \cup \{1\}$ in Equation (5.10), we find $\lambda + \lambda^2 \notin K$, a contradiction. So $\widetilde{B}(a, c) \neq 1$. On the other hand if $\widetilde{B}(a, c) = \alpha^i \in K^\#$ then we take $\lambda = \alpha^{3-i}$ so that equation 5.10 gives $\alpha^3 + \alpha^6 \notin K$. Therefore $\widetilde{B}(a, c) \notin K^\#$. The only remaining possibility is $\widetilde{B}(a, c) = 0$. Let $c = \sum_{i=1}^{m}(c_i e_i + d_i f_i)$. We now consider the cases $\varepsilon = +$ and $\varepsilon = -$ separately.

If $\varepsilon = +$ then the basis vectors $\{e_i, f_i\}_{i=1}^m$ for $W = \mathbb{F}_8^{2m}$ lie in $\operatorname{sing}(\Phi_0)$. Then taking $a = e_i$ or f_i in turn and imposing the conditions $\widetilde{B}(e_i, c) = d_i = 0$ and $\widetilde{B}(f_i, c) = c_i = 0$ implied by equation 5.10, we see that $c = 0$, a contradiction.

If $\varepsilon = -$ then the vectors $\{e_i, f_i\}_{i=1}^{m-1}$ lie in $\operatorname{sing}(\Phi_0)$. Then taking $a = e_i$ or f_i in turn and imposing the conditions $\widetilde{B}(e_i, c) = d_i = 0$ and $\widetilde{B}(f_i, c) = c_i = 0$ implied by Equation (5.10), we see that $c = c_m e_m + d_m f_m$. Further imposing $\Phi_0(c) = c_m d_m + c_m^2 + \alpha d_m^2 = 0$ we find using Equation (5.6) from Corollary 5.16 that $|\cap_{a \in A \cup \{0\}} \Theta(\varphi_a)| = (4^{1-1} - 1)(4^1 + 1) = 0$, a contradiction to $|\overline{\Delta}| \geqslant \frac{1}{2}|\mathcal{Q}^-|$.

Therefore, there is no subset $\Delta \subset \mathcal{Q}^\varepsilon(V)$ such that $X_\Delta \leqslant \mathrm{Sp}_{2m}(8) \rtimes C_3$ with $X\Delta$ acting transitively on $\Delta \times \overline{\Delta}$. $\square$

We finish this section by tying up loose ends associated with two special cases: the groups $\mathrm{Sp}_2(4) \rtimes C_2 < \mathrm{Sp}_4(2)$ and $\mathrm{Sp}_2(8) \rtimes C_3 < \mathrm{Sp}_6(2)$ acting on elliptic quadratic forms. Since an elliptic form on a two-dimensional space has no non-zero singular vectors, these groups act 2-transitively on $\mathcal{Q}^-(V)$.

Lemma 5.22
Suppose $\Delta \subset \mathcal{Q}^-$ and X_Δ acts transitively on $\Delta \times \overline{\Delta}$ where either

(i) $V = \mathbb{F}_2^4$ and $X_\Delta < \mathrm{Sp}_2(4) \rtimes C_2$, or

(ii) $V = \mathbb{F}_2^6$ and $X_\Delta < \mathrm{Sp}_2(8) \rtimes C_3$.

In case (i), X_Δ is reducible. In case (ii), no Δ with these properties exists.

Proof. In case (i) $|\mathcal{Q}^-| = 6$ so without loss of generality $|\Delta| \leqslant 3$. But by Lemma 5.1, if X_Δ acts irreducibly on V then $|\Delta| \geqslant 2n+1 = 5$. Therefore any examples arising in case (i) are reducible.

In case (ii) $|\mathcal{Q}^-| = 28$ and X_Δ is irreducible so by Lemma 5.1 we may assume $7 \leqslant |\Delta| \leqslant 14$. Since X_Δ acts transitively on $\Delta \times \overline{\Delta}$ we must have $|X_\Delta| \geqslant 8 \times (28-7) = 147$. Using the GAP command 'ConjugacyClassesMaximalSubgroups' and comparing the output with Table 8.1 in [**39**], every maximal subgroup of G is conjugate to one of $\{\mathrm{Sp}_2(8), (\mathbb{F}_2^3 \rtimes C_7) \rtimes C_3, D_{14} \rtimes C_3, D_{18} \rtimes C_3\}$. Since $|D_{14} \rtimes C_3| = 42$ and $|D_{18} \rtimes C_3| = 54$ are both less than 147, while $\mathrm{Sp}_2(8)$ and $(\mathbb{F}_2^3 \rtimes C_7) \rtimes C_3$ are transitive on $\mathcal{Q}^-$, Lemma 1.17 implies X_Δ must be contained in a subgroup of either $\mathrm{Sp}_2(8)$ or $(\mathbb{F}_2^3 \rtimes C_7) \rtimes C_3$. The maximal subgroups of $\mathrm{Sp}_2(8)$ and $(\mathbb{F}_2^3 \rtimes C_7) \rtimes C_3$ are given by $M_1 = \{\mathbb{F}_2^3 \rtimes C_7, D_{14}, D_{18}\}$ and $M_2 = \{\mathbb{F}_2^3 \rtimes C_7, C_7 \rtimes C_3, C_2 \times A_4\}$, respectively. Every group in $M_1 \cup M_2$ has order less than 147, therefore no such Δ exists. □

Combining the results of Lemmas 5.19, 5.20, 5.21 and 5.22 we arrive at the following conclusion.

Lemma 5.23
Let Γ be an X-strongly incidence-transitive code in $J(\mathcal{Q}^\varepsilon, k)$. If $\Delta \subset \mathcal{Q}^\varepsilon(\mathbb{F}_2^{2mb})$ is a codeword with $X_\Delta \leqslant \mathrm{Sp}_{2m}(2^b) \rtimes C_b$ then X_Δ is reducible and therefore Γ corresponds to one of the codes classified in Chapter 4.

5.3. Classical subgroups

Recall that $V = (\mathbb{F}_2^{2n}, B)$ denotes a symplectic space with $n \geqslant 3$ and X denotes the isometry group of V. We fix a symplectic basis $\{e_i, f_i \mid 1 \leqslant i \leqslant n\}$ for V throughout Section 5.3. Since X acts 2-transitively on $\mathcal{Q}^\varepsilon$ for each $\epsilon \in \{+,-\}$, its action is primitive and the point stabilisers in the Jordan-Steiner actions are maximal subgroups of X isomorphic to $\mathrm{GO}_{2n}^{\pm}(2)$. Due to [**38**, Chapter 3] we know these are the only maximal $\mathcal{C}_8$-subgroups of $\mathrm{Sp}_{2n}(2)$. Suppose $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X-strongly incidence-transitive code and let Δ be a codeword. If $X_\Delta \leqslant \mathrm{GO}_{2n}^{\varepsilon}(2)$ then by definition X_Δ fixes an element of $\mathcal{Q}^\varepsilon$, which is possible if and only if $k = 1$ or $|\mathcal{Q}^\varepsilon| - 1$. Therefore we only consider the case $\Delta \subset \mathcal{Q}^\varepsilon$ and $X_\Delta \leqslant \mathrm{GO}_{2n}^{-\varepsilon}(2)$. The results in Sections 1.1 and 3.4.2(e) of [**35**] show that $\mathrm{GO}_{2n}^{-\varepsilon}(2)$ acts transitively on $\mathcal{Q}^\varepsilon$ for each $\epsilon \in \{+,-\}$; see line 6 of the PSp component of [**35**, Table 1]. We begin by calculating the G_ϕ-orbits in $\mathrm{sing}(\phi)$ for $\phi \in \mathcal{Q}^\epsilon$.

Lemma 5.24
Let $\varphi \in \mathcal{Q}^{\varepsilon}$, $\psi \in \mathcal{Q}^{-\varepsilon}$ and $G = X_{\psi}$. Then the G_{φ}-orbits in $\operatorname{sing}(\varphi)$ are $\{0\}, S_0$ and S_1, where

$$S_0 = \{x \in \operatorname{sing}(\varphi)\backslash\{0\} | x \in \operatorname{sing}(\psi)\},$$
$$S_1 = \{x \in \operatorname{sing}(\varphi)\backslash\{0\} | x \notin \operatorname{sing}(\psi)\}.$$

Proof. By definition ψ and φ are fixed by G_{φ} and therefore S_0 and S_1 are invariant under the action of G_{φ}. Since X acts transitively on $\mathcal{Q}^{\varepsilon}$ and X_{φ} acts transitively on $\mathcal{Q}^{-\varepsilon}$, we may assume that for all $x = \sum_{i=1}^{n}(x_i e_i + y_i f_i) \in V$ we have

$$\varphi(x) = \begin{cases} \sum_{i=1}^{n} x_i y_i & \text{if } \varepsilon = + \\ \sum_{i=1}^{n} x_i y_i + x_n^2 + y_n^2 & \text{if } \varepsilon = - \end{cases} \tag{5.11}$$

$$\psi(x) = \begin{cases} \sum_{i=1}^{n} x_i y_i + x_n^2 + y_n^2 & \text{if } \varepsilon = + \\ \sum_{i=1}^{n} x_i y_i & \text{if } \varepsilon = - \end{cases} \tag{5.12}$$

Then $\psi(x) = \varphi(x) + B(x, w)$ with $w = e_n + f_n$. Note that for all $x \in \operatorname{sing}(\varphi)\backslash\{0\}$ and $\beta \in \mathbb{F}_2$, $x \in S_{\beta}$ if and only if $B(x, w) = \beta$.

Let $U = \oplus_{i=1}^{n-1}\langle e_i, f_i\rangle$ and note that $(U, \varphi|_U) = (U, \psi|_U)$ is a hyperbolic quadratic space of dimension $2(n-1)$. Let L denote the subgroup of G_{φ} fixing the subspace $\langle e_n, f_n\rangle$ pointwise. If $g \in X$ fixes $\langle e_n, f_n\rangle$ pointwise then $g \in L$ if and only if g is an isometry of $\varphi|_U = \psi|_U$ on U. Therefore $L \cong \mathrm{GO}_{2n-2}^{+}(2)$.

We claim that G_{φ} acts transitively on S_0. If $c \in S_0$ then we may write $c = \sum_{i=1}^{n-1}(c_i e_i + d_i f_i) + \alpha w$. Let $(u, v) = (e_1, e_1 + f_1 + w)$ and note that $u, v \in S_0$ for both values of ε. To prove our claim, it is sufficient to show that u and v lie in the same G_{ϕ}-orbit, and that c lies in the same G_{ϕ}-orbit as at least one of u or v. First we show that there exists $g \in G_{\phi}$ such that $ug = v$. Define a mapping $g : V \to V$ which fixes the subspace $\oplus_{i=2}^{n-1}\langle e_i, f_i\rangle$ pointwise and permutes vectors of the form $x = x_1 e_1 + y_1 f_1 + x_n e_n + y_n f_n$ according to the equation

$$xg = x_1 e_1 + (x_1 + y_1 + x_n + y_n) f_1 + (x_1 + x_n) e_n + (x_1 + y_n) f_n. \tag{5.13}$$

Let us verify that $g \in G_{\varphi}$. Indeed, setting $\phi'(x) = \sum_{i=1}^{n} x_i y_i$ we have

$$\begin{aligned} \phi'(xg) =& x_1(x_1 + y_1 + x_n + y_n) + (x_1 + x_n)(x_1 + y_n) \\ =& x_1 + x_1 y_1 + x_1 x_n + x_1 y_n + x_1 + x_1 x_n + x_1 y_n + x_n y_n \\ =& x_1 y_1 + x_n y_n \\ =& \varphi'(x). \end{aligned} \tag{5.14}$$

Therefore Equation (5.14) implies $g \in X_{\phi'}$. Setting $x_1 = y_1 = 0$ and $x_n = y_n = 1$ in Equation (5.13) implies $wg = w$ so $g \in X_w$. Since $\psi(x) = \phi(x) + B(x, w)$ for all $x \in V$, the previous two sentences show that $g \in G_{\phi}$. Since $g \in G_{\phi}$ and $e_1 g = e_1 + f_1 + w$, we observe that e_1 and $e_1 + f_1 + w$ are contained in the same G_{ϕ}-orbit. Therefore to show that G_{ϕ} is transitive on S_0 it is sufficient to demonstrate that c is contained in the same G_{ϕ}-orbit as either e_1 or $e_1 + f_1 + w$. If $\alpha = 0$ then $c, e_1 \in \operatorname{sing}(\varphi|_U) \cap U$ so $\varphi|_U(c) = \varphi|_U(e_1)$. Therefore there exists an element $h \in L$ mapping e_1 to c which, by Witt's Theorem, extends to an isometry on V. Similarly, if $\alpha = 1$ then there exists an element $h' \in L$ mapping $e_1 + f_1 + w$

to c which, by Witt's Theorem, extends to an isometry on V. Therefore c lies in the same G_ϕ-orbit as either e_1, e_1+f_1+w and therefore G_φ acts transitively on S_0.

Next we claim that G_ϕ acts transitively on S_1. If $c \in S_1$ then we may write $c = \sum_{i=1}^{n-1}(c_ie_i + d_if_i) + \alpha e_n + (\alpha+1)f_n$ for some $\alpha \in \mathbb{F}_2$. Let $(u,v) = (e_1+e_n, e_1+f_n)$ if $\epsilon = +$ and $(u,v) = (e_1+f_1+e_n, e_1+f_1+f_n)$ if $\epsilon = -$. Note that $u, v \in S_1$ and therefore to show that G_ϕ is transitive on S_1 it is sufficient to show that u and v lie in the same G_ϕ-orbit, and that c lies in the same G_ϕ-orbit as at least one of u or v. Define a map $g : V \to V$ which swaps e_n and f_n while fixing the subspace $U = \oplus_{i=1}^{n-1}\langle e_i, f_i\rangle$ pointwise. Clearly $g \in G_\varphi$ and for either $\epsilon \in \{+,-\}$ we have $ug = v$. Moreover, we have $(U, \phi|_U) = (U, \psi|_U)$. If $\alpha = 1$ then there exists an element $h \in L$ mapping u to c which, by Witt's Theorem, extends to an isometry on V. If $\alpha = 0$ then there exists an element $h' \in L$ mapping v to c which, by Witt's Theorem, extends to an isometry on V. This proves our claim that G_ϕ is transitive on S_1.

Therefore the sets S_0 and S_1 are G_ϕ-orbits. □

Corollary 5.25
Let $\varphi_0 \in \mathcal{Q}^\varepsilon$, $\psi \in \mathcal{Q}^{-\varepsilon}$. The orbits of G_{φ_0} in $\mathcal{Q}^\varepsilon \backslash \{\varphi_0\}$ are

$$\theta_0 = \{\varphi_c \in \mathcal{Q}^\varepsilon | c \in S_0\},$$
$$\theta_1 = \{\varphi_c \in \mathcal{Q}^\varepsilon | c \in S_1\}.$$

Proof. By Lemma 3.9, the action of G_{φ_0} on $\mathcal{Q}^\varepsilon$ is permutationally isomorphic to the action of G_{φ_0} on $\operatorname{sing}(\varphi_0)$. Therefore Lemma 5.24 implies that the orbits of G_{φ_0} in $\mathcal{Q}^\varepsilon \backslash \{\varphi_0\}$ are as stated above. □

Lemma 5.26
Let $G = \mathrm{GO}_{2n}^{-\varepsilon}(2)$ with $n \geqslant 3$ and suppose $\Delta \in \binom{\mathcal{Q}^\varepsilon}{k}$ with $k \leqslant \frac{1}{2}|\mathcal{Q}^\varepsilon|$ and $X_\Delta \leqslant G$. If X_Δ acts transitively on $\Delta \times \overline{\Delta}$ then for all $\varphi_0 \in \Delta$ we have

$$\overline{\Delta} \subseteq \begin{cases} \theta_1 & \text{if } \varepsilon = + \\ \theta_0 & \text{if } \varepsilon = - \end{cases} \tag{5.15}$$

Proof. We assume $n \geqslant 3$ on account of Lemma 5.1. Let $\varphi_0 \in \Delta$ and denote by ψ the quadratic form fixed by G. By Lemma 3.13 we have $|\operatorname{sing}(\psi) \cap \operatorname{sing}(\varphi_0)| = 2^{2(n-1)}$, so $|\theta_0| = 2^{2(n-1)} - 1$ and

$$\begin{aligned} \frac{1}{2}|\mathcal{Q}^\varepsilon| - |\theta_0| &= 2^{n-2}(2^n+\varepsilon) - (2^{2(n-1)} - 1) \\ &= 1 + \varepsilon 2^{n-2}. \end{aligned}$$

Therefore $|\theta_0| < \frac{1}{2}|\mathcal{Q}^+|$ for all $n \geqslant 3$ while $|\theta_0| > \frac{1}{2}|\mathcal{Q}^-|$ for all $n \geqslant 3$. Since $\overline{\Delta}$ is an X_{Δ,φ_0}-orbit and $X_\Delta \leqslant G$, it follows that $\overline{\Delta}$ must be contained in an G_{φ_0}-orbit. The assumption $|\Delta| \leqslant \frac{1}{2}|\mathcal{Q}^\varepsilon|$ then implies $\overline{\Delta}$ satisfies Equation (5.15). □

Lemma 5.26 enables us to apply Remark 1.22. Recall that for each $\varphi \in \Delta$ there exists a unique G_φ-orbit in $\mathcal{Q}^\varepsilon$ containing $\overline{\Delta}$ which we denote by $\Theta(\varphi)$.

Lemma 5.27
For $n \geqslant 3$ there exists no proper subset $\Delta \subset \mathcal{Q}^+$ such that $X_\Delta \leqslant \mathrm{GO}^-_{2n}(2)$ with X_Δ acting irreducibly on $V = \mathbb{F}_2^{2n}$ and transitively on $\Delta \times \overline{\Delta}$.

Proof. By Lemma 5.26, $\overline{\Delta} \subseteq \theta_1$. Let $\varphi_0(x) = \sum_{i=1}^n x_i y_i$, $w = e_n + f_n$, $\psi(x) = \varphi_0(x) + B(x, w)$ and $G = X_\psi \cong \mathrm{GO}^-_{2n}(2)$. From [**35**, Table 1] we have that G is transitive on $\mathcal{Q}^+$ so we may assume $\varphi_0 \in \Delta$. Let $A = \{e_i, f_i \mid 1 \leqslant i \leqslant n-1\}$. For all $a \in A$ we have $\varphi_0(a) = \psi(a) = 0$, therefore Lemma 5.26 implies $\{\varphi_a \in \mathcal{Q}^\varepsilon \mid a \in A\} \subseteq \Delta$. Let $c = \sum_{i=1}^n (c_i e_i + d_i f_i)$. If $\varphi \in \overline{\Delta}$ with $\varphi_0(x) + \varphi(x) = B(x, c)$ then Remark 1.22 implies $\varphi \in \Theta(\varphi_0)$, and so Lemma 5.26 implies that $\psi(c) = B(c, w) = c_n + d_n = 1$ is a necessary condition on c. Moreover, for all $a \in A$ and $\varphi_c \in \overline{\Delta}$ we have $\varphi_a(x) + \varphi_c(x) = B(x, a + c)$. Remark 1.22 implies $\varphi_c \in \Theta(\varphi_a)$, and so Lemma 5.26 implies

$$\psi(a + c) = 1 \text{ for all } a \in A. \tag{5.16}$$

We may expand the left hand side of Equation (5.16) as follows

$$\begin{aligned} \psi(a + c) &= \varphi_0(a + c) + B(a + c, w) \\ &= \varphi_0(a) + \varphi_0(c) + B(a, c) + B(a, w) + B(c, w) \\ &= B(a, c) + B(a, w) + B(c, w). \end{aligned} \tag{5.17}$$

Adding Equation (5.16) to (5.17) and rearranging we find

$$B(a, c) + B(a, w) + B(c, w) = 1 \text{ for all } a \in A. \tag{5.18}$$

Noting that $B(e_i, c) = d_i, B(f_i, c) = c_i, B(a, w) = 0$ and $B(c, w) = c_n + d_n$, we may apply Equation (5.18) to the elements of A and obtain

$$c_i + c_n + d_n = 1$$
$$d_i + c_n + d_n = 1$$

for all $1 \leqslant i \leqslant n-1$. Therefore $c_i = d_i = c_n + d_n + 1$ for all $1 \leqslant i \leqslant n-1$. We see therefore that for $n \geqslant 3$, if $\varphi_c \in \cap_{a \in A \cup \{0\}} \Theta(\varphi_a)$ then $c = c_n e_n + d_n f_n + (c_n + d_n + 1) \sum_{i=1}^{n-1} (e_i + f_i)$ for some $c_n, d_n \in \mathbb{F}_2$ with $c_n \neq d_n$. Therefore

$$|\overline{\Delta}| \leqslant | \cap_{a \in A \cup \{0\}} \Theta(\varphi_a)| \leqslant 2.$$

This contradicts the assumption $|\overline{\Delta}| \geqslant \frac{1}{2}|\mathcal{Q}^+|$, therefore no such Δ exists. □

Lemma 5.28
For $n \geqslant 3$ there exists no proper subset $\Delta \subset \mathcal{Q}^-$ such that $X_\Delta \leqslant \mathrm{GO}^+_{2n}(2)$ with X_Δ acting irreducibly on $V = \mathbb{F}_2^{2n}$ and transitively on $\Delta \times \overline{\Delta}$.

Proof. By Lemma 5.26, $\overline{\Delta} \subseteq \theta_0$. Let $\varphi_0(x) = \sum_{i=1}^n x_i y_i + x_n + y_n$ and $G = X_\psi \cong \mathrm{GO}^+_{2n}(2)$ where $\psi(x) = \sum_{i=1}^n x_i y_i$. From [**35**, Table 1] we have that G is transitive on $\mathcal{Q}^-$ so we may assume $\varphi_0 \in \Delta$. For all $x \in V$, $\psi(x) = \varphi_0(x) + B(x, w)$, where $w = e_n + f_n$. Let $A = \{e_i + f_i + e_n | 1 \leqslant i \leqslant n-1\}$. For all $a \in A$ we have $\varphi_0(a) = 0$ and $\psi(a) = 1$, therefore Lemma 5.26 implies $\phi_a \in \Delta$ for all $a \in A$.

Let $c = \sum_{i=1}^{n}(c_i e_i + d_i f_i)$. Suppose $\varphi \in \overline{\Delta}$ with $\varphi_0(x) + \varphi(x) = B(x, c)$. Then for all $a \in A$ we have $\varphi_a(x) + \varphi_c(x) = B(x, a + c)$. Therefore Remark 1.22 and Lemma 5.26 imply

$$\psi(c) = B(c, w) = c_n + d_n = 0 \tag{5.19}$$

and

$$\psi(a + c) = 0 \text{ for all } a \in A. \tag{5.20}$$

Expanding the left hand side of Equation (5.20) we have

$$\begin{aligned}\psi(a + c) &= \varphi_0(a + c) + B(a + c, w)\\ &= \varphi_0(a) + \varphi_0(c) + B(a, c) + B(a, w) + B(c, w)\\ &= B(a, c) + B(a, w) + B(c, w)\end{aligned}$$

and therefore if $\varphi_c \in \overline{\Delta}$ we must have

$$B(a, c) + B(a, w) + B(c, w) = 0 \text{ for all } a \in A. \tag{5.21}$$

Noting that

$$\begin{aligned}B(c, w) &= c_n + d_n\\ B(e_i + f_i + e_n, c) &= c_i + d_i + d_n\\ B(e_i + f_i + e_n, w) &= 1\end{aligned}$$

we apply Equation (5.21) to the elements of A and obtain

$$c_i + d_i + c_n + 1 = 0 \tag{5.22}$$

for $1 \leqslant i \leqslant n-1$. Therefore $d_i = c_i + c_n + 1$ for all $1 \leqslant i \leqslant n-1$. Therefore $|\overline{\Delta}| \leqslant |\cap_{a \in A \cup \{0\}} \Theta(\varphi_a)| \leqslant 2^n$. But if $n \geqslant 3$ then $2^n - 2^{n-2}(2^n - 1) = 2^{n-2}(5 - 2^n) < 0$, a contradiction to the assumption $|\overline{\Delta}| \geqslant \frac{1}{2}|\mathcal{Q}^-|$. Therefore no such $\overline{\Delta}$ exists for $n \geqslant 3$. □

Combining the results of Lemma 5.27 and Lemma 5.28 we arrive at the following.

Theorem 5.29
Let $V = \mathbb{F}_2^{2n}$. There exists no subset $\Delta \subset \mathcal{Q}^\varepsilon$ such that $X_\Delta \leqslant \mathrm{GO}_{2n}^{-\varepsilon}(2)$ acts transitively on $\Delta \times \overline{\Delta}$ and irreducibly on V.

5.4. Fully deleted permutation modules

Let $X = \mathrm{Sp}_{2n}(2)$ in either of its doubly-transitive actions of degree $2^{2n-1} \pm 2^{n-1}$. In Section 5.4 we study X-strongly incidence-transitive codes $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ where, for $\Delta \in \Gamma$, X_Δ acts on V as a *fully deleted permutation module* for a symmetric or alternating group. Technically, these are subgroups of Aschbacher type $\mathcal{C}_9$, but the mathematics of Section 5.4 fits naturally within Chapter 5. We begin with a description of the fully deleted permutation modules which follows [**38**, Section 5.3]. Let $m \geqslant 5$ and denote by W the vector space $\mathbb{F}_2^m$ with ordered basis $\mathscr{B} = \{e_1, e_2, \ldots, e_m\}$. For all $\sigma \in S_m$ and for all $x = \sum_{i=1}^{m} x_i e_i \in V$ we define

$$x\sigma = \sum_{i=1}^{m} x_{i\sigma^{-1}} e_i. \tag{5.23}$$

Equation (5.23) defines a group action of S_m on W. The $\mathbb{F}_2G$-module W is called the *permutation module* for G. Let $x = \sum_{i=1}^{m} x_i e_i$ and $y = \sum_{i=1}^{m} y_i e_i$. We equip W with a G-invariant symmetric bilinear form $\widetilde{B} : W \times W \to \mathbb{F}_2$ defined by

$$\widetilde{B}(x, y) = \sum_{i=1}^{m} x_i y_i.$$

The *weight* of a vector $x = \sum_{i=1}^{m} x_i e_i$ is defined to be the number of indices i such that $x_i \neq 0$. We denote the weight of x by $\mathrm{wt}(x)$. The action defined by Equation (5.23) is clearly weight preserving. Let $\mathbf{j} = \sum_{i=1}^{m} e_i$ and let $A = \{x \in W \mid B(x, \mathbf{j}) = 0\}$ be the subspace of even-weight vectors in W. Then $A^{\perp} = \{\alpha\mathbf{j} \mid \alpha \in \mathbb{F}_2\}$. By [**38**, Lemma 5.3.4], A and $A^{\perp}$ are the only proper, nontrivial G-invariant subspaces of W. The restriction of $\widetilde{B}$ to A is an alternating bilinear form with radical $A \cap A^{\perp}$. We define a $\mathbb{F}_2G$-module V by

$$V = A/(A \cap A^{\perp}).$$

This is is known as the *fully deleted permutation module* for G. We note that $A \cap A^{\perp}$ is nontrivial if and only if $A^{\perp} \leqslant A$, which occurs if and only if m is even. It follows that

$$\dim(V) = \begin{cases} m-2 & \text{if} \quad m \text{ is even} \\ m-1 & \text{if} \quad m \text{ is odd} \end{cases}$$

Following Lemma 3.3, we define a symplectic form $B : V \times V \to \mathbb{F}_2$ by

$$B(x + A \cap A^{\perp}, y + A \cap A^{\perp}) = \widetilde{B}(x, y).$$

The action of G on V is faithful, absolutely irreducible and preserves the symplectic form B.

Lemma 5.30 ([**38**], pg. 187)
Let m be an integer with $m \geqslant 5$. The function $\Phi : A \to \mathbb{F}_2$ defined by

$$\Phi(x) = \begin{cases} 0 & \text{if} \quad \mathrm{wt}(x) \equiv 0 \mod 4 \\ 1 & \text{if} \quad \mathrm{wt}(x) \equiv 2 \mod 4 \end{cases} \tag{5.24}$$

is a quadratic form on A which polarises to $\widetilde{B}$. Moreover, Φ is invariant under the action of $G = S_m$ on A defined by Equation (5.23).

If m is odd then $V \cong A$ and if m is even then $V \cong A/A^{\perp}$, In either case Φ, as defined in Lemma 5.30, is a G invariant quadratic form on A. Moreover, if m is even then for each $2n$-dimensional subspace U of A which does not contain $A^{\perp}$, Lemma 3.8 implies $\Phi \circ \pi|_U^{-1}$ is a quadratic form on V which polarises to B, where π denotes the natural projection map from A to $A/A^{\perp}$. We investigate this process in more detail in Lemma 5.32, but first we note the following embeddings.

Lemma 5.31 ([**38**], pg. 187)
Let m be an integer with $m \geqslant 5$ and consider the action of $G = S_m$ on A defined by Equation (5.23)

along with the induced action on V. Then G is fixed point free on $\mathcal{Q}(V)$ if and only if $m \equiv 2 \mod 4$. In particular, if $m \not\equiv 2 \mod 4$ then we have the following embeddings of G into an orthogonal group:

$$S_{2n+2} \leqslant \begin{cases} \mathrm{GO}_{2n}^{-}(2) & \text{if} \quad n \equiv 1 \mod 4, \\ \mathrm{GO}_{2n}^{+}(2) & \text{if} \quad n \equiv 3 \mod 4 \end{cases}$$

$$S_{2n+1} \leqslant \begin{cases} \mathrm{GO}_{2n}^{+}(2) & \text{if} \quad n \equiv 0 \mod 4, \\ \mathrm{GO}_{2n}^{-}(2) & \text{if} \quad n \equiv 2 \mod 4, \\ \mathrm{GO}_{2n}^{\mp}(2) & \text{if} \quad n \equiv \pm 1 \mod 4. \end{cases}$$

Since we are assuming that X_Δ acts irreducibly on V, we may also assume $m = 2n+2$ with n even. For if $m \not\equiv 2 \mod 4$ then Lemma 5.31 implies S_m is a subgroup of $\mathrm{GO}_{2n}^{\varepsilon}(2)$ for some $\varepsilon \in \{\pm\}$ and therefore Theorem 5.29 implies X_Δ is reducible.

Lemma 5.32
Let $n \geqslant 4$ and $G = S_{2n+2}$. Let $V = A/A^\perp$ be the fully deleted permutation module for G and set $\mathbf{j} = \sum_{i=1}^{2n+2} e_i$. For all hyperplanes $U \leqslant A$ which avoid $A^\perp = \langle \mathbf{j} \rangle$, the mapping $\varphi : V \to \mathbb{F}_2$ defined by

$$\varphi(x + A^\perp) := \Phi \circ \pi|_U^{-1}(x + A^\perp) = \begin{cases} \Phi(x) & \text{if} \quad x \in U \\ \Phi(x + \mathbf{j}) & \text{if} \quad x \notin U \end{cases} \tag{5.25}$$

is a quadratic form on V which polarises to B.

Proof. Since U is a hyperplane in A which avoids $A^\perp$, Lemma 5.32 follows directly from Lemma 3.8. However, we also provide a direct proof.

We show first that φ is well defined. Let $x + A^\perp, y + A^\perp \in V$ and suppose $x + A^\perp = y + A^\perp$. Then $y = x$ or $y = x + \mathbf{j}$. If $x = y$ then clearly $\varphi(x + A^\perp) = \varphi(y + A^\perp)$. Suppose $y = x + \mathbf{j}$. Then $y \in U$ if and only if $x \notin U$. In particular, if $x \in U$ then Equation (5.25) implies

$$\varphi(y + A^\perp) = \varphi(x + \mathbf{j} + A^\perp) = \Phi(x + \mathbf{j} + \mathbf{j}) = \Phi(x) = \varphi(x + A^\perp).$$

Similarly, if $x \notin U$ then Equation (5.25) implies

$$\varphi(y + A^\perp) = \varphi(x + \mathbf{j} + A^\perp) = \Phi(x + \mathbf{j}) = \varphi(x + A^\perp).$$

Therefore φ is well defined. Next note that if $\lambda \in \mathbb{F}_2$ and $x \in A \cap U$ then $\varphi(\lambda x + A^\perp) = \Phi(\lambda x) = \lambda^2 \Phi(x) = \varphi(x + A^\perp)$. Finally we show that φ polarises to B. Without loss of generality, assume $x, y \in U$. Then using the fact that Φ is a quadratic form on A which polarises to the degenerate symplectic form $\widetilde{B}$, we have

$$\begin{aligned} \varphi(x + A^\perp + y + A^\perp) &= \Phi(x + y) = \Phi(x) + \Phi(y) + \widetilde{B}(x, y) \\ &= \varphi(x + A^\perp) + \varphi(y + A^\perp) + B(x + A^\perp, y + A^\perp). \end{aligned}$$

Thus φ is a quadratic form on V which polarises to B. $\square$

It is convenient to fix some notation at this point.

Definition 5.33
For the remainder of Section 5.4 we set $U = \langle e_1, e_2, \ldots, e_{2n+1}\rangle$ and $H_0 = A \cap U$. In addition, we set $\varphi_0 = \Phi \circ \pi^{-1}|_{H_0}$ where Φ is the quadratic form on A defined in Lemma 5.30. Note that H_0 is the set of even weight vectors in W whose last coordinate is equal to zero, so H_0 is a hyperplane in A which does not contain $A^\perp$. In particular, $H_0 = \langle e_i + e_{i+1} \mid 1 \leqslant i \leqslant 2n\rangle$.

Lemma 5.34
The quadratic form φ_0 of Definition 5.33 is hyperbolic if $n \equiv 0 \mod 4$ and elliptic if $n \equiv 2 \mod 4$.

Proof. We will determine the type of φ_0 by counting the number of φ_0-singular vectors in $V = A/A^\perp$. We assume that each coset representative $x \in x + A^\perp$ lies in H_0 so that Lemma 5.32 implies $\varphi_0(x + A^\perp) = \Phi(x)$. Therefore

$$\operatorname{sing}(\varphi_0) = \{x + A^\perp \in V \mid x \in A \cap U,\ 4 \text{ divides } \operatorname{wt}(x)\} \tag{5.26}$$

from which it follows

$$|\operatorname{sing}(\varphi_0)| = \sum_{l=0}^{n/2} \binom{2n+1}{4l}. \tag{5.27}$$

Series' of this form were studied by Ramus in 1834. In particular, the formula on the cover page of [**58**] states that

$$S(m,n,q) := \sum_{k=0}^{m} \binom{m}{nk+q} \tag{5.28}$$

$$= \frac{1}{n}\sum_{k=1}^{n} 2^m \cos^m\left(\frac{k\pi}{n}\right)\cos\left(\frac{(m-2q)k\pi}{n}\right). \tag{5.29}$$

We may change the upper bound in Equation (5.27) from $n/2$ to $2n+1$ since terms with $l > n/2$ contribute nothing to the sum. Substituting the appropriate values in to Equation (5.29) we have

$$\begin{aligned}
|\operatorname{sing}(\varphi_0)| =& S(2n+1,4,0)\\
=& \frac{1}{4}\sum_{l=1}^{4}\left(2\cos\left(\frac{l\pi}{4}\right)\right)^{2n+1}\cos\left(\frac{(2n+1)l\pi}{4}\right)\\
=& 2^{2n-1}\Bigg(\left(\cos\left(\frac{\pi}{4}\right)\right)^{2n+1}\cos\left(\frac{(2n+1)\pi}{4}\right)+\left(\cos\left(\frac{\pi}{2}\right)\right)^{2n+1}\cos\left(\frac{(2n+1)\pi}{2}\right)\\
&+\left(\cos\left(\frac{3\pi}{4}\right)\right)^{2n+1}\cos\left(\frac{3(2n+1)\pi}{4}\right)+(\cos(\pi))^{2n+1}\cos((2n+1)\pi)\Bigg)\\
=& 2^{2n-1}\left(\left(\frac{1}{\sqrt{2}}\right)^{2n+1}(-1)^{n/2}\frac{1}{\sqrt{2}}+0+\left(-\frac{1}{\sqrt{2}}\right)^{2n+1}(-1)^{\frac{n}{2}-1}\frac{1}{\sqrt{2}}+1\right)\\
=& 2^{2n-1}\left(1+(-1)^{n/2}\frac{1}{2^n}\right)\\
=& 2^{n-1}\left(2^n+(-1)^{n/2}\right).
\end{aligned}$$

Therefore the number of φ_0-singular elements of V is

$$|\operatorname{sing}(\varphi_0)| = \begin{cases} 2^{n-1}(2^n+1) & \text{if} \quad n \equiv 0 \mod 4, \\ 2^{n-1}(2^n-1) & \text{if} \quad n \equiv 2 \mod 4. \end{cases} \tag{5.30}$$

Comparing Equation (5.30) with $|\mathcal{Q}^\varepsilon| = 2^{n-1}(2^m+\epsilon)$, we see that φ_0 is hyperbolic when $n \equiv 0 \mod 4$ and elliptic when $n \equiv 2 \mod 4$. $\square$

Lemma 5.35

Let $G = S_{2n+2}$ with $n \geqslant 4$, n even and let V be the fully deleted permutation module for G over $\mathbb{F}_2$. For each integer i with $1 \leqslant i \leqslant 2n+1$ we denote by τ_i the transposition $(i, i+1) \in G$. If φ_0 is the quadratic form defined in Definition 5.33 then $G_{\varphi_0} = \langle \tau_i \mid 1 \leqslant i \leqslant 2n \rangle \cong S_{2n+1}$ and $\varphi_0^{\tau_{2n+1}} = \varphi_d$, where $d = \sum_{i=1}^{2n} e_i + A^\perp$.

Proof. Suppose $v = x + A^\perp \in V$ with $x \in H_0$. Define $P = \langle \tau_i \mid 1 \leqslant i \leqslant 2n \rangle$ and note $P \cong S_{2n+1}$. Then for any $g \in P$ and we have

$$\begin{aligned} \varphi_0^g(x + A^\perp) =& \varphi_0(x^{g^{-1}} + A^\perp) \\ =& \Phi(x^{g^{-1}}) \text{ (since } x \in U) \\ =& \Phi(x) \text{ (since } g \text{ is weight preserving)} \\ =& \varphi_0(x + A^\perp). \end{aligned}$$

Therefore $P \leqslant G_{\varphi_0}$. But P is maximal in G, so G_{φ_0} is equal to either P or G. In particular, $H_0^{\tau_{2n+1}} = \langle e_i + e_{i+1}, e_{2n} + e_{2n+2} \mid 1 \leqslant i \leqslant 2n-1 \rangle$ so τ_{2n+1} does not fix H_0. By Lemma 3.8 we have

$$\varphi_0^{\tau_{2n+1}} = (\Phi \circ \pi^{-1}|_{H_0})^{\tau_{2n+1}} = \Phi \circ \pi^{-1}|_{H_0^{\tau_{2n+1}}},$$

therefore $\tau_{2n+1} \notin G_{\varphi_0}$ and $G_{\varphi_0} = P$.

Finally, we calculate $d \in V$ such that $\varphi_d = \varphi_0^{\tau_{2n+1}}$ using a method similar to the proof of Lemma 3.9. Let $\varphi = \varphi_0^{\tau_{2n+1}}$. Set $S = H_0 \cap H_0^{\tau_{2n+1}} = \langle e_i + e_{i+1} \mid 1 \leqslant i \leqslant 2n-1 \rangle$. Then S is a $(2n-1)$-dimensional subspace of A which avoids $A^\perp$, so $S/A^\perp$ is a $(2n-1)$-dimensional subspace of V. Therefore there exists a unique $c \in V$ such that $S/A^\perp = \langle c \rangle^\perp$. Specifically, $S/A^\perp = \langle e_i + e_{i+1} + A^\perp \mid 1 \leqslant i \leqslant 2n-1 \rangle$ and therefore setting $d = \sum_{i=1}^{2n} e_i + A^\perp = e_{2n+1} + e_{2n+2} + A^\perp$ we have $d \in (S/A^\perp)^\perp$ and therefore $c = d$. Now let $x \in V$. Since $\varphi_0 = \Phi \circ \pi^{-1}|_{H_0}$ and $\varphi = \Phi \circ \pi^{-1}|_{H_0^{\tau_{2n+1}}}$, we have $\varphi_0(x) = \varphi(x)$ if and only if $x \in S/A^\perp$. On the other hand, $\varphi_0(x) \neq \varphi(x)$ if and only if $x \notin S/A^\perp = \langle d \rangle^\perp$ if and only if $B(x, d) = 1$. Therefore $\varphi(x) = \varphi_0(x) + B(x, d)$ for all $x \in V$, so $\varphi = \varphi_d$. This completes the proof. $\square$

Lemma 5.36

Let $n \geqslant 4$ with n even and $G = S_{2n+2}$. Let W be the permutation module for G, A the subspace of even weight vectors in W and V the fully deleted permutation module for G. Let φ_0 denote the quadratic form from Definition 5.33. Then the G-orbits in $\mathcal{Q}$ are the sets

$$\theta_i = \{\varphi_{c+A^\perp} \in \mathcal{Q} \mid c \in A \cap U \text{ and } \operatorname{wt}(c) \in \{2i, 2(n-i)\}\}$$

where $0 \leqslant i \leqslant \frac{n}{2}$. If φ_0 is type ε then we have

$$\theta_i \subseteq \begin{cases} \mathcal{Q}^{\varepsilon} & \text{if } \; i \text{ is even} \\ \mathcal{Q}^{-\varepsilon} & \text{if } \; i \text{ is odd.} \end{cases} \tag{5.31}$$

In particular, the number of G-orbits in $\mathcal{Q}^{\varepsilon}$ is

$$\#\text{orbits} = \begin{cases} 1 + \lfloor \frac{n}{4} \rfloor & \text{if } \; \varepsilon = + \\ \lceil \frac{n}{4} \rceil & \text{if } \; \varepsilon = -. \end{cases} \tag{5.32}$$

Proof. By Definition 5.33, $\varphi_0 = \Phi \circ \pi_{H_0}^{-1}$ with $U = \langle e_1, e_2, \ldots, e_{2n+1} \rangle$ and $H_0 = A \cap U$. If $c + A^{\perp} \in V$ then we may assume without loss of generality that $c \in H_0$, since $A = H_0 \oplus A^{\perp}$. Note that $G = \langle \tau_i \mid 1 \leqslant i \leqslant 2n+1 \rangle$ and by Lemma 5.35, $G_{\varphi_0} = \langle \tau_i \mid 1 \leqslant i \leqslant 2n \rangle$. We begin by showing that the sets θ_k are G-invariant. Let $\varphi \in \theta_k$. Then there exists a unique $c + A^{\perp} \in V = A/A^{\perp}$ such that $\varphi = \varphi_{c+A^{\perp}}$, and since $\varphi \in \theta_k$, $\mathrm{wt}(c) \in \{2k, 2(n-k)\}$ by definition of θ_k. By Lemma 3.9, we have $\varphi_{c+A^{\perp}}^{\tau_i} = \varphi_{c^{\tau_i}+A^{\perp}}$. In particular, if $1 \leqslant i \leqslant 2n$ then τ_i fixes the hyperplane H_0 of A and therefore $c^{\tau_i} \in H_0$ and $\mathrm{wt}(c^{\tau_i}) = \mathrm{wt}(c)$. Therefore $\varphi_{c+A^{\perp}}^{\tau_i} \in \theta_k$ for $1 \leqslant i \leqslant 2n$. On the other hand, Corollary 3.12 and Lemma 5.35 imply $\varphi_{c+A^{\perp}}^{\tau_{2n+1}} = \varphi_{c^{\tau_{2n+1}}+y+A^{\perp}}$, where $y = \sum_{i=1}^{2n} e_i$. Since $\mathrm{wt}\,(c^{\tau_{2n+1}} + y) \in \{k, 2(n-k)\}$, it follows $\varphi_{c+A^{\perp}}^{\tau_{2n+1}} \in \theta_k$. Therefore the sets θ_k are G-invariant.

Next we show that the sets θ_k are G-orbits. Suppose $\varphi_{c+A^{\perp}}, \varphi_{c'+A^{\perp}} \in \theta_k$ and assume $c, c' \in H_0$. *Claim*: If $\mathrm{wt}(c) = \mathrm{wt}(c')$ then there exists an element of G_{φ_0} mapping $\varphi_{c+A^{\perp}}$ to $\varphi_{c'+A^{\perp}}$.

Indeed, If $\mathrm{wt}(c) = \mathrm{wt}(c')$ then, since $c, c' \in H_0$, the final coordinate of both c and c' is equal to zero and therefore there is an element of $G_{\varphi_0} = \langle \tau_i \mid 1 \leqslant i \leqslant 2n \rangle \cong S_{2n+1}$ mapping c to c'. It follows from Lemma 3.9 that there exists an element of G_{φ_0} mapping $\varphi_{c+A^{\perp}}$ to $\varphi_{c'+A^{\perp}}$.

Suppose instead that $\mathrm{wt}(c) \neq \mathrm{wt}(c')$. Without loss of generality we assume that $\mathrm{wt}(c) = 2k$ and $\mathrm{wt}(c') = 2(n-k)$. Define $c_k = \sum_{i=1}^{2k} e_i$ and note that since $1 \leqslant k \leqslant \frac{n}{2}$ we have $c_k \in H_0$, $\varphi_{c_k+A^{\perp}} \in \theta_k$ and $\mathrm{wt}(c_k) = 2k = \mathrm{wt}(c)$. By the claim, there exists an element of G_{φ_0} mapping $\varphi_{c+A^{\perp}}$ to $\varphi_{c_k+A^{\perp}}$. Let $\sigma = \tau_{2n+1}$ and note that σ fixes c_k for each $k \in [1 : n/2]$. By Corollary 3.12 and Lemma 5.35, for all $x \in V$ we have

$$\varphi_{c_k+A^{\perp}}^{\sigma}(x) = \varphi_{c_k^{\sigma}+y+A^{\perp}} = \varphi_{c_k+y+A^{\perp}},$$

where $y = \sum_{i=1}^{2n} e_i$. But $c_k + y \in H_0$ and $\mathrm{wt}\,(c_k + y) = 2(n-k) = \mathrm{wt}(c')$, so the previous claim implies there exists an element of $G_{\varphi_0} \cong S_{2n+1}$ mapping $c_k + y$ to c' and it follows from Lemma 3.9 that the same element maps $\varphi_{c_k+y+A^{\perp}}$ to $\varphi_{c'+A^{\perp}}$.

Therefore, there exists an element of G, contained in the double coset $G_{\varphi_0}\tau_{2n+1}G_{\varphi_0}$, which maps $\varphi_{c+A^{\perp}}$ to $\varphi_{c'+A^{\perp}}$, that is, θ_k is a G-orbit.

Having determined the G-orbits in $\mathcal{Q}$, it remains to determine the type ε of each orbit and count them. By Lemma 5.34, an orbit representative $\varphi_{c_k} \in \theta_k$ has the same type as φ_0 if an only if k is even. Equation (5.31) follows. For $\varepsilon = +$ or $-$, the number of orbits in $\mathcal{Q}^{\varepsilon}$ is determined respectively by the number of solutions to the equations $0 \equiv s \mod 4$ and $2 \equiv s \mod 4$ with $0 \leqslant s \leqslant \frac{n}{2}$. The number of G-orbits is therefore given by equation (5.32). $\square$

Lemma 5.37

Let $X = \mathrm{Sp}_{2n}(2)$ and let $V = \mathbb{F}^{2n}$ be the fully deleted permutation module for S_{2n+2}. Suppose

$\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X-strongly incidence-transitive code with $\Delta \in \Gamma$ and $X_\Delta \leqslant S_{2n+2}$. Then $n = 4, \varepsilon = +$ and either $\theta_0 \in \Gamma$ or $\theta_2 \in \Gamma$, as defined in Lemma 5.36. Conversely, the orbits θ_0^X and θ_2^X are X-strongly incidence-transitive codes which lie respectively in Johnson graphs $J(136, 10)$ and $J(136, 126)$.

Proof. If $\varepsilon = +$ and $n > 6$, or $n > 8$ and $\varepsilon = -$, then Lemma 5.36 implies G has at least three orbits in $\mathcal{Q}^\varepsilon$. We use GAP [**59**] to analyse the remaining cases:

(a) If $n = 4$ and $\varepsilon = +$ then $G = S_{10}$ and Lemma 5.36 implies the G-orbits in $\mathcal{Q}^+$ are θ_0 and θ_2. Let $\Delta = \theta_0$ and recall $H_0 = \langle e_i + e_{i+1} \mid 1 \leqslant i \leqslant 2n-1\rangle$. Then $\overline{\Delta} = \{\varphi_{c+A^\perp} \mid c \in H_0, \mathrm{wt}(c) = 4\}$ and $G_{\varphi_0} \cong S_9$ acts transitively on $\overline{\Delta}$. Therefore Δ^X is a strongly incidence-transitive code in $J(136, 10)$ and $\overline{\Delta}^X$ is a strongly incidence-transitive code in $J(136, 126)$.

(b) If $n = 6$ and $\varepsilon = +$ then $G = S_{14}$ and Lemma 5.36 implies the G-orbits in $\mathcal{Q}^+$ are θ_1 and θ_3. If $\varphi \in \theta_1$ and $\psi \in \theta_3$ then $G_\varphi \cong S_{11} \times S_3$ and $G_\psi \cong A_7 \times A_7 : D_8$. The group G_ψ has two orbits in θ_1, as does G_φ in θ_3.

(c) If $n = 4$ and $\varepsilon = -$ then $G = S_{10}$ and Lemma 5.36 implies G acts transitively on $\theta_1 = \mathcal{Q}^-$. Therefore X_Δ must be a proper subgroup of G. If $\varphi \in \mathcal{Q}^-$ then $G_\varphi \cong S_7 \times S_3$. The only G_φ-orbit with length at least $\frac{1}{2}|\mathcal{Q}^-|$ has length 63, so $57 \leqslant k \leqslant 60$. Moreover, invoking the fact that $|\Delta \times \overline{\Delta}| = k(120-k)$ divides $|G| = 10!$, we find the only possibility is $|\Delta| = 60$. There are two conjugacy classes of maximal subgroups of S_{10} with order divisible by 60^2; these have isomorphism type $A_5 \times A_5 : D_8$ and A_{10}. The former group has orbit lengths 20 and 100 in $\mathcal{Q}^-$, so $X_\Delta \neq A_5 \times A_5 : D_8$. The latter group is transitive on $\mathcal{Q}^-$ so we assume $X_\Delta < A_{10}$. The is a unique conjugacy class of maximal subgroups of A_{10} with order divisible by 60; these have isomorphism type $A_5 \times A_5 : C_4$, but have orbit lengths 20 and 100 in $\mathcal{Q}^-$. Therefore no X-strongly incidence-transitive codes arise in this case. See Program D.4 for the relevant GAP code.

(d) If $n = 6$ and $\varepsilon = -$ then $G = S_{14}$ and Lemma 5.36 implies the G-orbits in $\mathcal{Q}^-$ are θ_0 and θ_2. If $\varphi \in \theta_1$ and $\psi \in \theta_3$ then $G_\varphi \cong S_{13}$ and $G_\psi \cong S_9 \times S_5$. The group G_φ has two orbits in θ_0, as does G_ψ in θ_2.

(e) If $n = 8$ and $\varepsilon = -$ then $G = S_{18}$ and Lemma 5.36 implies the G-orbits in $\mathcal{Q}^-$ are θ_1 and θ_3. If $\varphi \in \theta_1$ and $\psi \in \theta_3$ then $G_\varphi \cong S_{15} \times S_3$ and $G_\psi \cong S_{11} \times S_7$. The groups G_φ and G_ψ are intransitive on θ_1 and θ_3.

Therefore the only strongly incidence-transitive codes which arise from the fully deleted permutation modules for the symmetric and alternating groups are $\theta_0^X \subset J(136, 10)$ and $\theta_2^X \subset J(136, 126)$. □

The X-strongly incidence-transitive codes $\theta_0^X \subset J(136, 10)$ and $\theta_2^X \subset J(136, 126)$ are block sets of 2-$(136, 10, 64)$ and 2-$(136, 126, 11200)$ designs, respectively. Each contains 13056 blocks. The intersection numbers for the first code were calculated in GAP [**59**]; they are $6, 8, 9$ and 10. In particular, $\delta = 6$ for both codes and therefore both codes are neighbour-transitive by Theorem 1.9.

Remark 5.38

Looking back at Chapters 4 and 5, we have provided constructions for each of the codes which are described in Theorem 4.3, and proved that no other examples arise when X_Δ is contained in a geometric maximal subgroup of X or X_Δ acts on V as a subgroup of the fully deleted permutation module for the alternating or symmetric groups.

CHAPTER 6

Almost-simple codeword stabilisers

Problem: Let G be a subgroup of $X = \mathrm{Sp}_{2n}(2)$ of Aschbacher type $\mathcal{C}_9$. Classify the X-strongly incidence transitive codes $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ with $X_\Delta = G$ for $\Delta \in \Gamma$.

6.1. Introduction

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space with isometry group $X = \mathrm{Sp}_{2n}(2)$. Let $\mathcal{Q}^\varepsilon$ be the set of all ε-type quadratic forms on V which polarise to B. Let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ be an X-strongly incidence-transitive code with $\Delta \in \Gamma$ and $3 \leqslant |\Delta| \leqslant 2^{n-1}(2^n + \varepsilon) - 3$. Recall that the fully deleted permutation modules for the alternating and symmetric groups were treated in Section 5.4, leading to the construction of a pair of complementary strongly incidence-transitive codes. In Chapter 6 we work towards a proof that no further examples of strongly incidence-transitive codes of Jordan-Steiner type exist with $X_\Delta \in \mathcal{C}_9$. See Chapter 8 for an outline open cases.

Definition 6.1
If X is a classical group and $G \leqslant X$ then $G \in \mathcal{C}_9$ if the following conditions hold:

(a) G is not contained in any Aschbacher class $\mathcal{C}_i$ for any $i \in [1:8]$,
(b) the action of G on its natural module is absolutely irreducible, and
(c) there exists a nonabelian simple group T such that $T \trianglelefteqslant G/Z(G) \leqslant \mathrm{Aut}(T)$.

If $X = \mathrm{Sp}_{2n}(2)$ then $Z(X)$ is trivial, therefore if G is a $\mathcal{C}_9$-subgroup of X then G itself is almost-simple. Moreover, if Γ is an X-strongly incidence-transitive code and $\Delta \in \Gamma$ with X_Δ contained in a maximal $\mathcal{C}_9$ subgroup of X, Lemma 1.17 implies that either $G = X_\Delta$, or G acts transitively on $\mathcal{Q}^\varepsilon$. The maximal subgroups G for which the latter case holds are listed in [**35**, Tables 2 and 3]. The associated factorisations are $\mathrm{Sp}_8(2) = S_{10}\,\mathrm{GO}_8^-(2)$, $\mathrm{Sp}_6(2) = G_2(2)\,\mathrm{GO}_6^\varepsilon(2)$ and $\mathrm{Sp}_8(2) = L_2(17)\,\mathrm{GO}_8^+(2)$. The former of these is considered in Lemma 5.37. The latter pair are to be studied in Lemmas 6.5 and 6.6. In all other cases, we assume without loss of generality that X_Δ is a maximal $\mathcal{C}_9$-subgroup of X.

Lemma 1.15 implies that X_Δ must admit a nontrivial factorisation. The maximal factorisations of the classical simple groups of Lie type are known, and all factorisations of the exceptional simple groups of Lie type and the sporadic groups are known [**35, 60, 36**]. The main problem in Chapter 6 is identifying which of these, if any, are associated with the Jordan-Steiner actions.

If T is a classical simple group then usually there are more factorisations that we wish to deal with directly. In this case we combine Lemma 6.9 with lower bounds on the dimension of the minimal modules for T to rule out the majority of factorisations and then decide which of the remaining factorisation can be associated with the Jordan-Steiner actions.

Throughout Chapter 6, for any $z \in \mathbb{Z}$ we denote by $\nu_e(z)$ the largest power of 2 which divides z. We set $\nu_o(z) = z/\nu_e(z)$. These are called, respectively, the even and odd parts of z.

Lemma 6.2
Let $X = \mathrm{Sp}_{2n}(2)$ and suppose $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X-strongly incidence-transitive code with $\Delta \in \Gamma$. Then for $\varphi \in \Delta$ and $\psi \in \overline{\Delta}$ we have

$$\nu_o(|X_\Delta : X_{\Delta,\varphi}| + |X_\Delta : X_{\Delta,\psi}|) = \nu_e(|X_\Delta : X_{\Delta,\varphi}| + |X_\Delta : X_{\Delta,\psi}|) \pm 1.$$

Proof. We have $|\mathcal{Q}^\epsilon| = 2^{n-1}(2^n + \epsilon)$ so $\nu_e(|\mathcal{Q}^\epsilon|) = 2^{n-1}$ and $\nu_o(|\mathcal{Q}^\epsilon|) = 2^n + \epsilon$. Therefore $\nu_o(|\mathcal{Q}^\epsilon|) = 2\nu_e(|\mathcal{Q}^\epsilon|) \pm 1$. But Lemma 1.15 implies $|\mathcal{Q}^\epsilon| = |X_\Delta : X_{\Delta,\varphi}| + |X_\Delta : X_{\Delta,\psi}|$, which completes the proof. □

Lemma 6.3
Let $X = \mathrm{Sp}_{2n}(2)$ and suppose $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X-strongly incidence-transitive code with $\Delta \in \Gamma$. If X_Δ is almost-simple with socle T then $|\operatorname{Aut}(T)| > 2^{2(n-1)}$. In particular, if $e(T)$ denotes the minimum dimension of an $\mathbb{F}_2T$-module then $\log_2(|\operatorname{Aut}(T)|) - e(T) + 2 > 0$.

Proof. Since X_Δ acts transitively on $\Delta \times \overline{\Delta}$ we have $|X_\Delta| \geqslant |\Delta \times \overline{\Delta}| = |\Delta|\left(|\mathcal{Q}^\varepsilon| - |\Delta|\right)$. Therefore $|\mathcal{Q}^\varepsilon| \leqslant |\Delta| + \frac{|X_\Delta|}{|\Delta|}$. Also, $|\Delta| \geqslant 2$, so $|\Delta| + |X_\Delta|/|\Delta| \leqslant |X_\Delta| \leqslant |\operatorname{Aut}(T)|$ and therefore $|\mathcal{Q}^\epsilon| \leqslant |\operatorname{Aut}(T)|$. Finally, $|\mathcal{Q}^\varepsilon| \geqslant 2^{n-1}(2^n - 1) > 2^{2(n-1)}$ therefore $|\operatorname{Aut}(T)| \geqslant 2^{2(n-1)}$. Moreover, by definition, $e(T) \leqslant 2n$ and therefore $|\operatorname{Aut}(T)| > 2^{e(T)-2}$. Applying $\log_2$ to both sides of the inequality and rearranging completes the proof. □

Lemma 6.4
Let $X = \mathrm{Sp}_{2n}(2)$ and suppose $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X-strongly incidence-transitive code with $k \geqslant 2$ and $\Delta \in \Gamma$. If X_Δ is almost-simple with socle T and X_Δ acts irreducibly on $V = \mathbb{F}_2^{2n}$ then T is fixed point free on $\mathcal{Q}^\varepsilon$ and X_φ does not contain T for any $\varphi \in \mathcal{Q}^\varepsilon$.

Proof. Consider first the induced action of T on Δ. Since $T \trianglelefteqslant G$, every T-orbit in Δ has the same length and therefore the action of T on Δ is either trivial or fixed point free. If T acts trivially on Δ then, since $k \geqslant 2$, there exists $\varphi_0, \varphi_c \in \Delta$ with $c \neq 0$. Lemma 3.8 implies c is fixed by G. This contradicts the assumption that G acts reducibly on V, so T acts nontrivially on Δ. In particular, every T-orbit in Δ has length greater than one and therefore T is fixed point free in Δ. Application of the same argument to $\overline{\Delta}$ shows that T is fixed point free on $\mathcal{Q}^\varepsilon$. Finally, note that for all $\varphi \in \mathcal{Q}^\varepsilon$ the group X_φ fixes φ by definition. Therefore T is not contained in X_φ for any $\varphi \in \mathcal{Q}^\varepsilon$. □

In [**61**] Praeger and Seress provide bounds on the order of a finite classical group. Their upper bounds are presented in Table 6.1 below along with a weaker upper bound on $|\operatorname{Aut}(T)|$ of the form

T	Upper bound on $\lvert\mathrm{Aut}(T)\rvert$ using [**61**]	Weakened upper bound on $\lvert\mathrm{Aut}(T)\rvert$
$\mathrm{PSL}_m(q)$	$\frac{2f}{q-1}q^{m^2}$	$2q^{m^2}$
$\mathrm{PSU}_m(q)$	$\frac{8f}{3(q+1)}q^{m^2}$	$\frac{2}{3}q^{m^2}$
$\mathrm{PSp}_{2m}(q)$	$fq^{m(2m-1)}$	q^{2m^2-m+1}
$\mathrm{P}\Omega^{\circ}_{2m+1}(q)$	$fq^{m(2m+1)}$	q^{2m^2+m+1}
$\mathrm{P}\Omega^{\varepsilon}_{2m}(q)$	$2fq^{m(2m-1)}(1-\varepsilon q^{-m})$	$\frac{10}{4}q^{2m^2-m+1}$

TABLE 6.1. Upper bounds on the order of the automorphism group of a classical simple group. Note that $q = p^f$.

$cq^{p(m)}$, where c is a constant and $p(m)$ is a polynomial. We use the bounds in Table 6.1 in combination with Lemma 6.3 in Sections 6.3 and 6.4.

6.2. Some basic results in dimension at most twelve

Before we begin our general calculations for Chapter 6 we note that the $\mathcal{C}_9$-subgroups of $\mathrm{Sp}_{2n}(2)$ for $n \leqslant 6$ are enumerated in [**39**]. Excluding the fully deleted permutation modules for the symmetric and alternating groups, the maximal $\mathcal{C}_9$-subgroups of $\mathrm{Sp}_{2n}(2)$ for $3 \leqslant n \leqslant 6$ are $G_2(2) < \mathrm{Sp}_6(2)$, $\mathrm{PSL}_2(17) < \mathrm{Sp}_8(2)$ and $\mathrm{PSL}_2(25).2_2 < \mathrm{Sp}_{12}(2)$. We show below that there are no X-strongly incidence-transitive codes associated with these maximal subgroups.

Lemma 6.5
Let $X = \mathrm{Sp}_6(2)$ and consider the maximal subgroup $M = G_2(2)$ of X. There does not exist an X-strongly incidence-transitive code $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ such that $X_\Delta \leqslant M$ for $\Delta \in \Gamma$.

PROOF. Suppose $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ is an X-strongly incidence-transitive code. Let $\Delta \in \Gamma$ and assume $X_\Delta \leqslant M$. By [**35**, Section 1.3, Table 2], $G_2(2)$ acts transitively on $\mathcal{Q}^{\varepsilon}$. Strong incidence-transitivity implies X_Δ has two orbits in $\mathcal{Q}^{\varepsilon}$, therefore X_Δ is a proper subgroup of $G_2(2)$. Without loss of generality we may assume $2k < v = 2^2(2^3+\varepsilon)$. By definition, X_Δ acts transitively on $\Delta \times \overline{\Delta}$ and therefore $k(v-k)$ divides $|X_\Delta|$, which in turn divides $|G_2(2)|$. Using Program D.2 we determine that if $\varepsilon = +$ then $k = 8$ or 12, and if $\varepsilon = -$ then $k = 4$. However, if $\varepsilon = +$ and $k = 8$ or 12 then the only subgroup of $G_2(2)$ with order divisible by $k(v-k)$ is $G_2(2)$ itself, a contradiction to the requirement that $X_\Delta < G_2(2)$. On the other hand, if $k = 4$ then $k < 2n+1$, which contradicts Lemma 5.1. Therefore X_Δ is not a subgroup of $G_2(2)$. □

Lemma 6.6
Let $X = \mathrm{Sp}_8(2)$ and consider the maximal subgroup $M = \mathrm{PSL}_2(17)$. There exists no X-strongly incidence-transitive code $\Gamma \subseteq \binom{\mathcal{Q}^{\varepsilon}}{k}$ with $X_\Delta \leqslant M$ for $\Delta \in \Gamma$.

PROOF. Since $\dim(V) = 8$ we have $v = 2^3(2^4+\varepsilon)$. Assume Γ is X-strongly incidence-transitive and $X_\Delta \leqslant \mathrm{PSL}_2(17)$. Then $k(v-k)$ divides $|X_\Delta|$ and therefore divides $|\mathrm{PSL}_2(17)|$ also. However, Program D.2 shows that there are no values of k such that $k(v-k)$ divides $|\operatorname{PSL}_2(17)|$ for either value of ε. Therefore no such Γ exists. $\square$

Lemma 6.7
Let $X = \operatorname{Sp}_{12}(2)$ and consider the maximal subgroup $M = \operatorname{PSL}_2(25).2_2$. There exists no X-strongly incidence-transitive code $\Gamma \subseteq \binom{\mathcal{Q}^{\varepsilon}}{k}$ with $X_\Delta \leqslant M$ for $\Delta \in \Gamma$.

Proof. Since $\dim(V) = 12$ we have $v = 2^5(2^6 + \varepsilon)$. Assume Γ is X-strongly incidence-transitive and $X_\Delta \leqslant \operatorname{PSL}_2(25).2_2$. Then $k(v-k)$ divides $|X_\Delta|$ and therefore divides $|\operatorname{PSL}_2(25).2_2|$ also. However, Program D.2 shows that there are no values of k such that $k(v-k)$ divides $|\operatorname{PSL}_2(25).2_2|$ for either value of ε. Therefore no such Γ exists. $\square$

6.3. Simple classical groups in even characteristic

We begin with an overview of the twisted tensor product modules for the special linear groups. A more detailed discussion can be found in [**56**, Section 5.1]. Let $G = \operatorname{SL}_m(q^f)$ for some prime power $q = p^r$ and let $W = W^{(0)}$ be a $\mathbb{F}_q G$-module. For each integer i with $1 \leqslant i \leqslant f-1$ we introduce a $\mathbb{F}_q G$-module $W^{(i)}$. As a vector space, $W^{(i)}$ is isomorphic to W. The action of G on $W^{(i)}$ is defined by

$$(w, g) \mapsto w g^{(q^i)}, \text{ for all } w \in W \text{ and } g \in G,$$

where g^{q^i} denotes g with each entry raised to the q^ith power. By extension, G acts on the tensor product

$$V = \bigotimes_{i=0}^{f-1} W^{(i)}.$$

Moreover, the action of G on V yields an embedding $\operatorname{SL}_m(q^f) < \operatorname{SL}_{m^f}(q)$.

Theorem 6.8 ([**38**], special case of Proposition 5.4.6)
Let T be a simply connected group of Lie type over $\mathbb{F}_{2^f}$, and suppose that V is an absolutely irreducible $\mathbb{F}_2 T$-module. Let $\mathbb{F}_{2^\infty}$ denote the algebraic closure of $\mathbb{F}_2$. Then $\dim(V) = \dim(M)^f$ and one of the following occurs:

(i) T is untwisted and there exists an irreducible $\mathbb{F}_{2^\infty} T$-module M such that

$$V \otimes \mathbb{F}_{2^\infty} \cong \bigotimes_{i=0}^{f-1} M^{(i)}$$

where $M^{(i)}$ denotes the natural module for T twisted by a field automorphism.

(ii) T is of type ${}^2A_l, {}^2D_l$ or ${}^2E_6$ with an associated graph automorphism τ_0 such that $V \cong V^{\tau_0}$, and there exists an irreducible $\mathbb{F}_{2^\infty} T$-module M such that $M \cong M^{\tau_0}$ and

$$V \otimes \mathbb{F}_{2^\infty} \cong \bigotimes_{i=0}^{f-1} M^{(i)}.$$

Lemma 6.9
Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space and $X = \mathrm{Sp}_{2n}(2)$. Let $\Gamma \subset \binom{\mathcal{Q}^{\varepsilon}}{k}$ be an X-strongly incidence-transitive code with $\Delta \in \Gamma$ and $2 \leqslant |\Delta| \leqslant 2^{n-1}(2^n + \varepsilon) - 2$. Suppose $T_m(2^f)$ is an absolutely irreducible simple group of Lie type acting on V as a subgroup of X_Δ. Then $|\mathrm{Aut}(T)| > 2^{m^f-2}$ and $3 + \log_2(f) + fm^2 - m^f > 0$.

Proof. By Lemma 6.3 we have $2^{2n-2} < |\mathrm{Aut}(T)|$. By Theorem 6.8 there exists a module M such that $\dim(M)^f = \dim(V) = 2n$. By [**38**, Proposition 5.4.13], $\dim(M) \geqslant m$. Therefore $n \geqslant m^f/2$ and therefore $2^{m^f-2} \leqslant 2^{2n-2} < |\mathrm{Aut}(T)|$. On the other hand, Table 6.1 implies $|\mathrm{Aut}(T)| \leqslant 2fq^{m^2}$, where $q = 2^f$. Therefore

$$2^{m^f-2} < 2fq^{m^2}. \tag{6.1}$$

Applying $\log_2$ to each side of Inequality (6.1) we have

$$\log_2(2^{m^f-2}) = m^f - 2 < \log_2(2f2^{fm^2}) = 1 + \log_2(f) + fm^2 \tag{6.2}$$

and therefore

$$3 + \log_2(f) + fm^2 - m^f > 0. \tag{6.3}$$

$\square$

Lemma 6.10
Let $T = T_m(2^f)$ be a nonabelian simple classical group with $m \geqslant 2$ and $f \geqslant 3$. There are no codes X-strongly incidence-transitive codes Γ with $\mathrm{soc}(X_\Delta) \cong T$.

Proof. Let $b(m,f) = 3 + \log_2(f) + fm^2 - m^f$, viewed as a differentiable function defined for $(m,f) \in \mathbb{R}^2$ with $m > 1$ and $f > 2$. If Γ is strongly incidence-transitive and $\mathrm{soc}(X_\Delta) \cong T$ then Lemma 6.9 implies $b(m,f) > 0$. Differentiating b, we have

$$\begin{aligned}\frac{\partial b}{\partial m} &= mf(2 - m^{f-2})\\ \frac{\partial b}{\partial f} &= m^2(1 - \ln(m)m^{f-2}) + \frac{1}{\ln(2)f}.\end{aligned}$$

Since $m \geqslant 2$ and $f \geqslant 3$, if $\frac{\partial b}{\partial m} = 0$ then $f = \frac{\ln(2)}{\ln(m)} + 2$ and in particular, $\frac{\partial b}{\partial m} < 0$. Therefore if $m' > m \geqslant 2$ and $f \geqslant 3$ we have $b(m',f) < b(m,f)$. Similarly, if $f \geqslant 3$ and $m \geqslant 2$ then $m^2(1 - \ln(m)m^{f-2}) + \frac{1}{\ln(2)f} \leqslant m^2(1 - m\ln(m)) + \frac{1}{3\ln(2)} < 0$. Thus if $f' \geqslant f > 3$ we have $b(m,f') < b(m,f)$. Noting that $b(4,3) \approx -11.4$, $b(3,4) \approx -40.0$ and $b(2,5) \approx -6.69$, it follows that the only integral values of (m,f) which can satisfy Equation (6.5) with $m \geqslant 2$ and $f \geqslant 3$ are $(2,3)$, $(2,4)$ and $(3,3)$. By Theorem 2.2, it remains therefore to consider $\mathrm{soc}(X_\Delta) \in \{\mathrm{PSL}_2(8), \mathrm{PSL}_2(16), \mathrm{PSL}_3(8), \mathrm{PSU}_3(8)\}$.

By Lemma 1.15, there exists a factorisation $X_\Delta = X_{\Delta,\varphi}X_{\Delta,\psi}$ with $(\varphi,\psi) \in \Delta \times \overline{\Delta}$. Using the tables in [**35**, Chapter 1] to check which of the candidates for $\mathrm{soc}(X_\Delta)$ is factorisable, we find $\mathrm{soc}(X_\Delta) \in \{\mathrm{PSL}_2(16), \mathrm{PSU}_3(8)\}$. In particular, if $T = \mathrm{PSL}_2(16)$ then we have $16384 = 2^{2^4-2} < |\mathrm{Aut}(T)| = 16320$, a contradiction to Lemma 6.9. Similarly, if $T = \mathrm{PSU}_3(8)$ then $33554432 = 2^{3^3-2} < |\mathrm{Aut}(T)| = 12096$, a contradiction to Lemma 6.9.

Therefore there are no X-strongly incidence-transitive codes $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ with $\mathrm{soc}(X_\Delta) \cong T_m(2^f)$, $m \geqslant 2$ and $f \geqslant 3$. $\square$

Lemma 6.11 ([**38**] pg. 199)
Let T be one of $\mathrm{PSL}_d^{\pm}(p^f)$, $\mathrm{PSp}_d(p^f)'$ or $\mathrm{P}\Omega_d^\varepsilon(p^f)$ and let $\mathbb{K}$ be an algebraically closed field of characteristic p. Suppose that M is a nontrivial irreducible projective $\mathbb{K}T$-module satisfying $\dim_{\mathbb{K}}(M) \leqslant \frac{1}{2}m(m+1), \frac{1}{2}m^2$ or $\frac{1}{2}m^2 - 1$ in the respective cases. Then either M is quasiequivalent to the natural projective $\mathbb{K}T$-module of dimension m or M is quasiequivalent to one of the modules in Table 6.3.

Lemma 6.12
Let $T = T_m(4)$ be a nonabelian simple classical group and $V \cong M \otimes M^{(1)}$ an absolutely irreducible $\mathbb{F}_2T$-module. If $\dim(M) \geqslant \frac{1}{2}m(m-1) - 2$ then Γ is not X-strongly incidence-transitive.

Proof. By Theorem 6.8 there exists a module M such that $\dim(V) = 2n = \dim(M)^2$. Suppose $\dim(M) \geqslant \frac{1}{2}m(m-1) - 2$. Then $\dim(V) \geqslant (\frac{1}{2}m(m-1)-2)^2 = \frac{m^4}{4} - \frac{m^3}{2} - \frac{7m^2}{4} + 2m + 4$ and Lemma 6.3 implies $2^{\frac{m^4}{4} - \frac{m^3}{2} - \frac{7m^2}{4} + 2m + 2} < 2^{m^2+2}$. Taking $\log_2$ of each side and rearranging we have

$$m\left(\frac{m^2}{2} + \frac{11m}{4} - \frac{3m^3}{4} - 2\right) > 0 \tag{6.4}$$

Since $m \geqslant 2$, Equation (6.4) holds if and only if

$$\frac{m^2}{2} + \frac{11m}{4} - \frac{3m^3}{4} - 2 > 0. \tag{6.5}$$

Let $b(m) = \frac{m^2}{2} + \frac{11m}{4} - \frac{3m^3}{4} - 2$. Then $\frac{db}{dm} = \frac{11}{4} + m - \frac{9m^2}{4} = (m - \omega_+)(m - \omega_-)$ where $\omega_\pm = \frac{2 \pm \sqrt{103}}{9} \approx 1.35$ and $-.091$. In particular, if $m \geqslant 2 > \omega_+$ then $\frac{db}{dm} < 0$. Then for any $m \geqslant 2$ we have $b(m) \leqslant b(2) = -\frac{1}{2}$, contradicting Equation (6.5). $\square$

If $q = 4$, Lemma 6.11 and Lemma 6.12 imply it remains only to consider the natural modules T as well as those modules in Table 6.3. This is currently an open problem.

6.4. Simple classical groups in odd characteristic

Let $V = (\mathbb{F}_2^{2n}, B)$ be a symplectic space and $X = \mathrm{Sp}_{2n}(2)$. Let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ be an X-strongly incidence-transitive code with $\Delta \in \Gamma$ and $3 \leqslant |\Delta| \leqslant 2^{n-1}(2^n + \varepsilon) - 3$. Suppose $T_m(q)$ is an absolutely irreducible simple group of Lie type acting on V as a subgroup of X_Δ, where q is an odd prime power. This notation is fixed throughout Section 6.4.

Our main tool in the analysis of the cross characteristic subgroups of $\mathrm{Sp}_{2n}(2)$ are lower bounds on the linear degree of a faithful representation of a simple group of Lie type in cross characteristic.

Lemma 6.13 (Special case from [**62**])
Let T be a nonabelian simple classical group of Lie type in odd characteristic. Then the rank of a

T	M	$\dim(M)$
$\mathrm{PSL}^{\pm}(d,q)$	$\Lambda^2 W$ $S^2 W$ $\Lambda^3 W, d=6$	$\frac{1}{2}d(d-1)$ $\frac{1}{2}d(d+1)$ 20
$\mathrm{P}\Omega^{\circ}(2d+1,q)$ $d \geqslant 3$, q odd	$\Lambda^2 W$ Spin module, $d \leqslant 6$	$\frac{1}{2}d(d-1)$ 2^d
$\mathrm{Sp}(2d,q)$	Section of $\Lambda^2 W$ Spin module, $d \leqslant 6$ Section of $\Lambda^3 W, m=3, q$ odd $T \cong \mathrm{Sp}(4,2)'$	$\frac{1}{2}d(d-1)-1$ if $\gcd(m,p)=1$ $\frac{1}{2}d(d-1)-2$ if $p \mid m$ 2^d 14 3
$\mathrm{P}\Omega^{\varepsilon}_{2m}(q)$	Section $\Lambda^2 W$ Spin module $m \leqslant 7$	$\frac{1}{2}d(d-1), q$ odd $\frac{1}{2}d(d-1)-\gcd(2,m), q$ even 2^{m-1}

TABLE 6.2. Projective modules M associated with Lemma 6.11. Note that W denotes the natural module for T and $q=p^f$.

T	$e(T)$	Case	Exceptions
$\mathrm{PSL}_m(q)$	$\frac{1}{2}(q-1)$ $q^{m-1}-1$	$m=2$ $m \geqslant 3$	$e(\mathrm{PSL}_2(9))=3$
$\mathrm{PSU}_m(q)$	$(q^m-1)/(q+1)$ $q(q^{m-1}-1)/(q+1)$	$m \geqslant 4$ even $m \geqslant 3$ odd	$e(\mathrm{PSU}_4(3))=6$
$\mathrm{PSp}_{2m}(q)$	$\frac{1}{2}(q^m-1)$	$m \geqslant 2$	-
$\mathrm{P}\Omega^{\circ}_{2m+1}(q)$	$q^{2(m-1)}-1$ $q^{m-1}(q^{m-1}-1)$	$m \geqslant 3, q>5$ $m \geqslant 3, q=3,5$	$e(\mathrm{P}\Omega^{\circ}_7(3))=27$
$\mathrm{P}\Omega^{+}_{2m}(q)$	$(q^{m-1}-1)(q^{m-2}+1)$ $q^{m-2}(q^{m-1}-1)$	$m \geqslant 4, q>5$ $m \geqslant 4, q=3,5$	-
$\mathrm{P}\Omega^{-}_{2m}(q)$	$(q^{m-1}+1)(q^{m-2}-1)$	$m \geqslant 4$	-

TABLE 6.3. Minimal degrees for linear representations of the odd characteristic classical simple groups in even characteristic. See [**38**] for full details.

faithful representation of T over a field of even characteristic is at least $e(T)$, where $e(T)$ is defined in Table 6.4.

Lemma 6.14

Let q be an odd prime power and let $T=T_m(q)$ be a simple classical group over $\mathbb{F}_q$ with $m \geqslant 3$. To each possible T we associate a function $b_T(m,q)$ as defined in Table 6.4. If X_Δ is almost-simple with socle T then $b_T(m,q) \geqslant 0$.

Case	$T_m(q)$	$b_T(m,q)$
(a)	$\mathrm{PSL}_m(q)$	$\log_2(q)m^2 - q^{m-1} + 4$
(b)	$\mathrm{PSU}_m(q)$	$\log_2(q)m^2 - \frac{3}{4}q^{m-1} + \frac{15}{4} + \log_2(3)$
(c)	$\mathrm{PSp}_{2m}(q)$	$\log_2(q)(2m^2 - m + 1) - \frac{1}{2}q^m + \frac{5}{2}$
(d)	$\mathrm{P}\Omega^{\varepsilon}_{2m}(q)$	$\log_2(q)(2m^2 - m + 1) - q^{2m-4} + \log_2(5) + 1$
(e)	$\mathrm{P}\Omega^{\circ}_{2m+1}(q)$	$\log_2(q)(2m^2 + m + 1) - q^{2(m-1)} + 3$ if $q \geqslant 7$ $\log_2(q)(2m^2 + m + 1) - q^{2(m-1)} + q^{m-1} + 2$ if $q = 3, 5$

TABLE 6.4. $b_T(m,q)$ for the classical simple groups with $m \geqslant 3$ and q an odd prime power.

PROOF. By Lemma 6.3 we have $\log_2(|\operatorname{Aut}(T)|) - e(T) + 2 > 0$, where $e(T)$ is provided in Table 6.4. We provide bounds $|\operatorname{Aut}(T)| \leqslant cq^{p(m)}$ in Table 6.1 so that

$$\log_2(cq^{p(m)}) - e(T) + 2 > 0. \tag{6.6}$$

Using Inequality (5.17) as a starting point, we have:

(a) If $T = \mathrm{PSL}_m(q)$ with $m \geqslant 3$ then $e(T) = q^{m-1} - 1$ and $|\operatorname{Aut}(T)| \leqslant 2q^{m^2}$. Inequality (5.17) implies

$$0 < \log_2(2q^{m^2}) - (q^{m-1} - 1) + 2 = \log_2(q)m^2 - q^{m-1} + 4 = b(m,q).$$

(b) If $T = \mathrm{PSU}_m(q)$ with $m, q \geqslant 3$ then $e(T) \geqslant q(q^{m-1} - 1)/(q+1) \geqslant 3(q^{m-1} - 1)/4$ and $|\operatorname{Aut}(T)| \leqslant \frac{2}{3}q^{m^2}$. Inequality (5.17) implies

$$0 < \log_2\left(\frac{2}{3}q^{m^2}\right) - \frac{3}{4}(q^{m-1} - 1) + 2 = \log_2(q)m^2 - \frac{3}{4}q^{m-1} + \frac{15}{4} - \log_2(3) = b(m,q).$$

(c) If $T = \mathrm{PSp}_{2m}(q)$ with $m \geqslant 2$ and $q \geqslant 3$ then $e(T) = \frac{1}{2}(q^m - 1)$ and $|\operatorname{Aut}(T)| \leqslant q^{2m^2 - m + 1}$. Inequality (5.17) implies

$$0 \leqslant \log_2(q^{2m^2 - m + 1}) - \frac{1}{2}(q^m - 1) + 2 = \log_2(q)(2m^2 - m + 1) - \frac{1}{2}q^m + \frac{5}{2} = b(m,q).$$

(d) If $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ with $m \geqslant 4$ and $q \geqslant 3$ then $e(T) \geqslant (q^{m-1} + 1)(q^{m-2} - 1) \geqslant q^{2m-4}$ and $|\operatorname{Aut}(T)| \leqslant \frac{10}{4}q^{2m^2 - m + 1}$. Then Inequality (5.17) implies

$$0 < \log_2\left(\frac{10}{4}q^{2m^2 - m + 1}\right) - q^{2m-4} + 2 = \log_2(q)(2m^2 - m + 1) - q^{2m-4} + \log_2(5) + 1 = b(m,q).$$

(e) If $T = \mathrm{P}\Omega^{\circ}_{2m+1}(q)$ with $m \geqslant 3$ and $q \geqslant 7$ then $e(T) = q^{2(m-1)} - 1$ and $|\operatorname{Aut}(T)| \leqslant q^{2m^2 + m + 1}$. Inequality (5.17) implies

$$0 \leqslant \log_2(q^{2m^2 + m + 1}) - q^{2(m-1)} + 3 = \log_2(q)(2m^2 + m + 1) - q^{2(m-1)} + 3 = b(m,q).$$

On the other hand if $q = 3$ or 5 then Inequality (5.17) implies

$$0 \leqslant \log_2(q^{2m^2+m+1}) - q^{m-1}(q^{m-1} - 1) + 2 = \log_2(q^{2m^2+m+1}) - q^{2m-2} - q^{m-1} + 2 = b(m, q).$$

Therefore, for each $T_m(q)$ with $m \geqslant 3$ we have $b_T(m, q) \geqslant 0$. □

Lemma 6.15
Let q be an odd prime power and $m \geqslant 3$. Then $\mathrm{soc}(X_\Delta) \neq \mathrm{PSL}_m(q)$.

PROOF. Let $\Gamma \subset J(\mathcal{Q}^\varepsilon, k)$ be an X-strongly incidence-transitive code. If $T = \mathrm{PSL}_m(q)$ with q odd and $m \geqslant 3$ then by Lemma 6.14 we must have $b(m, q) \geqslant 0$, where

$$b(m, q) = \log_2(q)m^2 - q^{m-1} + 4$$

Computing the partial derivatives of b we find

$$\frac{\partial b}{\partial m} = \log_2(q)(2m - \ln(2)q^{m-1})$$
$$\frac{\partial b}{\partial q} = \frac{m^2}{\ln(2)q} + (1 - m)q^{m-2}.$$

For all $m, q \geqslant 3$ we have

$$\frac{\partial b}{\partial q} < 0 \Leftrightarrow \frac{m^2}{\ln(2)q} + (1 - m)q^{m-2} < 0 \Leftrightarrow \frac{m^2}{\ln(2)q} < (m - 1)q^{m-2}$$
$$\Leftrightarrow \frac{m^2}{\ln(2)(m - 1)} < q^{m-1} \Leftrightarrow \left(\frac{m^2}{\ln(2)(m - 1)}\right)^{\frac{1}{m-1}} < q.$$

But $m \geqslant 3$ so

$$\frac{\partial b}{\partial q} < 0 \Leftrightarrow \left(\frac{m^2}{\ln(2)(m - 1)}\right)^{\frac{1}{m-1}} \leqslant \sqrt{\frac{9}{8\ln(2)}} \approx 1.27 < q.$$

On the other hand

$$\frac{\partial b}{\partial m} < 0 \Leftrightarrow 2m - \ln(2)q^{m-1} < 0 \Leftrightarrow \left(\frac{2m}{\ln(2)}\right)^{\frac{1}{m-1}} < q,$$

so $\frac{\partial b}{\partial m} < 0$ for all $m, q \geqslant 3$. Therefore, for all $m > m' \geqslant 3$ and $q > q' \geqslant 3$ we have $b(m', q') > b(m, q)$. In particular, for all $m, q \geqslant 3$ we have $b(m, q) < b(3, 3) \approx -20.1 < 0$. This contradicts Lemma 6.14, so $\mathrm{soc}(X_\Delta) \neq \mathrm{PSL}_m(q)$ for $m, q \geqslant 3$ with q an odd prime power. □

Lemma 6.16
Let q be an odd prime power and $m \geqslant 3$. If $\mathrm{soc}(X_\Delta) \cong \mathrm{PSU}_m(q)$ then $(m, q) = (3, 3), (3, 5)$ or $(4, 3)$.

PROOF. Let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ be an X-strongly incidence-transitive code. If $T = \mathrm{PSU}_m(q)$ with q odd and $m \geqslant 3$ then by Lemma 6.14 must have $b(m, q) \geqslant 0$, where

$$b(m, q) = \log_2(q)m^2 - \frac{3}{4}q^{m-1} + \frac{15}{4} - \log_2(3).$$

Computing the partial derivatives of b we find

$$\begin{aligned}\frac{\partial b}{\partial m} &= \log_2(q)(2m - \frac{3}{4}\ln(2)q^{m-1})\\ \frac{\partial b}{\partial q} &= \frac{m^2}{\ln(2)q} + \frac{3}{4}(1-m)q^{m-2}.\end{aligned}$$

Then

$$\frac{\partial b}{\partial q} < 0 \Leftrightarrow \frac{m^2}{\ln(2)q} < \frac{3}{4}(m-1)q^{m-2} \Leftrightarrow \frac{4m^2}{3\ln(2)(m-1)} < q^{m-1} \Leftrightarrow \left(\frac{4m^2}{3\ln(2)(m-1)}\right)^{\frac{1}{m-1}} < q.$$

If $m \geqslant 4$ we have

$$\left(\frac{4m^2}{3\ln(2)(m-1)}\right)^{\frac{1}{m-1}} \leqslant \left(\frac{64}{9\ln(2)}\right)^{1/3} \approx 2.2.$$

and therefore $\frac{\partial b}{\partial q} < 0$ for all $m \geqslant 4$ and $q \geqslant 3$.

Similarly,

$$\frac{\partial b}{\partial m} < 0 \Leftrightarrow 2m < \frac{3}{4}\ln(2)q^{m-1} \Leftrightarrow \left(\frac{8m}{3\ln(2)}\right)^{\frac{1}{m-1}} < q.$$

Again, if $m \geqslant 4$ then

$$\left(\frac{8m}{3\ln(2)}\right)^{\frac{1}{m-1}} \leqslant \left(\frac{32}{3\ln(2)}\right)^{\frac{1}{3}} \approx 2.5$$

so $\frac{\partial b}{\partial m} < 0$ for all $m \geqslant 4$ and odd prime powers $q \geqslant 3$.

Therefore, for all $m > m' \geqslant 4$ and $q > q' \geqslant 3$ with $(m,q) \neq (4,3)$ we have $b(m',q') > b(m,q)$. In particular, we have $b(4,5) \approx -54.4$ and $b(5,3) \approx -19.0$, so $b(m,q) < 0$ for all $m \geqslant 4$ and $q \geqslant 3$ with $(m,q) \neq (4,3)$. Additionally, if $m = 3$ then, since X_Δ must admit a factorisation, [**35**, Corollary 2] implies $q = 3$ or 5. □

Lemma 6.17

Let q be an odd prime power and $m \geqslant 3$. If $\mathrm{soc}(X_\Delta) \cong \mathrm{PSp}_{2m}(q)$ then $(m,q) = (3,3)$ or $(4,3)$.

PROOF. If $T = \mathrm{PSp}_{2m}(q)$ and $m \geqslant 2$ then from Table 6.4 we have

$$b(m,q) = \log_2(q)(2m^2 - m + 1) - \frac{1}{2}q^m + \frac{5}{2}. \tag{6.7}$$

Computing the partial derivatives of b we find

$$\begin{aligned}\frac{\partial b}{\partial m} &= \frac{1}{2}\log_2(q)(8m - 2 - \ln(2)q^m)\\ \frac{\partial b}{\partial q} &= \frac{2m^2 - m + 1}{\ln(2)q} - \frac{mq^{m-1}}{2}.\end{aligned}$$

If $m, q \geqslant 3$ but $(m,q) \neq (3,3)$ or $(4,3)$ then $\frac{\partial b}{\partial m} < 0$. On the other hand we have

$$\frac{\partial b}{\partial q} < 0 \Leftrightarrow \frac{2m^2 - m + 1}{\ln(2)q} < \frac{mq^{m-1}}{2} \Leftrightarrow \frac{2m^2 - m + 1}{\ln(2)m} < q^m \Leftrightarrow \left(\frac{2m^2 - m + 1}{\ln(2)m}\right)^{\frac{1}{m}} < q.$$

So $\frac{\partial b}{\partial q} < 0$ if and only if $\left(\frac{2m^2-m+1}{\ln(2)m}\right)^{\frac{1}{m}} < q$. In particular, if $m \geqslant 3$ then $q > \left(\frac{18-3+1}{\ln(2)3}\right)^{\frac{1}{3}} \approx 2.0$ is sufficient to ensure $\frac{\partial b}{\partial q} < 0$. In particular, $b(3,5) \approx -23.0$, $b(4,5) \approx -242.7$ and $b(5,3) \approx -46.1$. This contradicts Lemma 6.14 unless $(m,q) = (3,3)$ or $(4,3)$. □

Lemma 6.18

Let q be an odd prime power and $m \geqslant 4$. Then $\mathrm{soc}(X_\Delta) \neq \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$.

PROOF. If $T = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ and $m \geqslant 4$ then we have

$$b(m,q) = \log_2(q)(2m^2 - m + 1) - q^{2m-4} + \log_2(5) + 1. \tag{6.8}$$

Computing the partial derivatives of b we find

$$\frac{\partial b}{\partial m} = \log_2(q)\left(4m - 1 - 2\ln(2)q^{2m-4}\right)$$
$$\frac{\partial b}{\partial q} = \frac{2m^2 - m + 1}{\ln(2)q} + (4-2m)q^{2m-5}.$$

Since $m \geqslant 4$ and $q \geqslant 3$, we have

$$\frac{\partial b}{\partial q} < 0 \Leftrightarrow \frac{2m^2 - m + 1}{\ln(2)(2m-4)} < q^{2m-4} \Leftrightarrow \left(\frac{2m^2 - m + 1}{\ln(2)(2m-4)}\right)^{\frac{1}{2m-4}} < q.$$

In particular, since $m \geqslant 4$ we have

$$\left(\frac{2m^2 - m + 1}{\ln(2)(2m-4)}\right)^{\frac{1}{2m-4}} \leqslant \left(\frac{29}{4\ln(2)}\right)^{\frac{1}{4}} \approx 1.8,$$

so $\frac{\partial b}{\partial q} < 0$ for all $m \geqslant 4$ and $q \geqslant 3$. Similarly, we have

$$\frac{\partial b}{\partial m} < 0 \Leftrightarrow \frac{4m-1}{2\ln(2)} < q^{2m-4} \Leftrightarrow \left(\frac{4m-1}{2\ln(2)}\right)^{\frac{1}{2m-4}} < q.$$

In particular, since $m \geqslant 4$ we have

$$\left(\frac{4m-1}{2\ln(2)}\right)^{\frac{1}{2m-4}} \leqslant \left(\frac{15}{2\ln(2)}\right)^{\frac{1}{4}} \approx 1.8,$$

so $\frac{\partial b}{\partial m} < 0$ for all $m \geqslant 4$ and $q \geqslant 3$.

Therefore, for all $m \geqslant 4$ and $q \geqslant 3$ we have $b(m,q) < b(4,3) \approx -31.7$. This contradicts Lemma 6.14, so $\mathrm{soc}(X_\Delta) \neq \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$ for any $m \geqslant 4$ and odd prime power $q \geqslant 3$. □

Lemma 6.19

Let $m \geqslant 3$ and $q = 3$ or 5. Then $\mathrm{soc}(X_\Delta) \neq \mathrm{P}\Omega^{\circ}_{2m+1}(q)$.

PROOF. If $T = \mathrm{P}\Omega^{\circ}_{2m+1}(q)$ and $m \geqslant 3$ then from Table 6.4 we have

$$b(m) = \log_2(q)(2m^2 + m + 1) - q^{2(m-1)} + q^{m-1} + 2, \tag{6.9}$$

where q is treated as a parameter. Computing the derivative of b we find

$$\frac{db}{dm} = \log_2(q)\left(4m + 1 - \ln(2)q^{m-1}(2q^{m-1} - 1)\right).$$

Since $m, q \geqslant 3$ we have

$$\frac{db}{dm} < 0 \Leftrightarrow \frac{4m+1}{\ln(2)} < q^{m-1}(2q^{m-1} - 1). \tag{6.10}$$

Now, note that

$$q^{m-1}(2q^{m-1} - 1) > q^{2m-2} \Leftrightarrow 2q^{m-1} - 1 > q^{m-1} \Leftrightarrow q^{m-1} > 1. \tag{6.11}$$

Since $m, q \geqslant 3$ we have $q^{m-1} > 1$ and therefore, combining Inequalities (6.11) and (6.10) we have

$$\frac{4m+1}{\ln(2)} < q^{2m-2} \Rightarrow \frac{db}{dm} < 0. \tag{6.12}$$

We have

$$\frac{4m+1}{\ln(2)} < q^{2m-2} \Leftrightarrow \left(\frac{4m+1}{\ln(2)}\right)^{\frac{1}{2m-2}} < q.$$

In particular, since $m \geqslant 3$ and $q = 3$ or 5, we have

$$\left(\frac{4m+1}{\ln(2)}\right)^{\frac{1}{2m-2}} \leqslant \left(\frac{13}{\ln(2)}\right)^{\frac{1}{4}} < 2.1 < q.$$

Therefore $\frac{db}{dm} < 0$ for $m, q \geqslant 3$. Therefore, for all $m \geqslant 3$ we have $b(m) \leqslant b(3) \approx -31.7$ and -554.3, for $q = 3$ and 5 respectively. This contradicts Lemma 6.14, so $\mathrm{soc}(X_\Delta) \neq \mathrm{P}\Omega^{\circ}_{2m+1}(3)$ or $\mathrm{P}\Omega^{\circ}_{2m+1}(5)$ for any $m \geqslant 3$. □

Lemma 6.20
Let $q \geqslant 7$ be an odd prime power and let $m \geqslant 3$. Then $\mathrm{soc}(X_\Delta) \neq \mathrm{P}\Omega^{\circ}_{2m+1}(q)$.

Proof. If $T = \mathrm{P}\Omega^{\circ}_{2m+1}(q)$ and $m \geqslant 3$ then from Table 6.4 we have

$$b(m, q) = \log_2(q)\,(2m^2 + m + 1) - q^{2(m-1)} + 3. \tag{6.13}$$

Computing the partial derivatives of b we find

$$\begin{aligned}\frac{\partial b}{\partial m} &= \log_2(q)\left(4m + 1 - 2\ln(2)q^{2m-4}\right)\\ \frac{\partial b}{\partial q} &= \frac{2m^2 + m + 1}{\ln(2)q} - (2m-2)q^{2m-3}.\end{aligned}$$

For $m \geqslant 3$ and $q \geqslant 7$ we have

$$\frac{\partial b}{\partial q} < 0 \Leftrightarrow \frac{2m^2+m+1}{\ln(2)q} < (2m-2)q^{2m-3} \Leftrightarrow \left(\frac{2m^2+m+1}{\ln(2)(2m-2)}\right)^{\frac{1}{2m-2}} < q.$$

Since $m \geqslant 3$, we have

$$\left(\frac{2m^2+m+1}{\ln(2)(2m-2)}\right)^{\frac{1}{2m-2}} \leqslant \left(\frac{22}{4\ln(2)}\right)^{\frac{1}{4}} \approx 1.7,$$

so $\frac{\partial b}{\partial q} < 0$ for all $q \geqslant 7$. Similarly, we have

$$\frac{\partial b}{\partial m} < 0 \Leftrightarrow 4m + 1 < 2\ln(2)q^{2m-4} \Leftrightarrow \left(\frac{4m+1}{2\ln(2)}\right)^{\frac{1}{2m-4}} < q.$$

Since $m \geqslant 3$, we have

$$\left(\frac{4m+1}{2\ln(2)}\right)^{\frac{1}{2m-4}} \leqslant \left(\frac{13}{2\ln(2)}\right)^{\frac{1}{4}} \approx 1.7,$$

so $\frac{\partial b}{\partial m} < 0$ for all $q \geqslant 7$. Therefore, for all $m \geqslant 3$ and odd prime powers $q \geqslant 7$, we have $b(m, q) \leqslant b(3, 7) \approx -2336$. This contradicts Lemma 6.14, so $\mathrm{soc}(X_\Delta) \neq \mathrm{P}\Omega^{\circ}_{2m+1}(q)$ for any $m \geqslant 3$ and $q \geqslant 7$. □

Lemma 6.21
Let q be an odd prime power with $q > 50$. Then $\mathrm{soc}(X_\Delta) \neq PSL_2(q)$.

Proof. Suppose Γ is X-strongly incidence-transitive. If $T = \mathrm{PSL}(2, q)$ we have $|\mathrm{Aut}(T)| = qf(q^2 - 1) \leqslant q^4$ and from Table 6.4, $e(T) = \frac{1}{2}(q - 1)$. Applying Lemma 6.3 we have $q^4 \geqslant |\mathrm{Aut}(T)| > 2^{n-2} \geqslant 2^{e(T)-2}$. Therefore

$$4\log_2(q) > e(T) - 2 = \frac{1}{2}(q - 1). \tag{6.14}$$

Let $b(q) = 4\log_2(q) - \frac{1}{2}q + \frac{5}{2}$. Then Inequality (6.14) implies $b(q) > 0$. The derivative of $b(q)$ is

$$\frac{db}{dm} = \frac{1}{\ln(2)q} - \frac{1}{2}$$

and therefore $q \geqslant 3$ implies $b(q)$ is decreasing. In particular, if $q > 50$ then we have $b(q) < b(51) \approx -0.31$. Therefore $\mathrm{soc}(X_\Delta) \neq \mathrm{PSL}_2(q)$ for odd prime powers $q > 50$. □

It seems reasonable to suspect that the nonexistence of Jordan-Steiner type codes with $\mathrm{soc}(X_\Delta) = \mathrm{PSL}_2(q)$ with $q \leqslant 50$ can be checked computationally. This is currently an open problem. Note that the factorisations of $\mathrm{PSL}_2(q)$ enumerated in [**35**] may provide hints towards a solution.

6.5. Some loose ends in the odd characteristic case

Several cases remain open; it is currently unknown whether there exists X-strongly incidence-transitive codes of Jordan-Steiner type with $\mathrm{soc}(X_\Delta)$ equal to one of $\mathrm{PSU}_3(3)$, $\mathrm{PSU}_3(5)$, $\mathrm{PSU}_4(3)$, $\mathrm{PSp}_4(q)$, $\mathrm{PSp}_6(3)$, $\mathrm{PSU}_8(3)$, or with $\mathrm{soc}(X_\Delta) = \mathrm{PSL}_2(q)$ with $q < 50$.

We use GAP [**59**] to eliminate some of the open cases from Section 6.4. Let $X = \mathrm{Sp}_{2n}(2)$ and let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ be an X-strongly incidence-transitive code. We denote the natural module of X by $V \cong \mathbb{F}_2^{2n}$. Let $\Delta \in \Gamma$ and suppose X_Δ is almost simple with $T = \mathrm{soc}(X_\Delta)$. Our treatment is similar in each case. A rough outline is as follows:

(a) Use Program D.1 to compute the largest value of n such that $|\mathrm{Aut}(T)| \geqslant 2^{n-1}(2^n - 1)$.
(b) Use the Atlas of Brauer Characters [**63**] or GAP [**59**] to find the absolutely irreducible 2-modular representations of symplectic, but not orthogonal type with dimension compatible with part (a).
(c) Use Program D.2 to compute the values of $k \in [2 : v/2]$ such that $k(v - k)$ divides $|X_\Delta|$.

Example 6.22
We analyse the case $X_\Delta = \mathrm{PSU}_3(3)$. By [**38**, Table 5.3.A], the minimum degree of an absolutely irreducible $\mathbb{F}_2T$-module is 6. Moreover, $|X_\Delta|$ is divisible by $|\overline{\Delta}| \geqslant 2^{n-2}(2^n-1)$, so $|\operatorname{Aut}(T)| \geqslant 2^{n-2}(2^n-1)$. This implies the dimension of V is at most 14. By [**63**], the only absolutely irreducible representation of $\mathrm{PSU}_3(3)$ in characteristic two which preserves a symplectic form, but is fixed point free on $\mathcal{Q}^\varepsilon$, occurs in dimension 6. However Lemma 6.5 shows that there are no X-strongly incidence-transitive codes associated with the maximal subgroup $G_2(2) \cong \mathrm{PSU}_3(3)$ of $\mathrm{Sp}_6(2)$.

Example 6.23
We analyse the case $\mathrm{soc}(X_\Delta) = \mathrm{PSU}_3(5)$. Since $|X_\Delta|$ is divisible by $|\overline{\Delta}| \geqslant 2^{n-2}(2^n-1)$, so $|\operatorname{Aut}(T)| \geqslant 2^{n-2}(2^n-1)$. This implies the dimension of V is at most 20. By [**63**], the only absolutely irreducible representation of $U_3(5)$ in characteristic two which preserves a symplectic form, but is fixed point free on $\mathcal{Q}^\varepsilon$, occurs in dimension 20. However, Program D.2 shows that there are no values of k such that $k(v-k)$ divides $|\operatorname{Aut}(T)|$. Therefore no X-strongly incidence-transitive codes arise in this case.

Example 6.24
We analyse $T = \mathrm{PSp}_6(3)$. We must have $|\operatorname{Aut}(T)| \geqslant 2^{n-1}(2^n-1)$, so Program D.1 implies $\dim(V) \leqslant 34$. The 2-modular character table of T is available in GAP [**59**]. There are no 2-modular representations of T of even dimension at most 34. Therefore no codes of interest arise in this case.

6.6. Sporadic simple groups

Suppose $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is X-strongly incidence-transitive and for $\Delta \in \Gamma$, $\mathrm{soc}(X_\Delta)$ is a sporadic simple group. The factorisations of the sporadic simple groups and their automorphisms are enumerated in [**36**]. We use this information to show such a code does not exist. The majority Section 6.6 follows from GAP calculations. The relevant code is available from [**64**].

Theorem 6.25
Let $X = \mathrm{Sp}_{2n}(2)$ and let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ be an X-strongly incidence-transitive code. Let Δ be a codeword of Γ. Then $\mathrm{soc}(X_\Delta)$ is not a sporadic simple group.

Proof. The factorisations of the sporadic simple groups and their automorphism groups are enumerated in [**36**, Tables 1,2,3]. We begin by considering five factorisations $G = AB$ where B is not known explicitly. Suppose $G = X_\Delta$, $A = X_{\Delta,\varphi}$ and $B = X_{\Delta,\psi}$ for $(\varphi,\psi) \in \Delta \times \overline{\Delta}$. If $G = AB$ with $B \leqslant C$, write $\kappa = |C : B|$. Recall from Lemma 6.2 that $\nu_o(|G:A|+|G:B|) = \nu_e(|G:A|+|G:B|) \pm 1$, where ν_e and ν_o denote the even and odd parts of a given integer.

(a) Suppose $G = Co_1$, $A = Co_3$ and $G_2(4).2 \leqslant B \leqslant (A_4 \times G_2(4)).2$. We know $|G_2(4).2|$ divides $|B|$, which in turn divides $(A_4 \times G_2(4)).2$, therefore $|B : G_2(4).2|$ divides 12. For each divisor, a GAP [**59**] computation yields a contradiction to Lemma 6.2.

(b) Suppose $G = Co_1$, $A = Co_2$ and $G_2(4) \leqslant B \leqslant (A_4 \times G_2(4)).2$. We have $|G : A| + |G : B| = 2^3(12285 + 2^3 \cdot 10758825\kappa)$, but $12285 + 2^3 \cdot 10758825\kappa > 2^3 \pm 1$ for all $\kappa \in \mathbb{Z}^+$. This contradicts Lemma 6.2.

(c) Suppose $G = \mathrm{Aut}(HS)$, $A = M_{22}.2$ and $B \leqslant 5^{1+2}_{+}[2^5]$. We have $|G : A| + |G : B| = 2^2(25 + 5544\kappa)$, but $25 + 5544\kappa > 2^2 \pm 1$ for all $\kappa \in \mathbb{Z}^+$. This contradicts Lemma 6.2.

(d) Suppose $G = \mathrm{Aut}(He)$, $A = \mathrm{Sp}_4(4).4$ and $B \leqslant 7^{1+2}_{+} \rtimes (S_3 \times C_6)$. Here we have $|G : A| + |G : B| = 2(1029 + 2^8 \cdot 1275\kappa)$, but $1029 + 2^8 \cdot 1275\kappa > 2 \pm 1$ for all $\kappa \in \mathbb{Z}^+$. This contradicts Lemma 6.2.

(e) Suppose $G = \mathrm{Aut}(J_2)$, $A = \mathrm{PSU}_3(3).2$ and $B \leqslant 5^2 \rtimes (C_4 \times S_3)$. We have $|G : A| + |G : B| = 2^2(25 + 2^3 \cdot 63\kappa)$, but $25 + 2^3 \cdot 63\kappa > 2^2 \pm 1$ for all $\kappa \in \mathbb{Z}^+$. This contradicts Lemma 6.2.

Therefore none of the factorisations in cases (a)-(e) above are associated with a Jordan-Steiner action. For the remaining factorisations of the sporadic simple groups and their automorphism groups, both factors are known explicitly. These are eliminated with GAP [**59**] (see [**64**]). Therefore $\mathrm{soc}(X_\Delta)$ is not a sporadic simple group. $\square$

CHAPTER 7

Affine type strongly incidence-transitive codes over $\mathbb{F}_2$

7.1. Introduction

Let $\mathcal{V}$ be an n-dimensional vector space over $\mathbb{F}_q$. For each $w \in \mathcal{V}$, denote by t_w the translation defined by $v^{t_w} = v + w$ for all $v \in \mathcal{V}$. Denote by T the group of all translations of $\mathcal{V}$, and by $\mathrm{A\Gamma L}_n(q) = T \rtimes \Gamma\mathrm{L}_n(q)$ the group of all affine semilinear transformations of $\mathcal{V}$. By an X-strongly incidence-transitive code of *affine type*, we mean an X-strongly incidence-transitive code $\Gamma \subset J(\mathcal{V}, k)$, where $T \lhd X \leqslant \mathrm{A\Gamma L}_n(q)$ and X acts 2-transitively on $\mathcal{V}$. We assume throughout that $n \geqslant 3$ and $2 \leqslant k \leqslant n-2$. The articles [**1**, Section 6] and [**28**] together provide a classification of affine-type X-strongly incidence-transitive codes, provided that $q \neq 2$. For the remainder of the Chapter we set $q = 2$ and investigate some of the possibilities.

Definition 7.1
Let Γ be an X-strongly incidence-transitive code of affine type. We define $\mathcal{M}_\Gamma = \{T \cap X_\Delta \mid \Delta \in \Gamma\}$, and for each $M \in \mathcal{M}_\Gamma$ we define $\Gamma_M \subseteq \Gamma$ by $\Gamma_M = \{\Delta \in \Gamma \mid T \cap X_\Delta = M\}$. We refer to the elements of $\mathcal{P} = \{\Gamma_M \subseteq \Gamma \mid M \in \mathcal{M}_\Gamma\}$ as the *components* of Γ. We call Γ an X-*single-component* code if for all $\Delta_1, \Delta_2 \in \Gamma$ we have $T \cap X_{\Delta_1} = T \cap X_{\Delta_2}$. We call Γ an X-*translation-free* code if $T \cap X_\Delta$ is the trivial group for all $\Delta \in \Gamma$.

When there is little ambiguity, we write $\mathcal{M} = \mathcal{M}_\Gamma$ and $\mathcal{P} = \mathcal{P}_\Gamma$. In Section 7.2 we construct a projection from a single-component code onto a translation-free code. In Section 7.3 we classify the translation-free codes and provide one possible method for lifting a translation-free code to a single-component code. The classification of all affine-type strongly incidence-transitive codes with $q = 2$ remains an open problem.

We fix the following notation throughout Chapter 7: $\mathcal{V} = \mathbb{F}_2^n$ and $\mathcal{V}^{\#} = \mathcal{V} \backslash \{0\}$, X is a subgroup of $\mathrm{AGL}_n(2)$ which contains the translation group T and acts 2-transitively on $\mathcal{V}$, and $\Gamma \subset \binom{\mathcal{V}}{k}$ is an X-strongly incidence-transitive code. Note that for all $\Delta \in \Gamma$, $T_\Delta = X_\Delta \cap T$ is a normal subgroup of X_Δ and $TX_\Delta/T \cong X_\Delta/T_\Delta$ is isomorphic to a subgroup of $\mathrm{GL}_n(2)$.

Lemma 7.2
Let $\Gamma \subset \binom{\mathcal{V}}{k}$ be an X-strongly incidence-transitive code of affine-type.

(a) The set of components $\mathcal{P} = \{\Gamma_M \mid M \in \mathcal{M}\}$ is a system of imprimitivity preserved by X, and the action of X on the parts of $\mathcal{P}$ is equivalent to the transitive action of X on $\mathcal{M}$.
(b) For each $M \in \mathcal{M}$, Γ_M is an $N_X(M)$-strongly incidence-transitive code in $J(\mathcal{V}, k)$.

(c) We have $N_X(M) = T \rtimes N_{X_0}(M)$, $|\mathcal{M}| = |X : N_X(M)| = |X_0 : N_{X_0}(M)|$, and $|\Gamma_M| = |N_X(M) : X_\Delta|$.

PROOF. (a) Clearly Γ is a disjoint union $\cup_{M\in\mathcal{M}}\Gamma_M$. For $x \in X$ and $\Delta \in \Gamma_M$, the codeword $\Delta' := \Delta^x$ is such that $T_{\Delta'} = T \cap X_{\Delta'} = T \cap X_\Delta^x = T_\Delta^x$. Therefore for each $M \in \mathcal{M}$ we have

$$\begin{aligned}(\Gamma_M)^x &= \{\Delta^x \in \Gamma \mid T_\Delta = M\} = \{\Delta \in \Gamma \mid T_{\Delta^{x^{-1}}} = M\} \\ &= \{\Delta \in \Gamma \mid (T_\Delta)^{x^{-1}} = M\} = \{\Delta \in \Gamma \mid T_\Delta = M^x\} = \Gamma_{M^x}.\end{aligned}$$

Therefore $(\Gamma_M)^x \in \mathcal{P}$ and the action of X on the parts of $\mathcal{P}$ is equivalent to the transitive action of X on $\mathcal{M}$.

(b) Let $M \in \mathcal{M}$. Part (a) implies Γ_M is a block of imprimitivity in the transitive action of X on Γ, and the stabiliser of Γ_M is $N_X(M)$. Since, for a transitive action, the setwise stabiliser of a block acts transitively on the points of the block, we have that $N_X(M)$ is transitive on Γ_M. If $\Delta \in \Gamma_M$, then $X_\Delta \leqslant N_X(M) \leqslant X$ so X_Δ is also the stabiliser of Δ in the action of $N_X(M)$ on Γ_M. Since X_Δ is transitive on $\Delta \times \overline{\Delta}$, it follows that Γ_M is an $N_X(M)$-strongly incidence-transitive code.

(c) The translation group T centralises M, so $T \leqslant N_X(M)$, and hence $N_X(M) = T \rtimes N_{X_0}(M)$. Note also that T acts trivially on $\mathcal{M}$, so $|\mathcal{M}| = |X : N_X(M)| = |X_0 : N_{X_0}(M)|$. Finally $|\Gamma_M| = |\Gamma|/|\mathcal{M}| = |N_X(M) : X_\Delta|$.

□

7.2. Single-component strongly incidence-transitive codes

In Section 7.2 we show that every single-component strongly incidence-transitive code of affine type can be projected onto a translation-free strongly incidence-transitive code which is also of affine type.

Lemma 7.3
If $\Gamma = \Gamma_M \subset \binom{\mathcal{V}}{k}$ is an X-single-component code then M is a normal subgroup of X and the set of M-orbits in $\mathcal{V}$ is a system of imprimitivity preserved by X. Moreover, the M-orbits in $\mathcal{V}$ are the translations of the subspace $U = \{m \in \mathcal{V} \mid t_m \in M\}$.

PROOF. First, Lemma 7.2 implies $\Gamma = \Gamma_M$ if and only if $|\mathcal{M}| = |X : N_X(M)| = 1$ if and only if $N_X(M) = X$ if and only if $M \lhd X$. By Definition 7.1, M leaves each $\Delta \in \Gamma$ invariant. Since each codeword is a proper subset of $\mathcal{V}$, $M \neq T$ and M is an intransitive normal subgroup of X. Therefore the set of M-orbits in $\mathcal{V}$ is a system of imprimitivity preserved by the action of X. For all $v \in \mathcal{V}$ we have $v^M = \{v + m \mid t_m \in M\} = v + \{m \mid t_m \in M\} = v + U$. Finally, $u, v \in U$ if and only if $t_u, t_v \in M$ if and only if $t_{u+v} \in M$ if and only if $u + v \in U$, that is, U is a subspace of $\mathcal{V}$ and the M-orbits are translates of U. □

Of course, if M is the trivial group then the system of imprimitivity constructed in Lemma 7.3 is also trivial.

Construction 7.4 ([**1**], Example 4.4)

Input: A set $\mathcal{V}$ of v points, a partition $\mathcal{U}$ of $\mathcal{V}$ into b parts, each of size a with $a, b > 1$, and a code Γ in $J(b, k_0)$ with point set $\mathcal{U}$.

Output: A code $\widehat{\Gamma}$ in $J(v, k)$ with $v = ab$ and $k = bk_0$.

Description: For each $\Delta \in \Gamma$ define $\widehat{\Delta} \in \binom{\mathcal{V}}{k}$ by $\widehat{\Delta} := \bigcup_{U \in \Delta} U$ where with $k = k_0 b$. Return $\widehat{\Gamma} := \{\widehat{\Delta} \mid \Delta \in \Gamma\}$.

Lemma 7.5 ([**1**], Lemma 7.6)

Let $\Gamma \subseteq \binom{\mathcal{U}}{k_0}$ and let $\widehat{\Gamma}$ denote the code obtained by applying Construction 7.4 to Γ. Let $A = \mathrm{Aut}(\Gamma) \cap \mathrm{Sym}(\mathcal{U})$. Then $\mathrm{Aut}(\widehat{\Gamma})$ contains $S_a \wr A$ and $\delta(\widehat{\Gamma}) = a\delta(\Gamma)$. Further, we have the following:

(a) If Γ is A-strongly incidence-transitive then $\widehat{\Gamma}$ is $(S_a \wr A)$-strongly incidence-transitive, and either $\Gamma = \binom{\mathcal{U}}{k_0}$ or $\delta(\Gamma) \geqslant 2$.

(b) If $S_a \wr A$ is neighbour-transitive on $\widehat{\Gamma}$ then either Γ is A-strongly incidence-transitive, or $a = 2$ and $\delta(\Gamma) = 1$.

Lemma 7.6

Suppose $\Gamma = \Gamma_M \subset \binom{\mathcal{V}}{k}$ is an X-single-component code and M is nontrivial and $\Delta \in \Gamma$. Then either Δ or $\overline{\Delta}$ is an affine flat, or Γ arises as the output of Construction 7.4 applied to a code in $J(v/|M|, k/|M|)$.

Proof. Let $\mathcal{U}$ denote the set of M-orbits in $\mathcal{V}$ and let $a = 2^\ell$ and $b = 2^{n-\ell}$. By Lemma 7.3, $\mathcal{U}$ is a system of imprimitivity preserved by X, and therefore Lemma 1.21 implies that each $\Delta \in \Gamma$ is a union blocks of imprimitivity in $\mathcal{U}$. In particular, [**1**, Proposition 4.7] implies that Γ arises from [**1**, Examples 4.1 or 4.4]. The only code from [**1**, Example 4.1] for which codewords are unions of M-orbits come from Line 1 of [**1**, Table 3] where Δ (or $\overline{\Delta}$) is an M-orbit, and hence codewords (or their complements) are ℓ-flats. The codes from [**1**, Example 4.4] all arise from Construction 7.4, where the input code is in $J(\mathcal{U}, k/2^\ell)$. □

We provide some further details in the case that Δ is an affine flat in Appendix C.3. For the remainder of Chapter 7 we focus our attention on codes which arise as the output of Construction 7.4.

Definition 7.7

Let $\Delta \subset \mathcal{V}$ and let L be a ℓ-flat in $\mathrm{AG}_n(2)$. We call L a Δ-shared ℓ-flat if $L \cap \Delta$ and $L \cap \overline{\Delta}$ are nonempty. If $v \in \mathcal{V}^\#$ then we use $\langle v \rangle^T$ to denote the parallel class of affine 1-flats which contains the 1-dimensional subspace of $\mathcal{V}$ spanned by v.

Lemma 7.8

Let $\mathcal{V} = \mathbb{F}_2^n$ and let $\Gamma = \Gamma_M \subset \binom{\mathcal{V}}{k}$ be an X-single-component code. Let $\Delta \in \Gamma$ and $U = \{m \in \mathcal{V} \mid t_m \in M\}$. Then:

(a) $v \in U^\#$ if and only if the parallel class $\langle v \rangle^T$ contains no Δ-shared 1-flats, and

(b) X_Δ acts transitively on the set $\mathcal{D} = \{\langle v \rangle^T \mid v \in \mathcal{V} \backslash U\}$.

PROOF. By Lemma 7.2, $N_X(M) = T \rtimes Y_0$, where $Y_0 = N_{X_0}(M)$. Recall that $X_\Delta \leqslant N_X(M)$.

(a) Suppose $v \in U^\#$. Then $t_v \in M = T_\Delta$, and for all $u \in \Delta$ we have $u^{t_v} = u + v \in \Delta$. In other words, if $u \in \Delta$ then $\{u, u+v\} \subseteq \Delta$, so $\langle v\rangle^T$ contains no Δ-shared 1-flats. Conversely, suppose that $\langle v\rangle^T$ contains no shared 1-flats. Then for all $u \in \Delta$, $\langle v\rangle^{t_u} = \{u, v+u\}$ is contained in Δ, so $u^{t_v} = u + v \in \Delta$ for all $u \in \Delta$, and hence $t_v \in T_\Delta$. Therefore $v \in U^\#$.

(b) Let $\langle u\rangle^T, \langle v\rangle^T$ be two members of $\mathcal{D}$. By part (a), each contains a Δ-shared 1-flat, so there exists $a, c \in \Delta$ and $b, d \in \overline{\Delta}$ such that $\{a, b\}, \{c, d\}$ are Δ-shared 1-flats in $\langle u\rangle^T, \langle v\rangle^T$, respectively. Since Γ_M is $N_X(M)$-strongly incidence-transitive, by Lemma 7.2, there exists $x \in N_X(M)$ such that $(a, b)^x = (c, d)$, and hence $(\langle u\rangle^T)^x = \langle v\rangle^T$.

□

Theorem 7.9

Let $\Gamma = \Gamma_M \subset \binom{\mathcal{V}}{k}$ be an X-single-component code with $|M| = 2^\ell \neq 1$ and let $\mathcal{U}$ denote the set of M-orbits in $\mathcal{V}$. For each $\Delta \in \Gamma$, define $\breve{\Delta} \in \binom{\mathcal{U}}{k/|M|}$ to be the set of M-orbits contained in Δ, and define $\breve{\Gamma} := \{\breve{\Delta} \mid \Delta \in \Gamma\}$. Let $U = \{m \in \mathcal{V} \mid t_m \in M\}$. The following hold:

(a) $\breve{\Gamma}$ is an $N_X(M)/M$-strongly incidence-transitive code in $J(\mathcal{V}/U, k/2^\ell)$.

(b) Let $Z = \langle T, X_\Delta\rangle = T \rtimes Z_0$. Then Z_0 is transitive on the sets $\mathcal{D} = \{\langle v\rangle^T \mid v \in \mathcal{V}\backslash U\}$ and $\mathcal{V}\backslash U$.

(c) $N_X(M)/M \cong (T/M) \rtimes N_{X_0}(M)$ is a 2-transitive subgroup of $\mathrm{AGL}(\mathcal{V}/U)$, and $\breve{\Gamma}$ is translation-free.

PROOF. First, note that if $\Delta \in \Gamma$ then Lemma 7.3 implies that $\breve{\Delta}$ is well defined. Then we have:

(a) By definition, M fixes each element of $\mathcal{U}$, so the quotient group $N_X(M)/M$ acts on $\breve{\Gamma}$. Moreover, $N_X(M)$ is transitive on Γ_M and therefore $N_X(M)/M$ acts transitively on $\breve{\Gamma}$. Let $\breve{\Delta} \in \breve{\Gamma}$, and let $\Delta := \cup_{U+v\in\breve{\Delta}}(U + v)$, so $\Delta \in \Gamma_M$. Now, $X_\Delta \leqslant N_X(M)$ and X_Δ is transitive on $\Delta \times \overline{\Delta}$, so it follows that X_Δ induces a transitive action on $\breve{\Delta} \times (\mathcal{U}\backslash\breve{\Delta})$. This proves part (a).

(b) Let $Z = \langle T, X_\Delta\rangle = T \rtimes Z_0$ and note $Z_0 \leqslant N_{X_0}(M)$. Since T acts trivially on $\mathcal{D}$, it follows that $Z = \langle T, X_\Delta\rangle$ acts transitively on $\mathcal{D}$ with T in the kernel of the action. Then, since $Z = T \rtimes Z_0 = TX_\Delta$, the groups Z_0 and X_Δ induce the same group of permutations on $\mathcal{D}$, though M lies in the kernel of the second action. In particular, Lemma 7.8 implies Z_0 is transitive on $\mathcal{D}$. Then since Z_0 fixes 0, we must have that Z_0 is transitive on $\mathcal{V}\backslash U$.

(c) The structure of $N_X(M)/M$ follows from the equation $N_X(M) = T \rtimes N_{X_0}(M)$. The group $N_X(M)/M$ acts on $\mathcal{V}/U$ as a group of affine type containing the translation group T/M. The stabiliser of the zero vector in this action is isomorphic to $N_{X_0}(M)$ acting on the quotient space $\mathcal{V}/U$. Since $N_{X_0}(M)$ contains Z_0, and since Z_0 is transitive on $\mathcal{V}\backslash U$, it follows that both Z_0 and $N_{X_0}(M)$ induce transitive actions on $(\mathcal{V}/U)^\#$. Thus $N_X(M)/M$ is a 2-transitive group of affine type on $\mathcal{V}/U$. Finally, since $T_\Delta = M$, for $\Delta \in \Gamma_M$, it follows that X_Δ is the stabiliser in $N_X(M)$ of the corresponding codeword $\breve{\Delta} \in \breve{\Gamma}$, and that in $N_X(M)/M$ we have $(X_\Delta/M) \cap (T/M) = M/M = 1$. Thus $\breve{\Gamma}$ is translation-free.

□

7.3. Translation-free strongly incidence-transitive codes

Let $\mathcal{V} = \mathbb{F}_2^n$ and let $\Gamma \subset \binom{\mathcal{V}}{k}$ be an X-strongly incidence-transitive code of affine type. Recall from Definition 7.1 that Γ is called *translation-free* if $T_\Delta = \{1\}$ for all $\Delta \in \Gamma$. In Section 7.3 we classify the translation-free codes in $J(\mathcal{V}, k)$. We begin by stating a special case of Lemma 7.8.

Corollary 7.10
Let $\Gamma \subset \binom{\mathcal{V}}{k}$ be an X-translation-free code with $\Delta \in \Gamma$. Then:
(a) every parallel class of 1-flats in $\mathrm{AG}_n(2)$ contains a Δ-shared 1-flat, and
(b) X_Δ acts transitively on the set of all parallel classes of 1-flats in $\mathrm{AG}_n(2)$.

Recall that a 2-(v, k, λ) design is called *symmetric* if the number of points is equal to the number of blocks. Below we describe some families of symmetric 2-(v, k, λ) designs which are used in Lemma 7.13.

Example 7.11
Let $\mathcal{V} = \mathbb{F}_2^{2n}$ with $n \geqslant 2$ and equip $\mathcal{V}$ with a symplectic form B. Consider the set $\mathcal{Q}$ of all quadratic forms on $\mathcal{V}$ which polarise to B. Associate with each pair $(\varphi, \varepsilon) \in \mathcal{Q} \times \{\pm\}$ the set $\Delta^\varepsilon(\varphi) \subset \mathcal{V}$ defined by

$$\Delta^\varepsilon(\varphi) = \begin{cases} \mathrm{sing}(\varphi) & \text{if } \varphi \in \mathcal{Q}^\varepsilon \\ \mathcal{V} \backslash \mathrm{sing}(\varphi) & \text{if } \varphi \in \mathcal{Q}^{-\varepsilon} \end{cases}.$$

For each $\varepsilon \in \{\pm\}$ we define a code $\mathcal{S}^\varepsilon(\mathcal{V}) = \{\Delta^\varepsilon(\varphi) \mid \varphi \in \mathcal{Q}(V)\}$ in $J(2^{2n}, 2^{n-1}(2^n + \varepsilon))$. The codewords of $\mathcal{S}^\varepsilon(\mathcal{V})$ are precisely the blocks of the 2-transitive symmetric 2-designs with full automorphism group $X = \mathrm{ASp}_{2n}(2)$ which were described by Kantor in [**50**].

William Kantor classified the symmetric 2-transitive 2-(v, k, λ) designs. His classification is used in our classification of translation-free strongly incidence-transitive codes, so we recall the result below.

Theorem 7.12 ([**65**])
Let $\mathcal{D}$ be a symmetric 2-(v, k, λ) design with $v \geqslant 2k$ and suppose $\mathrm{Aut}(\mathcal{D})$ acts 2-transitively on points. Then $\mathcal{D}$ is one of:
(i) a projective space with full automorphism group $\mathrm{P\Gamma L}_n(q)$ for some $n \geqslant 3$, $v = \frac{q^n-1}{q-1}$ and $k = \frac{q^{n-1}-1}{q-1}$;
(ii) the unique Hadamard 2-$(11, 5, 2)$ design $H(11)$ with full automorphism group $X = \mathrm{PSL}_2(11)$ and block stabiliser $X_\Delta = A_5$;
(iii) Higman's 2-$(176, 50, 14)$ design D_{176} with full automorphism group $X = HS$ and block stabiliser $X_\Delta = \mathrm{PSU}_3(5) \rtimes C_2$; or
(iv) the 2-designs $\mathcal{S}^+(V)$ described in Example 7.11, with full automorphism group $\mathrm{ASp}_{2m}(2)$.

Theorem 7.13
Let Γ be an X-translation-free code and let $\Delta \in \Gamma$. Define $Y = T \rtimes X_\Delta$ and define a code $\Gamma' \subseteq J(\mathcal{V}, k)$ by $\Gamma' = \Delta^Y$. Then $\Gamma' \subseteq \Gamma$ and the codewords of Γ' are the blocks of a point 2-transitive symmetric 2-design with point set $\mathcal{V}$. In particular, Γ' is the block set of one of the designs $\mathcal{S}^+(\mathcal{V})$ and $\mathcal{S}^-(\mathcal{V})$ defined in Example 7.11. Conversely, if $X = \mathrm{ASp}_{2n}(2)$ then for each $\varepsilon \in \{\pm\}$, $\Gamma = \mathcal{S}^\varepsilon(\mathcal{V})$ is an X-strongly incidence-transitive code in $J(v,k)$, where $v = 2^{2n}$ and $k = 2^{n-1}(2^n + \varepsilon)$.

Proof. Let $Y = TX_\Delta$ and $\Gamma' = \Delta^Y$. Then $Y = T \rtimes Y_0$, where Y_0 is the stabiliser of the zero vector in Y. Since Γ is translation-free, $T \cap X_\Delta = \{1\}$ and therefore

$$Y_0 \cong Y/T \cong TX_\Delta/T \cong X_\Delta/(X_\Delta \cap T) \cong X_\Delta.$$

By Corollary 7.10, X_Δ is transitive on the set of parallel classes of 1-flats in $\mathcal{V}$. It follows that Y and Y_0 are transitive on the set of parallel classes of 1-flats in $\mathcal{V}$, and in particular Y_0 is transitive on $\mathcal{V}\backslash\{0\}$. Therefore Y is 2-transitive on $\mathcal{V}$ and $\Gamma' = \Delta^Y$ is the block set of a 2-design with point set $\mathcal{V}$. Moreover,

$$\begin{aligned} |\Gamma'| &= |Y : Y_\Delta| = |Y : X_\Delta| \text{ (since } Y_\Delta = X_\Delta) \\ &= \frac{|Y_0||T|}{|X_\Delta|} = |T| \text{ (since } Y_0 \cong X_\Delta). \end{aligned}$$

Therefore Γ' is the block set of a 2-transitive symmetric 2-design with point set $\mathcal{V}$. The point 2-transitive symmetric 2-designs were classified by Kantor [**65**] (see Theorem 7.12). In particular, Γ' is the block set of $\mathcal{S}^+(\mathcal{V})$ or $\mathcal{S}^-(\mathcal{V})$. It remains to prove that these designs yield strongly incidence-transitive codes.

By Lemma 1.20, $\mathcal{S}^\varepsilon(\mathcal{V})$ is X-strongly incidence-transitive if and only if

(i) X is transitive on $\mathcal{V}$;
(ii) there exists $u \in \mathcal{V}$ such that X_u acts transitively on the set Γ_u of blocks containing u; and
(iii) there exists $\Delta \in \Gamma$ with $u \in \Delta$ such that $X_{u,\Delta}$ acts transitively on $\overline{\Delta}$.

We know $X = \mathrm{ASp}_{2n}(2)$ acts transitively on $\mathcal{V}$ since the group of translations is transitive on $\mathcal{V}$. Therefore property (i) holds. Next we choose $u = 0$ and consider the set Γ_0 of codewords in Γ that contain 0. Since $\varphi(0) = 0$ for all $\varphi \in \mathcal{Q}$, it follows that $\Gamma_0 = \{\Delta^\varepsilon(\varphi) \mid \varphi \in \mathcal{Q}^\varepsilon\}$. For any $\psi, \psi' \in \mathcal{Q}^\varepsilon$, Theorem 3.1 implies there exists $g \in X_0$ such that $\psi' = \psi^g$. Therefore

$$\begin{aligned} \Delta^\varepsilon(\psi)^g &= \{xg \in \mathcal{V} \mid \psi(x) = 0\} \\ &= \{y \in \mathcal{V} \mid \psi(yg^{-1}) = 0\} \\ &= \{y \in \mathcal{V} \mid \psi^g(y) = 0\} \\ &= \Delta^\varepsilon(\psi'). \end{aligned}$$

Therefore X_0 acts transitively on Γ_0 and property (ii) holds. Finally, for any codeword $\Delta = \Delta^\varepsilon(\varphi)$ containing 0 we have $\overline{\Delta} = \{v \in \mathcal{V} \mid \varphi(v) = 1\}$ so Theorem 2.28 implies that $X_{0,\Delta}$ acts transitively on $\overline{\Delta}$. Therefore $\Gamma = \mathcal{S}^\varepsilon(\mathcal{V})$ is an X-strongly incidence-transitive code in $J(\mathcal{V}, 2^{n-1}(2^n+\varepsilon))$ for each $\varepsilon \in \{\pm\}$ the code. $\square$

We provide below a construction which lifts a translation-free code on a space of dimension r to a single-component code on a space of dimension $r+s$, where s is an arbitrary positive integer.

Lemma 7.14
Let Γ be a Y-translation-free code in $J(\mathcal{U},k)$ where $|\mathcal{U}|=2^r$, $Y=T\rtimes Y_0\leqslant \mathrm{AGL}(\mathcal{U})$, $s\in\mathbb{Z}^+$ and $\mathcal{V}=\mathbb{F}_2^s\times\mathcal{U}$. Write the vectors in $\mathcal{V}$ as ordered pairs (u,v) with $u\in\mathbb{F}_2^s$, $v\in\mathcal{U}$. For each $\Delta\in\Gamma$ define $\widehat{\Delta}=\mathbb{F}_2^s\times\Delta\in\binom{\mathcal{V}}{2^sk}$, and let $\widehat{\Gamma}=\{\widehat{\Delta}\mid\Delta\in\Gamma\}$. Let $X=T\rtimes X_0$, where T is the translation group on $\mathcal{V}$ and

$$X_0=\left\{\begin{pmatrix}A&0\\B&C\end{pmatrix}\mid A\in GL_s(2),B\in\mathbb{F}_2^{r\times s},C\in Y_0\right\}.$$

Then $\widehat{\Gamma}$ is an X-single-component code in $J(\mathcal{V},2^sk)$, and for each $\widehat{\Delta}\in\widehat{\Gamma}$ we have $T_{\widehat{\Delta}}=\{t_{(u,0)}\in T\mid u\in\mathbb{F}_2^s\}$.

Proof. We begin by demonstrating that X is an automorphism group of $\widehat{\Gamma}$. Let $\Delta\in\Gamma$ and let $x_0\in X_0$ so that $(u,v)x_0=(uA+vB,vC)$ for all $(u,v)\in\mathcal{V}$. Then for all $\Delta\in\Gamma$ we have $\widehat{\Delta}^{x_0}=(\mathbb{F}_2^s\times\Delta)^{x_0}=\mathbb{F}_2^s\times\Delta^C=\widehat{\Delta^C}$. But $C\in\mathrm{Aut}(\Gamma)$ so $\Delta^C\in\Gamma$ and therefore $\widehat{\Delta^C}\in\widehat{\Gamma}$. Therefore $x_0\in\mathrm{Aut}(\widehat{\Gamma})$. Also, the translation $t_{(u',v')}\in T$ maps (u,v) to $(u+u',v+v')$ and hence maps $\widehat{\Delta}$ to $\widehat{\Delta}^{t_{(0,v')}}$, and since $t_{(0,v')}\in T\leqslant Y$, we have $t_{(u',v')}\in\mathrm{Aut}(\widehat{\Gamma})$. Thus $X\leqslant\mathrm{Aut}(\widehat{\Gamma})$. Moreover, Y acts transitively on Γ and therefore X is transitive on $\widehat{\Gamma}$. Let $\widehat{\Delta}\in\Gamma$. The computation above shows that $T_{\widehat{\Delta}}$ consists of all $t_{(u',v')}$ such that $\Delta^{t_{(0,v')}}=\Delta$. Since Γ is translation-free, it follows that $T_{\widehat{\Delta}}=\{t_{(u,0)}\in T\mid u\in\mathbb{F}_2^s\}$. We claim that $X_{\widehat{\Delta}}$ is transitive on $\widehat{\Delta}\times\overline{\widehat{\Delta}}$. To prove this, let $a_i:=(u_i,v_i)\in\widehat{\Delta}$ and $b_i=(w_i,z_i)\in\overline{\widehat{\Delta}}$, for $i=1,2$. We need to find $x\in X$ such that $(a_1,b_1)^x=(a_2,b_2)$. Now, $(v_1,z_1),(v_2,z_2)\in\Delta\times\overline{\Delta}$, and since Γ is Y-strongly incidence-transitive, there exists $C\in Y$ such that $(v_1,z_1)^C=(v_2,z_2)$, and hence $\begin{pmatrix}I&0\\0&C\end{pmatrix}\in X_0$ maps a_1 to (u_1,v_2) and b_1 to (w_1,z_2). Thus it is sufficient to prove the claim in the case where $v_1=v_2=v\in\Delta$ and $z_1=z_2=z\in\overline{\Delta}$. Note that $v\neq z$, since these lie in different subsets of $\mathcal{U}$. Next we argue that it is sufficient to prove the claim in the case where both v,z are nonzero. Indeed, if one of v,z is zero then, since $2\leqslant k<|\mathcal{U}|$, we have $|\mathcal{U}|=2^r\geqslant 4$. Hence there exists a translation t of $\mathcal{U}$ such that v^t,z^t are both non-zero. Therefore, if the claim holds when u and z are both non-zero, then there exists $x\in X_{\widehat{\Delta}^t}$ such that $(a_1^t,b_1^t)^x=(a_2^t,b_2^t)$, and since $t^{-1}=t$, $txt\in X_\Delta$. Moreover, $(a_1,b_1)^{txt}=(a_2,b_2)$. Thus we may assume that both v,z are non-zero. Since we work over the field $\mathbb{F}_2$, this means that v,z are linearly independent vectors in $\mathcal{U}=\mathbb{F}_2^r$. We shall prove that some matrix $x_0\in X_0$ of the form $\begin{pmatrix}I&0\\B&I\end{pmatrix}$ maps (a_1,b_1) to (a_2,b_2). We see x_0 maps $a_1=(u_1,v)$ to (u_1+vB,v) and b_1 to (w_1+zB,z). Hence x_0 maps (a_1,b_1) to (a_2,b_2) if and only if $u_1+vB=u_2$ and $w_1+zB=w_2$, or equivalently, $vB=u_1+u_2$ and $zB=w_1+w_2$. Clearly such a matrix exists, since B represents a linear map $\mathbb{F}_2^r\to\mathbb{F}_2^s$ and the images of two linearly independent vectors of $\mathbb{F}_2^r$ may be chosen arbitrarily and independently. This proves the claim. Therefore $\widehat{\Gamma}$ is X-strongly incidence-transitive and $T_{\widehat{\Delta}}=\{t_{(u,0)}\in T\mid u\in\mathbb{F}_2^s\}$. □

It is currently unknown whether there are alternative methods of lifting translation-free codes to single-component codes.

CHAPTER 8

Conclusion

This thesis is a contribution towards the classification of *strongly incidence-transitive codes*. Recall that a code in $J(\mathcal{V},k)$ is a vertex subset $\Gamma\subset\binom{\mathcal{V}}{k}$. The code Γ is called X-strongly incidence-transitive for $X\leqslant \mathrm{Aut}(\Gamma)$ if X acts transitively on Γ, and for each $\Delta\in\Gamma$, X_Δ acts transitively on $\Delta\times\overline{\Delta}$. The majority of our work focuses on the following problem, which was originally posed by Bob Liebler and Cheryl Praeger.

Problem 8.1 ([**1**])
For $\varepsilon\in\{\pm\}$, let $\mathcal{V}=\mathcal{Q}^\varepsilon$ denote the set of all ε-type quadratic forms on the vector space $V=\mathbb{F}_2^{2n}$ which polarise to a particular symplectic form B. Let $X=\mathrm{Sp}_{2n}(2)$ be the isometry group of B, and consider the 2-transitive action of X on $\mathcal{Q}^\varepsilon$ defined by $\varphi^g(x)=\varphi(xg^{-1})$ for all $\varphi\in\mathcal{Q}^\varepsilon$, $g\in X$, and $x\in V$. Classify the X-strongly incidence-transitive codes $\Gamma\subset\binom{\mathcal{Q}^\varepsilon}{k}$ with $2\leqslant k\leqslant|\mathcal{Q}^\varepsilon|-2$.

We have had success in attacking Problem 8.1 using a combination of methods from permutation group theory, representation theory and combinatorics. Aschbacher's Theorem [**37**] on the maximal subgroups of a classical group forms the backbone of our divide and conquer style analysis.

Theorem 8.2
Suppose Γ is one of the codes described in Problem 8.1 and let $\Delta\in\Gamma$. Further, suppose that X_Δ lies in one or more of the geometric Aschbacher classes $\mathcal{C}_1-\mathcal{C}_8$. Then there exists a subspace $U<V$ fixed setwise by X_Δ, and one of the following holds:
(a) U is nondegenerate with $2\leqslant\dim(U)\leqslant 2(n-1)$ and for $\varepsilon'\in\{+,-\}$, Δ consists of all quadratic forms $\varphi\in\mathcal{Q}^\varepsilon$ such that $\varphi|_U$ is type ε', $\varphi|_{U^\perp}$ is type $\varepsilon\varepsilon'$. Moreover, $X_\Delta\cong\mathrm{Sp}(U)\oplus\mathrm{Sp}(U^\perp)$; or
(b) U is totally isotropic with either $\varepsilon=+$ and $1\leqslant\dim(U)\leqslant n$, or $\varepsilon=-$ and $1\leqslant\dim(U)\leqslant n-1$, and Δ consists either of the set of quadratic forms $\varphi\in\mathcal{Q}^\varepsilon$ such that U is φ-singular or the set of quadratic forms $\varphi\in\mathcal{Q}^\varepsilon$ such that the set of φ-singular vectors in V intersects U in a hyperplane. Moreover, $X_\Delta\cong 2^{d(d+1)/2}.2^{d(2n-d)}\rtimes(\mathrm{GL}(U)\times\mathrm{Sp}(U^\perp/U))$.

Conversely, for each Δ described above, $\Gamma=\Delta^X$ is an X-strongly incidence-transitive code in $J(\mathcal{Q}^\varepsilon,k)$ with full automorphism group $\mathrm{Sp}_{2n}(2)$.

The proof of Theorem 8.2 uses the geometric structures in V associated with each of Aschbacher classes $\mathcal{C}_1$-$\mathcal{C}_8$. The maximal subgroups of $\mathrm{Sp}_{2n}(2)$ which do not lie in any of the geometric Aschbacher classes must lie in $\mathcal{C}_9$. For $X=\mathrm{Sp}_{2n}(2)$ we have $X_\Delta\in\mathcal{C}_9$ if and only if there exists a nonabelian simple group T with $T \trianglelefteqslant X_\Delta \leqslant \mathrm{Aut}(T)$ and the action of X_Δ on V is absolutely irreducible. We construct in total only two examples of X-strongly incidence-transitive codes with $X_\Delta \in \mathcal{C}_9$, both of which are constructing by considering the action of S_{10} on its 8-dimensional fully deleted permutation module. On the other hand, we use the Classification of the Finite Simple Groups to show that several possible families of X-strongly incidence-transitive codes with $X_\Delta \in \mathcal{C}_9$ do not yield any examples, though we are left with several open cases.

Theorem 8.3
Suppose Γ is one of the codes described in Problem 8.1 and let $\Delta \in \Gamma$. Suppose further that G is a symmetric or alternating group on m letters, V is the fully deleted permutation module for G and $X_\Delta \leqslant G$. Then $V = \mathbb{F}_2^8, X_\Delta = S_{10}$ and Γ corresponds to the code in $J(136, 10)$ constructed in Section 5.4, or its complement in $J(136, 126)$. Conversely, each of the codes above is X-strongly incidence-transitive.

The codes in the Theorem 8.3 are block sets for 2-$(136, 10, 64)$ and 2-$(136, 126, 11200)$ designs.

Theorem 8.4
Suppose Γ is one of the codes described in Problem 8.1 and let $\Delta \in \Gamma$. Suppose further that $T \trianglelefteqslant X_\Delta \leqslant \mathrm{Aut}(T)$ for a simple nonabelian classical group $T = T_m(q)$. Then one of the following holds:

(a) $q = 2$,
(b) $q = 4$ and $\dim(V) \leqslant \frac{1}{2}m(m+1)$ (see Theorem 6.12 and Table 6.3 for a list of specific cases), or
(c) q is odd and one of the following holds
  (i) $\mathrm{soc}(X_\Delta) = \mathrm{PSU}_4(3), \mathrm{PSp}_4(q)$ or $\mathrm{PSU}_8(3)$; or
  (ii) $\mathrm{soc}(X_\Delta) = \mathrm{PSL}_2(q)$ with $q < 50$.

None of the cases in Theorem 8.4 are known to give rise to strongly incidence-transitive codes of symplectic type. Analysis of these cases is currently an open problem. We suspect that a computational approach using GAP [**59**] should eliminate the remaining cases. Next we turned our attention to the exceptional groups of Lie type and the sporadic groups. All factorisations of the exceptional simple groups of Lie type and the sporadic simple groups are known [**60, 36**]. This information is used to show that no X-strongly incidence-transitive codes exist with $X_\Delta \in \mathcal{C}_9$ and $\mathrm{soc}(X_\Delta)$ a sporadic simple group. A similar result holds for the exceptional simple groups of Lie type. The details are provided in Appendix C.2, though there is a small open case associated with Lemma C.6

Theorem 8.5
Suppose Γ is one of the codes described in Problem 8.1 and let $\Delta \in \Gamma$. Then there is no sporadic simple group or exceptional simple group of Lie type T such that $T \trianglelefteqslant X_\Delta \leqslant \mathrm{Aut}(T)$.

Analysis of the $\mathcal{C}_9$-subgroups of $\mathrm{Sp}_{2n}(2)$ with alternating socle is currently an open problem, excluding of course the fully deleted permutation modules for the symmetric and alternating groups, which are covered by Theorem 8.3. Some hints towards Problem 8.6 are provided in Appendix C.1.

Problem 8.6
Let $V = \mathbb{F}_2^{2n}$ and let Γ be an X-strongly incidence-transitive code in $J(\mathcal{Q}^\varepsilon, k)$. Are there any examples such that if $\Delta \in \Gamma$, then $\mathrm{soc}(X_\Delta)$ is an alternating group acting absolutely irreducibly on V, but V is not the fully deleted permutation module? Can they be classified?

The final component of our work focuses on the following problem, which builds on the work of Bob Liebler and Cheryl Praeger in [**1**], and Nicola Durante in [**28**].

Problem 8.7 ([**1**])
Let $\mathcal{V} = \mathbb{F}_2^n$. Classify the strongly incidence-transitive codes $\Gamma \subset \binom{\mathcal{V}}{k}$ with 2-transitive automorphism group $X \leqslant \mathrm{AGL}_n(2)$, where X contains the group of translations of $\mathcal{V}$ and $2 \leqslant k \leqslant |\mathcal{V}| - 2$.

Note that a generalised version of Problem 8.7 was considered in [**1**], namely with $\mathcal{V} = \mathbb{F}_q$, leading to new families of strongly incidence-transitive codes. However, during the course of our studies, we discovered that the case $q = 2$ is not fully covered by the work in [**1**] (see Appendix A for further details). Problem 8.7 remains open at the present time, though the following results constitute a contribution towards its solution. In Chapter 7 we introduced *single-component* strongly incidence-transitive codes which, in addition to satisfying the properties described in Problem 8.7, also have the property that $T \cap X_{\Delta_1} = T \cap X_{\Delta_2}$ for any pair of codewords Δ_1 and Δ_2. We showed that every X-strongly incidence-transitive code can be expressed as a disjoint union of single-component codes, each of which was again strongly incidence-transitive satisfying the conditions of Problem 8.7. We also introduced *translation-free* strongly incidence-transitive codes, which are single-component codes with the additional condition that $T \cap X_\Delta$ is the trivial group for every codeword Δ. Our next result was the construction of a projection from an arbitrary single-component code Γ in $J(2^n, k)$ onto a *translation-free* code in $J(2^{n-m}, k/2^\ell)$, where the number of translations fixing a given codeword setwise is 2^ℓ.

Theorem 8.8
Let $\Gamma \subset \binom{\mathcal{V}}{k}$ be an X-single-component code with $|X_\Delta \cap T| = 2^\ell \neq 1$ for each codeword Δ. Let $M = X_\Delta \cap T$ and let $\mathcal{U}$ denote the set of M-orbits in $\mathcal{V}$. For each $\Delta \in \Gamma$, define $\check{\Delta} \in \binom{\mathcal{U}}{k/2^\ell}$ to be the set of M-orbits contained in Δ, and define $\check{\Gamma} := \{\check{\Delta} \mid \Delta \in \Gamma\}$. Let $U = \{m \in \mathcal{V} \mid t_m \in M\}$. Then X/M is a 2-transitive subgroup of $\mathrm{AGL}(\mathcal{V}/U)$ which contains the translation group of $\mathcal{V}/U$, and $\check{\Gamma}$ is an (X/M)-strongly incidence-transitive code in $J(\mathcal{V}/U, k/2^\ell)$.

Finally, we classified the translation-free X-strongly incidence-transitive codes and introduced a construction which lifts a translation-free strongly incidence-transitive code in $J(2^n, k)$ to a single-component code in $J(2^{n+s}, 2^s k)$ for an arbitrary positive integer s. It is currently unknown whether there are alternative methods for lifting translation-free codes to single-component codes. The classification of translation-free X-strongly incidence-transitive codes is provided below.

Theorem 8.9
Let $\mathcal{V} = \mathbb{F}_2^n$ with $n \geqslant 3$ and $X = T \rtimes X_0 \leqslant \mathrm{AGL}_n(2)$. Let $\Gamma \subset \binom{\mathcal{V}}{k}$ be an X-strongly incidence-transitive code such that $X_\Delta \cap T$ is the trivial group for all $\Delta \in \Gamma$. Then n is even, $X_0 = \mathrm{Sp}_n(2)$ or $\mathrm{GL}_n(2)$, and there exists an ε-type quadratic form φ on $\mathcal{V}$ such that $\Delta = \{x \in V \mid \varphi(x) = 0\}$ is a codeword of Γ. Conversely, taking $\varepsilon \in \{\pm\}$, $X_0 = \mathrm{Sp}_{2m}(2)$ or $\mathrm{GL}_{2m}(2)$ and $\Gamma = \Delta^X$ yields an X-strongly incidence-transitive code in $J(2^{2n}, 2^{n-1}(2^n + \varepsilon))$.

Perhaps the most interesting of the open problems related to the classification of strongly incidence-transitive codes concerns the so-called *self-complementary* strongly incidence-transitive codes. As discussed in Chapter 1, the full automorphism group group of a Johnson graph on a finite set $\mathcal{V}$ of v points is given by

$$\mathrm{Aut}(J(v,k)) = \begin{cases} \mathrm{Sym}(\mathcal{V}) \times C_2 & \text{if } k = \frac{1}{2}v \\ \mathrm{Sym}(\mathcal{V}) & \text{otherwise} \end{cases}$$

Here, C_2 denotes the group of order two generated by the complementary automorphism of $J(2k, k)$ which maps each vertex to its complement in $\mathcal{V}$. Throughout this thesis we have studied X-strongly incidence-transitive codes in $J(v, k)$, possibly with $v = 2k$, but under the assumption that $X \leqslant \mathrm{Sym}(\mathcal{V})$. The same assumption is true in [**1**]. However, five examples of self-complementary strongly incidence-transitive codes are constructed in [**27**]. This leads naturally to the following problem.

Problem 8.10
Let $k \geqslant 2$. Classify the X-strongly incidence-transitive codes Γ contained in the Johnson graphs $J(2k, k)$ with X acting 2-transitively on $\mathcal{V}$, $X \leqslant \mathrm{Sym}(\mathcal{V}) \times C_2$ and $X \nleqslant \mathrm{Sym}(\mathcal{V})$.

The research outlined above will be submitted for publication upon submission of this thesis.

Appendices

APPENDIX A

A note on [**1**, Proposition 6.6]

We note that there is a small oversight in Proposition 6.6 of [**1**], though we show in Lemma A.1 that the conclusions draw in in Proposition 6.6 remain valid for all $q > 2$. Recall that set of Δ of points in V is called a $[0, x, q]_1$ set if every affine 1-flat in V intersects Δ in $0, x$ or q points.

Lemma A.1
Let $V = \mathbb{F}_q^m$ with $q > 2$ and let $\Delta \subset V$ be a $[0, x, q]_1$ set, where $x \in \{1, q-1\}$. Suppose $T \trianglelefteq X \leqslant \mathrm{A\Gamma L}(m, q)$ and X_Δ acts transitively on $\Delta \times \overline{\Delta}$. Then Δ is an affine subspace or the complement of an affine subspace in V.

Proof. Interchanging Δ and $\overline{\Delta}$ if necessary, we may assume that $x = 1$. The automorphism group $\mathrm{Aut}(\Gamma)$ is transitive on codewords so we may assume further that $0 \in \Delta$. Since Δ is a $[0, 1, q]_1$ set, any affine 1-flat that contains two points of Δ must be contained in Δ. In particular, if $u \in \Delta \backslash \{0\}$ then $\{0, u\} \subseteq \langle u \rangle \cap \Delta$ and hence $\langle u \rangle \subseteq \Delta$. Therefore Δ is closed under scalar multiplication. If $\langle u \rangle = \Delta$ we are done. If not, there must exist $v \in \Delta$ which does not lie along $\langle u \rangle$. Let $\beta \in \mathbb{F}_q \backslash \{0, 1\}$. Then the affine 1-flat $L = \langle u + v \rangle + (1 - \beta)v$ contains $(1 - \beta)v, \beta u + v$ and $(\beta - 1)u$. Since both $(1 - \beta)v$ and $(\beta - 1)u$ are contained in Δ, it follows that $L \subseteq \Delta$ and therefore $\beta u + v \in \Delta$. Similarly, the affine 1-flat $L' = \langle u \rangle + v$ contains $v, u + v$ and $\beta u + v$, and hence $L' \subseteq \Delta$ so $u + v \in \Delta$. Therefore Δ is also closed under addition, and Δ is a subspace of V. □

APPENDIX B

Some known primitive strongly incidence-transitive codes

The primitive codes are divided into several subcategories: projective type, affine type, rank 1 type, Jordan-Steiner type, and sporadic. We describe some of these.

B.1. Projective type codes

Let $\mathcal{V} = \mathrm{PG}_{n-1}(q)$ and $X = \mathrm{P\Gamma L}_n(q)$. We collect below some essential results from [**1**] regarding the X-strongly incidence-transitive codes in $J(\mathcal{V}, k)$.

Example B.1 (Projective subspace codes [**1**])
Let Γ denote the set of all $(s-1)$-dimensional projective subspaces of $\mathcal{V}$. Then X acts transitively on Γ and for each $\Delta \in \Gamma$, the setwise stabiliser X_Δ acts transitively on $\Delta \times \overline{\Delta}$. Therefore Γ is an X-strongly incidence-transitive code in $J(\mathcal{V}, k)$ with $v = \frac{q^n-1}{q-1}$, $k = \frac{q^s-1}{q-1}$ and $\delta = q^{s-1}$. Similarly, the set of all complements of $(s-1)$-dimensional subspaces of $\mathcal{V}$ is an X-strongly incidence-transitive code in $J(\mathcal{V}, k')$ with $v = \frac{q^n-1}{q-1}$, $k' = \frac{q^n-q^s}{q-1}$ and $\delta = q^{s-1}$.

Example B.2 (Baer subline codes [**1**])
Let $q = q_0^2 \geqslant 4$, $\mathcal{V} = \mathrm{PG}_1(q)$ and $X = \mathrm{P\Gamma L}_2(q)$. Identify $\mathcal{V}$ with $\mathbb{F}_q \cup \{\infty\}$ and let $\Delta = \mathbb{F}_{q_0} \cup \{\infty\}$. The X-images of Δ in $\mathrm{PG}_1(q)$ are called *Baer sublines*. Let Γ denote the set of all Baer sublines in $\mathrm{PG}_1(q)$. Then Γ is an X-strongly incidence-transitive code in $J(q+1, q_0+1)$ with minimum distance $\delta = q_0 - 1$ and $X_\Delta = N_X(\mathrm{PSL}_2(q_0))$.

Theorem B.3 ([**1**])
Let $\mathcal{V} = \mathrm{PG}_1(q)$ with $q \geqslant 4$. Let $\mathrm{PSL}_2(q) \leqslant X \leqslant \mathrm{P\Gamma L}_2(q)$ and suppose $\Gamma \subset J(q+1, k)$ is an X-strongly incidence-transitive code with $3 \leqslant k \leqslant q-2$. Then for each $\Delta \in \Gamma$, one of Δ and $\overline{\Delta}$ is a Baer subline, as in Example B.2.

Theorem B.4 ([**1**])
Let $\mathcal{V} = \mathrm{PG}_{n-1}(q)$. Suppose $\mathrm{PSL}_n(q) \leqslant X \leqslant \mathrm{P\Gamma L}_n(q)$ and $\Gamma \subset J(\mathcal{V}, k)$, where $v \geqslant 3$ and $3 \leqslant k \leqslant |\mathcal{V}| - 3$. If Γ is X-strongly incidence-transitive and $\Delta \in \Gamma$ then, interchanging Δ and $\overline{\Delta}$ if necessary, one of the following holds:

(i) Δ is a projective subspace as in Example B.1;
(ii) Δ is a subset of class $[0, 2, q+1]_1$ and $\frac{|\mathcal{V}|-1}{q} + 1 \leqslant k \leqslant \frac{2(|\mathcal{V}|-1)}{q}$; or

(iii) Δ is a subset of class $[0, \sqrt{q}+1, q+1]_1$, $\frac{|\mathcal{V}|-1}{\sqrt{q}} + 1 \leqslant k \leqslant \frac{|\mathcal{V}|-1}{\sqrt{q}} + \frac{|\mathcal{V}|-1}{q}$ and if λ is a Δ-shared line then $\lambda \cap \Delta$ is a a Baer subline.

Durante demonstrates in [**28**] that there are no further examples of strongly incidence-transitive codes in the projective case.

B.2. Affine type codes

Let $\mathcal{V} = \mathrm{AG}_n(q)$ and $X = \mathrm{A\Gamma L}_n(q)$. We collect below some essential results from [**1**] regarding the X-strongly incidence-transitive codes in $J(\mathcal{V}, k)$.

Example B.5 ([**1**])
Let $V = \mathbb{F}_q^n$ and $X = \mathrm{A\Gamma L}(V)$. For any positive integer $m < n$, the set of all affine m-flats is an X-strongly incidence-transitive code in $J(q^n, q^m)$. Similarly, the set of all complements in V of affine m-flats is an X-strongly incidence-transitive code in $J(q^n, q^n - q^m)$.

Example B.6 ([**1**])
Let $W = \mathbb{F}_4$ and $V = \mathbb{F}_{16}$. Let $X = \mathrm{A\Gamma L}_1(16)$. Then V is a 4-dimensional vector space over $\mathbb{F}_4$ containing W as a 1-dimensional subspace. Then Δ^X and $\overline{\Delta}^X$ are X-strongly incidence-transitive codes in $J(16, 4)$ and $J(16, 12)$ respectively.

Example B.7 ([**1**])
A set of 6 points in $\mathrm{PG}(2, 4)$, no 3 collinear is a *hyperoval* (see). Let Δ be a 2-transitive hyperoval in the projective plane $\mathrm{PG}(2, 4)$, and let λ be an affine line containing no points of Δ. Then $k = |\Delta| = 6$ and the complement of λ in the point set of $\mathrm{PG}(2, 4)$ is an affine space $V = \mathrm{AG}(2, 4)$ containing Δ. Let X be the stabiliser of λ in $\mathrm{P\Gamma L}_3(4)$. Then X acts faithfully on V and $\Gamma = \Delta^X$ is an X-strongly incidence-transitive code in $J(V, 6)$ and $X_\Delta \cong S_5$. By Remark 1.5, the complementary code in $J(V, 12)$ is also X-strongly incidence-transitive.

Theorem B.8 ([**1**])
Suppose $V = \mathbb{F}_q^n$ with $n \geqslant 2$ and suppose $\Gamma \leqslant J(V, k)$ is an X-strongly incidence-transitive code, where $X \leqslant \mathrm{A\Gamma L}_n(q)$ is 2-transitive on V. Let $\Delta \in \Gamma$. Then one of the following holds:

(i) Δ or $\overline{\Delta}$ is an affine subspace, as in Example B.5;

(ii) $V = \mathbb{F}_4^n$ and interchanging Δ and $\overline{\Delta}$ if necessary, every affine line in V lies in Δ or $\overline{\Delta}$, or intersects Δ in a Baer subline. Moreover, $\frac{q^n+2}{3} \leqslant k \leqslant \frac{2(q^n-1)}{3}$; or

(iii) $V = \mathbb{F}_{16}^n$ and interchanging Δ and $\overline{\Delta}$ if necessary, every affine line in V either lies in Δ or $\overline{\Delta}$ or intersects Δ in a Baer subline of size 4. Moreover, $\frac{q^n+4}{5} \leqslant k \leqslant \frac{4(q^n-1)}{15}$.

Example B.7 provides an example for case (ii) of Theorem B.8. At her 2012 plenary lecture in Ferrara at the Conference of Finite Geometry in honor of Frank De Clerck, Praeger asked what was known about subsets of class $[0, m, q]_1$ in $\mathrm{AG}(n, q)$, regardless of the symmetry restrictions.

Theorem B.9 ([**1**],[**28**])
Let $\Delta \subset \mathbb{F}_q^n$ with $n \geqslant 2$ and suppose the setwise stabiliser X_Δ of Δ in $X \leqslant \mathrm{A\Gamma L}(V)$ acts transitively on $\Delta \times \overline{\Delta}$. Then Δ or $\overline{\Delta}$ is one of the following:

(i) an affine subspace, as per Example B.5
(ii) a cylinder $Cyl(\mathcal{V}_\infty, M)$ of $\mathbb{F}_4^n$, where M is either a hyperoval or the complement of a hyperoval of a plane Π whose line at infinity is skew with the $(n-3)$-dimensional projective subspace $\mathcal{V}_\infty$
(iii) A pair of parallel hyperplanes in $\mathbb{F}_4^n$; or
(iv) Four parallel hyperplanes in $\mathbb{F}_{16}^n$ with the secant lines meeting the set in affine Baer sublines

B.3. Rank one codes

Example B.10 (The classical unital)
Let $V = \mathbb{F}_{q^2}^3$ and equip V with a nondegenerate Hermitian form. Then $X = \mathrm{P\Gamma U}_3(q)$ acts faithfully and 2-transitively on the set $\mathcal{V}$ of q^3+1 totally-isotropic 1-spaces in V. Every nondegenerate 2-space in V contains $q+1$ elements of $\mathcal{V}$. Define a code $\Gamma \subset J(q^3+1, q+1)$ by

$$\Gamma = \{\mathcal{V} \cap U \mid U \text{ a nondegenerate 2-space}\}.$$

Then Γ is X-strongly incidence-transitive and $\delta(\Gamma) = q$.

Example B.11
Let $\mathcal{V} = \mathbb{F}_9^3$ and $T = \mathrm{PSU}_3(3)$. Let $\Gamma \subset J(\mathcal{V}, 12)$ be the set of all 'unitary bases' of size 12 for V as a 12-dimensional vector space over $\mathbb{F}_3$. Then $T_\Delta \cong 4^2 \rtimes S_3$ and Γ is a $(T.2)$-strongly incidence transitive code with $\delta(\Gamma) = 6$. Moreover, Γ is not T-strongly incidence transitive.

APPENDIX C

Open and partially solved problems

C.1. $\mathcal{C}_9$ codeword stabilisers with alternating socle

Problem C.1
Let $V = \mathbb{F}_2^{2n}$. Are there any X-strongly incidence-transitive codes Γ in $J(\mathcal{Q}^\varepsilon, k)$ such that if $\Delta \in \Gamma$, then $\mathrm{soc}(X_\Delta)$ is an alternating group acting absolutely irreducibly on V, but not as a fully-deleted permutation module? Can they be classified?

We provide some basic observations related to Problem C.1. Let Γ be an X-strongly incidence-transitive code and Δ a codeword. Let $G = X_\Delta$ and suppose $T \trianglelefteqslant G \leqslant \mathrm{Aut}(T)$ where $T = A_m$ with $m \geqslant 5$. If $m \geqslant 15$ and V is not the fully deleted permutation module for S_m then [**66**, Theorem 7] implies $\dim(V) \geqslant \frac{1}{4}m(m-5)$. Applying this bound in combination with the inequality $|\mathrm{Aut}(T)| > 2^{\dim(V)-2}$, we arrive at the necessary condition

$$\log_2(m!) - \frac{1}{8}m(m-5) + 2 > 0. \tag{C.1}$$

Figure C.1 below suggests that in order to satisfy Inequality (C.1), we must have $15 \leqslant m \leqslant 36$. Note that this says nothing about $m < 15$. Further, by Lemma 1.15, for each $(\varphi, \psi) \in \Delta \times \overline{\Delta}$ there exists a factorisation $X_\Delta = X_{\Delta,\varphi} X_{\Delta,\psi}$. The factorisations of almost-simple groups with alternating socle are known, and the details are provided below.

Theorem C.2 ([**35**], Theorem D)
Let $m \geqslant 5$ and consider $T = A_m$ acting naturally on a set Ω of m points. Let G be an almost-simple

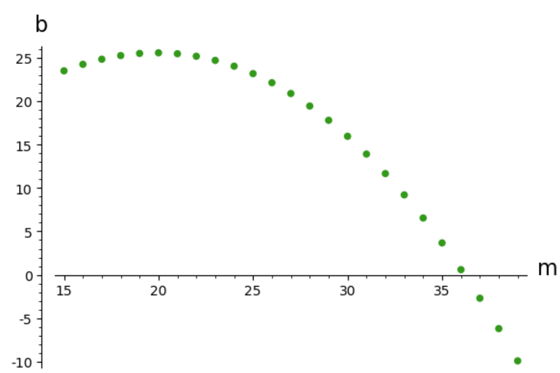

FIGURE C.1. A plot of $b(m) = \log_2(m!) - \frac{1}{8}m(m-5) + 2$ against m for $15 \leqslant m \leqslant 40$.

group with socle T and let A and B be subgroups of G which do not contain T. If $G = AB$ then one of the following holds:

(a) $A_{m-k} \lhd A \leqslant S_k \times S_{m-k}$ for an integer $k \in [1:5]$, and B is k-homogeneous on Ω;
(b) $m = 10$, $A = \mathrm{PSL}_2(8)$ or $\mathrm{PSL}_2(8) \rtimes \mathbb{Z}_3$, and $A_5 \times A_5 \trianglelefteq B \leqslant S_5 \wr S_2$ with B transitive on Ω;
(c) $m = 8$, $A = \mathrm{AGL}_3(2)$ and $\mathbb{Z}_5 \times \mathbb{Z}_3 \leqslant B$
(d) $m = 6$ and one of:
 (i) $A \cap T = \mathrm{PSL}_2(5)$ and $B \cap T \leqslant S_3 \wr S_2$, with $A \cap S_6$ and $B \cap S_6$ both transitive on Ω,
 (ii) $A \cap T = \mathbb{Z}_5$ or D_{10} and $B \cap T \leqslant S_3 \wr S_2$,
 (iii) $G \nleqslant S_6$ and the intersections $A \cap S_6$ and $B \cap S_6$ are as in item (a)

By Theorem C.1, the problem of classifying the X-strongly incidence-transitive codes with $X_\Delta \in \mathcal{C}_9$ and $\mathrm{soc}(X_\Delta) = A_m$ can, in theory, be solved by identifying which of the factorisations described above can be associated with the Jordan-Steiner actions. This is currently an open problem.

C.2. $\mathcal{C}_9$ codeword stabilisers with exceptional Lie type socle

We denote by $V \cong \mathbb{F}_2^{2n}$ the natural module for X and by $\mathcal{Q}^\varepsilon$ the set of ε-type quadratic forms on V which polarise to the symplectic form fixed by X. If $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is X-strongly incidence-transitive and $\Delta \in \Gamma$ then Lemma 1.15 implies $X_\Delta = X_{\Delta,\varphi} X_{\Delta,\psi}$ is a factorisation, where $(\varphi, \psi) \in \Delta \times \overline{\Delta}$. Suppose X_Δ is an exceptional group of Lie type. Then part (a) of Theorem C.3 implies that $T = G_2(3^f), G_2(4)$ or $F_4(2^f)$. We consider each case in turn.

Theorem C.3 ([**60**])
Let G be an exceptional group of Lie type and let $G = AB$ for proper subgroups $A, B < G$. Then one of the following holds:

(a) $G = T$ and one of the following holds:
 (i) $G = G_2(q)$, $\mathrm{SL}_3(q) \leqslant A \leqslant \mathrm{SL}_3(q).2$, $\mathrm{SU}_3(q) \leqslant B \leqslant \mathrm{SU}_3(q).2$, $q = 3^f$;
 (ii) $G = G_2(q)$, $A = {}^2G_2(q)$, $\mathrm{SL}_3(q) \leqslant B \leqslant \mathrm{SL}_3(q).2$, $q = 3^{2f+1}$; or
 (iii) $G = G_2(4)$, $A = J_2$, $\mathrm{SU}_3(4) \leqslant B \leqslant \mathrm{SU}_3(4).2$;
 (iv) $G = F_4(q)$, $A = \mathrm{Sp}_8(q)$, ${}^3D_4(q) \leqslant B \leqslant {}^3D_4(q).3$, $q = 2^f$.
(b) $G \neq T$ and one of the following holds:
 (i) $T = (T \cap A)(T \cap B)$ with T, $T \cap A$ and $T \cap B$ as in part (a); or
 (ii) $G = G_2(4).2$, $A = G_2(2) \times 2$, $B = \mathrm{SU}_3(4).4$.

Lemma C.4
Let $X = \mathrm{Sp}_{2n}(2)$ and let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X strongly incidence-transitive code with $\Delta \in \Gamma$ and X_Δ almost-simple and irreducible. Then $\mathrm{soc}(X_\Delta) \neq G_2(3^f)$.

PROOF. Example D.3 shows that $X_\Delta \neq G_2(3)$ or $G_2(3).2$. Suppose then that $f > 1$. We have $|\operatorname{Aut}(T)| = 2fq^6(q^6-1)(q^2-1) \leqslant 2q^{15}$, and by [**62**], $\dim(V) \geqslant q(q^2-1)$. Therefore Lemma 6.3 implies

$$0 < \log_2(|\operatorname{Aut}(T)|) - e(T) + 2 < 15\log_2(q) - q^3 + q + 3.$$

Set $b(f) = 15\log_2(3^f) - 3^{3f} + 3^f + 3$. Then for all $f > 1$ we have

$$\begin{aligned} b(f+1) - b(f) &= 15\log_2(3^{f+1}) - 3^{3(f+1)} + 3^{f+1} + 3 - 15\log_2(3^f) + 3^{3f} - 3^f - 3 \\ &= 15\log_2(3) + (3^{3f} - 3^{3(f+1)}) + (3^{f+1} - 3^f) \\ &= 15\log_2(3) + 3^{3f}(1-3^3) + 3^f(3-1) \\ &= 15\log_2(3) - 26\cdot 3^{3f} - 2\cdot 3^f. \end{aligned}$$

Note that $b(f)$ is decreasing and therefore for all $f \geqslant 2$, $b(f) \leqslant b(2) \approx -662.5$. This contradicts Lemma 6.3. Therefore $\operatorname{soc}(X_\Delta) \neq G_2(3^f)$ for any $f \geqslant 1$. $\square$

Lemma C.5
Let $X = \mathrm{Sp}_{2n}(2)$ and let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X strongly incidence-transitive code with $\Delta \in \Gamma$ and X_Δ almost-simple. Then $\operatorname{soc}(X_\Delta) \neq G_2(4)$.

PROOF. We apply Theorem C.3. If $T = G_2(4) = G$ then we have $A = J_2$ and $B = \mathrm{SU}_3(4)$ or $\mathrm{SU}_3(4).2$. Another possibility is $G = T.2$ with $A = N_G(J_2) = J_2.2$ and $B = N_G(\mathrm{SU}_3(4)) = N_G(\mathrm{SU}_3(4).2) = \mathrm{SU}_3(4).4$. For the cases above we have $|\Omega| = |G:A| + |G:B| \in \{4448, 2432\}$ and $\nu_e(|\Omega|) \in \{2^5, 2^7\}$. But if $n \in \{6,8\}$ then $|\mathcal{Q}^\epsilon(\mathbb{F}_2^{2n})| \in \{2016, 2080, 32640, 32896\}$, so $|\Omega| \neq |\mathcal{Q}^\varepsilon|$. Finally, suppose $G = T.2$ with $A = G_2(2)\times 2$ and $B = \mathrm{SU}_3(4).4$. Then $|\Omega| = |G:A| + |G:B| = 73856 = 2^7\cdot 577$, which contradicts Lemma 6.2. Therefore $\operatorname{soc}(X_\Delta) \neq G_2(4)$. $\square$

Lemma C.6
Let $X = \mathrm{Sp}_{2n}(2)$ and let $\Gamma \subset \binom{\mathcal{Q}^\varepsilon}{k}$ is an X strongly incidence-transitive code with $\Delta \in \Gamma$ and X_Δ almost-simple. Then $X_\Delta \neq F_4(q)$ with $q = 2^f$.

PROOF. Suppose $T = F_4(q)$ with $A = \mathrm{Sp}_8(q)$, $B = {}^3D_4(q)$ or ${}^3D_4(q).3$ and $q = 2^f$. Then $|T| = q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$, $|A| = q^{16}(q^2-1)(q^4-1)(q^6-1)(q^8-1)$, $|B| = q^{12}(q^2-1)(q^6-1)(q^8+q^4-1)$ or $3q^{12}(q^2-1)(q^6-1)(q^8+q^4-1)$. Then

$$|T:A| = \frac{q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)}{q^{16}(q^2-1)(q^4-1)(q^6-1)(q^8-1)} = q^8(q^8+q^4+1)$$

$$|T:B| = \frac{q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)}{q^{12}(q^2-1)(q^6-1)(q^8+q^4-1)} = q^{12}(q^4-1)(q^8-1)$$

Therefore

$$|T:A| + |T:B| = q^8\left(q^8+q^4+1) + q^4(q^4-1)(q^8-1)\right) = q^8(q^{12}(q^4-1)+1). \tag{C.2}$$

Since $q = 2^f$, $\nu_e\left(|T:A| + |T:B|\right) = q^8$. If $|\mathcal{Q}^\varepsilon| = |T:A| + |T:B|$ then $q^8 = 2^{n-1}$ and therefore

$$|\mathcal{Q}^\varepsilon| = q^8(2 \cdot q^8 + \varepsilon). \tag{C.3}$$

Comparing equation (C.3) with equation (C.2), we have $|\mathcal{Q}^\varepsilon| = |T:A| + |T:B|$ if and only if

$$q^{12}(q^4-1) + 1 - 2\cdot q^8 - \varepsilon = q^8(q^8 - q^4 - 1) + 1 - \varepsilon = 0. \tag{C.4}$$

But $q^8(q^8-q^4-1)+1-\varepsilon \geqslant q^8(q^8-q^4-1)$. Since $q > 0$ and $q^8 - q^4 - 1 > 0$, equation (C.4) does not hold. Therefore $X_\Delta \neq F_4(q)$. □

Remark C.7
It is desirable to extend or modify Lemma C.6 so as to eliminate completely the possibility that $\mathrm{soc}(X_\Delta) = F_4(q)$. We note that $\nu_e(|F_4(q)|) = q^{24}$, $\nu_e(|\operatorname{Sp}_8(q)|) = q^{16}$, $\nu_e(|{}^3D_4(q)|) = q^{12}$. Therefore $\nu_e(|F_4(q) : \operatorname{Sp}_8(q)|) = q^8$ and $\nu_e(|F_4(q) : {}^3D_4(q)|) = q^{12}$. If $F_4(q) \trianglelefteq G = X_\Delta \leqslant \operatorname{Aut}(F_4(q))$ then we have $q^{12} \leqslant |G:B| \leqslant 2fq^{12}$ and $q^8 \leqslant |G:A| \leqslant 2fq^8$.

C.3. Binary affine subspace codes

Suppose $N_X(T_\Delta) = X_\Delta$, where T_Δ is a nontrivial proper subgroup of T. T_Δ acts regularly on Δ and therefore Δ is a subspace of $\mathcal{V}$. In this case $|\mathcal{M}| = |\Gamma|$ so Γ is a collection of affine flats.

Example C.8
Let $V = \mathbb{F}_2^n$ with $n \geqslant 3$ and $1 < d < n$. Let Γ be the set of all d-flats in $\mathrm{AG}(V)$. Then $\operatorname{Aut}(\Gamma) = \mathrm{AGL}(V)$ and Γ is X-strongly incidence-transitive. In particular, let $\{e_i \mid 1 \leqslant i \leqslant n\}$ be a basis for V and let $U = \langle e_i \mid 1 \leqslant i \leqslant d\rangle$ where $d < n$. As a matter of convenience we let W be a complement of U in V so that $V = U \oplus W$. Since X is transitive on the set of affine d-flats we may take $\Delta = U$. We have $X_\Delta = T_U \rtimes P$ where $T = \{t_u \in T \mid u \in U\}$ and $P = X_{0,U}$ is the group of matrices of the form

$$P = X_{0,U} = \left\{ \begin{pmatrix} a & O \\ r & b \end{pmatrix} \mid a \in \mathrm{GL}(U), b \in \mathrm{GL}(W), r \in \mathbb{F}_2^{(n-d)} \times \mathbb{F}_2^d \right\} = R \rtimes (\mathrm{GL}(U) \times \mathrm{GL}(W)).$$

We write $(r,a,b) \in R \rtimes (\mathrm{GL}(U) \times \mathrm{GL}(W))$. Then for $v = u + w \in V$ the action of P can be expressed as $(u+w)(r,a,b) = ua + wr + wb$ where $u \in U$ and $w \in W$. Note that $ua + wr \in U$ and $wb \in W$.

Lemma C.9
Let $H = \{(O, I_d, b) \in P\}$, where O is the $(n-d) \times d$ zero matrix. With the notation of Example C.8, H is transitive on the nonzero vectors in the quotient space V/U.

Proof. By definition $W = \langle e_i \mid d+1 \leqslant i \leqslant n\rangle$ and $V/U = \langle U + e_i \mid d+1 \leqslant i \leqslant n\rangle$. The canonical quotient mapping $\pi : W \to V/U$ defined by $e_i \mapsto U + e_i$ is an isomorphism of vector spaces. Moreover, for all $U + w \in V/U$ with $w \in W$ we have $(U+w)(O, I_d, b) = U + wb$. Since $\mathrm{GL}(W)$ acts transitively on $W\backslash\{0\}$, it follows that H acts transitively on the nonzero vectors in V/U. □

Lemma C.10
Given $v \in V \backslash U$, the unipotent radical R acts transitively on the coset $U + v$.

Proof. We may assume without loss of generality that $v \in W$. Let $u_1 + v, u_2 + v \in U + v$.

Let $(r, I_d, I_{n-d}) \in R$. Then $(u_1 + v)(r, I_d, I_{n-d}) = u_1 + vr + v$, so R is transitive on $U + v$ if and only if there exists a $(n-d) \times d$ matrix r such that $vr = u_2 + u_1$. Since $v \neq 0$ there exists a $j \in [1 : n]$ such that the jth coordinate of v is 1. Then we define r to be the matrix whose jth row is equal to $u_2 + u_1$ and we set all other entries equal to zero. Then $vr = u_2 + u_1$ and R is transitive on $U + v$. □

Lemma C.11
Let $X = \mathrm{AGL}_n(2)$ and let Γ denote the code defined in Example C.8. Then Γ is an X-strongly incidence-transitive code in $J(2^n, 2^d)$.

Proof. By Lemma 1.20, Γ is X-strongly incidence-transitive if and only if

(i) X is transitive on V;
(ii) there exists $u \in V$ such that X_u acts transitively on the set Γ_u of codewords which contain u; and
(iii) there exists $\Delta \in \Gamma$ with $u \in \Delta$ such that $X_{u,\Delta}$ acts transitively on $\overline{\Delta}$.

Clearly X acts transitively on V since the subgroup of translations is transitive on V. Therefore property (i) holds. Next we choose $u = 0$ and consider the set Γ_0 of codewords that contain 0. Specifically, Γ_0 is the set of m-dimensional subspaces of V and $X_0 = \mathrm{GL}(V)$ acts transitively on Γ_0, so property (ii) holds. Next, consider the vectors $x, y \in V \backslash \Delta$ where $x = e_{d+1}$ and $y = u + w$ with $u \in U$ and $w \in W \backslash \{0\}$. By Lemma C.9 H acts transitively on V/U and therefore there exists an element $h \in H$ such that $U + xh = U + y = U + v$. Finally, the unipotent radical R fixes the quotient space V/U pointwise but permutes transitively the set of points within a given coset by Lemma C.10. Therefore there exists $r \in R$ such that $U + v$ is fixed setwise but $xhr = y$. Therefore property (iii) holds. □

Lemma C.11 shows that the set of all d-flats in V is a strongly incidence-transitive code with automorphism group $\mathrm{AGL}(V)$. It remains to determine whether there are any strongly incidence-transitive subcodes with automorphism group $X = T \rtimes X_0$, where $X_0 < \mathrm{GL}(V)$ is transitive on the nonzero vectors in V. Theorem C.12 provides a list of subgroups of $\mathrm{GL}_n(2)$ which act transitively on $\mathbb{F}_2^n \backslash \{0\}$. Note that this is a special case of Herring's Theorem; see [**67**] for further details.

Theorem C.12 ([**67**])
If X_0 is a subgroup of $\mathrm{GL}_n(2)$ which is transitive on $\mathbb{F}_2^n \backslash \{0\}$ then X_0 lies in one of the following classes:

(i) $X_0 \leqslant \Gamma\mathrm{L}_1(2^n)$,
(ii) $X_0 \lhd \mathrm{SL}_a(2^b)$ with $n = ab$,
(iii) $X_0 \lhd \mathrm{Sp}_{2a}(2^b)$ with $n = 2ab$,
(iv) $X_0 = A_7 < A_8 = \mathrm{SL}_4(2)$,
(v) $X_0 = A_6 \cong \mathrm{Sp}_4(2)'$ and $n = 4$, or

(vi) $X_0 \lhd G_2(2)'$ and $n = 6$.

Conversely, each of the above classes gives rise to a subgroup of $\mathrm{GL}_n(2)$ which acts transitively on $\mathbb{F}_2^n \backslash \{0\}$.

Let Γ be the code from Example C.8. Given one of the groups X_0 from Theorem C.12 we can potentially construct codes $\Gamma' \subseteq \Gamma$ by computing the orbits of X_0 on the r-dimensional subspaces of V for $2 \leqslant r \leqslant n-2$. If Δ is an orbit representative and $X_{0,\Delta}$ is transitive on $V \backslash \Delta$ then we may take Γ to be the set of all translations of each subspace in Δ^{X_0}. The next example shows that there are translation-regular strongly incidence-transitive codes other than the family presented in Example C.8. Note that $\Gamma' = \Gamma$ if and only if Δ_0^X is the full set of r-dimensional subspaces of V. In particular, X_0 always acts transitively on the set of 1-spaces and the set of $(n-1)$-spaces in $\mathbb{F}_2^n$ by definition.

Example C.13

We consider the final two cases from Theorem C.12 using GAP [**59**].

(1) Let $V = \mathbb{F}_2^4$ and $X_0 = A_6 \cong \mathrm{Sp}_4(2)'$. X_0 acts transitively on the set of 3-spaces V but has two orbits in the set of 2-spaces with representatives $U_1 = \langle e_2, e_3 \rangle$ and $U_2 = \langle e_1 + e_3, e_2 + e_3 \rangle$. Using GAP we find $X_{0,U_1} \cong S_4$ acts transitively on $V \backslash U_1$ while $X_{0,U_2} \cong C_3 \times C_3 \rtimes C_2$ is intransitive on $V \backslash U_2$. Therefore, taking $\Delta = U_1$ and $X = T \rtimes A_6$ yields a strongly incidence transitive code in $J(16, 4)$.

(2) Let $V = \mathbb{F}_2^6$ and $X_0 \rhd G_2(2)'$. Suppose $X_0 = G_2(2)'$. Then X_0 has orbit lengths $[252, 63, 336]$ on lines, $[756, 504, 36, 63, 36]$ on planes, and $[336, 252, 63]$ on solids. Only one of these orbits yields a strongly incidence-transitive code. Taking $\Delta = \langle e_1, e_2, e_3, e_6 \rangle$, we find $k = 16$, $|\Gamma_0| = 63$ and $X_{0,\Delta} = \mathrm{SL}_2(3) \rtimes C_4$. Taking $X_0 = G_2(2)$ yields only the code code above with $X_{0,\Delta} = (\mathrm{SL}_2(3) \rtimes C_4) \rtimes C_2$.

Note that replacing Δ by $\overline{\Delta}$ in Example C.13 yields strongly incidence-transitive codes. There are no new examples arising from item (iv) of Theorem C.12 since A_7 acts transitively on the 2 and 3-spaces in $\mathbb{F}_2^4$. A full classification of the translation-regular affine type codes requires only an analysis of Theorem C.12 (cases (i) - (iii)) and is an open problem at present.

APPENDIX D

GAP code

Additional code is available from [**64**].

D.1. Tools

Program D.1

```
# Compute largest dim(V) such that 2^{n-1}(2^n-1) <= order (of an unspecified group)
LargestDim := function(order)
  local n;
  n := 1;
  while 2^(n-2)*(2^n-1) <= order do;
    n := n+1;
  od;
  return 2*(n-1);
end;
```

Program D.2

```
# Compute the values of k such that k(v-k) divides order
KPossible := function(order,dim,eps)
  local v, n;
  n := dim/2;
  v := 2^(n-1)*(2^n+eps);
  return Filtered([2..v/2], k->order/(k*(v-k)) in Integers);
end;
```

Example D.3

Consider $X = \mathrm{Sp}_{2n}(2)$ acting 2-transitively on $\mathcal{Q}^{\varepsilon}$. Does there exist an X-strongly incidence-transitive code Γ with $\Delta \in \Gamma$ and $X_\Delta \cong G_2(3)$? We use GAP to provide an answer.

```
gap> g:=AtlasGroup("G2(3)");;
gap> order:=Order(g);
4245696
gap> LargestDim(order);
24
```

```
gap> KPossible(order,14,1);
[ ]
gap> KPossible(order,14,-1);
[ ]
```

D.2. Examples

Program D.4

Some calculations used in the proof of Lemma 5.37

```
# The primitive action of S10 on 120 points is available from the PrimGrp package
gap> omega:=[1..120];;
gap> g := PrimitiveGroup(120,19);
Sym(10)
gap> NrMovedPoints(g);
120
gap> cc:=ConjugacyClassesMaximalSubgroups(g);;
gap> rep:=List(cc,Representative);;
gap> filt:=Filtered(rep, grp -> Order(grp)/(60^2) in Integers);;
gap> List(filt,StructureDescription);
[ "A10", "(A5 x A5) : D8" ]
gap> for grp in filt do; Display(OrbitLengths(grp,omega)); od;
[ 120 ]
[ 20, 100 ]

# A10 is transitive so we must investigate further
gap> h:=filt[1];;
gap> cc:=ConjugacyClassesMaximalSubgroups(h);;
gap> rep:=List(cc,Representative);;
gap> filt:=Filtered(rep, grp -> Order(grp)/(60^2) in Integers);;
gap> List(filt,StructureDescription);
[ "(A5 x A5) : C4" ]
gap> for grp in filt do; Display(OrbitLengths(grp,omega)); od;
[ 20, 100 ]
```

Bibliography

[1] R. A. Liebler and C. E. Praeger, "Neighbour-transitive codes in Johnson graphs," *Des. Codes Cryptogr.*, vol. 73, no. 1, pp. 1–25, 2014.

[2] C. E. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423, 623–656, 1948.

[3] R. W. Hamming, "Error detecting and error correcting codes," *Bell Labs Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[4] M. J. E. Golay, "Notes on digital coding," *Proc. IRE*, vol. 37, no. 657, 1949.

[5] R. Wilson, *The Finite Simple Groups*. Graduate Texts in Mathematics, Springer London, 2009.

[6] N. J. A. S. John Horton Conway, *Sphere Packings, Lattices and Groups*. Grundlehren der mathematischen Wissenschaften v. 290, Springer, 3ed. ed., 1998.

[7] E. Assmus and J. Key, *Designs and Their Codes*. Cambridge Tracts in Mathematics, Cambridge University Press, 1994.

[8] J. H. v. L. P. J. Cameron, *Designs, Graphs, Codes and their Links*. London Mathematical Society Student Texts, Cambridge University Press, 1991.

[9] J. H. Van Lint, *Introduction to coding theory*, vol. 86. Springer Science & Business Media, 2012.

[10] J. van Lint, R. Wilson, and R. Wilson, *A Course in Combinatorics*. A Course in Combinatorics, Cambridge University Press, 2001.

[11] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Rep. Suppl.*, no. 10, pp. vi+97, 1973.

[12] N. Biggs, "Perfect codes in graphs," *J. Combinatorial Theory Ser. B*, vol. 15, pp. 289–296, 1973.

[13] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.

[14] J. H. van Lint, "A survey of perfect codes," *Rocky Mountain J. Math.*, vol. 5, pp. 199–224, 1975.

[15] N. Silberstein, "Properties of codes in the johnson scheme," *CoRR*, vol. abs/1004.4882, 2010.

[16] W. Martin, "Completely regular codes: a viewpoint and some problems," *Proceedings of 2004 Com2MaC Workshop on Distance-Regular Graphs and Finite Geometry, July 24 - 26*, 2004.

[17] A. Neumaier, "Completely regular codes," *Discrete Mathematics*, vol. 106-107, 1992.

[18] A. Brouwer, A. Cohen, and A. Neumaier, *Distance-Regular Graphs*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer Berlin Heidelberg, 2011.

[19] N. Gillespie, *Neighbour Transitivity on Codes in Hamming Graphs*. Dissertation, University of Western Australia, 2011.

[20] P. Solé, "Completely regular codes and completely transitive codes," *Discrete mathematics*, vol. 81, pp. 193 – 201, 1990.

[21] M. Giudici and C. E. Praeger, "Completely transitive codes in hamming graphs," *European Journal of Combinatorics*, vol. 20, no. 7, pp. 647 – 662, 1999.

[22] M. H. D. R. P. C. E. Gillespie, Neil I.; Giudici, "Entry-faithful 2-neighbour transitive codes," *Designs, Codes and Cryptography*, vol. 79, 6 2016.

[23] N. Gillespie and D. Hawtin, "Alphabet-almost-simple 2-neighbour-transitive codes," *Ars Mathematica Contemporanea*, vol. 14, no. 2, pp. 345–357, 2018.

[24] N. I. Gillespie and C. E. Praeger, "Neighbour transitivity on codes in hamming graphs," *Designs, Codes and Cryptography*, vol. 67, pp. 385–393, Jun 2013.

[25] D. R. Hawtin, N. I. Gillespie, and C. E. Praeger, "Elusive codes in hamming graphs," *Bulletin of the Australian Mathematical Society*, vol. 88, no. 2, p. 286296, 2013.

[26] C. D. Godsil and C. E. Praeger, "Completely transitive designs," 2014.

[27] M. Neunhöffer and C. E. Praeger, "Sporadic neighbour-transitive codes in johnson graphs," *Designs, Codes and Cryptography*, vol. 72, pp. 141–152, Jul 2014.

[28] N. Durante, "On sets with few intersection numbers in finite projective and affine spaces," *Electron. J. Combin.*, vol. 21, no. 4, pp. Paper 4.13, 18, 2014.

[29] W. J. Martin, "Completely regular designs of strength one," *Journal of Algebraic Combinatorics*, vol. 3, pp. 177–185, 1994.

[30] W. J. Martin, "Completely regular designs," *Journal of Combinatorial Designs*, vol. 6, pp. 261–273, 1998.

[31] A. Meyerowitz, "Cycle-balance conditions for distance-regular graphs," *Discrete Mathematics*, vol. 264, pp. 149–165, 2003.

[32] J. Dixon and B. Mortimer, *Permutation Groups*. Graduate Texts in Mathematics, Springer, 1996.

[33] P. Cameron, *Permutation Groups*. London Mathematical Society St, Cambridge University Press, 1999.

[34] A. Delandtsheer, "Finite antiflag transitive linear spaces," *Mitteilungen aus dem Mathem. Seminar Giessen*, 1984.

[35] M. Liebeck, C. Praeger, and J. Saxl, *The Maximal Factorizations of the Finite Simple Groups and Their Automorphism Groups*. No. no. 432 in American Mathematical Society: Memoirs of the American Mathematical Society, American Mathematical Soc., 1990.

[36] M. Giudici, "Factorisations of sporadic simple groups," *Journal of Algebra*, vol. 304, pp. 311–323, 2006.

[37] M. Aschbacher, "On the maximal subgroups of the finite classical groups," *Invent. Math.*, vol. 76, no. 3, pp. 469–514, 1984.

[38] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*. London Mathematical Society Lecture Note Series, Cambridge University Press, 1990.

[39] J. Bray, D. Holt, and C. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. London Mathematical Society Lecture Note Series, Cambridge University Press, 2013.

[40] J. Gallian, *Contemporary Abstract Algebra*. Brooks/Cole, Cengage Learning, 2010.

[41] M. Aschbacher, *Finite Group Theory*. Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2000.

[42] D. Taylor, *The geometry of the classical groups*. Sigma series in pure mathematics, Heldermann Verlag, 1992.

[43] H. Wielandt, *Finite permutation groups*. Academic paperbacks, Academic Press, 1964.

[44] C. D. Godsil, R. A. Liebler, and C. E. Praeger, "Antipodal distance transitive covers of complete graphs," *European J. Combin.*, vol. 19, no. 4, pp. 455–478, 1998.

[45] W. M. Kantor, "k-homogeneous groups," *Math. Z.*, vol. 124, pp. 261–265, 1972.

[46] P. Cameron, *Classical Groups*. University of London M.Sc. course A31: Classical Groups, 2000.

[47] R. Brauer, "A characterization of null systems in projective space," *Bull. Amer. Math. Soc.*, vol. 42, no. 4, pp. 247–254, 1936.

[48] P. Dembowski, *Finite Geometries*. Springer My Copy UK, 1996.

[49] P. Delsarte and J.-M. Goethals, "Alternating bilinear forms over gf (q)," *Journal of Combinatorial Theory, Series A*, vol. 19, no. 1, pp. 26–50, 1975.

[50] W. M. Kantor, "Symplectic groups, symmetric designs, and line ovals," *J. Algebra*, vol. 33, pp. 43–58, 1975.

[51] N. N. Sastry and P. Sin, "Codes associated with nondegenerate quadrics of a symplectic space of even order," *Journal of Combinatorial Theory, Series A*, vol. 94, no. 1, pp. 1 – 14, 2001.

[52] N. S. N. Sastry and P. Sin, "On the doubly transitive permutation representations of $\mathrm{Sp}(2n, \mathbb{F}_2)$," *J. Algebra*, vol. 257, no. 2, pp. 509–527, 2002.

[53] P. Cameron and J. Seidel, "Quadratic forms over gf(2)," *Indagationes Mathematicae (Proceedings)*, vol. 76, no. 1, pp. 1–8, 1973.

[54] J. T. a. J.W.P Hirschfeld, *General Galois Geometries*. Springer Monographs in Mathematics, Springer-Verlag London, 1 ed., 2016.

[55] G. Mullen and D. Panario, *Handbook of Finite Fields*. Discrete Mathematics and Its Applications, Taylor & Francis, 2013.

[56] O. King, "The subgroup structure of finite classical groups in terms of geometric configurations," *Surveys in Combinatorics 2005*, pp. 509–527, 2005.

[57] N. Gill, "Polar spaces and embeddings of classical groups," *New Zealand Journal of Mathematics*, vol. 36, pp. 175–184, 2007.

[58] J. Konvalina and Y.-H. Liu, "Arithmetic progression sums of binomial coefficients," *Applied Mathematics Letters*, vol. 10, no. 4, pp. 11–13, 1997.

[59] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.2*, 2019.

[60] C. Hering, M. W. Liebeck, and J. Saxl, "The factorizations of the finite exceptional groups of lie type," *Journal of Algebra*, vol. 106, no. 2, pp. 517–527, 1987.

[61] C. E. Praeger and A. Seress, "Probabilistic generation of finite classical groups in odd characteristic by involutions," *J. Group Theory*, vol. 14, no. 4, pp. 521–545, 2011.

[62] V. Landazuri and G. M. Seitz, "On the minimal degrees of projective representations of the finite Chevalley groups," *J. Algebra*, vol. 32, pp. 418–443, 1974.

[63] C. Jansen, K. Lux, R. Parker, and R. Wilson, *An Atlas of Brauer Characters*. London Mathematical Society Monographs New Series, Oxford University Press, 1997.

[64] M. Ioppolo. `https://github.com/mioppolo/JohnsonCodes/`. Accessed: 17-10-2019.

[65] W. M. Kantor, "Classification of 2-transitive symmetric designs," *Graphs and Combinatorics*, vol. 1, no. 2, pp. 165–166, 1985.

[66] G. D. James, "On the minimal dimensions of irreducible representations of symmetric groups," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 94, 1983.

[67] M. W. Liebeck, "The affine permutation groups of rank three," *Proceedings of the London Mathematical Society*, vol. s3-54, no. 3, pp. 477–516, 1987.