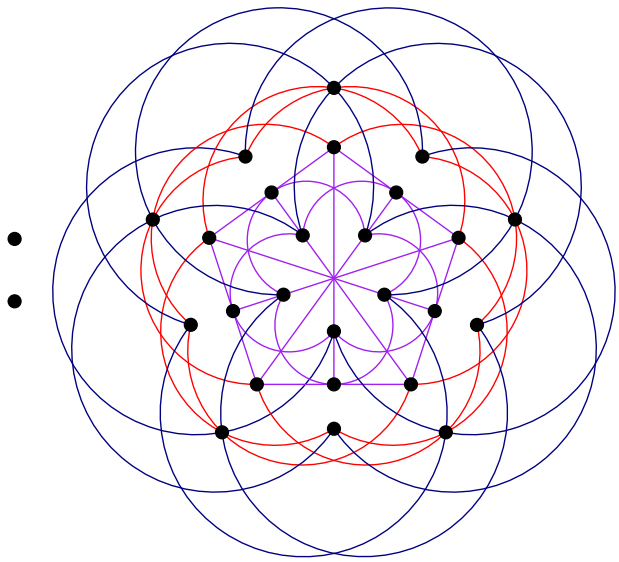
Relative Hemisystems on the Hermitian Surface

Author:
Melissa Lee
School of Mathematics
and Statistics

Supervisors:
Dr. John Bamberg
Dr. Eric Swartz
School of Mathematics
and Statistics



This thesis is presented for the partial requirements of the degree of
Bachelor of Science with Honours
of the University of Western Australia
October 10, 2014

Abstract

Relative hemisystems on the Hermitian surface are a concept in finite geometry, first defined by by Penttila and Williford in 2011. They were introduced as an analogous and fruitful concept to hemisystems, another class of geometric objects which have had a compelling history since their introduction by B. Segre almost 50 years ago. Penttila and Williford's definition of relative hemisystems was motivated by the desire to generate a class of previously undiscovered association schemes which are primitive, Q-polynomial and do not arise from distance regular graphs. Since their definition, only three families and one supposedly sporadic example of relative hemisystems have been found.

In this thesis, after covering some background theory on finite geometry and group theory, we explore the rich history of hemisystems and relative hemisystems. We examine in depth the geometric objects arising from these structures and provide constructions of the known examples of relative hemisystems. We subsequently discuss the results of our quest to classify and find new examples of relative hemisystems. We present the findings from our independent discovery of two recent examples of relative hemisystems and from these produce a previously unknown set of criteria sufficient to determine a relative hemisystem. These criteria provide the basis for new constructions of the Penttila-Williford and a Cossidente family of relative hemisystems. We also completely classify the relative hemisystems on the Hermitian space $\mathrm{H}(3, 16)$, and some of the relative hemisystems on $\mathrm{H}(3, 64)$ with certain primes dividing their collineation groups. Finally, we reflect on our results and provide some open problems and ideas for future work.

Acknowledgements

I must first and foremost express my greatest gratitude to my supervisors, Res/A/Prof. John Bamberg and Dr. Eric Swartz. To John – thank you for motivating me, encouraging me, teaching me resilience and being a mentor and friend throughout the year. To Eric – thank you for being so patient and understanding, and taking the time to go through concepts with me, all with good humour.

Thank you also to the UWA Mathematics Union and my friends at home and abroad, for their unwavering support during the year. I am also grateful to my colleagues in honours for sharing this experience with me, providing some much needed comic relief and reminding me why I have chosen to pursue mathematics.

I would also like to express my appreciation to the School of Mathematics and Statistics at UWA, for their continuing guidance and support during a tumultuous year for myself and the UWA Mathematics Union.

Finally, I would like to thank my family for always encouraging me to do what I love, and Mitchell for loving me and loving what I do.

Contents

List of Figures

List of Tables

Introduction

> "Get up and commit, show the power trapped within. Do just what you want to, and now stand up and begin."
>
> Muse, *Panic Station*

Consider a complex train network, like the Paris Métro, where each station may be on more than one train route. Is there a way that we can make the system more efficient? We could begin by attempting to select a set of train lines such that every station is visited exactly once.

Figure 1.1: A section of a map of the Paris Métro [46].

Let us create an abstract version of this situation by defining an *incidence structure* $(\mathcal{P}, \mathcal{L}, I)$, where the set of *points* denoted $\mathcal{P}$ correspond to train stations, the set of *lines* $\mathcal{L}$ correspond to train lines, and an *incidence relation* I, that tells us which stations are on each train line. The problem of choosing a set of train lines that visits every train station exactly once turns into a problem of choosing lines such that every point lies on exactly one line in the set. If such a set of lines exists, it is called a *spread* of the incidence structure.

We can generalise the concept of a spread to sets of lines such that every point of the geometric structure has exactly m lines on it. We call this a *regular system of order* m. Beniamino Segre, who was one of the founders of combinatorial geometry, was particularly interested in regular systems of order m on Hermitian spaces.

A *Hermitian space* $\mathrm{H}(3, q^2)$ is the set of totally isotropic subspaces of a Hermitian form in $\mathrm{PG}(3, q^2)$. A Hermitian space with these parameters is also a generalised quadrangle of order (q^2, q).

In an epic 200 page treatise, Segre proved that the only value of m for which $\mathrm{H}(3, q^2)$, q odd, has a regular system is $\frac{q+1}{2}$ [51]. He called a regular system of order $\frac{q+1}{2}$ a *hemisystem*, because there are $q+1$ lines on every point in the Hermitian space, and so a hemisystem is exactly half of these lines.

The history of hemisystems is quite astounding. When Segre defined them in 1965, he gave an example of a hemisystem on the Hermitian space $\mathrm{H}(3, 9)$ and proved this was the sole example up to equivalence on a Hermitian space with these parameters. For the next forty years, there was an unsuccessful search by many members of the mathematical community to find a different example of a hemisystem. Along the way, many properties and consequences of hemisystems were proven, but these gave no insight into other hemisystems that may exist. In

fact, in 1995, Thas conjectured that there are no hemisystems on any Hermitian spaces apart from Segre's [55]. Then, forty years after Segre's original treatise, Penttila and Cossidente found an infinite family of hemisystems [23]. Since then, several infinite families of hemisystems have been found by a variety of authors [3, 4, 25]. In addition to being interesting structures in their own right, various authors have proved that hemisystems give rise to partial quadrangles, strongly regular graphs and rare association schemes that are 4-class, imprimitive, cometric, and Q-antipodal [43, 53].

In 2011, Penttila and Williford defined relative hemisystems as an analogous concept to hemisystems for q even, motivated by the desire to generate a previously undiscovered type of association scheme, which is 3-class, primitive and Q-polynomial.

Let S be a generalised quadrangle of order (q^2, q) containing a generalised quadrangle S' of order (q, q). Then all lines of S meet S' in $q + 1$ points or are disjoint from S'. We call a subset $\mathcal{H}$ of the lines disjoint from S' a *relative hemisystem* of S with respect to S' provided that for each point x of $S \setminus S'$, exactly half the lines through x disjoint from S' lie in $\mathcal{H}$.

In order to make sense of this definition, we will construct an example of a dual relative hemisystem using the game SET.[1] In other words, we will demonstrate a set of points $\mathcal{R}$ in a generalised quadrangle $\tilde{S}$ of order $(2, 4)$ such that every line in $\tilde{S}$ which is disjoint from the embedded generalised quadrangle of order $(2, 2)$ is incident with one point of $\mathcal{R}$.

In the game SET, there are 81 cards, each with four symbol traits – shape, shading, colour and number, with three variations of each trait. The aim of the game is to make SETs of three cards where each of these four traits is either all the same or all different across the three cards. We visualise SET cards as points, with lines joining three points if the corresponding cards form a SET. Using this model, we can create the generalised quadrangle S of order $(2, 4)$ with the generalised quadrangle S' of order $(2, 2)$ inside it from SET cards, and we exhibit this in Figure 1.2. For simplicity, we call the points and lines that are included in S but are disjoint from S' *external points* and *external lines* respectively. Notice that we can't quite draw this generalised quadrangle in a planar fashion and so have two points off to the side. The top card forms SETs with the pairs of cards on the edges of the pentagon, and the bottom card forms SETs with pairs of cards corresponding to a card above a vertex of the pentagon, and the card on the opposite edge of the pentagon.

The cards with yellow bordering correspond to the points that form a dual relative hemisystem in the generalised quadrangle. Notice that since we are choosing half of the external points to form the dual relative hemisystem, the remaining external points (cards), which have green bordering also form a relative hemisystem.

[1] SET is a registered trademark of Set Enterprises, Inc.. All rights reserved.

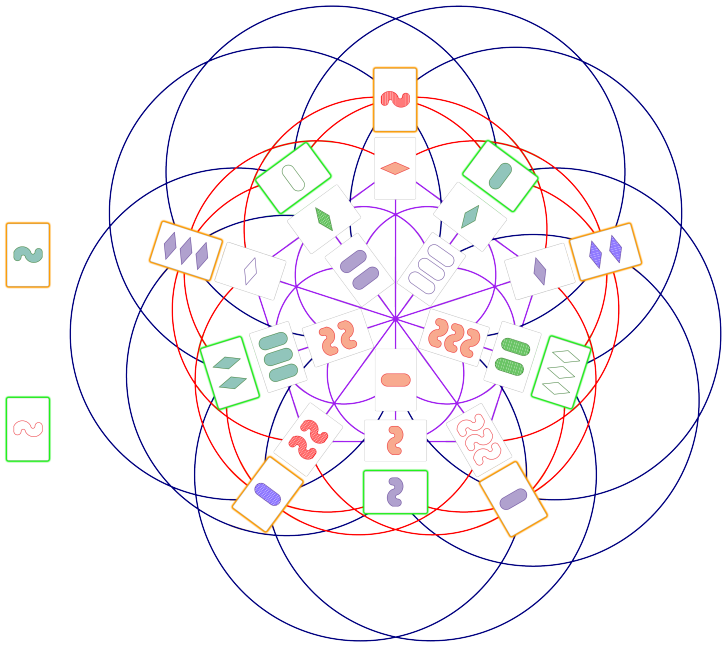


Figure 1.2: A SET card representation of the generalised quadrangle of order $(2, 4)$, with dual relative hemisystems highlighted in yellow and green.

This is the smallest possible example of a dual relative hemisystem. The number of lines contained in a relative hemisystem increases rapidly as q increases and it soon becomes unfeasible to describe relative hemisystems by the lines they contain. Instead, we choose to describe them using groups. A *collineation* is an incidence preserving automorphism from an incidence structure to itself. The set of all collineations of an incidence structure form a group under composition, called the *collineation group* of the incidence structure. We may therefore classify relative hemisystems by their collineation groups. We say that a relative hemisystem *admits* a group if it is a subgroup of the relative hemisystem's collineation group. By using collineation groups to describe geometric structures, we can take advantage of the symmetry inherent in group theory to give us neat and sometimes unexpected results, as we will see in later chapters.

The known examples of relative hemisystems are reasonably few. When they first defined the notion of relative hemisystems in [49], Penttila and Williford gave an example of an infinite family that admits $\mathrm{P}\Omega^{-}(4, q)$ as a collineation group for each q, a power of two. Cossidente subsequently discovered two more infinite families of relative hemisystems admitting $\mathrm{PSL}(2, q)$ and a group of order $q^2(q+1)$ respectively, which were mild perturbations of the Penttila-Williford family of relative hemisystems [20, 21]. Cossidente and Pavese also discovered a supposedly sporadic example of a relative hemisystem arising from a Suzuki-Tits ovoid [22].

The objective of this project was to attempt to find more examples of relative hemisystems on $\mathrm{H}(3, q^2)$, and to classify all of the relative hemisystems on $\mathrm{H}(3, 64)$.

We worked towards this aim by designing programs in GAP [30] and Gurobi [38] to exhaustively search for new relative hemisystems. Despite large improvements in the efficiency of our computation, we found the problem of classification to be intractable with our current methods. However, we did manage to independently discover the infinite family of relative hemisystems admitting an automorphism group of order $q^2(q+1)$ originally found by Cossidente and the conjectured sporadic example found by Cossidente and Pavese. We subsequently completed some analysis on them before their discoveries were published by the respective authors. In doing so, we found a new construction of the infinite family of relative hemisystems admitting a group of order $q^2(q+1)$ as well as the Penttila-Williford family. We also formulated a set of previously unknown sufficient criteria for a relative hemisystem. We show that the Penttila-Williford family and the $q^2(q+1)$ Cossidente family satisfy these conditions, and provide a partial proof of the $\mathrm{PSL}(2,q)$ Cossidente family, for $q = 4, 8, 16$. We also classify all of the relative hemisystems on $\mathrm{H}(3,16)$, a result that was previously unknown. All of these results will be discussed in depth later in this dissertation.

In Chapters 2 and 3, we present the foundations of finite geometry and group theory necessary for the study of relative hemisystems. In Chapter 4, we explore the history and properties of hemisystems and relative hemisystems, as well as give a survey of the known examples of relative hemisystems and their constructions. In Chapter 5, we present the outcomes of this research project, starting with the attempt to computationally classify all relative hemisystems on $\mathrm{H}(3,64)$, which lead to the independent discovery of two recently discovered examples of relative hemisystems. We also present a new set of sufficient criteria to determine a relative hemisystem, and prove that the Penttila-Williford and Cossidente families of relative hemisystems satisfy them.

For clarity throughout this dissertation, we will mark an original proof by an asterisk *.

Projective Geometry

> "A straight line may be the shortest distance between two points, but it is by no means the most interesting."
>
> The Third Doctor, *Doctor Who*

This chapter introduces many of the structures and concepts that will be used extensively in this dissertation. Projective geometry is a level of abstraction above the Euclidean geometry that we are accustomed to in every day life. We will begin by discussing finite fields and then introduce projective spaces using a series of axioms. We will build on these concepts and describe objects that can be embedded in projective spaces, such as quadrics, Hermitian spaces and symplectic spaces, all of which are crucial to the discussion of relative hemisystems in subsequent chapters.

2.1 Finite fields

Definition 2.1. A *field* is a set $\mathbb{F}$ equipped with two associative binary operations called addition and multiplication, denoted $+$ and $\times$ that satisfy the following properties.

i) $(\mathbb{F}, +)$ is an Abelian group[1].

ii) For all $a, b, c \in \mathbb{F}$, $a \times (b + c) = a \times b + a \times c$, and $(b + c) \times a = b \times a + c \times a$.

iii) There exists a multiplicative identity $1_{\mathbb{F}}$ such that $1_{\mathbb{F}} \times a = a$ for all $a \in \mathbb{F}$.

iv) Multiplication is commutative on $\mathbb{F}$, i.e., $a \times b = b \times a$ for all $a, b \in \mathbb{F}$.

v) For all nonzero $a \in \mathbb{F}$, there exists an element $a^{-1} \in \mathbb{F}$ such that $a \times a^{-1} = a^{-1} \times a = 1_{\mathbb{F}}$.

We usually omit the multiplication sign $\times$ when multiplying elements of the field, and denote repeated multiplication using index notation. We also sometimes omit the subscript $\mathbb{F}$ on $1_{\mathbb{F}}$ if it is clear which field is being discussed. An example of a field that is very familiar to us is the real numbers. This is an example of an infinite field; most of the fields of interest to us will be finite. For example, $\mathbb{Z}_p$, the integers modulo p, where p is a prime, is a finite field with addition and multiplication modulo p. Finite fields are always of order $q = p^k$, for some prime number p, and for some $k \in \mathbb{N}$ [29]. Furthermore, there is a unique finite field of order q up to isomorphism. We denote a finite field by $\mathrm{GF}(q)$, where q is the number

[1] See Appendix B for missing definitions from elementary group theory.

of elements in the field. We also call q the *order* of the field. The notation $\mathrm{GF}(q)$ arises from the alternate name for finite fields, *Galois fields*, after Évariste Galois, who made large contributions to finite field theory. The *field characteristic* is the smallest positive integer $\eta \in \mathbb{N}$ such that $\eta a = 0$ for all $a \in \mathbb{F}$. In the infinite case, if there is no such η, we define the characteristic to be zero.

Example 2.2 ([29])**.** *Let p be a prime. The characteristic of any finite field $\mathrm{GF}(p^k)$ is p.*

Notice that $\mathrm{GF}(q) \setminus \{0\}$ forms a group under the multiplication $\times$ of the field. We call this the *multiplicative* group of the field, and it is a cyclic group of order $q-1$. This implies that for any nonzero $x \in \mathrm{GF}(q)$, $x^q = x$.

A *subfield* is defined as a subset of a field that is a field itself when equipped with the addition and multiplication of its parent field. For example, the real numbers are a subfield of the complex numbers. In the finite case, since all fields have prime power order, any subfield must have order which is a smaller power of the same prime[2]. A *field automorphism* is a bijection from a field $\mathbb{F}$ to itself that preserves addition and multiplication. Symbolically, a field automorphism $\alpha : \mathbb{F} \to \mathbb{F}$ satisfies $\alpha(ab) = \alpha(a)\alpha(b)$ and $\alpha(a+b) = \alpha(a) + \alpha(b)$ for all $a, b \in \mathbb{F}$. In the case of finite fields, if $q = p^k$ for some prime number p, then the automorphisms of $\mathrm{GF}(q)$ are the maps that raise each element to a power p^j, where $0 < j \leq k$ [42, p. 53]. Notice that the structure preserving property of automorphisms implies that for all $a, b \in \mathrm{GF}(q)$, $(a+b)^{p^j} = a^{p^j} + b^{p^j}$.

We now have enough to prove the following lemma. This lemma will prove useful later in Chapter 5 when constructing relative hemisystems.

Lemma 2.3. *Suppose $q = 2^n$. Then for all $z \in \mathrm{GF}(q^2)$ that satisfy $z + z^q = 1$, the polynomial $z^{q+1}x_2^2 + x_1x_2 + x_1^2$ is irreducible over $\mathrm{GF}(q)$.*

Proof. * Firstly notice that $z^{q+1} \in \mathrm{GF}(q)$, because $(z^{q+1})^q = z^{q+1}$. Suppose that $z^{q+1}x_2^2 + x_1x_2 + x_1^2$ was reducible. Then $z^{q+1}x_2^2 + x_1x_2 + x_1^2 = 0$ for some $x_1, x_2 \in \mathrm{GF}(q)$, with at least one of x_1, x_2 nonzero. Now, notice that $(zx_2 + x_1)^{q+1} = z^{q+1}x_2^{q+1} + x_1^{q+1} + zx_2x_1^q + z^qx_2^qx_1 = z^{q+1}x_2^2 + x_1^2 + zx_2x_1 + z^qx_2x_1$. Then, from the definition of z,

$$\begin{aligned} z^{q+1}x_2^2 + x_1x_2 + x_1^2 &= (zx_2 + x_1)^{q+1} + zx_2x_1 + z^qx_2x_1 + x_1x_2 \\ &= (zx_2 + x_1)^{q+1} + (z^q + z + 1)(x_1x_2) \\ &= (zx_2 + x_1)^{q+1} \end{aligned}$$

So $(zx_2 + x_1)^{q+1} = 0$. Since a field has no zero divisors[3], we must have $zx_2 + x_1 = 0$. Since $\mathrm{GF}(q)$ is a field and is therefore closed under addition and multiplication,

[2] See Lagrange's Theorem in Appendix B.

[3] nonzero elements whose product is zero.

$z \in \mathrm{GF}(q)$. It follows that $z^q + z = z + z = 0$, which is a contradiction because by definition, z must satisfy $z + z^q = 1$. Therefore, $z^{q+1}x_2^2 + x_1x_2 + x_1^2$ must be irreducible. □

Notice that this is only guaranteed to hold for q even, since we extensively make use of the characteristic of $\mathrm{GF}(q)$.

2.2 Projective spaces

We will introduce projective spaces in an axiomatic fashion, building up from incidence structures and projective planes, and making use of the finite fields discussed in the previous section.

Definition 2.4. ([61, p. 215]) A *point-line incidence structure* is a triple $(\mathcal{P}, \mathcal{L}, I)$, with points $\mathcal{P}$, lines $\mathcal{L}$ and a symmetric incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$. We say the incidence structure is *finite* when $\mathcal{P}$ is finite.

A point P is said to be *incident* with a line ℓ if $(P, \ell) \in I$. Since I is symmetric, we also say that ℓ is incident with P. We describe two points as being *collinear* if they are incident with the same line. Furthermore, we say that two lines ℓ and m meet if there exists a point P such that $(P, \ell) \in I$ and $(P, m) \in I$. We sometimes denote that a point or line x is incident with another point or line y by $x \,\mathrm{I}\, y$. Although we have defined incidence structures using points and lines, there are other higher dimensional structures such as planes and solids, which will be discussed later in Section 2.2.2. We will also always assume that our incidence structures are finite.

2.2.1 Projective planes

Definition 2.5. A projective plane is an incidence structure such that:

1. Any two points span a unique line.
2. Any two lines meet in a unique point.
3. There exist four points such that there is no line which meets three of them.

Notice that if P is a point and ℓ is a line not incident with P, there exists a line for every point on ℓ that is incident with P. Additionally, each line through P must meet ℓ in a single point. Since these statements hold for every pair P and ℓ, there must be the same number of points incident with each line as there are lines incident with each point. If there are $q + 1$ points incident with every line, then we say that a projective plane has *order* q.

The Fano plane is the smallest example of a projective plane, illustrated in Figure 2.1. It has seven points, and seven lines and has order two. We may assign non-zero

vectors from GF(2)^3 to each of the points in the Fano plane,[4] with lines forming the span of two points.

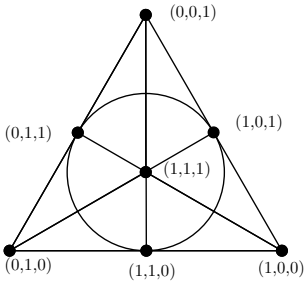


Figure 2.1: The Fano plane, a projective plane of order two.

We say that two triangles are *in perspective* from a point P if their corresponding vertices lie on lines that are incident with P. Similarly, we say that two triangles are in perspective with respect to a line ℓ if the lines forming the corresponding edges of the triangles meet on ℓ. A projective space is said to be *Desarguesian* if whenever two triangles are in perspective from a point, they are also in perspective with respect to a line, and vice versa. This property is named after Desargues, a 17th century mathematician who proved that the projective spaces over the real numbers are Desarguesian [68]. For example, the Fano plane is Desarguesian. See Figure 2.2 for an example of two triangles in the Fano plane that satisfy the Desarguesian property. Projective spaces that are not Desarguesian are said to be *non-Desarguesian*, and the first examples of non-Desarguesian planes were discovered by Veblen and Wedderburn [63]. The smallest non-Desarguesian projective planes are three examples of order nine, which each have 91 points and 91 lines. For a survey of the known non-Desarguesian planes, see [68]. As we will find out in the next section, all projective spaces which have higher rank than a two dimensional projective plane are Desarguesian.

2.2.2 Projective spaces

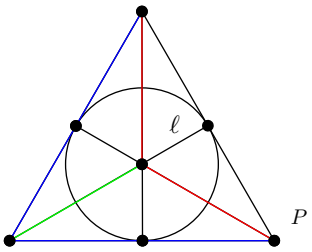


Figure 2.2: Two triangles in the Fano plane which are in perspective from P and in perspective with respect to ℓ.

Definition 2.6. A *projective space* is an incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ which obeys the following set of axioms.

i) Any two points P and Q are incident with exactly one common line, denoted PQ,

ii) Each line is incident with at least three points,

iii) Suppose A, B, C, D are distinct points. Then, if AB intersects CD, then AC intersects BD.

The last axiom is called the *Veblen-Young axiom*, first described by the axiom's namesakes in 1908 [64]. It ensures that every pair of lines on a plane meet in a point. An illustration of the axiom is given in Figure 2.3. If we know that two lines in the incidence structure always meet, we are not required to prove that the Veblen-Young axiom holds to show that the incidence structure is a projective space.

[4] That is, non-zero, three dimensional vectors over GF(2).

A projective space is said to be *nondegenerate* when it contains at least two lines. We assume that all of the projective spaces we work with are nondegenerate.

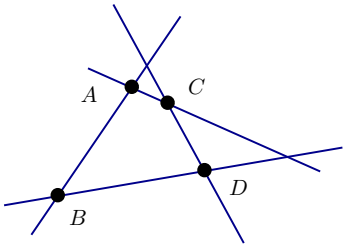


Figure 2.3: An illustration of the Veblen-Young axiom.

We will now describe an intuitive way of building projective spaces by considering vector spaces over fields. Let V be an $(n+1)$-dimensional vector space over a finite field $\mathrm{GF}(q)$, where q is a prime power. We will define the incidence structure $\mathrm{PG}(n,q)$ as follows. Define the set of points of $\mathrm{PG}(n,q)$ as the set of one dimensional subspaces of V. In the same way, define the set of lines of $\mathrm{PG}(n,q)$ to be the set of two-dimensional subspaces of V and so on. We define the incidence relation I associated with $\mathrm{PG}(n,q)$ by taking a symmetric version of inclusion on subspaces. Given a subspace of dimension k, we define its codimension to be $n-k$. A *hyperplane* is defined to be a subspace with codimension 1. We also sometimes refer to the dimension of a projective space as its *rank*.

Theorem 2.7. $\mathrm{PG}(n,q)$ *satisfies the axioms for a projective space.*[5]

Moreover, every Desarguesian projective space can be constructed from $\mathrm{PG}(n,q)$.

Example 2.8. *The Fano plane is isomorphic to* $\mathrm{PG}(2,2)$.

In fact, Vahlen [59] and Hessenberg [34] showed that not only does $\mathrm{PG}(n,q)$ meet the conditions for a projective space, but every projective space of rank $n \geq 3$ can be constructed from it. This gives us a nice way of visualising projective spaces in terms of the less abstract notion of vector spaces. Despite Vahlen and Hessenberg's earlier proof of the following theorem, it is almost universally attributed to Veblen and Young.

Theorem 2.9 (The Veblen-Young Theorem [65, 66])**.** *Any finite projective space with rank* $n \geq 3$ *is isomorphic to the Desarguesian projective space* $\mathrm{PG}(n,q)$*, with the same order.*

This immediately implies that the only non-Desarguesian projective spaces have rank less than or equal to two. We sometimes take advantage of the Veblen-Young Theorem and denote lines by a $2 \times (n+1)$ matrix whose rowspace is the associated vector subspace of that line. We will see this notation used extensively in the discussion of reguli. We can also now consider higher dimensional subspaces of projective spaces in terms of the underlying vector space. If U is an m-dimensional subspace of an $(n+1)$-dimensional vector space V over $\mathrm{GF}(q)$, then U is a $(m-1)$-dimensional subspace of $\mathrm{PG}(n,q)$. For example, if $m=3$, the corresponding subspace of $\mathrm{PG}(n,q)$ is a plane, and if $m=4$, the corresponding subspace is a solid. Furthermore, if $m=n$, then the corresponding subspace of $\mathrm{PG}(n,q)$ is a hyperplane.

[5]The proof is omitted here, see [8].

2.2.3 Collineations Let $\mathrm{PG}(n,q)$ be a projective space. A *collineation* φ is a permutation of the points of $\mathrm{PG}(n,q)$ which maps every subspace to a subspace of the same dimension [14]. Collineations preserve incidence, namely if U and W are subspaces of the underlying vector space V of $\mathrm{PG}(n,q)$, then $\phi(W) \subseteq \phi(U)$ if and only if $W \subseteq U$. The set of all collineations of $\mathrm{PG}(n,q)$ forms a group[6] under composition. A collineation group acting on a geometric structure is an example of a group action, which will be covered further in Chapter 3. Collineation groups form the basis for the Fundamental Theorem of Projective Geometry, which will also be discussed in Chapter 3. We sometimes denote the collineation group of an incidence structure T by $\mathrm{Coll}(T)$.

In the study of relative hemisystems, we also frequently encounter Baer involutions. Suppose Θ is a subspace of a finite Desarguesian projective space $\mathrm{PG}(n,q^2)$ such that Θ has dimension n and order q. Then, we call Θ a *Baer subspace* of $\mathrm{PG}(n,q^2)$. Furthermore, if φ is a non-identity collineation that fixes a Baer subspace, we say that φ is a *Baer collineation*, or a *Baer involution* if φ has order two.[7]

2.2.4 Generalised quadrangles Generalised polygons were introduced by J. Tits in 1959 in order to describe the rank two residues of irreducible spherical buildings [56]. Amongst the generalised polygons are the generalised quadrangles, which are of particular interest to us.

Definition 2.10. A generalised quadrangle of order (s,t) is an incidence structure of points and lines such that:

i) Any two points are incident with at most one line.

ii) Every point is incident with $t+1$ lines.

iii) Every line is incident with $s+1$ points.

iv) For any point P and line ℓ that are not incident, there is a unique point K on ℓ that is collinear with P.

We sometimes denote the generalised quadrangle of order (s,t) by $\mathrm{GQ}(s,t)$. The last axiom is often called the 'GQ axiom' because it is a distinguishing feature of generalised quadrangles. If we take the point-line dual of a generalised quadrangle of order (s,t), we have another generalised quadrangle, of order (t,s). A simple counting argument shows that a generalised quadrangle of order (s,t) has $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines. There are many examples of generalised quadrangles, for a good

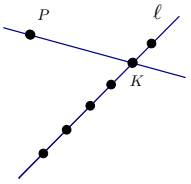


Figure 2.4: An illustration of the GQ axiom.

[6] See Appendix B for background on elementary group theory.

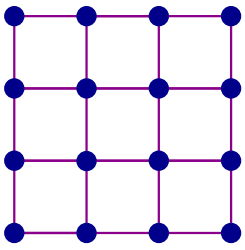
[7] For more background on Baer subplanes and collineations, see [7].

reference for the finite cases, see [48]. A trivial example of a generalised quadrangle is of order $(n, 1)$, which can be visualised as a grid.

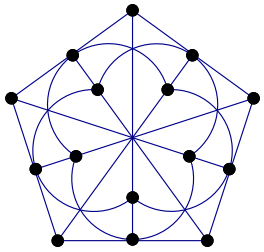
Example 2.11. *The symplectic space* $\mathrm{W}(3, q)$*, which will be explored further in Section 2.4.1, is an example of a family of generalised quadrangles of order* (q, q)*. The points of the symplectic space are the points of a projective space* $\mathrm{PG}(3, q)$*. Recall that points are the one dimensional subspaces of the underlying four dimensional vector space. The lines of* $\mathrm{W}(3, q)$ *are exactly the lines of* $\mathrm{PG}(3, q)$ *that are fixed under the map:*

$$\ell^\tau = \bigcap_{(x_1,x_2,x_3,x_4)\in\ell} \{(y_1, y_2, y_3, y_4) \in \mathrm{PG}(3, q) \mid x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 = 0\}.$$

The smallest nontrivial example of a generalised quadrangle is the symplectic space $\mathrm{W}(3, 2)$. It is sometimes called the 'doily' because of its shape in certain representations. See Figure 2.5.



$GQ(3, 1)$.



The doily - $GQ(2, 2)$.

Figure 2.5: Two examples of generalised quadrangles.

2.2.5 Partial quadrangles Cameron defined partial quadrangles in 1975 as a generalisation of generalised quadrangles [17]. Later in Chapter 4, we will show that every hemisystem give rise to a partial quadrangle.

Definition 2.12. A *partial quadrangle* is an incidence structure with parameters (s, t, μ), $s \geq 2, t \geq 2, \mu \geq 1$ that satisfies

i) every point is incident with $t + 1$ lines,

ii) every line is incident with $s + 1$ points,

iii) any two points are on at most one line together,

iv) there are no triangles, and

v) any two noncollinear points have μ points collinear with both of them.

When $\mu = t + 1$, then the partial quadrangle is also a generalised quadrangle.

Surprisingly, examples of partial quadrangles which are not generalised quadrangles are scarce. Out of the known partial quadrangles, the only examples are those arising from taking away points from a generalised quadrangle of order (s, s^2), three exceptional examples, and triangle-free strongly regular graphs [3]. The three exceptional examples were discovered by Calderbank when he almost completely classified the partial quadrangles arising from linear representations in [16].

2.2.6 Dualities

Definition 2.13. Suppose $\Pi = (\mathcal{P}, \mathcal{L}, I)$ is a projective space. We define the *dual projective space* $\Pi^* = (\mathcal{P}^*, \mathcal{L}^*, I^*)$ with the following properties:

i) The set of points $\mathcal{P}^*$ consists of the subspaces of Π with codimension 1.

ii) The set of lines $\mathcal{L}^*$ consists of the subspaces of Π with codimension 2.

iii) The incidence relation I^* is identical to I, i.e., two elements V and W are incident in Π^* if they are incident in Π.

Note that the dimension of Π^* is the same as the dimension of Π. If Π has finite dimension n then for every subspace V of Π, we have $\dim_{\Pi^*}(V) = (n-1) - \dim_{\Pi}(V)$ [58].

Definition 2.14. Suppose Π is a projective space and Π^* is its dual projective space. Then a collineation $\gamma : \Pi \to \Pi^*$ from Π to Π^* is called a *duality*. A duality of order two, is called a *polarity*.

The map τ in Example 2.11 is an instance of a duality. It is also of order two, and is hence a polarity. A natural question to ask about dualities concerns the relationship between the image of a subspace of projective space under a duality and the images of its subspaces under the same duality.

Theorem 2.15. *Suppose Π is a projective space, and γ is a duality of Π. If U is a subspace of Π, then*

$$U^\gamma = \bigcap_{u \in U} u^\gamma.$$

Proof. Since γ is a collineation, the set $S_U := \{u^\gamma \mid u \in U\}$ is a subspace of Π^*. Therefore,

$$U^\gamma = S_U = \langle u^\gamma \mid u \in U \rangle = \bigcap_{u \in U} u^\gamma$$

as required. □

For the purposes of this dissertation, we are mainly concerned with polarities and the polar spaces associated with them.

2.2.7 Polarities We first state an important and useful theorem about the properties of polarities.

Proposition 2.16 ([58])**.** *Suppose* Π *is a projective space, and let* γ *be a bijection not equal to the identity map from the set of points of* Π *to the set of hyperplanes of* Π*. Then the following statements are equivalent:*

i) The map γ *is a polarity.*

ii) If P, Q *are points of* Π*, then* $P \in Q^\gamma$ *implies* $Q \in P^\gamma$*.*

We say that a point P contained in a projective space Π is *absolute* with respect to a polarity γ if $P \in P^\gamma$. On the other hand, a subspace V of Π is said to be *absolute* with respect to γ if $V \subseteq V^\gamma$.

Proposition 2.17 ([58])**.** *Suppose* Π *is a projective space and* γ *is a polarity of* Π*. Then:*

i) If a subspace V *of* Π *is absolute with respect to* γ*, then every point of* V *is absolute with respect to* γ*.*

ii) If P *and* Q *are two points of* Π *that are absolute with respect to* γ*, then the line* PQ *is absolute with respect to* γ *if and only if* Q *is contained in* P^γ*.*

Proof. i): For any point $R \in V$, we have by definition of a polarity, $R \in V \subseteq V^\gamma \subseteq R^\gamma$.
ii): Forward direction: Suppose $\ell = PQ$ is an absolute line with respect to γ. By Theorem 2.15, we have $Q \in \ell \subseteq \ell^\gamma \subseteq Q^\gamma$.
Backward direction: Suppose P and Q are two absolute points of Π such that $Q \in P^\gamma$. Since γ is a polarity, we also have $P \in Q^\gamma$. Furthermore, since P and Q are absolute, we have $P \in P^\gamma$ and $Q \in Q^\gamma$. This implies that $\ell = PQ \subseteq P^\gamma \cap Q^\gamma$. Suppose that R is a point incident with ℓ but is distinct from P and Q. Since γ is a polarity, we have $P^\gamma \cap Q^\gamma \subseteq R^\gamma$ and so $\ell \in R^\gamma$. Thus, $\ell^\gamma = \bigcap_{R \in \ell} R^\gamma \supseteq \ell$. Therefore, ℓ is absolute. □

We now present the following theorem which states how we can construct a polar space from a polarity. We leave the proof until later in the chapter, when we have more closely studied the definition and properties of polar spaces.

Theorem 2.18. *Suppose* Π *is a projective space, and let* γ *be a polarity of* Π *such that there is at least one absolute line with respect to* γ*. Then the absolute lines and absolute points with respect to* γ *define a polar space.*

2.3 Polar Spaces

We now discuss polar spaces at length, because they constitute many of the structures we need to discuss relative hemisystems in following sections. The notion of a polar space was first introduced in 1959 by Veldkamp [67] and the area grew rapidly in subsequent years. In this context, we will only consider finite polar spaces. The following definition is taken from Buekenhout and Shult [15].

Definition 2.19. An incidence structure $(\mathcal{P}, \mathcal{L}, I)$ is said to be a *finite polar space* if it satisfies the following properties

i) Any line contains at least three points,

ii) No point is collinear with all other points,

iii) If P is a point and ℓ is a line not incident with P, then P is collinear with exactly one or all of the points of ℓ.

The last axiom is sometimes called the 'one or all' axiom, and a depiction of the axiom is given in Figure 2.6. If we always have exactly one point on ℓ incident with P, then our finite polar space is a generalised quadrangle. The traditional way of constructing polar spaces arises from forms on vector spaces. Polar spaces which are created in this way are the *classical polar spaces*.

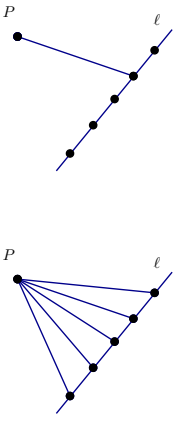


Figure 2.6: An illustration of the "one-all" axiom for polar spaces.

2.4 Classical Polar Spaces

The dualities that we explored in Section 2.2.6 can be defined algebraically by sesquilinear forms. Furthermore, polarities are defined algebraically by reflexive sesquilinear forms, and along with quadratic forms, these forms are used to define classical polar spaces. In addition, sesquilinear and quadratic forms are used to define classical groups, which will be discussed in Section 3.4 and are strongly linked to classical polar spaces. For background on reflexive sesquilinear forms and quadratic forms, see Appendix C.

The type of form used to define a classical polar space dictates how many points the space contains. We explicitly state the number of points in types of classical polar spaces in Table 2.1 below. More explicit proofs of these results may be found in [35].

Let us now examine the classical polar spaces over $\mathrm{GF}(q)$ in depth.

Classical Polar Space	Number of Points
$Q^+(2n-1,q)$	$(q^{n-1}+1)(q^n-1)/(q-1)$
$Q^-(2n+1,q)$	$(q^{n-1}+1)(q^n-1)/(q-1)$
$Q(2n,q)$	$(q^{2n-1})/(q-1)$
$W(2n-1,q)$	$(q^{2n}-1)/(q-1)$
$H(2n,q^2)$	$(q^{2n}-1)(q^{2n+1}+1)/(q^2-1)$
$H(2n-1,q^2)$	$(q^{2n}-1)(q^{2n+1}+1)/(q^2-1)$

Table 2.1: The number of points in classical polar spaces

2.4.1 Symplectic spaces A *symplectic polar space*, or symplectic space is the set of totally isotropic subspaces of a vector space $V(n+1,q)$, the underlying vector space of $\mathrm{PG}(n,q)$ with respect to an alternating form. We denote a symplectic space by $\mathrm{W}(n,q)$, as in Example 2.11. A nondegenerate symplectic form, and therefore a symplectic space, only exists on $V(n+1,q)$ if n is odd because there exists a totally isotropic subspace of dimension $\frac{n+1}{2}$ with respect to the form. When $n=3$, the resulting symplectic space $\mathrm{W}(3,q)$ is a generalised quadrangle of order (q,q) and therefore has $(q+1)(q^2+1)$ points and the same number of lines [48]. The smallest non-trivial example of a symplectic space for $n=3$ is the doily.

2.4.2 Hermitian spaces A *Hermitian polar space*, or Hermitian space, of $\mathrm{PG}(n,q^2)$, denoted $\mathrm{H}(n,q^2)$ is the set of totally isotropic points of a Hermitian form over the vector space $V(n+1,q^2)$. By the definition of a Hermitian form, we require an involutary automorphism. This only exists when the order of the field is a square, and the unique involutory field automorphism of $\mathrm{GF}(q^2)$ is $x \mapsto x^q$.

Consequently, the points of a Hermitian space satisfy an equation of the form $\sum_{i,j=0}^{n} b_{ij}x_i x_j^q$, with some of the b_{ij} coefficients nonzero and $b_{ij}^q = b_{ji}$ for all values of $i,j \in \{0,1,\ldots n\}$. The latter condition ensures that the form obeys the property $\beta(x,y) = \beta(y,x)^q$, which is required for a Hermitian form. Furthermore, if n is even, there is an $\frac{n}{2}$-dimensional totally isotropic subspace of $V(n+1,q^2)$ with respect to the Hermitian form. If n is odd, then there exists an $\frac{n+1}{2}$-dimensional totally isotropic subspace [26]. When $n=3$, the resulting Hermitian space $\mathrm{H}(3,q^2)$ is isomorphic to a generalised quadrangle of order (q^2,q) and therefore has $(q^2+1)(q^3+1)$ points and $(q+1)(q^3+1)$ lines [48].

2.4.3 Quadrics A *quadric* in a projective space $\mathrm{PG}(n,q)$ is the set of totally singular subspaces of the underlying vector space with respect to a quadratic form. Suppose Q is a nondegenerate quadratic form on the $(n+1)$-dimensional vector space over $\mathrm{GF}(q)$, $V(n+1,q)$. If n is even, then we can choose a suitable basis of $V(n+1,q)$ such that Q can be expressed as $Q(x_0,x_2,\ldots x_n) = x_0^2 + x_1x_2 + \ldots x_{n-1}x_n$. We say that the corresponding quadric is *parabolic*. On the other hand, if n is odd, then by a suitable choice of basis for $V(n+1,q)$, we can write Q in one of two ways – either as $Q(x_0,x_2,\ldots x_n) = x_0x_1 + \ldots x_{n-1}x_n$, or $Q(x_0,x_2,\ldots x_n) =$

$x_0x_1 + \ldots x_{n-3}x_{n-2} + f(x_{n-1}x_n)$, where f is an irreducible homogeneous degree two polynomial over GF(q). In the former case, the corresponding quadric is called *hyperbolic*, and in the latter case, *elliptic* [26].

A nondegenerate quadric in PG$(2, q)$ has $q + 1$ points and is called a *conic*. In fields of even characteristic, all tangent lines[8] to a conic meet in a single point, called the *nucleus* of the conic [14, p. 121]. In this dissertation, we will predominantly be working in PG$(3, q^2)$ and so only hyperbolic and elliptic quadrics are of interest to us. We denote a hyperbolic quadric by $\mathrm{Q}^+(n, q)$, and an elliptic quadric by $\mathrm{Q}^-(n, q)$.Notice that we only used nondegenerate forms when constructing quadrics. If we instead use a degenerate form, we do not create a quadric, rather, we create a *cone* [36].

Let PG(n, q) be a projective space, and suppose U and V are two subspaces of PG(n, q). Then we say that U and V are *skew* if they do not intersect. Furthermore, if $\mathscr{R}$ is a set of pairwise skew subspaces of PG(n, q), a line $\ell \in$ PG(n, q) is said to be a *transversal* of $\mathscr{R}$ if ℓ intersects every subspace in $\mathscr{R}$ in a single point.

Proposition 2.20. *Suppose ℓ and m are two skew lines of* PG$(3, q)$ *and let P be a point that is not incident with ℓ or m. Then there exists a single line n through P that intersects each of ℓ and m in a point.*

Proof. Existence: Let α be the plane that is generated by P and ℓ. Now, since we are working in PG$(3, q)$, α meets m in a point Q. Now, the lines ℓ and $n := PQ$ are contained in α and so they meet in a point R.
Uniqueness: Suppose there are two distinct lines ℓ_1 and ℓ_2 incident with P that intersect each of ℓ and m in a point. Then the plane β spanned by ℓ_1 and ℓ_2 contains both ℓ and m, which contradicts our initial assertion that they are skew lines. □

This proposition leads to a direct corollary which builds on the properties of transversals.

Corollary 2.21. *Let $\mathscr{L}$ be a set of three pairwise skew lines in* PG$(3, q)$ *and let $\mathscr{T}$ be the set of transversals on $\mathscr{L}$. Then,*

1. *Any two lines of $\mathscr{T}$ are skew,*
2. *Any point on a line contained in $\mathscr{L}$ is incident with exactly one transversal,*
3. *The lines in $\mathscr{L}$ are transversals of $\mathscr{T}$.*

We may now define reguli on PG$(3, q)$, a concept integral to our study of hemisystems and relative hemisystems in future chapters.

[8] i.e., points that meet the conic in one point.

Definition 2.22. Suppose $\mathscr{R}$ is a set of pairwise skew lines in $\mathrm{PG}(3,q)$. We say that $\mathscr{R}$ is a *regulus* if it satisfies the following conditions.

1. Each point incident with a line of $\mathscr{R}$ is also incident with a transversal of $\mathscr{R}$.
2. Each point on a transversal of $\mathscr{R}$ is incident with a line of $\mathscr{R}$.

The set of transversals $\mathscr{T}$ of $\mathscr{R}$ also forms a regulus, called the *opposite regulus*[9] of $\mathscr{R}$.

We now have the following theorem which aids in the visualisation of reguli.

Theorem 2.23. *Suppose $\mathscr{R}$ is a regulus of $\mathrm{PG}(3,q)$ with opposite regulus $\mathscr{T}$, and let S be the set of points on the lines of $\mathscr{R}$. Then,*

i) Each line $\ell \in \mathrm{PG}(3,q)$ intersects the regulus in up to two points, or is contained in S,

ii) A line is in S if and only if it is in $\mathscr{R} \cup \mathscr{T}$,

iii) Every point of S is incident with exactly one line of $\mathscr{R}$ and one line of $\mathscr{T}$

Proof. i) and ii): Suppose that $\ell \in \mathrm{PG}(3,q)$ intersects S in at least three points. Then, ℓ either meets three lines $m_1, m_2, m_3 \in \mathscr{R}$ in a point or is completely contained in $\mathscr{R}$. If it is the latter case, then the statement is proven. So suppose we have the former case. Let P be intersection of ℓ and m_1. By Corollary 2.21, ℓ must be the unique transversal of m_1, m_2 and m_3 through P. So ℓ is a transversal of $\mathscr{R}$ through P and so by the definition of a regulus, $\ell \in \mathscr{R}$.
iii): Since $\mathscr{R}$ and $\mathscr{T}$ are composed of pairwise skew lines, every point of S must be incident with one line of $\mathscr{R}$ and one line of $\mathscr{T}$. □

We can construct a hyperbolic quadric on $\mathrm{PG}(3,q^2)$ by using the Segre product of points to generate reguli. The Segre product[10] takes points $P = (x_1, x_2)$ and $Q = (y_1, y_2)$ in $\mathrm{PG}(1,q)$, to $(x_1y_1, x_1y_2, x_2y_1, x_2y_2)$. We fix the point P and let Q vary over all possible points in $\mathrm{PG}(1,q)$. This generates a line in the Segre product, and by fixing P on each point in $\mathrm{PG}(1,q)$ and then varying over all possible points Q, we generate a set of lines that form a regulus in $\mathrm{PG}(3,q^2)$. The opposite regulus is obtained by instead fixing Q at each point of $\mathrm{PG}(1,q)$ and letting P vary over all possible points. This implies that the points of the hyperbolic quadric are all points for the form $(x_1y_1, x_1y_2, x_2y_1, x_2y_2)$, where $x_1, x_2, y_1, y_2 \in \mathrm{GF}(q^2)$. Consider the form $Q(z_1, z_2, z_3, z_4) = z_1z_4 - z_2z_3$. Substituting the points of the hyperbolic quadric formed from the Segre product, we have $Q(x_1y_1, x_1y_2, x_2y_1, x_2y_2) =$

[9] See [58, p. 199].
[10] Named after Corrado Segre. See [36].

$x_1y_1x_2y_2 - x_1y_2x_2y_1 = 0$. Therefore, the points of the hyperbolic quadric are totally singular points of $Q(z_1, z_2, z_3, z_4)$. Further, there are $\frac{q^4-1}{q^2-1} = q^2+1$ points in $\mathrm{PG}(1, q)$ and therefore $(q^2 + 1)^2$ points in the Segre product. This is the exact number of points in a hyperbolic quadric on $\mathrm{PG}(3, q^2)$. Therefore, $Q(z_1, z_2, z_3, z_4) = z_1z_4 - z_2z_3$ is the defining equation for the hyperbolic quadric formed from the Segre product. Recalling that we can represent lines in a projective space as the span of two points, and therefore the rowspace of a $2 \times (n + 1)$ matrix, the reguli of this hyperbolic quadric are as follows:

$$\mathscr{R}_1 = \{\left[\begin{smallmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & \lambda \end{smallmatrix}\right] \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{\left[\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]\}$$

and

$$\mathscr{R}_2 = \{\left[\begin{smallmatrix} 1 & \lambda & 0 & 0 \\ 0 & 0 & 1 & \lambda \end{smallmatrix}\right] \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{\left[\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]\}$$

We will call this hyperbolic quadric the *canonical hyperbolic quadric* and use it to find the reguli of other quadrics using a change of basis.

As discussed in Appendix C, we can use a Gram matrix to represent a quadratic or reflexive sesquilinear form. Suppose A_1 and A_2 are the Gram matrices for hyperbolic quadrics Q_1^+ and Q_2^+ respectively. If we can find a matrix B such that $BA_2B^\top = A_1$, then we call B the *change of basis matrix* from Q_2^+ to Q_1^+. We may use the change of basis matrix B to find the reguli of Q_2^+ from the reguli of Q_1^+. Notice that for all lines $\ell \in \mathrm{PG}(3, q^2)$, $\ell BA_2B^\top\ell^\top = \ell A_1\ell^\top$ is equal to zero if and only if $\ell \in Q_1^+$, i.e., ℓ is contained in one of the reguli of Q_1^+. Since matrix multiplication is associative, $\ell BA_2B^\top\ell^\top = (\ell B)A_2(\ell B)^\top$. Therefore, ℓB is totally singular in Q_2^+ if and only if ℓ is totally singular in Q_1^+. Therefore, we can find the reguli of Q_2^+ by simply finding the images of the reguli of Q_1^+ under the change of basis matrix from Q_2^+ to Q_1^+. This technique will be used in Chapter 5. We now revisit Theorem 2.18. From a finite polar space perspective, we can produce polarities using the associated form. The classical polar spaces are constructed by taking all of the totally singular subspaces of an $(n + 1)$-dimensional vector space, where $n \geq 3$, over a field $\mathbb{F}$ with respect to a reflexive σ-sesquilinear or quadratic form, together with the natural incidence relation. For a quadratic form Q, let f be the associated symmetric bilinear form, and for a σ-sesquilinear form g, let $f = g$. Then, if W is a subspace of a vector space $V(n + 1, q)$, we define

$$W^\perp = \{v \in V \mid \forall w \in W : f(v, w) = 0\}$$

Now, viewing W as a set of subspaces of $\mathrm{PG}(n, q)$, the map $\perp$ that takes W to $W^\perp$ is a polarity. The subspaces of a polar space are exactly those that satisfy $W \subseteq W^\perp$.

If $n = 2$, then the totally isotropic subspaces with respect to the form create a generalised quadrangle . We may therefore think of polar spaces as substructures of $\mathrm{PG}(n, q)$. Tits showed in [57] that classical polar spaces are the only finite polar spaces with rank at least three. Note that this is not the case when we consider infinite polar spaces.

Group Theory

> "It has long been an axiom of mine that the little things are infinitely the most important."
>
> Arthur Conan Doyle, *The Memoirs of Sherlock Holmes*

In this chapter, we explore group actions and how they may be used to describe polar spaces and other geometric structures defined in Chapter 2. For a background of basic group theory, see Appendix B.

3.1 Group actions

Definition 3.1. A *group action* of a group G on a set Ω is a function $G \times \Omega \to \Omega$ defined by $(g, \omega) \mapsto \omega^g$ satisfying the following two properties.

i) $(\omega^{g_1})^{g_2} = \omega^{(g_1 g_2)}$ for all $\omega \in \Omega$ and $g_1, g_2 \in G$.

ii) $\omega^e = \omega$, for all $\omega \in \Omega$ and where e is the identity of G.

We say that a group action is *faithful* if it is injective. When we have a group action of a group G on a set Ω, we say that "G acts on Ω", and similarly for elements of Ω.

Example 3.2. *A group G acting on itself by right multiplication is a group action with trivial kernel, since for $g, h, h' \in G$, $gh = gh' \Rightarrow h = h'$.*

Another very natural group action is given by the rotational and reflectional symmetries of a regular n sided polygon. The corresponding group is called the dihedral group, denoted D_{2n}. It is generated by two elements – a rotation of $\frac{2\pi}{n}$ radians anticlockwise and a reflection along a fixed axis. The dihedral group acts on the vertices of the regular n-gon by permuting the vertices based on the rotation and/or reflection that is induced by the group element.

Definition 3.3. Suppose G is a group acting on a set Ω. Then the *orbit* of $\omega \in \Omega$ under G is the set $\omega^G = \{\omega^g \mid g \in G\}$.

We say a group action is *transitive* on a set if it only has one orbit. In other words, given two elements $\omega, \omega' \in \Omega$, there exists a $g \in G$ such that $\omega^g = \omega'$.

Definition 3.4. Suppose G is a group acting on a set Ω. The *stabiliser* of an element ω of Ω is the set $G_\omega = \{g \in G \mid \omega^g = \omega\}$.

If we stabilise a subset of elements S in Ω individually, we say that we have *pointwise stabilised* S in G. The *pointwise stabiliser* of S, that is, the subset of G that pointwise stabilises S, is the intersection of all of the stabilisers of elements of S. On the other hand, the *setwise stabiliser* of S in G is the set of elements of G that stabilise the elements of S up to permutation. For clarity, if S is pointwise stabilised in G, we write $G_{(S)}$, and if S is setwise stabilised, we simply write G_S. We say that a group G acts *fixed point freely* on S if none of the elements of S are fixed under the action of G.

Proposition 3.5. *Suppose G is a group acting on a set Ω. The stabilisers G_S and $G_{(S)}$ are both subgroups of G.*

Proof. Suppose $g, h \in G_S$. Then $S^g = S$ and $S^h = S$. So for all $x \in S$, there exist $y, z \in S$ such that $y^g = x$ and $z^h = x$. Therefore, $y^{gh^{-1}} = (y^g)^{h^{-1}} = (x)^{h^{-1}} = (z^h)^{h^{-1}} = z \in S$. Therefore, by Proposition B.6, the setwise stabiliser G_S is a subgroup of G. An analogous argument shows that $G_{(S)}$ is a subgroup of G as well. □

We now state one of the most powerful theorems in group theory, which ties together the concepts of orbits and stabilisers.

Theorem 3.6 (Orbit-Stabiliser Theorem)**.** *Suppose G is a group acting on a set Ω. Then for $\omega \in \Omega$, $|G| = |G_\omega||\omega^G|$.*

Proof. Define the function $f : \omega^g \mapsto G_\omega g$ for $g \in G$. We first show that this function is well-defined. Suppose $\omega^g = \omega^h$ for some $g, h \in G$. Then $\omega^{gh^{-1}} = \omega^{hh^{-1}} = \omega^e = \omega$. So $gh^{-1} \in G_\omega$ and $G_\omega g = G_\omega h$. Therefore, f is well-defined. It is onto because the preimage of any coset $G_\omega g$ contains ω^g. Suppose $f(\omega^g) = f(\omega^h)$ for some $g, h \in G$. Then $G_\omega g = G_\omega h$ and by the converse argument used to show f is well-defined above, $\omega^g = \omega^h$. Therefore, f is a bijection and so $|\omega^G| = |G|/|G_\omega|$. □

3.2 Permutation groups

Permutation groups give us a way of considering a group G that acts on a set Ω as a collection of permutations on Ω.

A *permutation group* is a set of permutations of a set Ω, which forms a group under function composition. All permutations on n elements can be written as the product of transpositions [29]. If a permutation can be written as an odd number of permutations, we call it an *odd permutation* and similarly, an *even permutation* is a permutation that can be written as a product of an even number of transpositions. This distinction is well defined, i.e., a permutation cannot be written as both an even and an odd number of transpositions [29]. We call the group consisting of all of the permutations of n elements the *symmetric group on n elements*, denoted

S_n, or $\mathrm{Sym}(\Omega)$ if we are considering the permutations of a particular set Ω with n elements. The order of the symmetric group on n elements is $n!$, because there are $n!$ ways to permute the elements. Also notice that we may generate the symmetric group by transpositions, since every permutation may be written as the product of transpositions.

The set of all even permutations in S_n forms a group called the *alternating group*, denoted A_n. The alternating group has index two in the symmetric group, and therefore has order $n!/2$. For example, the dihedral group D_{2n} can be viewed as a set of permutations of the vertices of a regular n-gon.

Notice that if we have a group G acting on a set Ω faithfully, then G is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$ because G permutes the elements of Ω. We now state the following theorem, which relates to a group acting on itself.

Theorem 3.7 (Cayley's Theorem)**.** *Every group G is isomorphic to a subgroup of the symmetric group* $\mathrm{Sym}(G)$.

Proof. By Example 3.2, G acts by right multiplication on itself, and it acts faithfully. Therefore, each element g of G can be regarded as a permutation φ_g of G. We can define the map $\phi : G \to \mathrm{Sym}(G)$ by $g \mapsto \varphi_g$. This is a homomorphism because for $g, h \in G$, $\phi(gh) = \varphi_{gh} = \varphi_g\varphi_h = \phi(g)\phi(h)$. The kernel of ϕ is exactly $\{e_G\}$ because it is the only element which fixes every element of G. Therefore, ϕ is injective and by the First Isomorphism Theorem, $G \cong \phi(G) \leq \mathrm{Sym}(G)$. □

Definition 3.8. Suppose G and H are groups which act on sets Ω and Δ respectively. We say that G and H are *permutation isomorphic* if there is an isomorphism $\varphi : G \to H$ and a bijective function from $f : \Omega \to \Delta$ such that

$$f(\omega^g) = f(\omega)^{\varphi(g)}$$

for all $\omega \in \Omega$ and $g \in G$.

Example 3.9. *Consider a group G acting on itself by right multiplication, and by left inverse multiplication. Now, the identity map on G is an isomorphism, and let us define a bijection $f : G \to G$ by $f(g) = g^{-1}$ for all $g \in G$. Now, for $g, h \in G$, $f(g^h) = f(gh) = h^{-1}g^{-1} = f(g)^{\varphi(h)}$. So the two actions are permutation isomorphic.*

The following example relates to the construction of reguli from the points of a projective line $\mathrm{PG}(1, q)$, introduced in Section 2.4.3.

Example 3.10. *The group* $\mathrm{PSL}(2, q)$ *acts on a projective line* $\mathrm{PG}(1, q)$ *by permuting the points on the line. Recall from Section 2.4.3 that we can construct a regulus $\mathscr{R}$ from* $\mathrm{PG}(1, q)$ *by taking the Segre product with another projective line and varying over the points on that line. We can therefore define a bijection $\varphi : \mathrm{PG}(1, q) \to \mathscr{R}$ by matching each point $P \in \mathrm{PG}(1, q)$ with its corresponding line in the regulus ℓ_P. Define an action of* $\mathrm{PSL}(2, q)$ *on $\mathscr{R}$ by $(\ell_P)^g = \ell_{P^g}$, for all $P \in \mathrm{PG}(1, q)$ and*

$g \in \mathrm{PSL}(2,q)$. Since $\mathrm{PSL}(2,q)$ is isomorphic to itself, the action of $\mathrm{PSL}(2,q)$ on $\mathrm{PG}(1,q)$ is permutation isomorphic to the action of $\mathrm{PSL}(2,q)$ on the lines of the regulus $\mathscr{R}$.

This permutation isomorphism will prove useful later in Chapter 5.

3.3 Group extensions and semidirect products

Group extensions are used to describe groups in terms of a normal subgroup and a quotient group. They will prove useful later in Chapters 4 and 5, when we are describing the stabilisers of hemisystems.

Suppose $N \trianglelefteq G$ and let $H = G/N$. Then, we can write $G = N.H$ and we say that G is an *extension* of H by N.

For example, the alternating group A_n is a normal subgroup of S_n. The quotient group S_n/A_n is of order two and is therefore the cyclic group C_2. So, we may write S_n as an extension of C_2 by A_n by having $S_n = A_n.C_2$. When we have a cyclic group as an element of the extension, we usually write the order of the cyclic group instead and so $S_n = A_n.2$.

Let N and H be groups, and let $\phi : H \to \mathrm{Aut}(N)$ be a homomorphism. We say that G is the *semidirect product* of N and H, denoted $G = N \rtimes_\phi H$ if $N \trianglelefteq G$ and $H \leq G$ such that $N \cap H = \{e_G\}$. We define multiplication in G by $(n_1, h_1)\cdot(n_2, h_2) = (n_1 n_2^{\phi(h_1)}, h_1 h_2)$, where $n_1, n_2 \in N$ and $h_1, h_2 \in H$, and where $\phi(h_1)$ acts on n_2 by conjugation. For example, S_n is the semidirect product of A_n and $C_2 = \langle a \rangle$, where $\phi(a)$ is a transposition. We will use semidirect products in Chapter 4 to describe the collineation groups of hemisystems and relative hemisystems.

3.4 Classical groups

Classical groups are fundamental in our understanding of the action of groups on geometric objects in later chapters. All of the families of classical groups apart from the linear groups arise from the σ-sesquilinear and quadratic forms described in Appendix C. It is therefore not surprising that there are such strong connections between classical groups and finite classical polar spaces. For further reading about classical groups, see Wilson [69].

Let f be a reflexive sesquilinear on a vector space V and let W be a vector space. An *isometry* of f is a linear transformation $g : V \to W$ such that $f(u^g, v^g) = f(u, v)$ for all $u, v \in V$. In other words, an isometry is form preserving. Similarly, an isometry of a quadratic form Q is a linear transformation $g' : V \to W$ such that $Q(u^{g'}) = Q(u)$ for all $u \in V$. The collection of isometries with respect to a form f equipped with composition forms a group. We call this the *isometry group* of f.

3.4.1 The linear groups A *linear transformation* is a map $f : V \to W$ between vector spaces V and W which preserves vector addition and scalar multiplication. Linear transformations can be represented by matrices, and conversely, every matrix gives rise to a linear transformation.

Let V be an n-dimensional vector space over the finite field $\mathrm{GF}(q)$. The *general linear group* $\mathrm{GL}(n, q)$ is the set of invertible linear transformations from V to itself. In other words, it is the set of invertible $n \times n$ matrices over $\mathrm{GF}(q)$. The centre $Z(\mathrm{GL}(n, q))$ of the general linear group is the set of nonzero scalar multiples of the identity matrix λI_n, $\lambda \in \mathrm{GF}(q) \setminus \{0\}$. Since the centre of a group is a normal subgroup, we take the quotient group $\mathrm{GL}(n, q)/Z(\mathrm{GL}(n, q))$, which we call the *projective general linear group*, denoted $\mathrm{PGL}(n, q)$. Now, the determinant function on $n \times n$ matrices satisfies $\det(AB) = \det(A)\det(B)$ so it is a group homomorphism between $\mathrm{GL}(n, q)$ and $\mathrm{GF}(q)$. Then, from Proposition B.15, the kernel of the determinant function, that is, the set of matrices with determinant 1, is a normal subgroup of $\mathrm{GL}(n, q)$. This kernel is called the *special linear group*, denoted $\mathrm{SL}(n, q)$. Similarly to the general linear group, we can quotient $\mathrm{SL}(n, q)$ by its centre (which is composed of only scalars that are roots of unity) to give us the *projective special linear group*, denoted $\mathrm{PSL}(n, q)$. We can form another group by taking the semidirect product of $\mathrm{GL}(n, q)$ with the group of field automorphisms of $\mathrm{GF}(q)$, and we denote this group $\Gamma\mathrm{L}(n, q)$. For further details on the construction of $\Gamma\mathrm{L}(n, q)$, see [40]. Similarly, we can construct $\mathrm{P}\Gamma\mathrm{L}(n, q)$ from $\mathrm{PGL}(n, q)$.

3.4.2 The symplectic groups The *symplectic group*, denoted $\mathrm{Sp}(2m, q)$ is the isometry group of a nonsingular alternating bilinear form on a $2m$-dimensional vector space over $\mathrm{GF}(q)$. Since the symplectic group arises from an alternating bilinear form f, we have $f(\lambda u, \lambda v) = \lambda^2 f(u, v)$. This equals $f(u, v)$ if and only if $\lambda = \pm 1$. Therefore, these are the only scalars in $\mathrm{Sp}(2m, q)$. Similar to the linear groups, we define the *projective symplectic group* $\mathrm{PSp}(2m, q)$ as $\mathrm{Sp}(2m, q)$ factored by its centre, which is the set of scalars of $\mathrm{Sp}(2m, q)$. We denote the semidirect product of $\mathrm{Sp}(2m, q)$ or $\mathrm{PSp}(2m, q)$ with the group of field automorphisms on $\mathrm{GF}(q)$ by $\Gamma\mathrm{Sp}(2m, q)$ or $\mathrm{P}\Gamma\mathrm{Sp}(2m, q)$ respectively.

3.4.3 The unitary groups The *general unitary group* is defined in a similar way to the symplectic group – it is the isometry group of a nonsingular Hermitian form f defined on a vector space V. In other words, it is the subgroup of $\mathrm{GL}(n, q^2)$ that contains the elements g satisfying $f(u^g, v^g) = f(u, v)$ for all $u, v \in V$.

By considering the Gram matrix[1] of f, we can also alternatively define the unitary group as the group of unitary matrices[2] over $\mathrm{GF}(q)$. It is easy to see that this is a subgroup of the general linear group $\mathrm{GL}(n, q)$. The subset of these matrices that have determinant 1 is a subgroup called the *special unitary group*, denoted $\mathrm{SU}(n, q)$. The *projective general unitary group* $\mathrm{PGU}(n, q)$ is obtained by factoring $\mathrm{GU}(n, q)$ by

[1] See Appendix C.

[2] Matrices whose inverse is their conjugate transpose.

its centre has index $q+1$ in $\mathrm{GU}(n,q)$ [69]. Similarly, the *projective special unitary group*, denoted $\mathrm{PSU}(n,q)$, is obtained by factoring the special unitary group by its centre. We define $\mathrm{P\Gamma U}(n,q)$ analogously to the linear and symplectic cases.

3.4.4 The orthogonal groups The remaining class of σ-sesquilinear forms is the symmetric examples. This family proves more complicated to consider because the resulting groups vary based on the characteristic of the field the form is defined over.

Let f be a nondegenerate quadratic form on an m-dimensional vector space V over $\mathrm{GF}(q)$. The *orthogonal group* $\mathrm{O}(V,f)$ is the group of linear maps g which satisfy $f(u^g) = f(u)$ for all $u \in V$.

Recall from Appendix C that if the characteristic of the field is odd, we may construct a symmetric bilinear form β_f from the quadratic form f. Note that all linear maps which preserve the quadratic form must preserve the corresponding bilinear form, and so we may equivalently define the orthogonal group as being the set of linear maps that preserve a symmetric bilinear form.

Alternatively, if B is a Gram matrix for β_f with respect to some basis of V, we may consider the orthogonal group as the set of $m \times m$ invertible matrices A which satisfy $A^\top BA = B$. This implies that all of the matrices in the orthogonal group have determinant ± 1, and that the orthogonal group is a subgroup of the general linear group $\mathrm{GL}(n,q)$.

Recall from Example C.4 that when V is even dimensional, there are two equivalence classes of symmetric bilinear forms – plus and minus type. Each of these gives rise to an orthogonal group – *plus type*, denoted $\mathrm{O}^+(2n,q)$, and *minus type* denoted $\mathrm{O}^-(2n,q)$. The groups corresponding to forms of the same type are isomorphic, so we only need denote the dimension and field order and not the form [69]. On the other hand, if V is odd dimensional, then there is one orthogonal group $\mathrm{O}(2n+1,q)$.

Now, let us consider the case where $\mathrm{GF}(q)$ has characteristic 2. When the dimension of V is odd (i.e., $2n+1$), the corresponding orthogonal group is isomorphic to the symplectic group $\mathrm{Sp}(2m,q)$, because in even characteristic, symmetric forms are also alternating [69]. Therefore, we only have orthogonal groups on vector spaces over fields with characteristic two when the dimension is even.

We describe some groups arising from orthogonal groups. For simplicity, we omit the plus and minus superscripts, and replace them with an ϵ, which denotes any of plus type, minus type, or odd dimensional orthogonal groups.. The subgroup of the orthogonal group $\mathrm{O}^\epsilon(n,q)$ containing only matrices with determinant $+1$ is called the *special orthogonal group*, denoted $\mathrm{SO}^\epsilon(n,q)$. Notice that when the chararacteristic of the field is two, $-1 = +1$ and therefore $\mathrm{SO}^\epsilon(n,2^k)$ is identical to $\mathrm{O}^\epsilon(n,2^k)$. Quotienting an orthogonal group $\mathrm{O}^\epsilon(n,q)$ by its centre gives us the *projective orthogonal group* $\mathrm{PO}^\epsilon(n,q)$. Similarly, factoring a special orthogonal group

by its centre results in the *projective special orthogonal group*, denoted $\mathrm{PSO}^\epsilon(n,q)$. The derived subgroup of the orthogonal group $\mathrm{O}^\epsilon(n,q)$ is denoted by $\Omega^\epsilon(n,q)$, and the group obtained by factoring by its centre is denoted $\mathrm{P}\Omega^\epsilon(n,q)$. As before, we denote the semidirect product of an orthogonal group with the set of automorphisms in $\mathrm{GF}(q)$ by $\Gamma\mathrm{O}^\epsilon(n,q)$, and the projective version by $\mathrm{P}\Gamma\mathrm{O}^\epsilon(n,q)$.

3.5 Group theory meets geometry

In this section, we explore the interplay between group theory and finite geometry, and build on the ideas briefly discussed in Chapter 2. One of the first mathematicians to explore this relationship in earnest was Felix Klein, in the publication of his Erlangen program manifesto in 1872 [41]. At the time, many models of non-Euclidean geometry had emerged, and it was unclear how these models related to each other. Klein proposed that group theory should be used to describe them through group actions on elements of these geometries. The starting point for this analysis is the identification of the group of collineations of a projective space with a classical group.

3.5.1 Collineation groups of polar spaces

Theorem 3.11 (Fundamental Theorem of Projective Geometry)**.** *The collineation group of* $\mathrm{PG}(n,q)$ *is isomorphic to* $\mathrm{P}\Gamma\mathrm{L}(n,q)$ *for* $n \geq 3$.

A proof of the Fundamental Theorem of Projective Geometry may be found in [28]. Therefore, we may describe a subspace of a projective space by stating the set of collineations that setwise stabilise it, which is isomorphic to a subgroup of $\mathrm{P}\Gamma\mathrm{L}(n,q)$. In particular, due to the dependence of both classical groups and classical polar spaces on σ-sesquilinear and quadratic forms, we find that the subgroups of $\mathrm{P}\Gamma\mathrm{L}(n,q)$ which stabilise classical polar spaces in $\mathrm{PG}(n,q)$ are classical groups. The classical polar spaces and their stabilisers are shown in Table 3.1.

Classical Polar Space	Collineation Group
$Q^+(2n-1,q)$	$\mathrm{P}\Gamma\mathrm{O}^+(2n,q)$
$Q^-(2n+1,q)$	$\mathrm{P}\Gamma\mathrm{O}^+(2n+2,q)$
$Q(2n,q)$	$\mathrm{P}\Gamma\mathrm{O}(2n+1,q)$
$W(2n-1,q)$	$\mathrm{P}\Gamma\mathrm{Sp}(2n,q)$
$H(n,q^2)$	$\mathrm{P}\Gamma\mathrm{U}(n+1,q^2)$

Table 3.1: The collineation groups of the classical polar spaces.

We very quickly find that it is much easier and much more concise to give a description of an arbitrary geometric object by the group that stabilises it, rather than attempting to list its subspaces.

3.5.2 Embeddings Much of our work on relative hemisystems relies on having a way to view classical polar spaces as subgeometries within a projective space. In order to reconcile the concepts of polar and projective spaces, we use embeddings.

Definition 3.12. Suppose S and T are projective spaces. An *embedding* of S in T is an injective, incidence preserving map $\phi : S \to T$ which maps lines to lines. We say that S is *embedded* in T, and denote it by $S \hookrightarrow T$.

Theorem 3.13 ([14] pg. 668)**.** *A finite polar space of rank at least 3 arises from a vector space equipped with a bilinear, Hermitian, or quadratic form, and therefore has an embedding into a projective space.*

In particular, Theorem 3.13 shows that we can embed Hermitian spaces and symplectic spaces into $\mathrm{PG}(3, q^2)$, which is exactly what we need in order to describe relative hemisystems. Suppose we have embedded a Hermitian space $\mathrm{H}(3, q^2)$, q even, in a projective space $\mathrm{PG}(3, q^2)$ by taking the totally isotropic subspaces under the form $x_1^{q+1} + x_2^{q+1} + x_3^{q+1} + x_4^{q+1} = 0$. The set of points $W = \{(x, x^q, y, y^q) \mid x, y \in \mathrm{GF}(q^2)\}$ are the points of a symplectic subgeometry $\mathrm{W}(3, q)$ embedded in $\mathrm{H}(3, q^2)$ [21]. This means that the collineation group of $\mathrm{W}(3, q)$, $\mathrm{P\Gamma Sp}(4, q)$, is a subgroup of $\mathrm{P\Gamma U}(4, q^2)$, which is the collineation group of $\mathrm{H}(3, q^2)$. In the same way, by Theorem 3.13, the collineation group of any polar space with rank $n \geq 3$ is a subgroup of $\mathrm{P\Gamma L}(n, q)$, the collineation group of the projective space $\mathrm{PG}(n, q)$ that it is embedded in.

Now that we are able to embed polar spaces in projective spaces, we can examine how they interact and intersect. The following proposition in particular will prove extremely useful in our study of relative hemisystems.

Proposition 3.14 (Aguglia and Giuzzi, [1])**.** *Suppose q is even and let $\mathrm{H}(3, q^2)$ be a Hermitian space and $\mathcal{Q}^+$ an irreducible hyperbolic quadric of $\mathrm{PG}(3, q^2)$ that share the same tangent plane to some non-singular point P. Then the intersection of $\mathcal{Q}^+$ and $\mathrm{H}(3, q^2)$ has size $q^2 + 1$ and is an elliptic quadric $Q^-(3, q)$.*

Hemisystems and Relative Hemisystems

"Prove, disprove or salvage."

Arnold Ross

We now introduce the main topics of this dissertation: hemisystems and relative hemisystems. The motivation for Beniamino Segre's definition of hemisystems in 1965 stemmed from the generalisation of spreads of Hermitian spaces [51].

A *spread* of an incidence structure is a set of lines L such that every point lies on exactly one line of L.

Example 4.1. *The symplectic space* $\mathrm{W}(3,2)$*, nicknamed the 'doily', contains a spread. Here, it is highlighted in red. Notice that all fifteen points in this structure lie on exactly one of the red lines.*

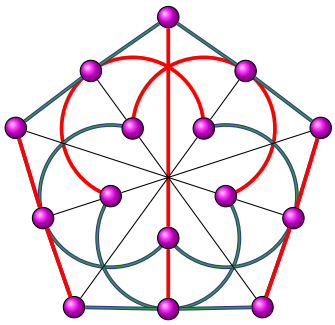


Figure 4.1: A spread of the symplectic space $\mathrm{W}(3,2)$.

In his epic treatise on Hermitian spaces, Segre [51] generalised the idea of a spread to a regular system of order m.

A *regular system of order* m of a Hermitian space $\mathrm{H}(3,q^2)$ is a set of lines such that each point of the Hermitian space lies on exactly m lines of the set. We place the restriction $0 < m < q+1$ on m to eliminate the trivial cases. Note that the Hermitian space $\mathrm{H}(3,q^2)$ is a generalised quadrangle of order (q^2,q).

Segre went on to explore what sorts of regular systems are possible in $\mathrm{H}(3,q^2)$ for different values of q and found that for q odd, the only regular system was of order $m = (q+1)/2$. In order to prove this, we require some facts about partial quadrangles, which will be covered later in this chapter. The $(q+1)/2$ case was of great interest to Segre. Since $(q+1)/2$ is exactly half the lines incident with a point in $\mathrm{H}(3,q^2)$, Segre called this regular system of order $(q+1)/2$ a *hemisystem*.

Definition 4.2. A *hemisystem* on the Hermitian space $\mathrm{H}(3,q^2)$ is a set of lines $\mathcal{L}$ such that every point in $\mathrm{H}(3,q^2)$ is incident with $(q+1)/2$ lines of $\mathcal{L}$.

Segre constructed an example of a hemisystem on $\mathrm{H}(3,3^2)$, admitting $\mathrm{PSL}(3,4)$ as a setwise stabiliser and proved that this hemisystem is the unique hemisystem up to equivalence (collineations) on $\mathrm{H}(3,3^2)$ [51]. This was the sole example given of a hemisystem, and for many subsequent years, the search was on to find another example.

The next major development in regular systems and hemisystems was by Bruen and Hirschfeld in 1978 who showed that there are no regular systems on $\mathrm{H}(3, q^2)$, q even [13]. This theorem provided part of the motivation for the definition of relative hemisystems more than thirty years later. Also in 1978, Cameron, Goethals, and Seidel explored the dual idea of a hemisystem on generalised quadrangles of order (s, s^2) [18].

An *ovoid* of an incidence structure is a set of points O such that every line in the incidence structure is incident with exactly one point of O. This is the dual concept of a spread. Therefore, a *dual hemisystem* or *hemisystem of points* is a set of points $\mathcal{T}$ such that every line of the generalised quadrangle meets $\mathcal{T}$ in $(s+1)/2$ points, or half of its points. Cameron, Goethals, and Seidel provided a construction of Segre's hemisystem in this dual setting and proved that the collinearity graph of a dual hemisystem of a generalised quadrangle of order (s^2, s) is strongly regular. In 1981, Thas proved that every hemisystem on $\mathrm{H}(3, q^2)$ gives rise to a partial quadrangle [54] and therefore, by Cameron's paper [17], a strongly regular graph.

Despite these developments in the area of hemisystems, no examples of hemisystems different to Segre's were found for four decades following his original treatise. In fact, thirty years after Segre's original paper, Thas conjectured that there were no hemisystems on $\mathrm{H}(3, q^2)$ for $q > 3$ [55]. Interest waned in the subject because of the lack of new developments.

However, forty years after Segre's original treatise, Penttila and Cossidente constructed an infinite family of hemisystems for all $q \geq 3$, q odd, as well as a sporadic example [23]. The Penttila-Cossidente family of hemisystems admit $\mathrm{P}\Omega^-(4, q)$ as a setwise stabiliser for each odd prime power q, and the sporadic example admits $3.A_7.2$ as an automorphism group. Penttila and Cossidente also used the results of Cameron, Goethals and Seidel to reveal a new family of strongly regular graphs and examples of partial quadrangles with previously unknown parameters for both the infinite family and the sporadic example. Through finding these two different examples (as well as stating some found computationally), Penttila and Cossidente showed that there was no uniqueness result like that for the hemisystem on $\mathrm{H}(3, 9)$, which opened the door for more infinite families to be found.

Since Penttila and Cossidente's breakthrough, there have been more than a dozen papers published on the topic of hemisystems, revealing the existence of several more infinite families. In 2009, Penttila and Cossidente provided a new construction of Segre's original hemisystem and used this to give an alternate construction of McLaughlin's strongly regular graph on 275 vertices [24]. In the same year, Bamberg, De Clerck and Durante constructed a sporadic example of a hemisystem on the non-classical Fisher-Thas-Walker-Kantor generalised quadrangle of order $(5^2, 5)$ [3]. This example also gives rise to a previously unknown partial quadrangle, and allows a new construction of Penttila and Cossidente's family of hemisystems admitting $3.A_7.2$ as a setwise stabiliser. Penttila and Cossidente went further, constructing three infinite families in a single paper [25], making use of the theory of orthogonal polarities

commuting with unitary polarities. They also show how to procure hemisystems in $\mathrm{H}(n, q^2)$ using hemisystems in higher dimensions, and show that not all regular systems of $\mathrm{H}(n, q^2)$ are hemisystems if $n \neq 3$. Bamberg, Giudici, and Royle also proved that all of the known generalised quadrangles of order (s^2, s), s odd, called the *flock generalised quadrangles*, contain a hemisystem [4]. Note that there exist generalised quadrangles with parameters (q^2, q) that are not isomorphic to $\mathrm{H}(3, q^2)$ [48]. In 2011, Vanhove generalised the results of Cameron, Goethals, and Seidel to prove that distance regular graphs can be obtained from a $(q+1)/2$-ovoid of a regular near $2d$-gon of order (q, t) [62].

There is also a strong link between hemisystems and intriguing sets. A set of points $\mathcal{I}$ of a partial quadrangle $\mathcal{G}$ is said to be *intriguing* if there exist positive integers m, n such that every point $P \in \mathcal{I}$ is collinear with m points of $\mathcal{I}$ and every point $Q \notin \mathcal{I}$ is collinear with n points of $\mathcal{I}$ [5]. The intriguing set is said to be *negative* if $m - n$ is negative. Bamberg, Law and Penttila proved in [5] that every intriguing set of a generalised quadrangle is either an m-ovoid (the dual concept to a regular system of order m) or a tight set (see [47]). They also constructed an infinite family of hemisystems of points of $\mathrm{W}(3, q)$ using reguli of parabolic quadrics. Bamberg, De Clerck, and Durante subsequently proved in [3] that every negative intriguing set of a partial quadrangle gives rise to a hemisystem of points and in certain circumstances, the converse is true. They also prove some strong results about intriguing sets of partial quadrangles arising from hemisystems [3, Section 6].

In 2013, Martin, Muzychuk, and van Dam proved that in addition to a strongly regular graph and a partial quadrangle, every hemisystem on $\mathrm{H}(3, q^2)$ gives rise to a 4-class imprimitive cometric Q-antipodal association scheme [60]. We will explore these association schemes in more depth in the next section.

4.1 Structures that arise from hemisystems

Hemisystems are of particular interest to mathematicians from a variety of fields because, as mentioned earlier, they give rise to partial quadrangles, strongly regular graphs and association schemes [23].

4.1.1 Partial quadrangles Partial quadrangles were defined in Section 2.2.5. Thas was the first to prove in [53] that regular systems give rise to partial quadrangles. Since a hemisystem is a regular system of order $(q+1)/2$, it follows that we can construct a partial quadrangle from it.

Suppose K is a regular system of order m of $\mathrm{H}(3, q^2)$. Let ϕ be an isomorphism between $\mathrm{H}(3, q^2)$ and its dual $Q^-(5, q)$ which preserves incidence. Then $\phi(K)$ is a set of points of $Q^-(5, q)$ which meets every line of $Q^-(5, q)$ in m points. Define the incidence structure $S = (\mathcal{P}, \mathcal{L}, I)$ set out in the following table.

Theorem 4.3 ([53])**.** *$\mathcal{S} = (\mathcal{P}, \mathcal{L}, I)$ is a partial quadrangle with parameters $s = q - m$, $t = q^2$ and $\mu = q^2 + 1 - m(q+1)$.*

$\mathcal{P}$	$Q^-(5,q) \setminus \phi(K)$
$\mathcal{L}$	The lines of $Q^-(5,q)$
I	The inherited incidence relation of $Q^-(5,q)$.

Table 4.1: The parameters of an incidence structure arising from a hemisystem.

Proof. Firstly, notice that every point of $\mathcal{P}$ lies on q^2+1 lines of $\mathcal{L}$, and every line in $\mathcal{L}$ lies on $q-m+1$ points of $\mathcal{P}$. Let $\ell \in \mathcal{L}$, $P \in \mathcal{P}$ such that P is not incident with ℓ. Then ℓ contains at most one point which is collinear with P in S. Consider two points $P, Q \in \mathcal{P}$ which are not collinear in S. Let μ be the number of points in $\mathcal{P}$ collinear with both P and Q. The q^2+1 points in $Q^-(5,q)$ that are collinear with P and Q (in $Q^-(5,q)$) are the points of an elliptic quadric in $\mathrm{PG}(3,q)$. Now, let us consider the $q+1$ hyperplanes, each of the form $\mathrm{PG}(4,q)$ containing $\mathrm{PG}(3,q)$ and take their intersections with $\phi(K)$. Every two distinct hyperplanes intersect in an elliptic quadric $Q^-(3,q)$, excluding the points collinear with both P and Q. Now, let ρ be the polarity associated to $Q^-(5,q)$. Then each of the $q+1$ hyperplanes are of the form R^ρ for some point R on the line PQ. Each R^ρ is a set of q^2+1 lines incident with R and the points on those lines. There are m points on each of these q^2+1 lines contained in $\phi(K)$. Furthermore, since $Q^-(5,q)$ is a generalised quadrangle of order (q,q^2) (since it is the dual of $\mathrm{H}(3,q^2)$), it contains $(q^2+1)(q^3+1)$ lines. Each line of $Q^-(5,q)$ contains m points in $\phi(K)$ and so the total number of points in $\phi(K)$ is $\frac{m(q^2+1)(q^3+1)}{q^2+1}$. Combining these ideas, we obtain

$$\begin{aligned} &2((q^2+1)m-(q^2+1-\mu)) \\ &\quad +(q-1)\left(\frac{(q^2+1)(q+1)m}{q+1}-(q^2+1-\mu)\right) \\ &\quad +(q^2+1-\mu) = |\phi(K)| = \frac{m(q^2+1)(q^3+1)}{q^2+1} \end{aligned}$$

Rearranging, $\mu = q^2+1-m(q+1)$. Therefore, S is a partial quadrangle with parameters $s=q-m$, $t=q^2$ and $\mu = q^2+1-m(q+1)$. □

Note that this implies that a hemisystem gives rise to a partial quadrangle with parameters $((q-1)/2, q^2, (q-1)^2/2)$. Also note that the points of this partial quadrangle are simply the points of $\mathrm{H}(3,q^2)$ and the lines of the partial quadrangle are the lines of the corresponding hemisystem [3]. This connection has enabled authors who have found families of hemisystems to uncover some previously unknown examples of partial quadrangles. We now have everything we need to prove that hemisystems are the only regular systems on $\mathrm{H}(3,q^2)$, q odd.

Theorem 4.4. *For q odd, the only value of m for which $\mathrm{H}(3,q^2)$ has a regular system is $(q+1)/2$.*

Proof. We follow Thas' proof in [54]. Suppose K is a regular system of order m, $0 < m < q+1$. Let $\mathcal{S} = (\mathcal{P}, \mathcal{L}, I)$ be the corresponding partial quadrangle

constructed from K. Then, from [17],

$$|\mathcal{P}| = 1 + (t+1)s\left(1 + \frac{ts}{\mu}\right)$$

Now, substituting in the parameters from Theorem 4.3, we have

$$|\mathcal{P}| = 1 + (q^2+1)(q-m)(1+q^2(q-m))/(q^2+1-m(q+1))$$

Then, from [48], the number of points in $Q^-(5,q)$ is $(q^3+1)(q+1)$. Moreover, from the construction of the partial quadrangle for K in Section 4.1.1, $\phi(K)$ contains $(q^3+1)m$ points and so $|\mathcal{P}| = (q^3+1)(q+1-m)$. Solving the two equations for $|\mathcal{P}|$ gives $m = (q+1)/2$. □

4.1.2 Strongly regular graphs For missing definitions from the basics of graph theory, the reader is directed to [32].

Definition 4.5. A graph Γ of order ν is said to be *strongly regular* with parameters (ν, k, λ, μ) when

i) Every vertex is adjacent to k other vertices,

ii) Every pair of adjacent vertices share λ common neighbours, and

iii) Every pair of non-adjacent vertices share μ common neighbours.

Example 4.6. *A pentagon is a strongly regular graph, with parameters* $(5, 2, 0, 1)$.

Note that the parameters of a strongly regular graph do not uniquely determine it. For example, there are two non-isomorphic strongly regular graphs that both have the parameter set $(16, 6, 2, 2)$. These are the Shrikande graph and the lattice graph $L_{4,4}$ illustrated in Figure 4.2 [32]. We also exclude complete and empty graphs from consideration as strongly regular graphs because μ and λ respectively are not well defined.

The *point graph* of an incidence structure is constructed by assigning a vertex to every point in the incidence structure, and drawing an edge between two vertices if and only if the corresponding points are collinear in the incidence structure. Cameron showed in [17] that a partial quadrangle gives rise to a strongly regular graph. Therefore, from Theorem 4.3, every hemisystem gives rise to a strongly regular graph. A strongly regular graph is said to have a *strongly regular decomposition* if its vertex set V can be partitioned into two subsets $\{V_1, V_2\}$ such that the induced subgraphs Γ_1 and Γ_2 on V_1 and V_2 respectively are strongly regular [33].

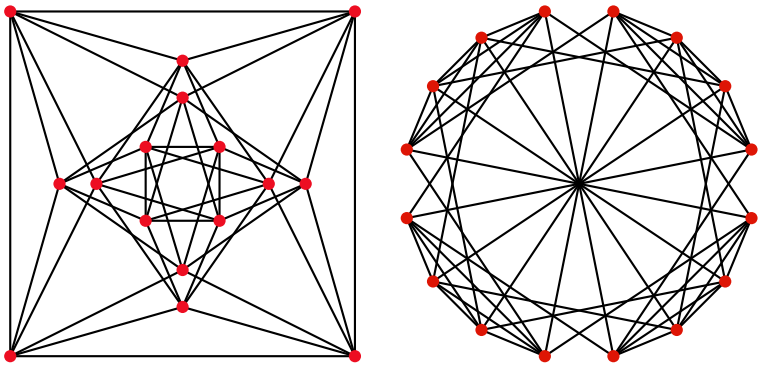


Figure 4.2: Two non-isomorphic strongly regular graphs with parameters (16,6,2,2) [39].

4.1.3 Association schemes Association schemes were initially devised in statistics for the analysis of variance by Bose and Shimamoto [10] . Since then, they have proven to be useful in a wide range of algebraic and combinatorial applications, from coding theory [19] to character theory [6].

Definition 4.7. Let X be a finite set equipped with a set of binary relations $R_0, R_1 \dots R_d$ which satisfy the following conditions:

i) $R_0 = \{(x, x) \mid x \in X\}$.

ii) $\bigcup_{i=0}^{d} R_i = X \times X$ and $R_i \cap R_j = \varnothing$ if $i \neq j$.

iii) $R_i' = R_i$ for all $i \in \{0, 1, \dots, d\}$, where $R_i' = \{(y, x) \mid (x, y) \in R_i\}$.

iv) For all $i, j, k \in \{0, 1, \dots, d\}$, there exist integers p_{ij}^k such that for every $x, y \in X$ with $(x, y) \in R_k$, we have

$$p_{ij}^k = |\{z \in X \mid (x, z) \in R_i, (y, z) \in R_j\}|.$$

Then $(X, \{R_0, \dots, R_d\})$ is called a *d-class symmetric association scheme.*

Notice that the criteria imply that the relations of an association scheme are symmetric and partition the associated set $X \times X$.

We can define matrices A_i for each of the relations R_i of an association scheme by setting $(A_i)_{xy} = 1$ if and only if $(x, y) \in R_i$, and 0 otherwise. We then have an alternative set of statements to those given in Definition 4.7 for the defining properties of an association scheme.

i) $A_0 = I$,

ii) $\sum_i A_i = J$, where J is the matrix with all entries equal to one (called the all-ones matrix),

iii) $A_i = A_i^\top$

iv) $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$ for some integers p_{ij}^k,

Example 4.8. *Let $\Gamma = (\nu, k, \lambda, \mu)$ be a strongly regular graph. Take V to be the set of vertices of Γ and consider the following relations*

i) R_0, the equality relation defined by $\{(v, v) : v \in V\}$,

ii) R_1, the adjacency relation defined by $\{(v, w) : v, w \in V, v \sim w\}$,

iii) R_2, the non-adjacency relation defined by $\{(v, w) : v, w \in V, v \neq w, v \nsim w\}$.

Then $(V, \{R_0, R_1, R_2\})$ is a 2-class association scheme.

We define the *Bose-Mesner algebra* to be the vector space over $\mathbb{C}$ generated by the set of matrices $\{A_i\}_{i=0}^d$ equipped with matrix multiplication. We see that $\{A_i\}_{i=0}^d$ is the natural basis for the Bose-Mesner algebra. An *idempotent* is an element E of this algebra that satisfies $E^2 = E$, under matrix multiplication. An idempotent is said to be *minimal* if it cannot be written as the sum of two non-zero idempotents. By [31, p. 224], there is a unique basis $\{E_i\}_{i=0}^d$ of the Bose-Mesner algebra composed of minimal idempotents. Furthermore, these minimal idempotents are orthogonal. In other words, $E_i E_j = \delta_{ij} E_i$, where δ is the Kronecker delta function. In addition, the minimal idempotents satisfy

$$\sum_{i=0}^{d} E_i = I$$

and

$$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{d} q_{ij}^k E_k$$

where $\circ$ denotes the *Hadamard product*, or entrywise multiplication of matrices. The coefficients q_{ij}^k are called the *Krein parameters*.

Now, suppose $E_0, E_1, \ldots E_d$ are the minimal idempotents of the Bose-Mesner algebra corresponding to a d-class symmetric association scheme on a set X. We define the *first eigenmatrix* $P = (P_{ij})_{i,j=0}^d$ and the *second eigenmatrix* $Q = (Q_{ij})_{i,j=0}^d$ to be the $(d+1) \times (d+1)$ matrices satisfying

$$A_j = \sum_{i=0}^{d} P_{ij} E_i$$

and

$$E_i = \frac{1}{|X|} \sum_{j=0}^{d} Q_{ji} A_j$$

for all i in the range $0 \leq i \leq d$.

Definition 4.9. A symmetric d-class association scheme is said to be a *P-polynomial* or *metric* association scheme with respect to an ordering $\{A_i\}_{i=0}^{d}$ if for each $i \in \{0, 1, \ldots, d\}$, there is a polynomial α_i of degree i such that $p_i(j) = \alpha_i(p_1(j))$ for all $j \in \{0, 1, \ldots, d\}$.

Delsarte observed that P-polynomial association schemes are exactly the association schemes that are generated by distance regular graphs [27]. We can also define a Q-polynomial scheme in a dual setting to a P-polynomial association scheme.

Definition 4.10. A symmetric d-class association scheme is said to be *Q-polynomial* or *cometric* if for each $i \in \{0, \ldots d\}$, there is a polynomial β_i of degree i such that $E_i = \beta_i(E_1)$, where β_i is applied entrywise to E_1.

There are very few known examples of Q-polynomial schemes that are neither P-polynomial schemes or duals of P-polynomial schemes. We say that a Q-polynomial scheme is *Q-antipodal* when $q^j_{1,j+1} = q^j_{1,d-(j+1)}$ for all j, except perhaps when j is the integer part of $d/2$ [43].

Furthermore, we say that a Q-polynomial scheme is *imprimitive* when for some $i > 0$, E_i has repeated columns i.e., it does not have full rank.

Martin, Muzychuk and van Dam proved in [60] that any strongly regular graph with a strongly regular decomposition gives rise to a 4-class imprimitive cometric Q-antipodal association scheme. They show that the strongly regular graph corresponding to a hemisystem has a strongly regular decomposition and therefore gives rise to such a scheme. These Q-polynomial association schemes do not arise from distance regular graphs, and so are one of the few examples which do not arise from P-polynomial or dual P-polynomial association schemes.

Proposition 4.11 ([60], Corollary 7.8)**.** *Suppose $(\mathcal{P}, \mathcal{L}, I)$ is a generalised quadrangle of order (t^2, t), with t odd and let $\mathcal{C}$ denote the set of all ordered pairs of distinct intersecting lines from $\mathcal{L}$. Now, suppose $\mathcal{L} = \mathcal{U}_1 \cup \mathcal{U}_2$ is a partition of the lines into hemisystems. Then the relations*

$$R_0 = \{(\ell, \ell) \mid \ell \in \mathcal{L}\},$$

$$R_1 = \mathcal{C} \cap ((\mathcal{U}_1 \times \mathcal{U}_2) \cup (\mathcal{U}_2 \times \mathcal{U}_1)),$$

$$R_2 = \mathcal{C} \cap ((\mathcal{U}_1 \times \mathcal{U}_1) \cup (\mathcal{U}_2 \times \mathcal{U}_2)),$$

$$R_3 = ((\mathcal{U}_1 \times \mathcal{U}_2) \cup (\mathcal{U}_2 \times \mathcal{U}_1)) - R_1,$$

$$R_4 = ((\mathcal{U}_1 \times \mathcal{U}_1) \cup (\mathcal{U}_2 \times \mathcal{U}_2)) - R_0 - R_2$$

give a cometric Q-antipodal association scheme on $X = \mathcal{L}$.

4.2 Relative hemisystems

As mentioned earlier, hemisystems only exist for q odd, because $(q+1)/2$ must be an integer. This prompted questions about whether there is an analogous and fruitful concept of hemisystems on $\mathrm{H}(3, q^2)$, for q even. In 2011, Penttila and Williford answered these questions by defining relative hemisystems [49].

Definition 4.12 (Penttila and Williford [49])**.** Let S be a generalised quadrangle of order (q^2, q) containing a generalised quadrangle S' of order (q, q). Then all lines of S meet S' in $q+1$ points or are disjoint from S'. We call a subset $\mathcal{H}$ of the lines disjoint from S' a *relative hemisystem* of S with respect to S' provided that for each point x of $S \setminus S'$, exactly half the lines through x disjoint from S' lie in $\mathcal{H}$.

When constructing a relative hemisystem, we are only concerned with the set of points of $\mathrm{H}(3, q^2)$ which are outside of $\mathrm{W}(3, q)$ and the lines of $\mathrm{H}(3, q^2)$ disjoint from $\mathrm{W}(3, q)$. For conciseness, we call the former the set of *external points*, denoted $\mathcal{P}_E$ and the latter the set of *external lines*, denoted $\mathcal{L}_E$.

Although relative hemisystems do not give rise to strongly regular graphs and partial quadrangles like their predecessors, they do give rise to a completely new type of Q-polynomial association schemes which does not arise from distance regular graphs. Let $\ell \in \mathcal{L}_E$ and let $\mathcal{O}_\ell$ be the set of lines of the Hermitian space $\mathrm{H}(3, q^2)$ which meet both ℓ and the embedded $\mathrm{W}(3, q)$.

Theorem 4.13 ([49])**.** *If $\mathrm{H}(3, q^2)$, $q > 2$ has a relative hemisystem $\mathcal{R}$ with respect to $\mathrm{W}(3, q)$, then a primitive Q-polynomial 3-class scheme can be constructed on the lines of the relative hemisystem with the following relations:*

$$R_0 = \{(\ell, \ell) \mid \ell \in \mathcal{R}\};$$

$$R_1 = \{(\ell, m) \mid \ell \not\perp m \,:\, |\mathcal{O}_\ell \cap \mathcal{O}_m| = 1\};$$

$$R_2 = \{(\ell, m) \mid \ell \not\perp m \,:\, |\mathcal{O}_\ell \cap \mathcal{O}_m| = q+1\};$$

$$R_3 = \{(\ell, m) \mid \ell \,\mathrm{I}\, m\}.$$

Until Penttila and Williford's result, the only known examples of Q-polynomial association schemes not arising from distance regular graphs were imprimitive, and either Q-antipodal or both Q-antipodal and Q-bipartite [49]. Therefore, the association schemes arising from relative hemisystems are completely uncharted territory, and are of great interest to algebraic graph theorists.

4.3 The known families of relative hemisystems

In this section, we give a survey of the known examples of relative hemisystems, and briefly describe their constructions. Using the equations given in Sections 2.4.1 and 2.4.2, we find that $|\mathcal{P}_E| = q(q^2+1)(q^2-1)$ and $|\mathcal{L}_E| = q^2(q^2-1)$. This in turn means that the number of lines in a relative hemisystem is $q^2(q^2-1)/2$.

4.3.1 The Pentilla-Williford relative hemisystems The first example of an infinite family of relative hemisystems, admitting $\mathrm{P\Omega}^-(4,q)$ as an automorphism group, was given by Penttila and Williford in their paper introducing the concept [49]. The full proof is outside the scope of this dissertation, but we give an outline of it to aid us in describing the Cossidente constructions in the next subsection.

Suppose S is a generalised quadrangle of order (s,t). Also suppose S contains a generalised subquadrangle S' of order (s,t'). Then, we find that for all points $P \in S \setminus S'$, $P^\perp \cap S'$ is an ovoid of S'. Let τ be the Baer involution that fixes $\mathrm{W}(3,q)$ in $\mathrm{H}(3,q^2)$. Then the *antipode* of a line ℓ of $\mathrm{H}(3,q^2)$ not contained in $\mathrm{W}(3,q)$, is the image of the line under the Baer involution ℓ^τ.

They subsequently compute the point and line orbits in the Hermitian space of the action of $\mathrm{P\Omega}^-(4,q)$. They show that $\mathrm{P\Omega}^-(4,q)$ is transitive on points of $\mathrm{H}(3,q^2)$. Next, they consider the action of a dihedral group D of order $2(q^2+1)$ that is the normaliser of a Singer cyclic group (see [37, p. 187]) of $\mathrm{P\Omega}^-(4,q)$ on $\mathrm{H}(3,q^2)$. Let A be a subgroup of D with prime order p. Since $q^2(q^2-1)$, the number of external lines, is congruent to 2 modulo p, A must fix at least two external lines. Let one of these be ℓ and let its antipode be ℓ^τ. Then A commutes with the Baer involution τ fixing every point of $\mathrm{W}(3,q)$ and interchanging ℓ and ℓ^τ. Therefore, A also fixes ℓ^τ. Some representation theory (namely Maschke's Theorem) is used to show that ℓ and ℓ^τ are the only lines fixed by A[1]. They use this to prove that $\mathrm{P\Omega}^-(4,q)$, q even, $q \geq 2$ has two orbits on external lines. These orbits are two relative hemisystems, H_1 and H_2. They further show that the Baer involution τ swaps H_1 and H_2 [49, Theorem 5].

4.3.2 The Cossidente relative hemisystems Excluding the family of relative hemisystems discovered by Penttila and Williford, the only other known examples are the two infinite families discovered by Cossidente, and one apparently sporadic example discovered by Cossidente and Pavese [21, 20, 22]. Both of the infinite families are perturbations of the Penttila-Williford relative hemisystems, and the sporadic example is derived from a Suzuki-Tits ovoid of $\mathrm{W}(3,8)$.

The first family on $\mathrm{H}(3,q^2)$, q even and $q > 4$ admits the linear group $\mathrm{PSL}(2,q)$ as an automorphism group [21]. Cossidente constructed it by considering the two Penttila-Williford relative hemisystems H_1 and H_2. He then took the stabiliser of

[1] We think that this implication is not true in general, and that it is possible that A could have fixed more than two lines.

a conic section of the elliptic quadric $\mathrm{Q}^-(3,q)$ fixed by $\mathrm{P}\Omega^-(4,q)$ in $\mathrm{W}(3,q)$. This stabiliser is isomorphic to $\mathrm{PSL}(2,q)$ and does not act transitively on H_1 and H_2. Cossidente then uses the involution τ, which switches H_1 and H_2 from the Penttila-Williford proof (mentioned above in Subsection 4.3.1), to delete some orbits of H_1 under $\mathrm{PSL}(2,q)$ and replace them with their images under τ. Every time this is done, it creates a distinct pair of relative hemisystems. Since the number of ways this can be done is greater than the number of Pentilla-Williford relative hemisystems for a given q, a power of two, Cossidente has constructed a new infinite family.

The second infinite family of relative hemisystems discovered by Cossidente admits a group of order $q^2(q+1)$ [20]. The construction of this infinite family is very similar to the last. Choose a point P of an elliptic quadric $\mathrm{Q}^-(3,q)$ which is an ovoid of $\mathrm{W}(3,q)$. Let M be the subgroup of the stabiliser of P in $\mathrm{P}\Omega^-(4,q)$ of order $q^2(q+1)$. Instead of orbits under $\mathrm{PSL}(2,q)$, Cossidente considers orbits of H_1 and H_2 under M, deleting orbits of H_1 and replacing them by their image under the involution τ. Since the number of relative hemisystems invariant under M exceeds that of the Penttila-Williford relative hemisystems, Cossidente must have found another infinite family of relative hemisystems.

4.3.3 The Cossidente-Pavese Example Finally, Cossidente and Pavese showed the existence of a relative hemisystem on $\mathrm{H}(3,64)$ admitting a group of order 168 as a setwise stabiliser computationally [22]. Let $\mathrm{W}(3,2^{2n+1})$ be a symplectic space. Then there is a polarity θ on $\mathrm{W}(3,2^{2n+1})$ [48]. The set of all absolute points of θ forms an ovoid of $\mathrm{W}(3,2^{2n+1})$. This ovoid is called a Suzuki-Tits ovoid, and its stabiliser up to field automorphisms is defined as the Suzuki group $\mathrm{Sz}(2^{2n+1})$ [52]. Cossidente and Pavese concretely define a Hermitian surface $\mathrm{H}(3,q^2)$ for $q=8$ by the equation $x_1^q x_4 + x_1 x_4^q + x_2^q x_3 + x_2 x_3^q = 0$. Then let $\mathrm{W}(3,q)$ be the canonical symplectic space of $\mathrm{H}(3,q^2)$. Define the Suzuki-Tits ovoid $\mathcal{O}$ by $\mathcal{O} = \{(1,x,y,x^\sigma + xy + y^{\sigma+2}) \mid x,y \in \mathrm{GF}(8)\} \cup \{(0,0,0,1)\}$, where σ is the automorphism of $\mathrm{GF}(8)$ mapping $x \mapsto x^4$. This ovoid has automorphism group $G = 2.\mathrm{Sz}(8).3$. There is a subgroup S of order 168 contained in the stabiliser of $(0,0,0,1)$ in G. With the help of MAGMA [11], Cossidente and Pavese construct a relative hemisystem by taking a union of the orbits of external lines under S [22]. Cossidente and Pavese conjecture that this example is sporadic, i.e., it cannot be extended to an infinite family including examples on higher values of q.

Results

> "A mathematical problem should be difficult in order to entice us, yet not completely inaccessible, lest it mock at our efforts."
>
> David Hilbert (1900)

In this section, we present the results of our search for new relative hemisystems. We describe our computational approach, which lead to the complete classification of relative hemisystems for $q = 4$, as well as the independent discovery of a Cossidente family of relative hemisystems and the Cossidente-Pavese example arising from a Suzuki-Tits ovoid. We also provide a previously unknown set of three criteria sufficient to determine a relative hemisystem. We show that we may narrow these criteria down to one condition if we are considering a perturbation of the Penttila-Williford relative hemisystems. We use this to give a new construction of the Penttila-Williford relative hemisystems, as well as the Cossidente family admitting a group of order $q^2(q+1)$ for each q even.

5.1 Computation

In early March, we developed a method for finding relative hemisystems on $\mathrm{H}(3, q^2)$ for $q = 4, 8, 16$ using GAP [30] and Gurobi [38]. We made use of the FinInG [2] package to create the incidence structures and the collineation groups associated with them. The code for the function may be found in Appendix A. We also took advantage of Cayley's theorem for groups and found the corresponding permutation groups for these collineation groups and indexed the external points and lines so that the action of the resulting permutation group was permutation isomorphic to the collineation group. For the rest of this section, the mention of collineation groups and external points and lines in the context of algorithms refers to the corresponding permutation groups and indices respectively. We wanted to create a linear program for solving in Gurobi which would solve for $q^2(q^2-1)$ binary variables, each corresponding to an external line. If the line was contained in the relative hemisystem, the corresponding variable would have a value of one in the solution set, and zero otherwise. The task became to generate constraints for Gurobi. We found the set of lines S_P incident with each external point P and added a constraint expressing that the variables corresponding to the elements of S_p should sum to $q/2$. In other words, only half of the q external lines incident with P should be contained in the relative hemisystem. We ran this linear program for $q = 4$ to completion in Gurobi, and so completely classified all of the relative hemisystems on $\mathrm{H}(3, q^2)$. We attempted to run this linear program to find all of the relative hemisystems on $\mathrm{H}(3, 8^2)$, but it proved to be intractable.

Next, we broke down the problem in an attempt to make it simpler and therefore quicker to solve. The basis for the method that we adopted was that Gurobi could solve several small linear programs with many constraints much faster than it could solve one large linear program with fewer constraints. We also noticed that there can exist collineations between relative hemisystems, which make some of them equivalent, and we only wanted to find non-equivalent examples. So, we could simply fix some external lines and look for relative hemisystems that contain those lines. In doing so, we remove the need to search for relative hemisystems containing sets of lines in the same orbit as those we had fixed, because they would be equivalent.

We adapted an algorithm designed by Bamberg, Martis and Morris in [44], and based on the 'orderly algorithm' described by McKay [45] and Royle [50], to optimise the search for relative hemisystems. The first step was to use a recursive GAP function to create a tab delimited computation tree of depth n. The function first found the orbits of external lines under $\mathrm{Coll}(\mathrm{H}(3,q^2))_{\mathrm{W}(3,q)}$ and took a representative v_i from each one to appear in the computation tree. The function then created an output file for each of the orbits, listing all of the elements in that orbit. The function proceeded to stabilise the first orbit representative v_1 and repeat the process to generate the orbits of all two tuples $\{v_1, w\}$ for w in the set of external lines. The process was repeated until the conclusion of the iteration on n-tuples. The algorithm returned and completed the remaining part of the computation tree in the same way, and generated the corresponding orbit enumeration files.

Once the computation tree was complete, another algorithm external to GAP ran to generate a shell script from the computation tree. This script listed the commands needed to run the separate Gurobi computations for each member of the computation tree and provided information about the progress of the computation.

5.1.1 Classification of examples for $q = 4$. Despite only being one power of two smaller than 8, the classification of relative hemisystems on $\mathrm{H}(3, q^2)$ for $q = 4$ was a significantly easier problem. We were able to successfully run the original relative hemisystem finder program to completion and found that there were 240 relative hemisystems on $\mathrm{H}(3, 16)$ and they are all equivalent (i.e., the same up to a collineation) to the Penttila and Williford example on $q = 4$. This was a previously unknown result, as none of the published literature has attempted to classify all examples of relative hemisystems for a fixed value of q.

5.1.2 Independent discovery of Cossidente relative hemisystems. After running the program for several hours for $q = 8$, we terminated the process and examined the returned solutions. The linear program had found three solutions given in the form of sets of 2016 numbers corresponding to lines. One solution was found to be isomorphic to a Penttila-Williford relative hemisystem and the other two were seemingly unknown examples. Despite our best efforts, it seemed that finding all non-equivalent examples of relative hemisystems on $\mathrm{H}(3, 64)$ was intractable.

We therefore began processing the two unknown examples we had found, beginning with the example which was subsequently found to be isomorphic to Cossidente's most recent infinite family discussed in [20]. The analysis of this example laid the groundwork for the new sufficient conditions for relative hemisystems discussed in the next section, and through these conditions, we have a new proof of Cossidente's result.

The second seemingly unknown example was explored later in the project. This example had a stabiliser G of order 168. We found that by "fusing" some of the orbits of G on external points, i.e., investigating the groups that are transitive on some of the orbits of G, we were able to fix a Suzuki-Tits ovoid that lies in $\mathrm{W}(3,8)$. Cossidente and Pavese's paper verifying our results appeared in subsequent days [22]. However, there is still future work to be done on producing a construction of this relative hemisystem beyond computation.

5.1.3 Stabiliser factorisation. Using the algorithm described above, we also attempted to characterise the relative hemisystems on $\mathrm{H}(3,64)$ based on the order of their stabilisers. We first obtained the conjugacy classes of $\mathrm{Coll}(\mathrm{H}(3,q^2))_{\mathrm{W}(3,q)}$ and then found those that contain collineations of a particular order m, and took a conjugacy class representative c_i from each of these. We then computed the collineation group G_i generated by each representative and calculated its normaliser N_i in $\mathrm{Coll}(\mathrm{H}(3,q^2))_{\mathrm{W}(3,q)}$. We examined the orbits of G_i on external lines and the action of N_i on these orbits. This action can be considered as a homomorphism from N_i to the symmetric group of the orbits of G_i on external lines. The image of this homomorphism forms the group used for the algorithm described at the beginning of this section.

The results of our computation are described in the table below. Note that the full collineation group of external points and lines $\mathrm{Coll}(\mathrm{H}(3,q^2))_{\mathrm{W}(3,q)}$ has prime factorisation $2^{12} \times 3^4 \times 5 \times 7^2 \times 13$.

Stabiliser divisor	Classification of Relative Hemisystems
13	Penttila-Williford example
7	Penttila-Williford example or Cossidente example admitting $\mathrm{PSL}(2,8)$
5	Penttila-Williford example

Table 5.1: The classification of relative hemisystems of $\mathrm{H}(3,8^2)$ with stabiliser orders divisible by certain primes.

We attempted to classify examples of relative hemisystems with stabiliser orders divisible by three and nine, but we were unsuccessful, and it seems that with our current method, this problem is intractable.

5.2 New sufficient conditions for relative hemisystems

We now give a set of new sufficient criteria to determine a relative hemisystem, and show that all but one of the known examples of relative hemisystems satisfy these criteria. We use Ω/G to denote the set of orbits of a set Ω under a group G. Note that if N is a normal subgroup of G, then G acts on Ω/N in its action on sets.

Let $\mathcal{Q}^+$ be a hyperbolic quadric which intersects $\mathrm{H}(3,q^2)$ in an elliptic quadric isomorphic to $\mathrm{Q}^-(3,q)$. The stabiliser of $\mathcal{Q}^+$ in $\mathrm{P\Gamma U}(4,q)$ is isomorphic to the orthogonal group $\mathrm{PSO}^-(4,q)$ [49]; and the subgroup of $\mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+}$ that stabilises the two families of reguli of $\mathcal{Q}^+$ is isomorphic to $\mathrm{P\Omega}^-(4,q)$ [49]. Penttila and Williford go on to prove in [49] that $\mathrm{P\Omega}^-(4,q)$ has two orbits on external lines, and $\mathrm{PSO}^-(4,q)$ is transitive on external lines. Taking $\ell \in \mathcal{L}_E$, the size of the orbit of ℓ under $\mathrm{PSO}^-(4,q)$ is twice as large as the orbit of ℓ under $\mathrm{P\Omega}^-(4,q)$. By the Orbit-Stabiliser Theorem, $|\mathrm{PSO}^-(4,q){:}\mathrm{PSO}^-(4,q)_\ell| = |\mathrm{P\Omega}^-(4,q){:}\mathrm{P\Omega}^-(4,q)_\ell|$. Since $|\mathrm{PSO}^-(4,q){:}\mathrm{P\Omega}^-(4,q)| = 2$ [40, Table 2.1d], we have $\mathrm{PSO}^-(4,q)_\ell = \mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+,\ell} = \mathrm{P\Omega}^-(4,q)_\ell$. Therefore, the size of the orbit of $\ell^{\mathrm{P\Omega}^-(4,q)}$ under $\mathrm{PSO}^-(4,q)$ is

$$|\mathrm{PSO}^-(4,q){:}\mathrm{PSO}^-(4,q)_\ell \cdot \mathrm{P\Omega}^-(4,q)| = |\mathrm{PSO}^-(4,q){:}\mathrm{P\Omega}^-(4,q)| = 2$$

and hence $\mathrm{PSO}^-(4,q) = \mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+}$ acts fixed point freely on the orbits of $\mathrm{P\Omega}^-(4,q)$ on external lines.

Proposition 5.1. *Let G be a subgroup of $\mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+}$, where $\mathcal{Q}^+$ is a hyperbolic quadric meeting $\mathrm{H}(3,q^2)$ in an elliptic quadric. Let D be the subgroup of $\mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+}$ that stabilises the two family of reguli of $\mathcal{Q}^+$. If G is not contained in D, then G acts fixed-point-freely on the orbits of $G \cap D$ on external lines.*

Proof. * Suppose the contrary, that G fixes an orbit $\ell^{G\cap D}$. Note that $\ell^G = \ell^{G\cap D}$ because if there exists $g \in G$ such that $\ell^g \notin \ell^{G\cap D}$ then G does not fix the orbit $\ell^{G\cap D}$, a contradiction. Then by the Orbit-Stabiliser Theorem we have

$$|G \cap D{:}(G \cap D)_\ell| = |\ell^{G\cap D}| = |\ell^G| = |G{:}G_\ell|$$

and hence

$$|G{:}G \cap D| = |G_\ell{:}(G \cap D)_\ell| \tag{5.1}$$

Now from the discussion at the beginning of this section, we have $\mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+,\ell} = D_\ell$. Since G is a subgroup of $\mathrm{P\Gamma U}(4,q)_{\mathcal{Q}^+}$, G_ℓ is a subgroup of D_ℓ. Hence $G_\ell = (G\cap D)_\ell$, and so by Equation 5.1, $|G{:}G\cap D| = 1$. This implies that $G = G\cap D$ and hence G is a subgroup of D. This is a contradiction since G is not contained in D, by our initial assumptions.. Therefore, G must act fixed-point-freely on the orbits of $G \cap D$ on external lines. □

Theorem 5.2. *Suppose $G < \overline{G}$, where $\overline{G}$ is a subgroup of the collineation group of $\mathrm{H}(3,q^2)$, stabilising $\mathrm{W}(3,q)$. Further suppose that $\overline{G}$ and G satisfy the following conditions:*

1. $|\overline{G}{:}G| = 2$,
2. $\overline{G}$ *acts fixed point freely on* $\mathcal{L}_E/G$,
3. $\mathcal{P}_E/\overline{G} = \mathcal{P}_E/G$.

Write $\mathcal{L}_E/\overline{G} = \{\ell_1^{\overline{G}}, \ell_2^{\overline{G}}, \dots \ell_n^{\overline{G}}\}$. *Then* $\bigcup_{i=1}^n \ell_i^G$ *is a relative hemisystem .*

Proof. * Let X be an external point. For $\ell \in \mathcal{L}_E$, we define the *line orbit incidence number* as

$$n_{X,\ell}^G = |\{m \in \ell^G \mid X \,\mathrm{I}\, m\}|$$

First note that for all $g \in G$,

$$n_{X,\ell}^G = n_{X^g,\ell}^G \tag{5.2}$$

because $X \,\mathrm{I}\, m \Leftrightarrow X^g \,\mathrm{I}\, m^g$. Now, since $|\overline{G}{:}G| = 2$, for all $\ell \in \mathcal{L}_E$, there exist $\ell_1, \ell_2 \in \mathcal{L}_E$ such that $\ell^{\overline{G}} = \ell_1^G \cup \ell_2^G$. Then, we can find $t \in \overline{G}$ such that $(\ell_1^G)^t = \ell_2^G$. Since $\overline{G}$ acts fixed point freely on $\mathcal{L}_E/G$, the orbits of $\overline{G}$ on $\mathcal{L}_E/G$ have size two and G is the kernel of the action. Therefore, there exists an element $t \in \overline{G}$ such that for all $\ell \in \mathcal{L}_E$, we have $\ell^{\overline{G}} = \ell^G \dot\cup (\ell^t)^G$. We then have $n_{X,\ell}^{\overline{G}} = n_{X,\ell^t}^G + n_{X,\ell}^G$. Consider $n_{X,\ell^t}^G = |\{m \in (\ell^t)^G \mid X \,\mathrm{I}\, m\}|$. Since G has index two and is therefore a normal subgroup of $\overline{G}$, $n_{X,\ell^t}^G = |\{n^t \in (\ell^G)^t \mid X \,\mathrm{I}\, n^t\}| = |\{n \in (\ell^G) \mid X^{t^{-1}} \,\mathrm{I}\, n\}|$. Now, since $\overline{G}$ and G have the same orbits on external points, there exists $u \in G$ such that $X^{t^{-1}} = X^u$. So $n_{X,\ell^t}^G = |\{n \in (\ell^G) \mid X^u \,\mathrm{I}\, n\}| = n_{X^u,\ell}^G = n_{X,\ell}^G$, by Equation 5.2. Therefore,

$$n_{X,\ell}^{\overline{G}} = 2n_{X,\ell}^G \tag{5.3}$$

Consider the orbit representatives $\ell_1, \ell_2, \dots \ell_n$ of $\mathcal{L}_E/\overline{G}$. The number q of external lines incident with X is then equal to the sum of the line orbit incidence numbers $n_{X,\ell_i}^{\overline{G}}$, for $i \in \{1, \dots n\}$. Then, from Equation 5.3, $q/2 = \sum_{i=1}^n n_{X,\ell_i}^G$. So the number of lines of $\bigcup_{i=1}^n \ell_i^G$ incident with X is $q/2$. Therefore, since X was any external point, $\bigcup_{i=1}^n \ell_i^G$ is a relative hemisystem. □

When we are dealing with the Penttila-Williford relative hemisystems and perturbations of them, we can condense the criteria given in Theorem 5.2 to two sufficient criteria to determine a relative hemisystem. We state these conditions in the following corollary to Theorem 5.2.

Corollary 5.3. *Suppose* $\overline{G}$ *is a subgroup of* $\mathrm{PSO}^-(4,q)$ *and* G *is the intersection of* $\overline{G}$ *and* $\mathrm{P\Omega}^-(4,q)$. *Further suppose that* $\overline{G}_P$ *is not contained in* $\mathrm{P\Omega}^-(4,q)$ *for all external points* $P \in \mathcal{P}_E$. *Then* $(G, \overline{G})$ *satisfies the conditions given in Theorem 5.2 and thus determines a relative hemisystem.*

Proof. * First notice that if $\overline{G}_P$ is not contained in $\mathrm{P\Omega}^-(4,q)$ for all external points $P \in \mathcal{P}_E$, then there exists an element $g \in \overline{G}$ such that $g \notin \mathrm{P\Omega}^-(4,q)$.

So $\overline{G}$ is not contained in $\mathrm{P\Omega}^-(4,q)$. We have $|\overline{G}{:}G| = |\overline{G}{:}\overline{G} \cap \mathrm{P\Omega}^-(4,q)| = |\overline{G} \cdot \mathrm{P\Omega}^-(4,q){:}\mathrm{P\Omega}^-(4,q)| = |\mathrm{PSO}^-(4,q){:}\mathrm{P\Omega}^-(4,q)| = 2$. Let $\ell \in \mathcal{L}_E$. Now, the discussion at the beginning of Section 5.2 implies that for any $\ell \in \mathcal{L}_E$, $\mathrm{PSO}^-(4,q)_\ell = \mathrm{P\Omega}^-(4,q)_\ell$. Thus $\overline{G}_\ell = \mathrm{PSO}^-(4,q)_\ell$ is contained in $\mathrm{P\Omega}^-(4,q)$. Therefore, $G_\ell = \overline{G}_\ell \cap \mathrm{P\Omega}^-(4,q) = \overline{G}_\ell$. Now, since $\overline{G}_P$ is not contained in $\mathrm{P\Omega}^-(4,q)$, $\overline{G}_P \neq \overline{G}_P \cap \mathrm{P\Omega}^-(4,q)$. So the stabiliser of P under $\overline{G}$ is not equal to the stabiliser under G. By the Orbit-Stabiliser Theorem,

$$\frac{|P^{\overline{G}}|}{|P^G|} = \frac{|\overline{G}{:}\overline{G}_P|}{|G{:}G_P|} = \frac{|\overline{G}{:}G|}{|\overline{G}_P{:}G_P|}$$

Since $|\overline{G}{:}G| = 2$, $|\overline{G}_P{:}G_P| = 2$ and therefore $P^{\overline{G}} = P^G$. Therefore, $(G, \overline{G})$ satisfies the conditions of Theorem 5.2. □

Let $\psi(x_1, x_2) = x_1^2 + \upsilon^{q+1}x_2^2 + x_1x_2$ be a form with $\upsilon \in \mathrm{GF}(q^2)$ satisfying $\upsilon^q + \upsilon = 1$, implying by Lemma 2.3 that ψ is irreducible over $\mathrm{GF}(q)$. Then

$$Q^+(3,q^2){:}x_1^2 + \upsilon^{q+1}x_2^2 + x_1x_2 + x_3x_4 = 0 \tag{5.4}$$

is a hyperbolic quadric that intersects the Hermitian space defined by the form $x_1x_2^q + x_2x_1^q + x_3x_4^q + x_4x_3^q = 0$ over $\mathrm{GF}(q^2)$ in an elliptic quadric. This elliptic quadric's defining equation is simply the equation for $Q^+(3,q^2)$ restricted to $\mathrm{GF}(q)$. We may use a change of basis from $Q^+(3,q^2)$ to the canonical hyperbolic quadric to obtain the reguli of $Q^+(3,q^2)$. The change of basis matrix is

$$B = \begin{pmatrix} \upsilon^q & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \upsilon & 1 & 0 & 0 \end{pmatrix}$$

The reguli of $Q^+(3,q^2)$ are therefore

$$\begin{aligned} \mathscr{R}_1 &= \{\left[\begin{smallmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & \lambda \end{smallmatrix}\right] B \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{\left[\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right] B\} \\ &= \{\left[\begin{smallmatrix} \upsilon^q & 1 & 0 & \lambda \\ \lambda\upsilon & \lambda & 1 & 0 \end{smallmatrix}\right] \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{\left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ \upsilon & 1 & 0 & 0 \end{smallmatrix}\right]\} \end{aligned}$$

$$\begin{aligned} \mathscr{R}_2 &= \{\left[\begin{smallmatrix} 1 & \lambda & 0 & 0 \\ 0 & 0 & 1 & \lambda \end{smallmatrix}\right] B \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{\left[\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right] B\} \\ &= \{\left[\begin{smallmatrix} \upsilon^q & 1 & \lambda & 0 \\ \lambda\upsilon & \lambda & 0 & 1 \end{smallmatrix}\right] \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{\left[\begin{smallmatrix} 0 & 0 & 1 & 0 \\ \upsilon & 1 & 0 & 0 \end{smallmatrix}\right]\} \end{aligned}$$

Proposition 5.4. *The Penttila-Williford family of relative hemisystems, admitting* $\mathrm{P\Omega}^-(4,q)$ *as an automorphism group for each q even, satsfies Corollary 5.3.*

Proof. * Take $G = \mathrm{P\Omega}^-(4,q)$ and $\overline{G} = \mathrm{PSO}^-(4,q)$, and let $\mathrm{H}(3,q^2)$ be the Hermitian space defined by the form $x_1x_2^q + x_2x_1^q + x_3x_4^q + x_4x_3^q = 0$ over $\mathrm{GF}(q^2)$. The embedded symplectic space $\mathrm{W}(3,q)$ is the restriction of the Hermitian form to $\mathrm{GF}(q)$. Recall from the beginning of the section that $\mathrm{PSO}^-(4,q)$ is isomorphic to the stabiliser of

$Q^+(3,q^2)$, and $\mathrm{P\Omega}^-(4,q)$ is isomorphic to the stabiliser in $\mathrm{PSO}^-(4,q)$ of the reguli of $Q^+(3,q^2)$. Consider $g \in \overline{G}$ defined by

$$g = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}$$

We claim that g does not fix the reguli of the hyperbolic quadric $Q^+(3,q^2)$. Finding the image of $\mathscr{R}_1$ under g gives us

$$[\begin{smallmatrix} v^q&1&0&\lambda\\ \lambda v&\lambda&1&0 \end{smallmatrix}]^g = [\begin{smallmatrix} v^q&1&\lambda&0\\ \lambda v&\lambda&0&1 \end{smallmatrix}]$$

for $\lambda \in \mathrm{GF}(q^2)$, and

$$[\begin{smallmatrix} 0&0&0&1\\ v&1&0&0 \end{smallmatrix}]^g = [\begin{smallmatrix} 0&0&1&0\\ v&1&0&0 \end{smallmatrix}]$$

which are exactly the lines of $\mathscr{R}_2$. Since g has order two, $g^{-1} = g$ and so $\mathscr{R}_2$ must map to $\mathscr{R}_1$ under the action of g. Therefore, since G stabilises the reguli of the hyperbolic quadric from the discussion at the beginning of this section, $g \in \overline{G} \setminus G$. Now, notice that $P_\omega = (\omega, 0, 1, 1) \in \mathrm{H}(3,q^2)$ for all $\omega \in \mathrm{GF}(q^2)$, and if we take $\omega \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$, then P_ω is an external point. Let $\omega \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$. Then $P_\omega^g = (\omega, 0, 1, 1)^g = (\omega, 0, 1, 1)$ and therefore g fixes P_ω. So $g \in \overline{G}_{P_\omega}$, but $g \notin G_{P_\omega}$ because $g \notin G$. Therefore, $\overline{G}_{P_\omega} \neq G_{P_\omega} = \overline{G}_{P_\omega} \cap G$ and $\overline{G}_{P_\omega}$ is not contained in $\mathrm{P\Omega}^-(4,q)$. Finally, from [49], $G = \mathrm{P\Omega}^-(4,q)$ is transitive on external points. It immediately follows that $\overline{G} = \mathrm{PSO}^-(4,q)$ is transitive on external points as well. This implies that $\overline{G}_Q$ is not contained in $\mathrm{P\Omega}^-(4,q)$ for all external points $Q \in \mathcal{P}_E$. Therefore, $(G, \overline{G})$ determine a relative hemisystem for every q even, and this relative hemisystem belongs to the Penttila-Williford family of relative hemisystems. □

Proposition 5.5. *The first family of Cossidente relative hemisystems admitting* $\mathrm{PSL}(2,q)$ *as a setwise stabiliser (described in [21]) satisfies Corollary 5.3 for* $q = 4, 8, 16$.

Proof. * Let $\mathrm{H}(3,q^2)$ be the Hermitian space in $\mathrm{PG}(3,q^2)$ with defining Gram matrix

$$H = \begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}.$$

Let $Q^+(3,q^2)$ be the hyperbolic quadric described in Equation 5.4. Recall that the reguli of this quadric are:

$$\mathscr{R}_1 = \{[\begin{smallmatrix} v^q&1&0&\lambda\\ \lambda v&\lambda&1&0 \end{smallmatrix}] \mid \lambda \in \mathrm{GF}(q^2)\} \cup [\begin{smallmatrix} 0&0&0&1\\ v&1&0&0 \end{smallmatrix}]$$

$$\mathscr{R}_2 = \{[\begin{smallmatrix} v^q&1&\lambda&0\\ \lambda v&\lambda&0&1 \end{smallmatrix}] \mid \lambda \in \mathrm{GF}(q^2)\} \cup [\begin{smallmatrix} 0&0&1&0\\ v&1&0&0 \end{smallmatrix}]$$

The Baer subspace that contains the symplectic space $\mathrm{W}(3,q)$ and the elliptic quadric $Q^-(3,q) = Q^+(3,q^2) \cap \mathrm{H}(3,q^2)$ consists of points whose coordinates lie

solely in GF(q). Define collineations τ and ϕ as follows.

$$\tau{:}(x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_4, x_3)$$
$$\phi{:}(x_1, x_2, x_3, x_4) \mapsto (x_1^q, x_2^q, x_3^q, x_4^q)$$

Notice that H$(3, q^2)$ and the Baer subspace are fixed under both τ and ϕ. Recall from Section 4.3.2 that the construction of this family of relative hemisystems stemmed from stabilising a conic of the elliptic quadric $\mathrm{Q}^-(3, q)$ fixed by $\mathrm{P\Omega}^-(4, q)$ in W$(3, q)$ [21]. Notice that τ does not fix the reguli because it is the same collineation as g in the proof of Proposition 5.2. Now, consider the application of ϕ to the reguli. For $\mathscr{R}_1$, we have the following:

$$\begin{aligned}
\left[\begin{smallmatrix} \upsilon^q & 1 & 0 & \lambda \\ \lambda\upsilon & \lambda & 1 & 0 \end{smallmatrix}\right]^\phi &= \left[\begin{smallmatrix} (\upsilon^q)^q & 1^q & 0 & \lambda^q \\ \lambda^q\upsilon^q & \lambda^q & 1^q & 0 \end{smallmatrix}\right] \\
&= \left[\begin{smallmatrix} \upsilon & 1 & 0 & \lambda^q \\ \lambda^q\upsilon^q & \lambda^q & 1 & 0 \end{smallmatrix}\right] \\
&= \left[\begin{smallmatrix} \lambda^q\upsilon^q & \lambda^q & 1 & 0 \\ \upsilon & 1 & 0 & \lambda^q \end{smallmatrix}\right] \\
&= \left[\begin{smallmatrix} \upsilon^q & 1 & \mu & 0 \\ \mu\upsilon & \mu & 0 & 1 \end{smallmatrix}\right] \in \mathscr{R}_2
\end{aligned}$$

where $\mu = \lambda^{q^2-q-1}$. Additionally,

$$\left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ \upsilon & 1 & 0 & 0 \end{smallmatrix}\right]^\phi = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ \upsilon^q & 1 & 0 & 0 \end{smallmatrix}\right] \in \mathscr{R}_2$$

Therefore, ϕ maps $\mathscr{R}_1$ to $\mathscr{R}_2$. Since ϕ has order 2 and so $\phi^{-1} = \phi$, $\mathscr{R}_2$ must map to $\mathscr{R}_1$ under ϕ. Consider the product $\tau\phi$. Since we have already proved that τ and ϕ individual interchange the reguli of $Q^+(3, q^2)$, it follows that their composition fixes reguli. Let $K = \langle \tau, \phi \rangle$, which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Now, take the collineation group isomorphic to PSL$(2, q)$ that fixes the hyperplane $x_3 = x_4$. Define $\overline{G} = \mathrm{PSL}(2, q) \times K$ and $G = \mathrm{PSL}(2, q) \times \langle \tau\phi \rangle$. We claim that these groups satisfy the conditions of Corollary 5.3. Firstly, notice that G is contained in the intersection of $\overline{G}$ and $\mathrm{P\Omega}^-(4, q)$ because PSL$(2, q)$ is a subgroup of $\mathrm{P\Omega}^-(4, q)$ [69], and $\tau\phi$ fixes the reguli of $Q^+(3, q^2)$, just as $\mathrm{P\Omega}^-(4, q)$ does. Furthermore, if $g \in \overline{G} \cap \mathrm{P\Omega}^-(4, q)$, then g must fix reguli, since $\mathrm{P\Omega}^-(4, q)$ does. Therefore, $g \in G$ and we have shown that $G = \overline{G} \cap \mathrm{P\Omega}^-(4, q)$. Furthermore, $\overline{G}$ is not contained in $\mathrm{P\Omega}^-(4, q)$ because τ and ϕ do not fix the reguli. We were able to show computationally in GAP [30] for $q = 4, 8, 16$ that for any external point $P \in \mathcal{P}_E$, $\overline{G}_P$ is not contained in $\mathrm{P\Omega}^-(4, q)$. □

We are yet to discover a constructive proof to show that the first family of Cossidente relative hemisystems satisfies the second criterion of Corollary 5.3; however, we are confident that they do, and we leave this as future work.

We claim that Cossidente's second family of relative hemisystems, admitting a group of order $q^2(q + 1)$, for each q even, described in [20], also satisfy these new conditions. To prove this, we first provide a concrete construction of this family of relative hemisystems. As before, we consider the Hermitian space H$(3, q^2)$ defined by the form $x_1x_2^q + x_2x_1^q + x_3x_4^q + x_4x_3^q = 0$ over GF(q^2), with the embedded symplectic

space $\mathrm{W}(3,q)$ defined as the restriction of the form to $\mathrm{GF}(q)$. We explicitly define the following two hyperbolic quadrics.

$$Q_1^+(3,q^2) : \alpha x_1^2 + \beta x_2^2 + x_1x_2 + x_3x_4 \tag{5.5}$$

$$Q_2^+(3,q^2) : \beta x_1^2 + \alpha x_2^2 + x_1x_2 + x_3x_4 \tag{5.6}$$

where $\alpha \in \mathbb{F}_{q^2}$, $\beta = \alpha + 1$ and $\alpha + \alpha^q + 1 = 0$.

Now, we may determine the reguli of $Q_1^+(3,q^2)$ by taking a suitable change of basis from $Q_1^+(3,q^2)$ to the canonical hyperbolic quadric described in Section 2.4.3. The change of basis matrix is as follows:

$$\tilde{B} = \begin{pmatrix} \sqrt{\alpha} & \sqrt{\alpha} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \sqrt{\alpha} & \beta/\sqrt{\alpha} & 0 & 0 \end{pmatrix}$$

We subsequently compute the reguli of $Q_1^+(3,q^2)$ by post-multiplying the reguli of the canonical hyperbolic quadric by the change of basis matrix.

$$\begin{aligned}
\tilde{\mathscr{R}}_1 &= \{ \left[\begin{smallmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & \lambda \end{smallmatrix}\right] \tilde{B} \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{ \left[\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right] \tilde{B}\} \\
&= \{ \begin{bmatrix} \sqrt{\alpha} & \sqrt{\alpha} & 0 & \lambda \\ \lambda\sqrt{\alpha} & \lambda\beta/\sqrt{\alpha} & 1 & 0 \end{bmatrix} \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{ \left[\begin{smallmatrix} 0 & & 0 & 0 & 1 \\ \sqrt{\alpha} & & \beta/\sqrt{\alpha} & 0 & 0 \end{smallmatrix}\right] \} \\
&= \{ \begin{bmatrix} \alpha & \alpha & 0 & \lambda\sqrt{\alpha} \\ \lambda\alpha & \lambda\beta & \sqrt{\alpha} & 0 \end{bmatrix} \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{ \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ \alpha & \beta & 0 & 0 \end{smallmatrix}\right] \}
\end{aligned}$$

$$\begin{aligned}
\tilde{\mathscr{R}}_2 &= \{ \left[\begin{smallmatrix} 1 & \lambda & 0 & 0 \\ 0 & 0 & 1 & \lambda \end{smallmatrix}\right] \tilde{B} \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{ \left[\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right] \tilde{B} \\
&= \{ \begin{bmatrix} \sqrt{\alpha} & \sqrt{\alpha} & \lambda & 0 \\ \lambda\sqrt{\alpha} & \lambda\beta/\sqrt{\alpha} & 0 & 1 \end{bmatrix} \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{ \left[\begin{smallmatrix} 0 & & 0 & 1 & 0 \\ \sqrt{\alpha} & & \beta/\sqrt{\alpha} & 0 & 0 \end{smallmatrix}\right] \} \\
&= \{ \begin{bmatrix} \alpha & \alpha & \lambda\sqrt{\alpha} & 0 \\ \lambda\alpha & \lambda\beta & 0 & \sqrt{\alpha} \end{bmatrix} \mid \lambda \in \mathrm{GF}(q^2)\} \cup \{ \left[\begin{smallmatrix} 0 & 0 & 1 & 0 \\ \alpha & \beta & 0 & 0 \end{smallmatrix}\right] \}
\end{aligned}$$

Proposition 5.6. *Suppose $\overline{M}$ is the stabiliser in $\mathrm{PGU}(4,q)$ of the two hyperbolic quadrics $Q_1^+(3,q^2)$ and $Q_2^+(3,q^2)$ described above. Now, let M be the stabiliser in $\overline{M}$ of a class of reguli in $Q_1^+(3,q^2)$. Then M is the group admitted by Cossidente's second family of relative hemisystems, and M and $\overline{M}$ satisfy Corollary 5.3.*

Proof. * Firstly we claim that, $\overline{M} = M \times Z$, where Z is the group generated by the involution z defined by $(x_1,x_2,x_3,x_4) \mapsto (x_2^q, x_1^q, x_4^q, x_3^q)$. From Example 3.10, we know that the action on lines of $\tilde{\mathscr{R}}_1$ (for instance) is permutation isomorphic to a group action on a projective line $\mathrm{PG}(1,q^2)$. Now, M fixes two lines which are in the intersection of $Q_1^+(3,q^2)$ and $Q_2^+(3,q^2)$, namely $\ell_1 = \left[\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right]$ and $\ell_2 = \left[\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$. Notice that $\ell_1 \in \tilde{\mathscr{R}}_1$ and $\ell_2 \in \tilde{\mathscr{R}}_2$. The group M fixing ℓ_1 is permutation isomorphic to $\mathrm{AGL}(1,q^2)$ fixing a point on $\mathrm{PG}(1,q^2)$. Now, $\mathrm{AGL}(1,q^2)$ is transitive on the remaining points of $\mathrm{PG}(1,q^2)$ [40], and so M is transitive on $\tilde{\mathscr{R}}_1 \setminus \{\ell_1\}$. Therefore,

to show that z maps $\tilde{\mathscr{R}}_1$ to $\tilde{\mathscr{R}}_2$, it is sufficient to prove it for ℓ_1 and another line of $\tilde{\mathscr{R}}_1$. Let $\ell_{\infty,1} = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ \alpha & \beta & 0 & 0 \end{smallmatrix}\right]$. Now,

$$\ell_1^z = \left[\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right]^q \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \left[\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right] \in \tilde{\mathscr{R}}_2$$

$$\ell_{\infty,1}^z = \left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ \alpha & \beta & 0 & 0 \end{smallmatrix}\right]^q \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \left[\begin{smallmatrix} 0 & 0 & 1 & 0 \\ \alpha & \beta & 0 & 0 \end{smallmatrix}\right] \in \tilde{\mathscr{R}}_2$$

A similar argument yields that the image of any line in $\tilde{\mathscr{R}}_2$ under z is contained in $\tilde{\mathscr{R}}_1$. Therefore, the involution z switches the reguli of $Q_1^+(3,q^2)$ and so $\overline{M} = M \times Z$. Let D_1 be the subgroup of $\mathrm{P\Gamma U}(4,q)_{Q_1^+}$ that stabilises two family of reguli on Q_1^+. Similarly, let D_2 be the subgroup of $\mathrm{P\Gamma U}(4,q)_{Q_2^+}$ that stabilises two family of reguli on Q_2^+. We now prove that the orbits of $\overline{M}$ and M on external points are identical. Since $\overline{M} = M \times Z$, it is sufficient to prove that for all $x \in \mathcal{P}_E, x^z \in x^M$ Since D_1 is transitive on $\mathcal{P}_E$, this is equivalent to showing that for all $g \in D_1$, we have $(P_0^g)^z \in (P_0^g)^M$ for all $P_0 \in \mathcal{P}_E$.

Claim: Given a point $P_0 \in \mathcal{P}_E$, we have $P_0^z = P_0^m$ and $P_0 = (P_0^z)^z = (P_0^m)^m$ for some $m \in M$. Since D_1 acts transitively on $\mathcal{P}_E$, it is sufficient for us to prove this claim for a specific point. Let $P_0 = \langle (1,0,1,0) \rangle$. Then we have the following

$$P_0^z = (1,0,1,0)^q \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (0,1,0,1).$$

Now, we must find an involution $m \in M$ such that $P_0^m = P_0^z = (0,1,0,1)$. This equivalent to finding $m \in M$ such that $P_0^{zm^{-1}} = P_0^{zm}$ fixes P_0. Take m to be the following collineation:

$$m = \phi \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

where ϕ is the automorphism $x \mapsto x^q$. Then,

$$P_0^m = (1,0,1,0)^q \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} = (0,1,0,1)$$

because we are working in a field with characteristic two. Furthermore,

$$\begin{aligned} P_0^{zm} &= (1,0,1,0)^{q^2} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \\ &= (1,0,1,0) \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \\ &= (1,0,1,0). \end{aligned}$$

It remains to show that $m \in M$. To show that $m \in M$, we must show that it is an involution and that it fixes the two hyperbolic quadrics that define M and also each

of the reguli in the intersection of the two hyperbolic quadrics. Firstly recalling that we are working with a field with characteristic 2,

$$m^2 = \begin{pmatrix} 1&0&1&1\\0&1&1&1\\1&1&1&0\\1&1&0&1 \end{pmatrix}\begin{pmatrix} 1&0&1&1\\0&1&1&1\\1&1&1&0\\1&1&0&1 \end{pmatrix} = I_4.$$

Secondly, we must show that m fixes the two hyperbolic quadrics $Q_1^+(3,q^2)$ and $Q_2^+(3,q^2)$. Recall the defining quadratic forms of the two hyperbolic quadrics $Q_1^+(3,q^2)$ and $Q_2^+(3,q^2)$ given in Equations 5.5 and 5.6 respectively. Any point $(x_1,x_2,x_3,x_4) \in Q_1^+(3,q^2)$ maps to $(x_1^q+x_3^q+x_4^q, x_2^q+x_3^q+x_4^q, x_1^q+x_2^q+x_3^q, x_1^q+x_2^q+x_4^q)$ under m. Substituting this into the form corresponding to $Q_1^+(3,q^2)$, we have

$$\begin{aligned}
&\alpha(x_1^q+x_3^q+x_4^q)^2+\beta(x_2^q+x_3^q+x_4^q)^2+(x_1^q+x_3^q+x_4^q)(x_2^q+x_3^q+x_4^q)\\
&+(x_1^q+x_2^q+x_3^q)(x_1^q+x_2^q+x_4^q)\\
&=(\alpha+1)x_1^{2q}+(\beta+1)x_2^{2q}+x_1^qx_2^q+x_3^qx_4^q+(\alpha+\beta+1)x_3^{2q}+(\alpha+\beta+1)x_4^{2q}\\
&=(\alpha x_1^2+\beta x_2^2+x_1x_2+x_3x_4)^q\\
&=0.
\end{aligned}$$

So m fixes $Q_1^+(3,q^2)$, and by symmetry, it fixes $Q_2^+(3,q^2)$ as well. Finally, we show that m fixes the reguli of $Q_1^+(3,q^2)$. Again, we only need to test two lines from each regulus - the line that is fixed by M and another line. For $\ell_1, \ell_{\infty,1} \in \tilde{\mathscr{R}}_1$:

$$\ell_1^m = \left[\begin{smallmatrix}1&1&0&0\\0&0&1&0\end{smallmatrix}\right]^q \begin{pmatrix} 1&0&1&1\\0&1&1&1\\1&1&1&0\\1&1&0&1 \end{pmatrix} = \left[\begin{smallmatrix}1&1&0&0\\1&1&1&0\end{smallmatrix}\right] = \left[\begin{smallmatrix}1&1&0&0\\0&0&1&0\end{smallmatrix}\right] \in \tilde{\mathscr{R}}_1,$$

$$\ell_{\infty,1}^m = \left[\begin{smallmatrix}0&0&0&1\\\alpha&\beta&0&0\end{smallmatrix}\right]^q \begin{pmatrix} 1&0&1&1\\0&1&1&1\\1&1&1&0\\1&1&0&1 \end{pmatrix} = \left[\begin{smallmatrix}1&1&0&1\\\beta&\alpha&0&0\end{smallmatrix}\right] = \left[\begin{smallmatrix}\sqrt{\alpha}&\sqrt{\alpha}&0&\sqrt{\alpha}\\\alpha&\beta&1&0\end{smallmatrix}\right] \in \tilde{\mathscr{R}}_1.$$

Using a similar argument, m fixes the reguli of $\tilde{\mathscr{R}}_2$ as well. Therefore, m preserves the reguli and so $m \in M$. Now that we have proved the claim, we continue with the proof as before. We have $P_0^{gz} \in P_0^{gM}$ if and only if $P_0^{gzg^{-1}} \in P_0^{gMg^{-1}}$ for all $g \in D_1$. This is equivalent to P_0 having identical orbits under $\overline{M}^g$ and M^g for all $g \in D_1$. By the Orbit-Stabiliser Theorem and since $|\overline{M}{:}M| = 2$, it follows that $|\overline{M}^g_{P_0}| = 2|M^g_{P_0}|$. Finally, this holds if and only if $|\overline{M}_{P_0}| = 2|M_{P_0}|$, which is true by the claim proven above. Since $M_{P_0} = \overline{M}_{P_0} \cap \mathrm{P}\Omega^-(4,q)$, we have shown that $\overline{M}_{P_0} \not\leq \mathrm{P}\Omega^-(4,q)$ and since D_1 is transitive, this holds for all external points $P \in \mathcal{P}_E$. Therefore, M and $\overline{M}$ determine a relative hemisystem. □

Interestingly, we have found by computation in GAP [30] that the relative hemisystem on $\mathrm{H}(3,q^2)$ arising from a Suzuki-Tits ovoid does not satisfy the criteria for Lemma 5.2.

Concluding Remarks

> "At the end of the day there's another day dawning, and the sun in the morning is waiting to rise."
>
> At the End of the Day, *Les Misérables*

Relative hemisystems are a new and exciting topic in finite geometry and group theory. Since not much is known about them, both in terms of properties and examples, there is a large potential for new work and it is reasonably straightforward to find a new section of the topic to work on.

One of the opportunity costs of researching such a new area is that publication rates are quite high. As a result, if new findings are not published in a timely manner, then it is likely they will be discovered and published by another author, as I have experienced in this project. Nevertheless, there are great benefits to completing the research for myself, as I have developed heuristics which will be helpful as I explore this area further in the future.

During this dissertation, we saw the interplay between group theory and finite geometry in describing abstract geometric objects like hemisystems and relative hemisystems. We have also followed the epic history of hemisystems, originating from B. Segre's definition and first example in 1965 [51], through the breakthroughs of the subsequent decades about the properties of hemisystems and the drought of new examples to Thas' conjecture about the non-existence of hemisystems apart from Segre's example [55]. The infinite family of hemisystems found by Penttila and Cossidente [23], ten years after Thas' conjecture and forty years after Segre's original paper, proved to be the start of many discoveries of families of relative hemisystems by a large variety of authors. We came to Penttila and Williford's definition of a relative hemisystem in [49], as an analogous concept to hemisystems for q even, and described how they give rise to a rare and previously undiscovered class of association schemes, We also discussed the constructions of the three known infinite families of relative hemisystems, as the conjectured sporadic example arising from a Suzuki-Tits ovoid.

The main outcomes of this research project were discussed in Chapter 5. We described the computation carried out with GAP [30] and Gurobi [38] in an effort to find and classify all of the relative hemisystems on $\mathrm{H}(3, 64)$. This computation lead to the independent discovery of an infinite family of relative hemisystems discovered by Cossidente in [25] and the conjectured sporadic example discovered by Cossidente and Pavese in [22]. Additionally, we were able to classify all of the relative hemisystems on $\mathrm{H}(3, 16)$ and determine that they were all members of the Penttila-Williford infinite family, a previously unknown fact. Finally, we described our use of the relative hemisystem finder and computation tree algorithm to find

and classify relative hemisystems on $\mathrm{H}(3, 64)$ with stabilisers which have 5, 7 or 13 as divisors.

Furthermore, we presented a set of three criteria which are sufficient for determining a relative hemisystem. We refined these criteria down to a single condition for perturbations of the Penttila-Williford family of relative hemisystems. Using this condition, we were able to give new constructions of the Penttila-Williford family, the Cossidente family admitting a group of order $q^2(q+1)$ for each q even, and the Cossidente family admitting $\mathrm{PSL}(2, q)$ for $q = 4, 8, 16$. We conjecture that the condition holds on the Cossidente family of relative hemisystems admitting $\mathrm{PSL}(2, q)$ for $q > 16$ and we leave this as future work.

There are many avenues for further work to be done on relative hemisystems.

One of the most obvious open problems is the classification of all relative hemisystems on $\mathrm{H}(3, q)$ for $q = 8$ and beyond. The attempts that we have made prove that it is not as easy as it may seem to have such a classification, but with the development of new methods and larger computing power, it does not seem far out of reach.

Another open question related to the original work presented in Chapter 5 is whether most examples of relative hemisystems satisfy the conditions given in Theorem 5.2. We have proved that all of the known infinite families satisfy the conditions, but given that we have a counterexample in the relative hemisystem arising from a Suzuki-Tits ovoid and our lack of knowledge about how many non-equivalent examples of relative hemisystems exist, it is hard to say whether this set of criteria describes most of the examples or not.

Another avenue for further research could also be to investigate whether we can construct relative hemisystems using the conditions given in Theorem 5.2. This could open the door to finding new infinite families of relative hemisystems.

Finally, there is future work to be done on proving or disproving that the Cossidente-Pavese relative hemisystem arising from a Suzuki-Tits ovoid, described in [22] is sporadic. Since these ovoids only exist on $\mathrm{W}(3, q)$ for q an odd power of two, it seems difficult to investigate the next possible occurence on $q = 32$. The number of lines in a hemisystem for $q = 32$ is 523776, which is a far cry from the mere 2016 lines for $q = 8$.

Index

Bibliography

[1] A. Aguglia and L. Giuzzi. Intersections of the Hermitian surface with irreducible quadrics in even characteristic. preprint.

[2] John Bamberg, Anton Betten, Philippe Cara, Jan De Beule, Michel Lavrauw, and Max Neunhöffer. FinInG – Finite Incidence Geometry, Version 1.0, 2014.

[3] John Bamberg, Frank De Clerck, and Nicola Durante. Intriguing sets in partial quadrangles. Journal of Combinatorial Designs, 19(3):217–245, 2011.

[4] John Bamberg, Michael Giudici, and Gordon F. Royle. Every flock generalized quadrangle has a hemisystem. Bull. Lond. Math. Soc., 42(5):795–810, 2010.

[5] John Bamberg, Maska Law, and Tim Penttila. Tight sets and m-ovoids of generalised quadrangles. Combinatorica, 29(1):1–17, 2009.

[6] Eiichi Bannai and Tatsuro Ito. Algebraic combinatorics. Benjamin/Cummings Menlo Park, 1984.

[7] Susan Barwick and Gary Ebert. Unitals in projective planes. Springer Monographs in Mathematics. Springer, New York, 2008.

[8] Albrecht Beutelspacher and Ute Rosenbaum. Projective geometry: from foundations to applications. Cambridge University Press, 1998.

[9] Garrett Birkhoff and John Von Neumann. The logic of quantum mechanics. Annals of Mathematics, 37(4):pp. 823–843, 1936.

[10] R. C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block designs with two associate classes. Journal of the American Statistical Association, 47(258):151–184, 1952.

[11] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[12] Richard Brauer. A characterization of null systems in projective space. Bull. Amer. Math. Soc., 42(4):247–254, 1936.

[13] A. A. Bruen and J. W. P. Hirschfeld. Applications of line geometry over finite fields. II. The Hermitian surface. Geom. Dedicata, 7(3):333–353, 1978.

[14] Francis Buekenhout. Handbook of incidence geometry: buildings and foundations. North Holland, 1995.

[15] Francis Buekenhout and Ernest Shult. On the foundations of polar geometry. Geometriae Dedicata, 3(2):155–170, 1974.

[16] Robert Calderbank. On uniformly packed $[n, n - -k, 4]$ codes over GF(q) and a class of caps in PG($k - -1, q$). Journal of the London Mathematical Society, 2(2):365–384, 1982.

[17] P. J. Cameron. Partial quadrangles. Quart. J. Math. Oxford Ser. (2), 26:61–73, 1975.

[18] P. J. Cameron, J.-M. Goethals, and J. J. Seidel. Strongly regular graphs having strongly regular subconstituents. J. Algebra, 55(2):257–280, 1978.

[19] Paul Camion. Codes and association schemes: basic properties of association schemes relevant to coding. Handbook of coding theory, 2:1441–1567, 1998.

[20] Antonio Cossidente. A new family of relative hemisystems on the hermitian surface. Designs, Codes and Cryptography, pages 1–9, 2013.

[21] Antonio Cossidente. Relative hemisystems on the Hermitian surface. J. Algebraic Combin., 38(2):275–284, 2013.

[22] Antonio Cossidente and Francesco Pavese. Intriguing sets of W$(5, q)$, q even. Journal of Combinatorial Theory, Series A, 127:303–313, 2014.

[23] Antonio Cossidente and Tim Penttila. Hemisystems on the Hermitian surface. Journal of the London Mathematical Society, 72(3):731–741, 2005.

[24] Antonio Cossidente and Tim Penttila. Segre's hemisystem and McLaughlin's graph. J. Combin. Theory Ser. A, 115(4):686–692, 2008.

[25] Antonio Cossidente and Tim Penttila. On m-regular systems on H$(5, q^2)$. J. Algebraic Combin., 29(4):437–445, 2009.

[26] Maarten De Boeck. Intersection problems in finite geometries. PhD thesis, PhD thesis, Ghent University, 2014.

[27] P. Delsarte. An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl., (10):vi+97, 1973.

[28] Claude-Alain Faure. An elementary proof of the fundamental theorem of projective geometry. Geom. Dedicata, 90:145–151, 2002.

[29] Joseph Gallian. Contemporary abstract algebra. Cengage Learning, 2009.

[30] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.7.5, 2014.

[31] C. D. Godsil. Algebraic combinatorics, volume 6. CRC Press, 1993.

[32] C. D. Godsil and Gordon F. Royle. Algebraic graph theory, volume 207. Springer New York, 2001.

[33] W. H. Haemers and D. G. Higman. Strongly regular graphs with strongly regular decomposition. Linear Algebra Appl., 114/115:379–398, 1989.

[34] Gerhard Hessenberg. Über einen geometrischen Calcül (Verknüpfungs-Calcül). Acta Math., 29(1):1–23, 1905.

[35] J. W. P Hirschfeld. Projective geometries over finite fields. Clarendon Press Oxford, 1998.

[36] J. W. P. Hirschfeld and J. A. Thas. General Galois geometries. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1991. Oxford Science Publications.

[37] Bertram Huppert. Endliche Gruppen: Vol.: 1. Springer-Verlag, 1967.

[38] Gurobi Optimization Inc. Gurobi optimizer reference manual, 2014.

[39] Wolfram Research Inc. Mathematica version 10.0, 2014.

[40] Peter B Kleidman and Martin W Liebeck. The subgroup structure of the finite classical groups, volume 129. Cambridge University Press, 1990.

[41] Felix Klein. Vergleichende Betrachtungen über neuere geometrische Forschungen. Math. Ann., 43(1):63–100, 1893.

[42] R. Lidl and H. Niederreiter. Finite Fields. Number v. 20, pt. 1 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[43] William J. Martin, Mikhail Muzychuk, and Jason Williford. Imprimitive cometric association schemes: constructions and analysis. J. Algebraic Combin., 25(4):399–415, 2007.

[44] Michael Martis, John Bamberg, and Sylvia Morris. An enumeration of certain projective ternary two-weight codes and their relationship to the cubic Segre variety. ArXiv e-prints, June 2014.

[45] Brendan D. McKay. Isomorph-free exhaustive generation. J. Algorithms, 26(2):306–324, 1998.

[46] Paris by Train: Schedules, Maps and Passes on Paris trains, RER and Metro. Map of the Paris Métro. Available at: `http://parisbytrain.com/wp-content/uploads/2014/01/paris-metro-map-2014.pdf`.

[47] Stanley E. Payne. Tight pointsets in finite generalized quadrangles. Congr. Numer., 60:243–260, 1987. Eighteenth Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, Fla., 1987).

[48] Stanley E. Payne and J. A. Thas. Finite generalized quadrangles, volume 110. European Mathematical Society, 2009.

[49] Tim Penttila and Jason Williford. New families of q-polynomial association schemes. Journal of Combinatorial Theory, Series A, 118(2):502–509, 2011.

[50] Gordon F. Royle. An orderly algorithm and some applications in finite geometry. Discrete Math., 185(1-3):105–115, 1998.

[51] Beniamino Segre. Forme e geometrie hermitiane, con particolare riguardo al caso finito. Ann. Mat. Pura Appl. (4), 70:1–201, 1965.

[52] Michio Suzuki. A new type of simple groups of finite order. Proc. Nat. Acad. Sci. U.S.A., 46:868–870, 1960.

[53] J. A. Thas. Ovoids and spreads of finite classical polar spaces. Geom. Dedicata, 10(1-4):135–143, 1981.

[54] J. A. Thas. Ovoids and spreads of finite classical polar spaces. Geometriae Dedicata, 10(1-4):135–143, 1981.

[55] J. A. Thas. Projective geometry over a finite field. In Handbook of incidence geometry, pages 295–347. North-Holland, Amsterdam, 1995.

[56] Jacques Tits. Sur la trialité et certains groupes qui s'en déduisent. Inst. Hautes Études Sci. Publ. Math., (2):13–60, 1959.

[57] Jacques Tits. Buildings of spherical type and finite BN-pairs. Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin-New York, 1974.

[58] Johannes Ueberberg. Foundations of Incidence Geometry: Projective and Polar Spaces. Springer, 2011.

[59] Theodor Vahlen. Abstrakte Geometrie. Untersuchungen über die Grundlagen der Euklidischen und nicht-Euklidischen Geometrie. S. Hirzel, Leipzig, 1940. Zweite, neubearbeitete Auflage. Zweites Beiheft zu Deutsche Mathematik.

[60] Edwin R. van Dam, William J. Martin, and Mikhail Muzychuk. Uniformity in association schemes and coherent configurations: cometric Q-antipodal schemes and linked systems. J. Combin. Theory Ser. A, 120(7):1401–1439, 2013.

[61] Jacobus Hendricus van Lint and Richard Michael Wilson. A course in combinatorics. Cambridge university press, 2001.

[62] Frédéric Vanhove. A Higman inequality for regular near polygons. J. Algebraic Combin., 34(3):357–373, 2011.

[63] Oswald Veblen and J. H. Maclagan-Wedderburn. Non-Desarguesian and non-Pascalian geometries. Trans. Amer. Math. Soc., 8(3):379–388, 1907.

[64] Oswald Veblen and John Wesley Young. A set of assumptions for projective geometry. American Journal of Mathematics, 30(4):347–380, 1908.

[65] Oswald Veblen and John Wesley Young. Projective geometry. Vol. 1. Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[66] Oswald Veblen and John Wesley Young. Projective geometry. Vol. 2 (by Oswald Veblen). Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[67] Ferdinand Douwe Veldkamp. Polar geometry. Universiteit te Utrecht., 1959.

[68] Charles Weibel. Survey of non-Desarguesian planes. Notices of the AMS, 54(10):1294–1303, 2007.

[69] Robert Wilson. The Finite Simple Groups, volume 251. Springer, 2009.

Appendices

Relative Hemisystem Finder for GAP

Below is the code produced in an attempt to find new relative hemisystems on $\mathrm{H}(3, 64)$.

```
#######
#Relative Hemisystem Finder
#Melissa Lee (UWA)
#Version Gamma
#
# We find the relative hemisystems using Gurobi by writing
# the problem as a linear program.
# The objective function is trivial and we have equations
# xM = (y,y,.....,y)
# Where y = half the number of external lines
# running through an external point.
# Each row of M is an incidence vector of a line such that
# M_{ij} =1 <=> point extpts[j] is on line extlines[i]
# and zero otherwise.
#######
LoadPackage("fining");
LoadPackage("Gurobify");
q:= 4;
H:=HermitianPolarSpace(3,q^2);
W:= SymplecticSpace(3,q);
em:= NaturalEmbeddingBySubfield(W,H);
Wpts := Points(W);
Hpts := Points(H);
Hpts := AsList(Hpts);
Wpts := AsList(Wpts);
Wpts2:= ImagesSet(em, Wpts);
Hlines := List(Lines(H));
Wlines := List(Lines(W));
Wlines2 := ImagesSet(em, Wlines);
#points external to W
extpts := Difference(Hpts, Wpts2);
#lines external to W
extlines:=Filtered(Hlines, l -> Filtered(Wpts2, p -> p * l) = []);
#choose an external point
pt := extpts[1];
#Find no. lines through external pts in the relative hemisystem
y :=Size(Filtered(extlines, l ->  (pt*l)))/2;
#Objective is to make sure all points have the
# necessary number of lines in RH
```

```
b:=Concatenation(ListWithIdenticalEntries(Size(extpts), y), [1]);
#Make matrix of all constraints
matrix:= NullMat(Size(extlines),Size(extpts)+1);

#incidence matrix
for i in [1..Size(extlines)] do
for j in [1..Size(extpts)] do
if extpts[j] * extlines[i] then
matrix[i][j] := 1;
fi;
od;
matrix[i][Size(extpts)+1] := 0;
od;

matrix[1][Size(extpts)+1] := 1;


#defining things for the linear program
comparisons := ListWithIdenticalEntries(Size(extpts)+1, '=');
objective:=ListWithIdenticalEntries(Size(extpts)+1, 0);
variables := ListWithIdenticalEntries(Size(extlines), "Binary");

lp := LinearProgram( objective, matrix, comparisons, b, variables );
#Use gurobi to find the solutions
allsolutions := GurobiFindAllSolutions(lp);
RH := List(allsolutions,
    t -> Filtered([1..Size(extlines)], i -> t[i] = 1));
col := CollineationGroup(H);
stab := FiningSetwiseStabiliser(col, Wlines2);
act := ActionHomomorphism(stab, extlines, OnProjSubspaces);
perm := Image(act);
uptoeq := Set(RH, t -> SmallestImageSet(perm,t));
Print(Size(uptoeq), " relative hemisystems found up to equivalence");
```

Group Theory

Here we introduce the basics of group theory. Groups are one of the most important algebraic structures in mathematics. In addition to being significant in their own right, groups are also critical to finite geometry.

B.1 Some Basics and Examples

Definition B.1. A *group* $(G, \cdot)$ is a set G equipped with a binary operation $\cdot$ on elements of G, that satisfies the following conditions.

i) There exists an identity element $e \in G$ such that $e \cdot g = g = g \cdot e$ for all $g \in G$.

ii) The operation $\cdot$ is associative. In other words, for every $x, y, z \in G$, we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

iii) For all $g \in G$, there exists an inverse of g, $h \in G$ such that $g \cdot h = e$.

There are many familiar examples of groups. For example, consider the integers, denoted $\mathbb{Z}$ with regular addition. This forms a group, with identity $e = 0$. Further, consider the integers $\{1, \ldots, n-1\}$ with multiplication modulo n. These form a group if n is a prime. If n is not prime, then integers in $\mathbb{Z}_n$ that are not coprime to n will not have an inverse.

A group $(G, \cdot)$ is said to be *Abelian* when its binary operation is commutative. Notice that the integers with addition and the integers with multiplication modulo p (p prime) described above are Abelian groups. However, there are many important examples of non-Abelian groups.

Example B.2. *The set of $n \times n$ invertible matrices over the reals, denoted* $\mathrm{GL}(n, \mathbb{R})$ *with matrix multiplication form a group. However, the group is not Abelian for $n > 1$, since matrix multiplication is not commutative in general.*

B.1.1 Simplifying notation It is common to simplify the group notation to make it easier to write and read. We often omit the $\cdot$ symbol when applying the binary operation to two elements of the group. So, for example, we write gh instead of $g \cdot h$. We call this the 'product' of g and h.

We also use index notation to denote the repeated application of the operation to a single element of the group. For example, we will write g^3 for ggg. By convention, we define $g^0 = e$.

We will also say "G is a group" instead of "$(G, \cdot)$ is a group". The group operation will usually be apparent and we will use the notation described in this section.

Another important concept is the *order of a group* G, denoted $|G|$, which is the total number of distinct elements the group contains. Note that this quantity might be finite or infinite.

On the other hand, the *order of an element* g in a group G is the smallest natural number n such that $g^n = e$. Again, this may be finite or infinite. We now prove some basic facts about groups.

Lemma B.3. *A group $(G, \cdot)$ has exactly one identity element.*

Proof. We know that G must contain an identity element, otherwise it wouldn't be a group. Suppose G contains two distinct identity elements e and e'. Then, consider $e \cdot e'$. Now, since e is an identity, $e \cdot e' = e'$. However, e' is also an identity so $e \cdot e' = e$. This implies that $e = e'$. □

Lemma B.4. *Let $(G, \cdot)$ be a group. Then, each element $g \in G$ has exactly one inverse in G.*

Proof. Suppose $g \in G$. Then, g must have at least one inverse, otherwise G would not be a group. Suppose g had two inverses, h and j. Then, consider $h \cdot g \cdot j$. Since h is an inverse of g, we have $h \cdot g \cdot j = e \cdot j = j$. We know j is also an inverse of g so $h \cdot g \cdot j = h \cdot e = h$. So $j = h$. □

B.2 Subgroups

Many groups have nonempty subsets which also form groups under the same operation as the larger group. These nonempty subsets are called *subgroups*. Notice that this subset does not need to be proper; indeed, a group is a subgroup of itself. The subset containing just the group identity e also forms a subgroup; it is called the *trivial group*. If H is a subgroup of G, then we sometimes write $H \leq G$.

Example B.5. *The set of integer multiples of n, denoted $n\mathbb{Z}$ is a subgroup of the integers with addition, $(\mathbb{Z}, +)$.*

Rather than checking all three of the group axioms if we wish to say that H is a subgroup of G, we may instead use the following result.

Proposition B.6. *Suppose G is a group and H is a nonempty subset of G. Then H is a subgroup of G if and only if for all $x, y \in H$, $xy^{-1} \in H$.*

Proof. Forward direction: Suppose H is a subgroup of G. Then H is closed under multiplication and every element $y \in H$ has $y^{-1} \in H$. Therefore, $xy^{-1} \in H$ for all $x, y \in H$.

Backward direction: Suppose $xy^{-1} \in H$ for all $x, y \in H$. Then, since H is nonempty, there exists an element $x \in H$ and $xx^{-1} = e \in H$. Also, H is associative

because the property is inherited from G. Any element $y \in H$ also has its inverse in H because $ey^{-1} = y^{-1} \in H$. Finally, for every two elements $x, y \in H$, since $y^{-1} \in H$, we have $x(y^{-1})^{-1}) = xy \in H$. So H is closed under multiplication. Therefore, H is a subgroup of G.

□

There are many special types of subgroups which are important in the study of groups. The first of these are subgroups which are invariant under conjugation by elements of the parent group. These are called *normal subgroups*, and if H is a normal subgroup of G, we denote this $H \lhd G$. Notice that it is not necessary for $gh = hg$ for all $h \in H$ and $g \in G$. There must simply exist $h, h' \in H$ satisfying $hg = gh'$ for all $g \in G$. Pre-multiplying by g^{-1} gives an equivalent definition of a normal subgroup – H is a normal subgroup of G if $g^{-1}hg \in H$ for all $g \in G, h \in H$. A group is said to be *simple* if its only normal subgroups are the trivial group and itself.

Let us now alter our perspective slightly and rather than having a conjugation condition that a subgroup must satisfy, we instead fix a subgroup and examine the elements that leave it invariant under conjugation. The *normaliser* $N_G(H)$ of a subgroup $H \leq G$ is the set of elements of G such that $ghg^{-1} \in H$ for all $g \in N_G(H)$ and $h \in H$.

We may strengthen this condition to consider group elements that fix all group elements under conjugation. The *centre* of a group G, denoted $Z(G)$ is the set of elements in G that commute with all other elements of G. The notation $Z(G)$ originates from the German word *zentrum*, meaning centre. The centre of a group is a normal subgroup of the parent group [29]. A similar concept is the *centraliser* $C_G(g)$ of a group element $g \in G$. It is the set of elements of G that commute with g. Notice that if G is Abelian, then the centre and the centraliser of any group element will be the entire group.

B.2.1 Generators A natural question that arises in the study of groups is whether we can write all of the elements of a group in terms of a smaller set of elements. This is the motivation for the notion of generators.

Definition B.7. Let G be a group. We say that G is *generated* by a set of elements $S \subseteq G$ if every element of G can be written as the product of elements of S and their inverses. We call the elements of S *generators* for G and write $G = \langle S \rangle$.

We say a group is *cyclic* if it is generated by a single element. For example, the group of the integers with addition modulo n is generated by any integer in the group which is coprime to n. If we have an element g of a group G, we define the set generated by g by $\langle g \rangle = \{g^k \mid g \in \mathbb{Z}\}$ [29].

Proposition B.8. *Let G be a group. Then for any element $g \in G$, $\langle g \rangle$ is a cyclic subgroup of G.*

Proof. Firstly, $\langle g \rangle$ is non empty, since $g \in \langle g \rangle$. Since G is closed under multiplication and taking inverses, $\langle g \rangle$ is a subset of G. Also note that the elements of $\langle g \rangle$ are of the form g^k for some integer k. By Proposition B.6, we only need prove that $xy^{-1} \in \langle g \rangle$ for all $x, y \in \langle g \rangle$. We have $xy^{-1} = g^k(g^m)^{-1} = g^{k-m} \in \langle g \rangle$ as required. □

As an example, $\langle 3 \rangle = \{3, 6, 9, 0\}$ is a subgroup of $\mathbb{Z}_{12}$. As we will see in Section B.4.2, we may think of the collection of cyclic groups of order n as being equivalent, because we can define a structure preserving bijective map between cyclic groups.

B.2.2 Direct Products Suppose G and H are groups. We define the *direct product* $G \times H$ as the set of ordered pairs (g, h) such that $g \in G$ and $h \in H$.

Proposition B.9. *The set $G \times H$ is a group with componentwise multiplication.*

Proof. * The identity of the group is (e_G, e_H) because for any $(g, h) \in G \times H$, $(e_G, e_H) \cdot (g, h) = (e_G g, e_H h) = (g, h)$. In addition, $G \times H$ is closed under componentwise multiplication and associative because G and H are. Finally, the inverse of any element $(g, h) \in G \times H$ is (g^{-1}, h^{-1}). □

The smallest example of a direct product of groups is the Klein-four group, which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. We can think of this group as being generated by two elements a and b of order 2. Its multiplication table is given below.

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Table B.1: The multiplication table for the Klein-four group.

B.3 Cosets and Quotients

The concept of cosets in group theory was first formulated by Galois in 1830 [29]. They are an important notion that leads us to one of the most important results in finite group theory, Lagrange's Theorem.

Suppose H is a subgroup of a group G, and let $g \in G$. We define $gH = \{gh \mid h \in H\}$ to be a *left coset* of H and $Hg = \{hg \mid h \in H\}$ to be a *right coset* of H. Notice that any statement we prove about right cosets is also true of left cosets by using an analogous argument.

We now state some basic properties about cosets.

Proposition B.10. *Suppose H is a subgroup of G and $x, y \in G$. Then:*

i) $x \in Hx$

ii) $|Hx| = |Hy|$

iii) $Hx = H$ *if and only if* $x \in H$

iv) The set of right cosets partition G.

Proof. i): We have $x = ex \in Hx$, since H is a group and so must contain the identity.
ii): To prove that Hx and Hy have the same size, we simply define a bijection between them. Define

$$f : Hx \longrightarrow Hy$$

by

$$hx \longmapsto hy$$

for all $h \in H$. This is clearly onto because the preimage of any element $hy \in Hy$ is hx. Suppose that $f(hx) = f(h'x)$ for some $h, h' \in H$. Then by the definition of f, we have $hy = h'y$ and multiplying on the right by the inverse of y gives $h = h'$. Therefore, f is a bijection and $|Hx| = |Hy|$.
iii): Firstly, assume that $Hx = H$. Then, $x = 1\dot{x} = h$ for some $h \in H$ and therefore $x \in H$. Conversely, suppose that $x \in H$. Then, since H is a group, it is closed under multiplication and $hx \in H$ for all $h \in H$. So $Hx \subseteq H$. Furthermore, since $x \in H$, we have $hx^{-1} \in H$ for all $h \in H$. So multiplying on the right by x gives us $h \in Hx$ and therefore $Hx = H$.
iv) Firstly, any element $x \in G$ is contained in Hx by i) and so the cosets cover the whole of G. Suppose there exist two cosets Hx and Hy such that $Hx \cap Hy \neq \varnothing$. Let $g \in Hx \cap Hy$. Then there exist elements $h_1, h_2 \in H$ such that $h_1 x = g = h_2 y$. Rearranging, $x = h_1^{-1} h_2 y$ and $y = h_2^{-1} h_1 x$. So any element of Hx is of the form $h h_1^{-1} h_2 y \in Hy$ for some $h \in H$ and therefore $Hx \subseteq Hy$. Similarly, any element of Hy is of the form $h h_2^{-1} h_1 x \in Hx$ for some $h \in H$. Thus $Hy \subseteq Hx$ and so $Hx = Hy$. □

Theorem B.11 (Lagrange's Theorem)**.** *Suppose G is a finite group and H is a subgroup of G. Then the order of H divides the order of G. Furthermore, the number of distinct right cosets of H in G is $|G|/|H|$.*

Proof. Let $Hg_1, Hg_2 \dots Hg_k$ be all of the distinct left cosets of H. Then for all $g \in G$, $Hg = Hg_i$ for some $i \in \{1, 2, \dots k\}$. Also recall that $g \in Hg$ for all $g \in G$. So $G = Hg_1 \cup Hg_2 \cup \cdots \cup Hg_k$. Since the cosets of H partition G, they are disjoint. So $|G| = |Hg_1| + |Hg_2| + \cdots + |Hg_k|$. By Proposition B.10, every coset has the same size. So since H is one of the cosets, $|G| = k|H|$. □

The *index* of a subgroup H in the parent group G, denoted $|G : H|$ is defined as the order of G divided by the order of H. A direct corollary of Lagrange's Theorem is that the index $|G : H|$ will always be an integer.

Proposition B.12. *If H is a subgroup of G of index two, then H is a normal subgroup of G.*

Proof. Consider the left cosets of H in G. Since the set of cosets partition G, and H has index two, there must be exactly two left cosets, H and gH for some $g \in G \setminus H$. Similarly, there must be only two right cosets of H, namely H and Hg. So $gH = Hg$ and there exist $h, h' \in H$ such that $gh = h'g$ and so H is a normal subgroup of G. □

Apart from being used to prove Lagrange's Theorem, cosets arise most frequently as elements of quotient groups. A *quotient group* is the set of all of the right cosets of a normal subgroup. The next proposition proves that this is indeed a group.

Proposition B.13. *Let G be a group and $H \trianglelefteq G$. The set $G/H := \{Hg \mid g \in G\}$ forms a group with binary operation defined by $(Hx)(Hy) = H(xy)$ for all $x, y \in G$.*

Proof. The set has identity H, since for all $x \in G$, $(H)(Hx) = H(e_G x) = Hx$ where e_G is the identity element of G. To prove associativity of G/H, consider $(Hx)(Hy)(Hz)$, for $x, y, z \in H$. Now, since G is associative, $((Hx)(Hy))(Hz) = (H(xy))(Hz) = H((xy)z) = H(x(yz)) = (Hx)(H(yz)) = (Hx)((Hy)(Hz))$. Next, we claim that the inverse of an element $Hx \in G/H$ is Hx^{-1}. We have $(Hx)(Hx^{-1}) = H(xx^{-1}) = H$, as required. Finally, since G is closed under multiplication, it is trivial that G/H is closed under multiplication. □

Perhaps the most natural example of a quotient group is $\mathbb{Z}/n\mathbb{Z}$, where the operation on both groups is addition. The resulting cosets (here using addition notation) are $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. Notice that if we have $k + n\mathbb{Z}$ for some $k \geq n$, we can split k up into $r + qn$, for $q, r \in \mathbb{Z}$, $0 \leq r < n$, and so $k + n\mathbb{Z} = (r + qn) + n\mathbb{Z}$. Since $n \in n\mathbb{Z}$, from Proposition B.10, $k + n\mathbb{Z} = r + n\mathbb{Z}$ and so is equivalent to one of the cosets listed earlier. The 'factoring out' by multiples of n is reminiscent of the group formed by $\mathbb{Z}_n$ under addition, and as we will see, the two have the same structure and are isomorphic.

The *derived subgroup* of a group G is the smallest normal subgroup of G such that G/N is Abelian. It is generated by all of the elements of G of the form $g^{-1}h^{-1}gh$ for $g, h \in G$. Elements in this form are called *commutators* of G. Notice that if G is Abelian, then the derived subgroup of G is the trivial group.

B.4 Homomorphisms and Isomorphisms

There are many groups that have the same algebraic structure but are presented to us differently. We say that such groups are *isomorphic* to each other. However, to begin to discuss isomorphisms in a formal sense, we must first introduce the notion of group homomorphisms.

B.4.1 Group Homomorphisms

Definition B.14. A *homomorphism* $\phi : G \to G'$ is a function between groups G and G' that preserves the group operation, i.e., $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$.

We define the *kernel* of a homomorphism ϕ, denoted $\mathrm{Ker}(\phi)$, to be the set of elements of G whose image under the homomorphism is the identity of G'. We now state some fundamental properties of homomorphisms.

Proposition B.15. *Suppose $\phi : G \to G'$ is a homomorphism between two groups G and G', and suppose $g \in G$.*
Then:

i) $\phi(e_G) = e_{G'}$,

ii) $\phi(g^k) = (\phi(g))^k$ *for all* $k \in \mathbb{Z}$.

iii) If the order of g is finite, then the order of $\phi(g)$ divides the order of g,

iv) The kernel of ϕ, denoted $\mathrm{Ker}(\phi)$ *is a normal subgroup of G.*

v) The image of ϕ, denoted $\mathrm{Im}(\phi)$*, is a subgroup of G'*

Proof. i): By the definition of a homomorphism, $\phi(g) = \phi(e_G g) = \phi(e_G)\phi(g)$ for all $g \in G$. Multiplying on the right by $(\phi(g))^{-1}$ on both sides (which exists because G' is a group), we have $e_{G'} = \phi(e_G)$ as required.
ii): This follows directly from the operation preserving property of the homomorphism. We have $\phi(g^k) = \underbrace{\phi(g)\phi(g)\dots\phi(g)}_{k \text{ times}} = (\phi(g))^k$.
iii): Suppose that the order of g is n, i.e., $g^n = e_G$. Then, by i) and ii), $(\phi(g))^n = \phi(g^n) = \phi(e_G) = e_{G'}$. So the order of $\phi(g)$ must divide n, which is the order of g.
iv): Firstly, by i), $\mathrm{Ker}(\phi)$ contains the identity of G. The kernel is associative because the property is inherited from G. Suppose $g \in \mathrm{Ker}(\phi)$. Then, from i) $e_{G'} = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = e_{G'}\phi(g^{-1}) = \phi(g^{-1})$. Therefore, every element in the kernel also has its inverse in the kernel. Finally, if $g, h \in \mathrm{Ker}(\phi)$, then $\phi(gh) = \phi(g)\phi(h) = e_{G'}$. Therefore, the kernel of ϕ is closed under multiplication and is therefore a group. Furthermore, it is a normal subgroup of G because for all $x \in G$ and $g \in \mathrm{Ker}(\phi)$, $\phi(x^{-1}gx) = \phi(x^{-1})\phi(g)\phi(x) = \phi(x^{-1})\phi(x) = e_{G'}$, so

$x^{-1}gx \in \text{Ker}(\phi)$.
v): Firstly, by i), $e_{G'} \in \text{Im}(\phi)$. The image of ϕ is associative because G' is associative. It is also closed because for every $\phi(g), \phi(h) \in \text{Im}(\phi)$, $\phi(g)\phi(h) = \phi(gh) \in \text{Im}(\phi)$ by the structure preserving property of ϕ. Finally, for $g \in G$, $e_{G'} = \phi(e_G) = \phi(gg^{-1} = \phi(g)\phi(g^{-1})$ and so $\phi(g)^{-1} = \phi(g^{-1}) \in \text{Im}(\phi)$. Therefore, $\text{Im}(\phi)$ is a subgroup of G'.

□

B.4.2 Isomorphisms Consider an Australian and a Frenchwoman counting baguettes. The Australian counts the baguettes saying "One, two, three ..." and so on, whereas the Frenchwoman counts "Un, deux, trois ...". Although these two people are counting in different languages, they are still completing the same task. Similarly, when the Australian says "four times four equals sixteen", and the Frenchwoman says "quatre multiplié par quatre égale seize", they are both conveying the same idea, just using different languages. In the same way, isomorphic groups have the same structure but are described with different 'terminology'.

Definition B.16. An *isomorphism* $\varphi : G \to G'$ between groups G and G' is a bijective homomorphism. When such an isomorphism exists, G and G' are said to be isomorphic, and we denote this by $G \cong G'$.

We define the kernel of an isomorphism analogously to the kernel of a homomorphism. Additionally, all of the properties described in Proposition B.15 also hold for isomorphisms, since isomorphisms are themselves homomorphisms.

The First Isomorphism Theorem relates all of the concepts described in this section. It was first described by Camille Jordan in 1870 [29].

Theorem B.17 (First Isomorphism Theorem)**.** *Let G be a group and $\phi : G \to G'$ be a homomorphism between groups G and G'. Then $G/\text{Ker}(\phi) \cong \text{Im}\phi$.*

Proof. Let $\varphi : G/\text{Ker}(\phi) \to \text{Im}\phi$ be defined by $\text{Ker}(\phi)g \mapsto \phi(g)$. We first check that this function is well-defined, i.e., if $\text{Ker}(\phi)g = \text{Ker}(\phi)h$ for some $g, h \in G$, then $\varphi(\text{Ker}(\phi)g) = \varphi(\text{Ker}(\phi)h)$. Suppose $\text{Ker}(\phi)g = \text{Ker}(\phi)h$. Then multiplying on the right by g^{-1} gives $\text{Ker}(\phi)hg^{-1} = \text{Ker}(\phi)$ and $hg^{-1} \in \text{Ker}(\phi)$. Then $\phi(hg^{-1}) = e_{G'}$. Since ϕ is a homomorphism, $\phi(h)\phi(g)^{-1} = e_{G'}$ and multiplying on the right by $\phi(g)$ gives $\phi(g) = \phi(h)$. Therefore, φ is well-defined. It is easy to see that the converse of the set of implications given to prove φ is well-defined also hold, and these prove that $\phi(g) = \phi(h) \Rightarrow \text{Ker}(\phi)g = \text{Ker}(\phi)h$. This shows that φ is injective. Moreover, φ is surjective because the preimage of any element $\phi(x) \in \text{Im}\phi$ is $\text{Ker}(\phi)x$. Finally, we need to check that φ is a homomorphism. We have $\varphi(\text{Ker}(\phi)g\text{Ker}(\phi)h) = \varphi(\text{Ker}(\phi)gh) = \phi(gh) = \phi(g)\phi(h) = \varphi(\text{Ker}(\phi)g)\varphi(\text{Ker}(\phi)h)$, as required. □

We apply the First Isomorphism Theorem to prove an intuitive result about cyclic groups.

Proposition B.18. *All cyclic groups of order n are isomorphic.*

Proof. Suppose $G = \langle g \rangle$ and $H = \langle h \rangle$ are cyclic groups of order n. Then, define $\phi : G \to H$ by $g^k \mapsto h^k$ for k in the range $0 \leq k < n$. We claim this is a homomorphism. Suppose $k, l \in \{0, 1, \ldots, n-1\}$ We have $\phi(g^k)\phi(g^l) = (h^k)(h^l) = h^{k+l} = \phi(g^{k+l})$ as required. Now, the kernel of ϕ is trivial because $\phi(g^k) = h^k = e_H \Rightarrow g^k = e_G$, because g and h have the same order. The image of ϕ is the whole of H because the preimage of $h^k \in H$ is g^k. Therefore, by the First Isomorphism Theorem, $G = G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi) = H$. □

Therefore, there is one cyclic group up to equivalence, and we denote it C_n.

An *automorphism* is an isomorphism from a group to itself. For our purposes, we will mostly consider automorphisms which permute elements of a set.

Sesquilinear and Quadratic Forms

Definition C.1. Suppose σ is an automorphism of a finite field $\mathrm{GF}(q)$. A *σ-sesquilinear form* of a vector space V over $\mathrm{GF}(q)$ is a map $\beta : V \times V \to \mathrm{GF}(q)$ such that for any $u, v, w \in V$ and $a, b \in \mathrm{GF}(q)$, β satisfies the following properties.

i) $\beta(u + v, w) = \beta(u, w) + \beta(v, w)$

ii) $\beta(u, v + w) = \beta(u, v) + \beta(u, w)$

iii) $\beta(au, bv) = ab^{\sigma}(u, v)$

Notice that the definition implies that σ-sesquilinear forms are linear in the first coordinate, but semilinear in the second. If σ is the identity automorphism, then clearly the corresponding σ-sesquilinear form is linear in both arguments and we call it a *bilinear form.*

A *quadratic form* $Q : V \to \mathrm{GF}(q)$ is a second degree homogeneous map.

When the characteristic of $\mathrm{GF}(q)$ is odd, we may use the quadratic form Q to define a symmetric bilinear form as follows

$$\beta_Q(u, v) = \frac{1}{2}(Q(u + v) - Q(u) - Q(v))$$

for $u, v \in V$. We may obtain a quadratic form back from a symmetric bilinear form β by simply letting $Q'(x) = \frac{1}{2}\beta(x, x)$. Notice that this does not apply when q is even because there is no well defined concept of a half.

A σ-sesquilinear form is said to be *degenerate* if there is a nonzero element $v \in V$ such that $\beta(v, w) = 0$ for all $w \in V$, and the vector v is called singular with respect to the form. A vector $v \in V$ is said to be *singular* with respect to a quadratic form if $Q(v + w) = Q(w)$ for all $w \in V$ [26]. Moreover, a form is *reflexive* if $\beta(v, w) = 0 \Leftrightarrow \beta(w, v) = 0$.

The following theorem was first proved by Brauer in [12], but is universally known as the Birkhoff-von Neumann theorem.

Theorem C.2 (Birkhoff and von Neumann [9])**.** *Suppose V is a vector space with dimension at least three. Then, up to a scalar multiple, a nondegenerate σ-sesquilinear reflexive form on V is one of the following types:*

i) ***alternating:*** *$\sigma = 1$ and $\beta(v, v) = 0$ for all $v \in V$.*

ii) ***Hermitian:*** *$\sigma^2 = 1$, $\sigma \neq 1$, and $\beta(u, v) = \beta(v, u)^{\sigma}$ for all $u, v \in V$.*

iii) ***symmetric:*** *$\sigma = 1$ and $\beta(u, v) = \beta(v, u)$.*

Furthermore, when GF(q) is a finite field with odd characteristic, there are exactly two equivalence classes of symmetric bilinear forms on a vector space V up to the choice of basis.[1].

Suppose $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ is a basis of a finite vector space V. Given a σ-sesquilinear form β, we can define a matrix $(M_\mathcal{B})_{ij} = \beta(b_i, b_j)$. Then $\beta(u, v) = [u]_\mathcal{B} M_\mathcal{B} [v]_\mathcal{B}^\top$ and $M_\mathcal{B}$ is called a *Gram matrix*.

A subspace W of a vector space V is said to be *totally isotropic* with respect to a σ-sesquilinear form when $\beta(u, v) = 0$ for all points $u, v \in W$, and *totally singular* with respect to a quadratic form when $Q(v) = 0$ for all points $v \in W$.

Theorem C.3 (Witt's Theorem)**.** *Suppose V and W are projective spaces equipped with non-singular forms f and g respectively, which are both either both reflexive sesquilinear forms or quadratic forms. Then any isometry from a subspace Y of V to a subspace Z of W can be extended to an isometry from V to W.*

A direct consequence of Witt's Theorem is that the isometry group of a non-singular reflexive sesquilinear or quadratic form f is transitive on totally isotropic subspaces of the same dimension. Another corollary of Witt's Theorem is that all maximal totally isotropic subspaces with respect to f have the same dimension, termed the *Witt index* of f.

Example C.4. *The two equivalence classes of symmetric bilinear forms on a $2n$-dimensional vector space are the plus type, which contains forms with Witt index n, and the minus type, which contains forms with Witt index $n - 1$ [69].*

[1] For further discussion, see [69].