University of Sussex

Luca Giuzzi

Hermitian varieties over finite fields

Thesis submitted for the award of the
degree of Doctor of Philosophy

November 2000

I hereby declare that this thesis has not been submitted, either in the same or different form, to this or any other University for a degree.

Signature:

Acknowledgements

This research work has been funded by an INDAM scholarship of the Italian 'Istituto Nazionale di Alta Matematica' and by a bursary of the Engineering and Physical Sciences Research Council, which covered tuition fees. I am most grateful to these organisations for their support.

Among the several people which have helped me during the work on this thesis I would like to explicitly thank my supervisor, Prof. J.W.P. Hirschfeld, both for his constant advice on the research and for having taught me how to write scientific prose. I would like to thank also Professors G. Korchmáros and A. Cossidente from Potenza for very helpful discussions on the topics investigated here.

I would like to express once more my gratitude towards my parents for their continuous support and understanding.

Finally, I wish to thank in a special way Jennifer Huynh for her kindness and our excellent friendship, and all the other people that, in one way or another, have been near me during all these years.

For Angling *may be said to be so much like the* Mathematicks*, that it can ne'er be fully learnt; at least not so fully, but that there will still be more new experiments left for the tryal of other men that succeed us.*

Izaak Walton, [WC76]

Summary

In this work, submitted for the award of the title of Doctor of Philosophy, we have investigated some properties of the configurations arising from the intersection of Hermitian varieties in a finite projective space.

Chapter 1 introduces some background material on the theory of finite fields, projective spaces, Hermitian varieties and classical groups.

Chapter 2 deals with the 2-dimensional case. In Section 2.1, we present the the point-line classification of the intersections, due to Kestenband. In Section 2.2, we determine the full linear collineation group stabilising any of the configurations of 2.1 and we prove that if two configurations have the same point-line structure, then they are in fact projectively equivalent. A new and simplified proof of the group theoretical characterization of the Hermitian curve as the unital stabilised by a Singer subgroup of order $q-\sqrt{q}+1$ closes the chapter in Section 2.3.

In **Chapter 3** we study the 3-dimensional case. In Section 3.1 we determine what incidence configurations fulfill the combinatorial properties required in order to be the intersection of Hermitian surfaces. Section 3.2 presents some further general remarks on linear systems of Hermitian curves and extensive computations on 4×4 Hermitian matrices. In Section 3.3, we produce models that realize all the possible intersection configurations in dimension 3.

Chapter 4 is organized in two independent sections. In Section 4.1 we provide a general formula to determine the list of possible sizes of Hermitian intersections in $\mathrm{PG}(n,q)$. The formula itself has been obtained by studying the geometry of the set $\mathscr{H}$ of all singular Hermitian hypersurfaces of $\mathrm{PG}(n,q)$. Such a set is endowed with the structure of an algebraic hypersurface of $\mathrm{PG}(n^2+2n,q)$ of degree $n+1$; the locus of the singular points of $\mathscr{H}$ is analyzed in detail. In Section 4.2 we introduce some computer code in order to explicitly compute the intersection configurations arising in $\mathrm{PG}(n,q)$.

Contents

List of Figures

List of Tables

Introduction

A projective space $\mathrm{PG}(n,q)$ admits at most three types of polarity: orthogonal, symplectic and unitary. The absolute points of an orthogonal polarity constitute a non-degenerate quadric in $\mathrm{PG}(n,q)$; for a symplectic polarity, all the points of $\mathrm{PG}(n,2^t)$ are absolute; the locus of all absolute points of a unitary polarity is a non-degenerate Hermitian variety.

Non-degenerate Hermitian varieties are unique in $\mathrm{PG}(n,q)$ up to projectivities. However, two distinct Hermitian varieties might intersect in many different configurations. Our aim in this thesis is to study such configurations in some detail.

In Chapter 1 we introduce some background material on finite fields, projective spaces, collineation groups and Hermitian varieties.

Chapter 2 deals with the two-dimensional case. Kestenband has proven that two Hermitian curves may meet in any of seven point-line configurations. In Section 2.1, we present this classification. In Section 2.2, we verify that any two configurations belonging to the same class are, in fact, projectively equivalent and we determine the linear collineation group stabilizing each of them. Such a group is usually quite large and is transitive on almost all the points of the intersection. A subset U of $\mathrm{PG}(2,q)$ such that any line of the plane meets U in either 1 or $\sqrt{q}+1$ points is called a *unital*. A Hermitian curve is a *classical unital*. However, there exist non-classical unitals as well. In Section 2.3 we present a short proof of a characterisation of the Hermitian curve as the unital stabilized by a Singer subgroup of order $q-\sqrt{q}+1$.

In Chapter 3, we describe the point-line-plane configurations arising in dimension 3 from intersecting two Hermitian surfaces. Our approach consists first in determining some combinatorial properties the configurations have to satisfy and then in actually constructing all the possible cases. Section 3.1 presents the list of all possible intersection classes; after some more technical results in Section 3.2, in Section 3.3 we construct linear systems of Hermitian surfaces yielding the wanted configurations for any class. In this chapter we deal with intersections which contain at least $\sqrt{q}+1$ points on a line.

Chapter 4 is divided into two independent sections: in Section 4.1 we study the determinantal variety of all the $(n+1)\times(n+1)$ Hermitian matrices as a hypersurface of $\mathrm{PG}(n^2+2n,\sqrt{q})$. From the study of such a variety we are able to determine the list of all possible intersection sizes for any dimension n. In Section 4.2 we present some computer code in order to produce pencils of Hermitian varieties in $\mathrm{PG}(n,q)$. This code, however, is able to provide useful results only for small values of n and q. Some possible improvements, both from the theoretic standpoint and the computational one, are suggested.

Chapter 1

Preliminary results

The aim of this first chapter is to recall some known results that will be used throughout the thesis.

1.1 Permutation Groups

Our main reference for the theory of finite permutation groups is [Wie64]. For general results on group theory, [Rob80] has been used.

1.1.1 Definitions

Definition 1.1.1. Let X be a non-empty set. A *permutation* of X is a bijective mapping of X into itself. The set of all permutations of X, together with map composition forms a group S_X, the *symmetric group* on X.

Definition 1.1.2. A *permutation group* G on a set X, or an X*-permutation group*, is any subgroup of S_X. The *degree* of a permutation group G is the cardinality of the set X it acts upon.

Definition 1.1.3. Let G be an X-permutation group and define † as the equivalence relation on X given by

$$x \dagger y \iff \exists \sigma \in G : x = \sigma(y).$$

The equivalence classes of † are the *orbits of* G *on* X. The orbit of any $x \in X$ will be denoted by the symbol x^G.

1.1.2 Transitivity and regularity

Definition 1.1.4. A permutation group G is *transitive* on X if and only if it has only one orbit, namely X itself.

Definition 1.1.5. For any X-permutation group G and for any $Y \subseteq X$, the *stabilizer* of Y in G is the set

$$St_G(Y) := \{\sigma \in G : \forall y \in Y : \sigma(y) \in Y\}.$$

A group G is *semi-regular* if for any $x \in X$, $St_G(x) = 1$; G is *regular* if it is semi-regular and transitive.

Definition 1.1.6. Let n be a positive integer. A permutation group G is 1-transitive on X if and only if it is transitive on X. A group G is *n-transitive* on a set X if and only if for any $x \in X$, $St_G(x)$ is $(n-1)$-transitive on $X \setminus \{x\}$.

Lemma 1.1.7. *Assume that G is a n-transitive group on X. Then,*

(i) *for any $x \in X$, $St_G(x)$ is $(n-1)$-transitive on $X \setminus \{x\}$;*

(ii) *given two tuples $l_x = (x_1, \ldots, x_n)$, $l_y = (y_1, \ldots, y_n)$ of elements of X, there exists a permutation $\sigma \in G$ such that $\sigma(l_x) = l_y$.*

Definition 1.1.8. A group G is *strictly* n-transitive on X if it is n-transitive and, given any two different n-tuples l_x, l_y of distinct elements of X, there exists exactly one $\sigma \in G$ such that $\sigma(l_x) = l_y$.

Lemma 1.1.9. *Let G be a permutation group on a set X. Then, for any $x \in X$,*

$$|G| = |x^G||St_G(x)|.$$

1.1.3 Similarities

Definition 1.1.10. Let G be an X-permutation group and H be a Y-permutation group. A *similarity* between G and H is a pair (α, β), where

(i) α is an isomorphism between G and H;

(ii) β is a bijection between X and Y;

(iii) for any σ in G and for any $x \in X$,

$$\beta(x^\sigma) = (\beta(x))^{\alpha(\sigma)}.$$

Two permutation groups are *similar* if there is a similarity between them.

The sets X and Y have to be isomorphic in order for G and H to be similar; still, $|X| = |Y|$ and $G \simeq H$ is not sufficient for G and H to be similar.

1.1.4 Actions and representations

Definition 1.1.11. Let G be a group and let X be a non-empty set. A *right action* of G on X is a function $\rho : X \times G \to X$ such that

$$\rho(x, g_1 g_2) = \rho(\rho(x, g_1), g_2).$$

In an analogous way, a *left action* of G on X is defined as a function $\lambda : G \times X \to X$ such that

$$\lambda(g_1 g_2, x) = \lambda(g_1, \lambda(g_2, x)).$$

Definition 1.1.12. Let G be any group and let X be a set. Any group homomorphism $\gamma : G \to S_X$ is a *permutation representation* of G on X and it induces a right action on X via the mapping $(x, g) \to \gamma(g)x$.

The cardinality of X is the *degree* of the representation γ. If $\ker \gamma = \{1\}$, then the representation is *faithful*; a representation is *transitive* if its image in S_X is transitive; γ is regular if its image in S_X acts regularly on X.

1.2 Finite fields

The reference text for most of the definitions and results presented in this section is [LN97].

1.2.1 Definitions and models

Definition 1.2.1. A ring $(R, +, \cdot)$ is an *integral domain* if, for all $x, y \in R$, $xy = 0$ implies $x = 0$ or $y = 0$; if $(R \setminus \{0\}, \cdot)$ is a group, then the ring R is a *division ring*. A division ring R in which the group $R^\star = (R \setminus \{0\}, \cdot)$ is Abelian is a *field*; a division ring in which the group $R^\star$ is non-commutative is a *skew-field*.

Theorem 1.2.2 (Wedderburn, 1905)**.** *Every finite division ring is a field.*

Definition 1.2.3. The *characteristic* of a ring $(R, +, \cdot)$ is the smallest positive integer $\text{char}(R) = n$ such that for all $r \in R$:

$$nr := \underbrace{r + \ldots + r}_{n \text{ times}} = 0.$$

If no such an n exists, R is said to have *characteristic* 0.

Definition 1.2.4. A *subfield* K of a field $(F, +, \cdot)$ is a subset of F which is closed under the field operations. The field $(F, +, \cdot)$ is called an *extension (field)* of $(K, + |_K, \cdot |_K)$. The symbol $K \leq F$ is used to denote that F is an extension field of K or, equivalently, that K is a subfield of F.

Any field contains itself, the empty set and the set consisting of its zero only as subfields. Those subfields are called *trivial*.

Definition 1.2.5. A field is *prime* if it does not contain any proper subfield.

Lemma 1.2.6. *Any subfield has the same characteristic as its parent field.*

Definition 1.2.7. Let K be a subfield of F and assume $f \in F$. The *extension of K by f* is the smallest subfield $K(f)$ of F such that,

$$K \cup \{f\} \subseteq K(f) \subseteq F.$$

Definition 1.2.8. Given a field K, its *algebraic closure* $\overline{K}$ is the smallest field containing K such that any polynomial

$$\sum_{i=0}^{n} k_i x^i \in K[x]$$

splits to linear factors in $\overline{K}[x]$.

Lemma 1.2.9. *Let $\mathbb{Z}$ be the ring of integers, p a prime number and let $p\mathbb{Z}$ be the ideal generated by p in $\mathbb{Z}$; then, $\mathbb{Z}/(p\mathbb{Z})$ is a finite field containing p elements.*

Proof. Let $F_p := \{0, \ldots, p-1\} \subset \mathbb{Z}$, and let ϕ be the projection mapping

$$\phi : \begin{cases} F_p & \rightarrow & \mathbb{Z}/(p\mathbb{Z}) \\ x & \rightarrow & x + (p\mathbb{Z}). \end{cases}$$

Define, for any $b, c \in F$,

$$b + c := \phi^{-1}(\phi(b+c)); \qquad b \cdot c := \phi^{-1}(\phi(bc)).$$

The structure $(F_p, +, \cdot)$ is closed under its operations and every non-zero element admits an inverse. It follows that F is a field. □

Definition 1.2.10. The field $(F_p, +, \cdot)$ constructed in the previous lemma is called the *Galois field with p elements*. It will be denoted by the symbol

$$\mathrm{GF}(p) := (F_p, +, \cdot).$$

Definition 1.2.11. Let $(F, +, \cdot)$ and $(G, \oplus, \odot)$ be two fields. A *morphism* between F and G is a mapping $\phi : F \rightarrow G$ preserving the algebraic structure; that is, for all $p, q \in F$:

(i) $\phi(p^{-1}) = \phi(p)^{-1}$,

(ii) $\phi(-p) = \ominus\phi(p)$,

(iii) $\phi(pq) = \phi(p) \odot \phi(q)$,

(iv) $\phi(p+q) = \phi(p) \oplus \phi(q)$.

A necessary condition for a morphism to exist between two fields F and G is that $\mathrm{char}(F) = \mathrm{char}(G)$.

Monomorphisms, epimorphisms, isomorphisms and automorphisms are defined the usual way.

Theorem 1.2.12. *Any field K contains a prime subfield F which is either isomorphic to the field of the rational numbers $\mathbb{Q}$ or to $\mathrm{GF}(p)$ for some prime p, according as the characteristic of K is 0 or p.*

Theorem 1.2.13. *Let F be a finite field. Then, the cardinality of F is p^n, where $p = \mathrm{char}(F)$ is a prime number and n is an integer. The integer n is called the* degree *of F over its prime field.*

As a matter of fact, the converse is true as well.

Theorem 1.2.14. *For every prime p and for every integer n there exists a finite field F of order p^n. All fields of given order $q = p^n$ are isomorphic to the splitting field of the polynomial $(x^q - x)$ over $\mathrm{GF}(p)$. This field F will be written as*

$$\mathrm{GF}(q) := \mathrm{GF}(p)[x]/(x^q - x).$$

Definition 1.2.15. Given any finite field $(F, +, \cdot)$, its multiplicative group $F^\star$ is cyclic. A generator of $F^\star$ is a *primitive element* of F.

1.2.2 Automorphisms and extensions

Lemma 1.2.16. *Let F be a finite extension field of $\mathrm{GF}(q)$. Then, there exists an integer $m > 0$ such that $F = \mathrm{GF}(q^m)$. This integer is the* degree *of F over $\mathrm{GF}(q)$ and is written as*

$$[F : \mathrm{GF}(q)] := m.$$

Definition 1.2.17. Let $\mathrm{GF}(q^m)$ be an extension field of $\mathrm{GF}(q)$, and let $\alpha \in \mathrm{GF}(q^m)$. The elements $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ are called the *conjugates* of α with respect to $\mathrm{GF}(q)$.

Definition 1.2.18. An *automorphism of* $\mathrm{GF}(q^m)$ *over* $\mathrm{GF}(q)$ is a field automorphism of $\mathrm{GF}(q^m)$ which fixes all the elements of $\mathrm{GF}(q)$. The group of all these automorphisms is the *Galois group* of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ and it is denoted by the symbol

$$\mathrm{Gal}(\mathrm{GF}(q^m) : \mathrm{GF}(q)).$$

Lemma 1.2.19. *For any $t \in \mathrm{GF}(q)$,*

$$t^q - t = 0.$$

Theorem 1.2.20. *The elements of* $\mathrm{Gal}(\mathrm{GF}(q^m) : \mathrm{GF}(q))$ *can be described as the automorphisms* $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ *given by*

$$\sigma_j : \begin{cases} \mathrm{GF}(q^m) & \rightarrow & \mathrm{GF}(q^m) \\ x & \rightarrow & \sigma_j(x) = x^{q^j}. \end{cases}$$

The automorphism σ_1 *which generates the Galois group is called the* Frobenius automorphism.

Lemma 1.2.21. *Let* K *be a field and let* σ *be one of its automorphisms. Then, the set* $\mathrm{Fix}_K\,\sigma$ *is a subfield of* K. *This subfield is called the* fixed field of σ in K.

Corollary 1.2.22. *The following equality holds:*

$$|\,\mathrm{Gal}(\mathrm{GF}(q^m)) : \mathrm{GF}(q))| = m = [\mathrm{GF}(q^m) : \mathrm{GF}(q)].$$

Definition 1.2.23. An automorphism σ is *involutory* if

(i) σ is not the identity;

(ii) σ^2 is the identity.

For any prime-power q, the field $F = \mathrm{GF}(q^2)$ admits one and only one non-identity automorphism over $\mathrm{GF}(q)$, namely the mapping sending $x \rightarrow x^q$. Since $|\,\mathrm{Gal}(F : \mathrm{GF}(q))| = 2$, this is an involutory automorphism of F.

Lemma 1.2.24. *Let* K *be a field and let* σ *be an involution of* K. *Then, there exist a subfield* $K' \leq K$ *and an element* $i \in K$ *such that,*

(i) $[K : K'] = 2$*;*

(ii) K' *is fixed by* σ*;*

(iii) $K = K'(i)$.

1.2.3 Trace and norm

Let F and K be finite fields with $K \leq F$. From Theorem 1.2.14, it is possible to assume without loss of generality that $F = \mathrm{GF}(q^m)$, $K = \mathrm{GF}(q)$ with q, m integers and q a prime power.

Definition 1.2.25. The *trace over* K of an element $x \in F$ is given by

$$\mathfrak{T}_{F/K}(x) := \sum_{\sigma \in \mathrm{Gal}(F:K)} \sigma(x) = x + x^q + \ldots + x^{q^{m-1}}.$$

The trace of x over the prime subfield of F is the *absolute trace* of x and is simply denoted as $\mathfrak{T}_F(x)$.

Theorem 1.2.26. *For any $x, y \in F$ and $f, g \in K$, the trace $\mathfrak{T}_{F/K}$ satisfies the following properties.*

(i) $\mathfrak{T}_{F/K}(x+y) = \mathfrak{T}_{F/K}(x) + \mathfrak{T}_{F/K}(y)$;

(ii) $\mathfrak{T}_{F/K}(fx) = f\mathfrak{T}_{F/K}(x)$;

(iii) $\mathfrak{T}_{F/K}$ *is a linear transformation from F onto K, where both F and K are viewed as vector spaces over K;*

(iv) $\mathfrak{T}_{F/K}(f) = mf$;

(v) $\mathfrak{T}_{F/K}(x^q) = \mathfrak{T}_{F/K}(x)$.

Theorem 1.2.27. *Let K be a finite field, and let F a finite extension of K. The linear transformations from F into K, both seen as vector spaces over K, are exactly the mappings L_t for $t \in F$ given by*

$$L_t : \begin{cases} F & \to & K \\ x & \to & \mathfrak{T}_{F/K}(tx). \end{cases}$$

Also, $L_t \neq L_{t'}$ when $t \neq t'$.

Theorem 1.2.28 (Composition of traces)**.** *Assume $K \leq F \leq E$ to be all finite fields. Then, for any $x \in E$,*

$$\mathfrak{T}_{E/K}(x) = \mathfrak{T}_{F/K}(\mathfrak{T}_{E/F}(x)).$$

Definition 1.2.29. The *norm over K* of an element $x \in F$ is given by

$$\mathfrak{N}_{F/K}(x) := \prod_{\sigma \in \mathrm{Gal}(F:K)} \sigma(x) = x^{(q^m-1)/(q-1)}.$$

The norm of x over the prime subfield of F is the *absolute norm* of x and is simply denoted by $\mathfrak{N}_F(x)$.

Theorem 1.2.30. *For any $x, y \in F$ and $f, g \in K$, the norm $\mathfrak{N}_{F/K}$ satisfies the following properties.*

(i) $\mathfrak{N}_{F/K}(xy) = \mathfrak{N}_{F/K}(x)\mathfrak{N}_{F/K}(y)$;

(ii) $\mathfrak{N}_{F/K}$ *maps F onto K and $F^\star$ onto $K^\star$;*

(iii) $\mathfrak{N}_{F/K}(f) = f^m$;

(iv) $\mathfrak{N}_{F/K}(x^q) = \mathfrak{N}_{F/K}(x)$.

Theorem 1.2.31 (Composition of norms)**.** *Assume $K \leq F \leq E$ to be all finite fields. Then, for any $x \in E$:*

$$\mathfrak{N}_{E/K}(x) = \mathfrak{N}_{F/K}(\mathfrak{N}_{E/F}(x)).$$

1.3 Projective spaces

Good references for the results presented in this section are [Dem68], [KSW73] and [BR98].

1.3.1 Incidence structures

Definition 1.3.1. A triple (P, L, I) is a *linear space* if

(i) P, L are non-empty sets;

(ii) I is a symmetric relation on $(P \times L) \cup (L \times P)$;

(iii) for all distinct $x, y \in P$ there exists exactly one element $l := xy$ of L such that $(x, l) \in I$ and $(y, l) \in I$.

The elements of P are the *points* of (P, L, I); those of L are called the *lines* of the incidence structure. The relation I is named *incidence relation*.

Definition 1.3.2. In a linear space (P, L, I) two lines l, m *intersect* if there exist a point $x \in P$ such that $(x, l) \in I$ and $(x, m) \in I$. The notation

$$l \cap m := \{x \in P : (x, l) \in I \text{ and } (x, m) \in I\}$$

will be used.

Definition 1.3.3. Three distinct points x, y, z in a linear space (P, L, I), are called *collinear* if $(x, yz) \in I$.

Definition 1.3.4. A mapping ϕ from a linear space (P, L, I) to a linear space (P', L', I') is a *collineation* (or *isomorphism*) if

(i) $\phi(p) \in P'$, for all $p \in P$;

(ii) $\phi(l) \in L'$, for all $l \in L$;

(iii) ϕ is bijective on P;

(iv) the incidence relation is preserved, that is,

$$(p, l) \in I \iff (\phi(p), \phi(l)) \in I'.$$

Definition 1.3.5. Let (P, L, I) be a linear space. A subset U of P is a *linear set* if, given any two distinct points $x, y \in U$,

$$t \in xy \Rightarrow t \in U.$$

The fact that U is a linear subset of P is written as $U \leq P$.

Lemma 1.3.6. *Assume (P, L, I) to be a linear space. For any linear subset U of P, let*

(i) $L_U := \{l \in L : \exists\, x, y \in U$ *such that* $x \neq y, (x, l) \in I, (y, l) \in I\}$*;*

(ii) $I_U := I \mid_{U \times L_U \cup L_U \times U}$.

Then, (U, L_U, I_U) is a linear space.

Definition 1.3.7. Given two linear spaces (P, L, I) and (P', L', I'), we say that (P', L', I') is a *subspace of* (P, L, I) *with support* P' if

(i) $P' \leq P$;

(ii) $L' = L_{P'}$;

(iii) $I' = I_{P'}$.

Definition 1.3.8. Given a linear space (P, L, I) and a set $V \subseteq P$, the *linear set* $\overline{V}$ *spanned by* V is given by

$$\overline{V} := \bigcap\{T \leq P : V \subseteq T\}.$$

Lemma 1.3.9. *For any $V \subseteq P$, the linear set spanned by V is characterised as follows:*

$$\overline{V} := \{x \in P : \exists h, k \in V \text{ such that } h \neq k, (x, hk) \in I\}.$$

Definition 1.3.10. A *projective space* (P, L, I) is a linear space in which the following axioms are satisfied:

(i) (Veblen-Young) If $a, b, c, d \in P$ are distinct points, then

$$ab \cap cd \neq \emptyset \Rightarrow ac \cap bd \neq \emptyset;$$

(ii) any line is incident with at least three points;

(iii) there are at least two lines.

A *finite* projective space is a projective space in which the set of points is finite.

Definition 1.3.11. A *projective plane* (P, L, I) is a projective space in which any two lines intersect.

Definition 1.3.12. The *dimension* of a projective space $\mathfrak{P} = (P, L, I)$ is the number

$$\dim \mathfrak{P} := \inf\{|U| : U \subseteq P \text{ and } \overline{U} = P\} - 1.$$

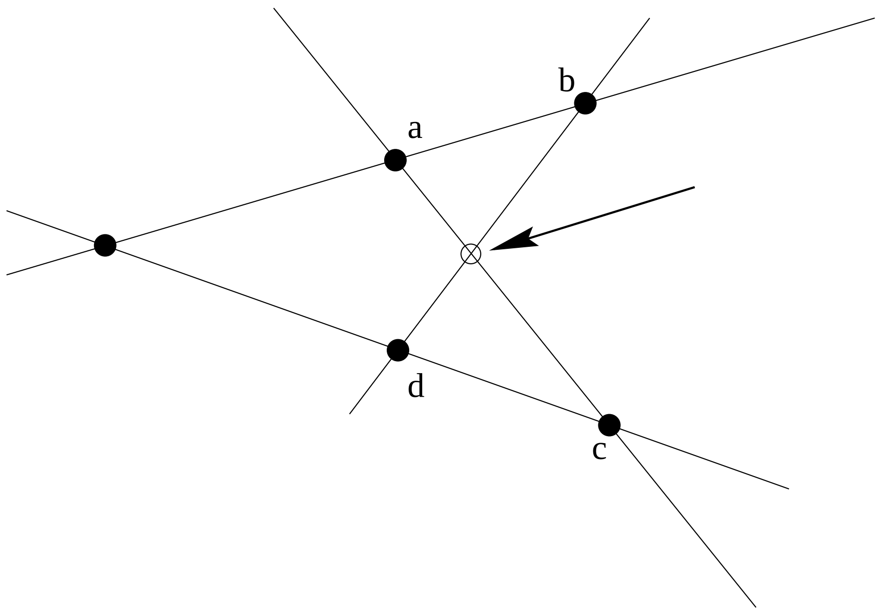


Figure 1.1: Veblen-Young configuration

Definition 1.3.13. Six distinct points x_i, y_i with $i \in \{1, 2, 3\}$ in a linear space (P, L, I) constitute a *Desargues configuration* if

(i) there exists $c \in P$ such that $(x_i, cy_i) \in I$ and $(y_i, cx_i) \in I$ for all i;

(ii) no three of the points c, x_1, x_2, x_3 and c, y_1, y_2, y_3 are collinear;

(iii) the points $p_{ij} := x_i x_j \cap y_i y_j$ are collinear.

Definition 1.3.14. A projective space (plane) $\mathfrak{P}$ is *Desarguesian* if, for any choice of six points satisfying (i) and (ii) of the Desargues configuration, condition (iii) holds.

Definition 1.3.15. Six distinct points g_i, h_i for $i \in \{1, 2, 3\}$ in a linear space (P, L, I) constitute the *Pappus configuration* if

(i) the g_i are all collinear;

(ii) the h_i are all collinear;

(iii) the line $G := g_1 g_2$ meets the line $H := h_1 h_2$ in a point c that is distinct from any of the g_i and any of the h_i;

(iv) given $q_{ij} := g_i h_j \cap g_j h_i$, then $(q_{12}, q_{13} q_{23}) \in I$.

Definition 1.3.16. A projective space (plane) $\mathfrak{P}$ is *Pappian* if, for any choice of six points satisfying conditions (i), (ii) and (iii) of Pappus configuration, condition (iv) holds as well.

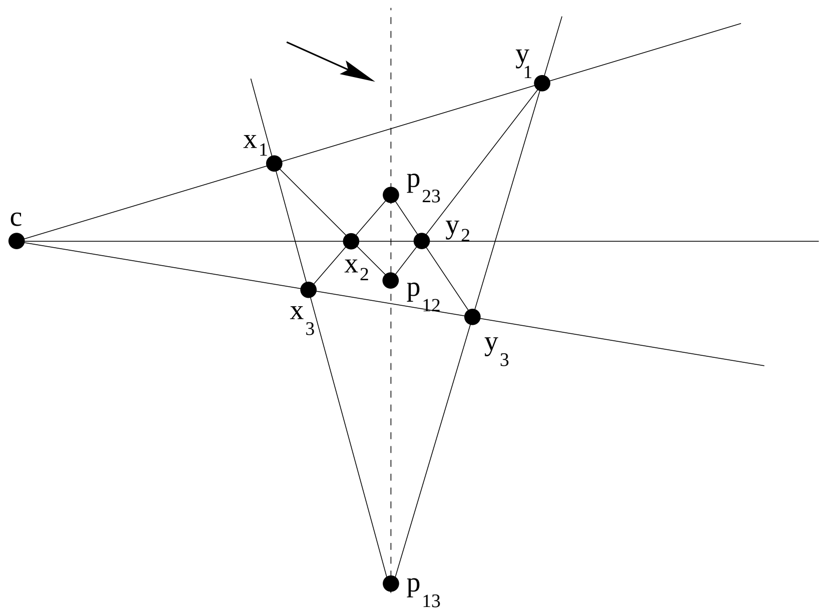


Figure 1.2: Desargues configuration

Theorem 1.3.17. *Any projective space of dimension at least* 3 *is Desarguesian.*

Still, there exist non-Desarguesian projective planes.

Theorem 1.3.18 (Hessenberg)**.** *A finite projective plane* $\mathfrak{P}$ *is Pappian only if it is Desarguesian.*

1.3.2 Algebraic constructions

Theorem 1.3.19. *Let* K *be a division ring and let* V *be a (left) vector space over* K *of dimension* $n \geq 3$*. Then, the triple* $(P, L, \subseteq)$ *where*

(i) P *is the set of all* 1*-dimensional (left) vector subspaces of* V*,*

(ii) L *is the set of all* 2*-dimensional (left) vector subspaces of* V*,*

(iii) '$\subseteq$' *is the natural inclusion,*

is a Desarguesian projective space of dimension $n - 1$*.*

Definition 1.3.20. The symbol $\mathfrak{P}(V)$ is used to denote a projective space constructed from a vector space V as in Theorem 1.3.19.

Theorem 1.3.21 (Projective derivation of a vector space)**.** *Let* V *be a vector space of dimension* $n \geq 3$ *over a field* K*. Define*

(i) $\underline{0} := (0, \ldots, 0) \in V$*;*

(ii) $V^\star := V \setminus \{\underline{0}\}$*;*

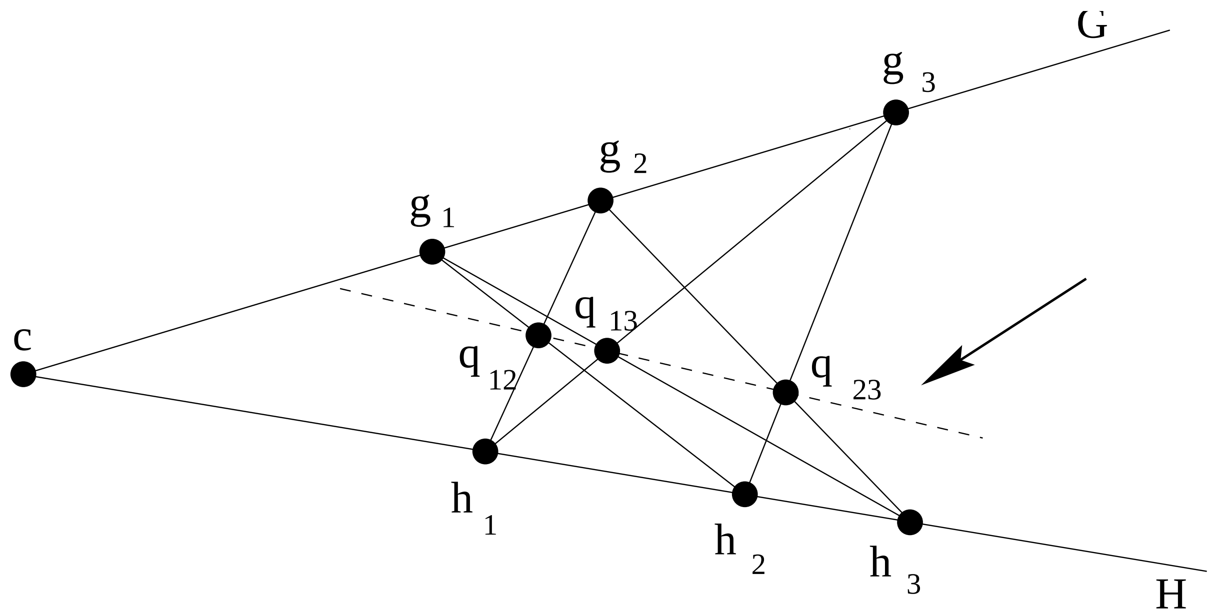


Figure 1.3: Pappus configuration

(iii) V_i *be the set of* i*-dimensional subspaces of* V*;*

(iv) $P := V^\star/K^\star := \{T \setminus \underline{0} : T \in V_1\}$*;*

(v) $L := \{\frac{X}{K^\star} : X \in V_2\}$.

Then, $\mathbb{P}V := (P, L, \in)$ *is a* $(n-1)$*-dimensional Pappian projective space which is isomorphic to* $\mathfrak{P}(V)$*.*

Definition 1.3.22. Let $\mathbb{P}V_n$ be the projective derivation of a vector space V of dimension n over a field K. Then, V is the *underlying vector space of* $(P, L, \in)$. The projection map

$$\mathbb{P} : \begin{cases} V^\star & \rightarrow & V^\star/K^\star \\ x & \rightarrow & [x] := K^\star x \end{cases}$$

is called the *projectivisation of* V.

Theorem 1.3.23. *Let* V *be a vector space over a division ring* K*; then* $\mathfrak{P}(V)$ *is Pappian if and only if* K *is a field.*

Definition 1.3.24. The symbol $\mathrm{PG}(n, K) := \mathbb{P}K^{n+1} \simeq \mathfrak{P}(K^{n+1})$ denotes the Pappian projective space obtained by projectivisation from a vector space of dimension $n+1$ over K.

Definition 1.3.25. Let $(P, L, I) = \mathrm{PG}(n, K)$ be a Pappian projective space. For any given t such that $-1 \leq t \leq n$, the symbol $\mathrm{PG}^t(n, K)$ denotes all projective subspaces of $\mathrm{PG}(n, K)$ with dimension t. In particular $\mathrm{PG}^{-1}(n, K) = \emptyset$, $\mathrm{PG}^0(n, K) = P$ and $\mathrm{PG}^n(n, K) = \{P\}$.

Theorem 1.3.26 (First representation theorem)**.** *Given any Desarguesian projective space P of dimension n, there exist a division ring K and a vector space V of dimension $n+1$ over K such that P is isomorphic to $\mathfrak{P}(V)$.*

Corollary 1.3.27. *Let P be a Pappian projective space of dimension n. Then, there exists a field K such that $P \simeq \mathrm{PG}(n, K)$.*

Proof. By Theorem 1.3.18, P is Desarguesian; Theorem 1.3.26 guarantees that $P = \mathfrak{P}(V)$, with V a vector space of dimension n over a division ring K; by Theorem 1.3.23, K is a field. Hence, $P \simeq \mathrm{PG}(n, K)$. □

Corollary 1.3.28. *Let P be a finite projective space of dimension at least 3. Then, P is Pappian.*

Proof. From Theorem 1.3.17, P is Desarguesian; hence, $P = \mathfrak{P}(V)$ for some vector space V over a finite division ring K; by Theorem 1.2.2, K is a field. It follows that P is isomorphic to $\mathrm{PG}(n, q) := \mathrm{PG}(n, K)$. Hence, P is Pappian. □

Theorem 1.3.29 (Tecklenburg)**.** *A Desarguesian finite plane is Pappian.*

This result can be proved as in Corollary 1.3.28 or in a more direct geometric way, as done in [Tec87]. Due to Theorem 1.3.23, this is equivalent to Wedderburn's result.

1.3.3 Morphisms

Definition 1.3.30. Let V be a vector space over a field K and let σ be an automorphism of K. A *semi-linear automorphism* of V with *companion automorphism* σ is a bijection θ from V into V such that, for all $x, y \in V$ and $g \in K$:

(i) $\theta(x + y) = \theta(x) + \theta(y)$;

(ii) $\theta(gx) = g^{\sigma}\theta(x)$.

Theorem 1.3.31 (Second representation theorem)**.** *For any collineation ϕ of a Desarguesian projective space $(P, L, I) = \mathfrak{P}(V)$, there exists a semi-linear automorphism θ of V that induces ϕ, in the sense that for all $x \in P$,*

$$\phi(x) := \{\theta(t) : t \in x\}.$$

Definition 1.3.32. Let $P = \mathfrak{P}(V)$ be a Desarguesian projective space. A *projectivity* of P is a collineation of P induced by a linear map of the underlying vector space V.

Definition 1.3.33. Let ϕ be a collineation of the projective space $\mathrm{PG}(n, K)$. A point $p \in \mathrm{PG}(n, K)$ is a *centre* of the collineation ϕ if

(i) $\phi(p) = p$;

(ii) any line L through p is fixed by ϕ.

A hyperplane H of $\mathrm{PG}(n, K)$ is an *axis* of the collineation ϕ if $\phi_{|H}$ is the identity.

Theorem 1.3.34. *A non-trivial collineation ϕ of $\mathrm{PG}(n, K)$ has at most one centre and one axis; furthermore, ϕ has a centre if and only if ϕ has an axis.*

Definition 1.3.35. A collineation ϕ is *central* (or *axial*) if it has a centre. A central collineation ϕ whose centre is incident with its axis is called an *elation*; if the centre of ϕ is not incident with its axis, then ϕ is called a *homology*.

Definition 1.3.36. The set of all collineations of the Pappian projective space $\mathrm{PG}(n, K)$ is denoted by the symbol

$$\mathrm{P\Gamma L}(n+1, K);$$

the set of all projectivities of $\mathrm{PG}(n, K)$ is written as

$$\mathrm{PGL}(n+1, K).$$

Theorem 1.3.37. *For all integers $n \geq 1$ and for all fields K, the set $\mathrm{P\Gamma L}(n+1, K)$ together with mapping composition constitutes a group. The set of all projectivities of $\mathrm{PG}(n, K)$ is a subgroup of $\mathrm{P\Gamma L}(n, K)$.*

Theorem 1.3.38. *Let K be a field, $n \geq 1$ and $\mathrm{GL}(n+1, K)$ be the group of all non-singular matrices of dimension $(n+1) \times (n+1)$ over K. Then,*

$$\mathrm{PGL}(n+1, K) \simeq \mathrm{GL}(n+1, K)/K^{\star}.$$

Definition 1.3.39. The stabilizer of a line of $\mathrm{PG}(n, K)$ in $\mathrm{PGL}(n+1, K)$ is the *affine linear group* $\mathrm{AGL}(n, K)$.

1.3.4 Singer cyclic groups

Singer cyclic groups have been introduced in [Sin38].

Definition 1.3.40. A *Singer cyclic group* of a projective space Π is a collineation group that is cyclic and transitive on the points of Π. A generator of a Singer cyclic group is a *Singer cycle*.

Definition 1.3.41. A projective space Π is *cyclic* if it admits a Singer cyclic group.

Lemma 1.3.42. *Any Desarguesian projective space $\mathrm{PG}(n, q)$ is cyclic.*

Lemma 1.3.43. *Any Singer cyclic group is transitive on the set of the lines of $\mathrm{PG}(2, q)$.*

Lemma 1.3.44. *Any Singer cycle of $\mathrm{PG}(n, q)$ is conjugate to a diagonal linear transformation in $\mathrm{PGL}(n+1, q^{n+1})$.*

1.4 Polynomials and matrices

The results in this section are taken from [Lan80] and [HH70].

1.4.1 Definitions

Definition 1.4.1. Let K be a field. By the symbol $\mathrm{Mat}(n, K)$ we denote the ring of all $n \times n$ matrices with entries in K. For any prime power q, the ring $\mathrm{Mat}(n, \mathrm{GF}(q))$ is written as $\mathrm{Mat}(n, q)$.

For any given matrix $M \in \mathrm{Mat}(n, K)$, we write its transposed matrix, obtained interchanging rows and columns of M, as $M^\star$.

Definition 1.4.2. Two matrices $A, B \in \mathrm{Mat}(n, K)$ are *equivalent* if there exist a matrix $C \in \mathrm{Mat}(n, K)$, such that

(i) $\det C \neq 0$;

(ii) $A = CBC^\star$.

Definition 1.4.3. Given any matrix $M \in \mathrm{Mat}(n, K)$, its *characteristic polynomial* $\mathcal{C}_M(x)$ is

$$\mathcal{C}_M(x) := \det(M - xI_n),$$

where I_n is the identity matrix in $\mathrm{Mat}(n, K)$.

Definition 1.4.4. For any matrix $M \in \mathrm{Mat}(n, K)$ and any polynomial $p(x) = \sum p_i x^i \in K[x]$, the *valuation* of $p(x)$ at M is

$$p(M) := \sum p_i M^i.$$

Lemma 1.4.5. *Let* $M \in \mathrm{Mat}(n, K)$*; the set*

$$J(M) := \{p \in K[x] : p(M) = 0\}$$

is an ideal of the ring $K[x]$.

Since $K[x]$ is a principal ideal domain, there exist a *generator element* for $J(M)$ that is unique up to multiplication by elements of $K^\star$.

Definition 1.4.6. The *minimal polynomial* of $M \in \mathrm{Mat}(n, K)$ is the monic generator $\mathcal{M}_M(x)$ of the ideal $J(M)$ of $K[x]$.

Lemma 1.4.7. *For any* $M \in \mathrm{Mat}(n, K)$,

(i) $\deg \mathcal{C}_M(x) = n$;

(ii) $\mathcal{C}_M(x) \in J(M)$*;*

(iii) $\mathcal{M}_M(x)$ *divides* $\mathcal{C}_M(x)$.

Definition 1.4.8. The *null space* of a matrix $M \in \mathrm{Mat}(n, K)$ is the set $\mathrm{Null}\, M$ of all vectors $x \in K^n$ such that

$$Mx^\star = \underline{0}.$$

Equivalently, the null space of M is the kernel of the homomorphism induced by M. The *null space of a polynomial* $p(x)$ *with respect to a matrix* M is the set

$$\mathrm{Null}_M\, p(x) := \{y \in K^n : p(M)y^\star = \underline{0}\}.$$

1.5 Varieties over finite fields

The few general algebraic geometry results presented in this section are from [Ful69]. References for the $\mathrm{GF}(q)$-case are [Hir98b] and our notes [Hir98a]; the conventions adopted are those of [Hir98b].

1.5.1 Polynomials as functions over projective spaces

For any field K, we shall denote by R_n the ring $R_n(K) := K[X_1, \dots, X_n]$ of polynomials in n indeterminates with coefficients in K. This ring is the free ring generated by the symbols $X_1, \dots, X_n$ over K.

Definition 1.5.1. Let K be a field; a *form* f *of degree* r in $n+1$ variables is a homogeneous polynomial $f \in K[X_0, \dots, X_n]$ of degree r.

Definition 1.5.2. We denote the set of all forms in $n+1$ variables over a field K by $\overline{R}_n(K) \subseteq K[X_0, \dots, X_n]$; the set of all forms in $n+1$ variables of given degree r over K is written as $\overline{R}^r_n(K)$.

Let $f \in \overline{R}_n(K)$ be a form, and let V be an $n+1$-dimensional vector space over K; for any vector $v = (v_0, \dots, v_n) \in V \simeq K^{n+1}$, the value of f at v is the scalar

$$f(v) := f(v_0, \dots, v_n).$$

Remark 1.5.3. Neither $\overline{R}_n(K)$ nor $\overline{R}^r_n(K)$ are subrings of $R_n[X_0]$, since the former is not closed under the sum and the latter under the product. On the other hand, $(\overline{R}_n(K)^\star, \cdot)$ is a monoid and $(\overline{R}^r_n(K) \cup \{0\}, +)$ is a group.

Lemma 1.5.4. *Let* $P = \mathrm{PG}(n, K) = \mathbb{P}K^{n+1}$ *be a projective space and consider a form* $f \in \overline{R}_n(K)$*. Then, for all* $v \in K^{n+1} \setminus \{\underline{0}\}$*,* $f(v) = 0$ *implies*

$$f(z) = 0, \textit{ for all } z \in \mathbb{P}v.$$

Proof. Since $z \in \mathbb{P}v$, there exists a $\lambda \in K^\star$ such that $z = \lambda v$. Denote by r be the degree of f; then,

$$f(\lambda v) = \lambda^r f(v) = 0.$$

□

1.5.2 Algebraic sets and ideals

Definition 1.5.5. Let K be a field and assume $\mathfrak{F} := \{f_1, \ldots, f_k\} \subseteq \overline{R}_n(K)$. The *set of zeros determined by* $\mathfrak{F}$ is

$$\mathfrak{V}(\mathfrak{F}) := \mathfrak{V}(f_1, \ldots, f_k) := \{\mathbb{P}v \in \mathbb{P}K^{n+1} : f_1(v) = f_2(v) = \ldots = f_k(v) = 0\}.$$

The *ideal of* $\mathfrak{F}$ *in* $R_n(K)$ is denoted by

$$\mathfrak{I}(\mathfrak{F}) := \mathfrak{I}(f_1, \ldots, f_k).$$

Lemma 1.5.6. *Let* $\mathfrak{F}, \mathfrak{F}' \subseteq \overline{R}_n(K)$*, with* $\mathfrak{I}(\mathfrak{F}) = \mathfrak{I}(\mathfrak{F}')$. *Then,*

$$\mathfrak{V}(\mathfrak{F}) = \mathfrak{V}(\mathfrak{F}').$$

Remark 1.5.7. Lemma 1.5.6 shows that the set $\mathfrak{V}(\mathfrak{F})$ does not depend on the list of forms $\mathfrak{F}$ but only on the ideal $\mathfrak{F}$ generates in $R_n(K)$.

Definition 1.5.8. Let K be a field and assume $\mathfrak{F} = \{f_1, \ldots, f_r\}$ to be a set of forms in $\overline{R}_n(K)$. The *projective variety defined by* $\mathfrak{F}$ is the pair

$$\mathcal{F}(\mathfrak{F}) := \mathcal{F}(f_1, \ldots, f_r) := (\mathfrak{V}(\mathfrak{F}), \mathfrak{I}(\mathfrak{F})).$$

The set $\mathfrak{I}(\mathfrak{F})$ is the *ideal* of $\mathcal{F}(\mathfrak{F})$.

Definition 1.5.9. The *intersection* of two varieties $\mathcal{F}(\mathfrak{F})$ and $\mathcal{F}(\mathfrak{G})$ is the projective variety

$$\mathcal{F}(\mathfrak{F}) \cap \mathcal{F}(\mathfrak{G}) := \mathcal{F}(\mathfrak{F} \cup \mathfrak{G}).$$

Definition 1.5.10. A *sub-variety* of a variety $\mathcal{F}(\mathfrak{F})$ is a projective variety $\mathcal{F}(\mathfrak{G})$ such that $\mathcal{F}(\mathfrak{G}) \cap \mathcal{F}(\mathfrak{F}) = \mathcal{F}(\mathfrak{G})$.

Lemma 1.5.11. *Let* $\mathcal{F}(\mathfrak{F})$ *and* $\mathcal{F}(\mathfrak{G})$ *be two projective varieties. Then,*

$$\mathcal{F}(\mathfrak{F}) \cap \mathcal{F}(\mathfrak{G}) = (\mathfrak{V}(\mathfrak{F}) \cap \mathfrak{V}(\mathfrak{G}), \mathfrak{I}(\mathfrak{F} \cup \mathfrak{G})).$$

Definition 1.5.12. Let $\mathfrak{F} = \{f_1, \ldots, f_r\} \subseteq \overline{R}_n(K)$ be a set of forms over a field K. A K-*rational point* of $\mathcal{F}(\mathfrak{F})$ is an element $\mathbb{P}v \in \mathfrak{V}(\mathfrak{F}) \cap \mathrm{PG}(n, K)$.

Let $\overline{K}$ denote the algebraic closure of K. A *point* of $\mathcal{F}(\mathfrak{F})$ is any $\mathbb{P}\,t \in \mathbb{P}\overline{K}^{n+1}$ such that $f(t) = 0$, for all $f \in \mathfrak{F}$. The set of all points of $\mathcal{F}(\mathfrak{F})$ is

$$\overline{\mathfrak{V}}(\mathfrak{F}).$$

For any subfield K' of K, a K'*-rational point* $\mathbb{P}\,t$ of $\mathcal{F}(\mathfrak{F})$ is a point of $\mathrm{PG}(n, K') \cap \mathfrak{V}(\mathfrak{F})$.

Definition 1.5.13. An *algebraic set* Y *in* $\mathrm{PG}(n,K)$ is a set of points of $\mathrm{PG}(n,K)$ such that there exists $\mathfrak{F} \subseteq \overline{R}_n(K)$, with

$$Y = \mathfrak{V}(\mathfrak{F}).$$

The *ideal of the set* Y is defined as

$$\tilde{\mathfrak{I}}(Y) := \mathfrak{I}(\mathfrak{F}).$$

1.5.3 Number of rational points: zeta functions

Definition 1.5.14. Let $X = \mathfrak{V}(\mathfrak{F})$ be a projective variety over a finite field $\mathrm{GF}(q)$. A point $\mathbb{P}\,t$ of X of *degree* i is a point that is $\mathrm{GF}(q^i)$-rational, but is not $\mathrm{GF}(q^j)$-rational for any $j < i$.

A *closed point of degree* i is a set

$$\overline{\mathbb{P}\,t} := \{\mathbb{P}\,t^{\sigma} : \sigma \in \mathrm{Gal}(\mathrm{GF}(q^i) : \mathrm{GF}(q))\} = \{\mathbb{P}\,t, \mathbb{P}\,t^{q}, \ldots, \mathbb{P}\,t^{q^{i-1}}\},$$

where $\mathbb{P}\,t$ is a point of X of degree i.

Definition 1.5.15. A *divisor* on a curve $X = \mathfrak{V}(\mathfrak{F})$ is an element of the free group generated by all its closed points.

The group of all divisors of X is written as $\mathrm{Div}(X)$.

Definition 1.5.16. A divisor D is a K*-divisor* if all its components are K-rational points.

Remark 1.5.17. A divisor D on a curve $X = \mathfrak{V}(\mathfrak{F})$ is a formal sum

$$D = \sum_{\mathbb{P}\,t \in \overline{\mathfrak{V}}(\mathfrak{F})} n_{\mathbb{P}\,t} \mathbb{P}\,t,$$

where

(i) $n_{\mathbb{P}\,t} \in \mathbb{Z}$;

(ii) $n_{\mathbb{P}\,t} = 0$, for all but a finite number of $\mathbb{P}\,t$;

(iii) if $\mathbb{P}\,t$ is a point of X of degree i, then $n_{\mathbb{P}\,t} = n_{\mathbb{P}\,t'}$, for all $\mathbb{P}\,t' \in \overline{\mathbb{P}\,t}$.

Definition 1.5.18. Let $X = \mathfrak{V}(\mathfrak{F})$ be a projective curve; its *zeta function* is the formal series

$$\zeta_X(T) := \sum_{D \in \mathrm{Div}_K(X)} T^{\deg(D)}.$$

Lemma 1.5.19. *For any projective curve* $X = \mathfrak{V}(\mathfrak{F})$ *defined over* $\mathrm{GF}(q)$*, let*

(i) N_i *be the number of points of* X *that are* $\mathrm{GF}(q^i)$*-rational;*

(ii) M_s *be the number of effective* $\mathrm{GF}(q)$*-divisors on* X *of degree* s*;*

(iii) *B_j be the number of closed points of degree j.*

Then,

(i)

$$\zeta_X(T) = 1 + \sum_{s=1}^{\infty} M_s T^s;$$

(ii)

$$N_i = \sum_{j|i} j B_j;$$

(iii)

$$\zeta_X(T) = \prod_{j=1}^{\infty} (1 - T^j)^{-B_j} = \exp(\sum_{i=1}^{\infty} N_i T^i / i).$$

1.5.4 Dimension and algebraic sets

Lemma 1.5.20. *The family of the algebraic sets of* $\mathrm{PG}(n, K)$ *is closed under finite union and intersection; both* $\emptyset$ *and* $\mathrm{PG}^0(n, K)$ *are algebraic sets.*

Definition 1.5.21. The *Zariski topology* on $\mathrm{PG}^0(n, K)$ is the topology whose open sets are the complements of algebraic sets.

Remark 1.5.22. Any sub-variety $\mathcal{F}(\mathfrak{G})$ of a projective variety $\mathcal{F}(\mathfrak{F})$ is closed in $\mathcal{F}(\mathfrak{F})$.

Definition 1.5.23. A non-empty subset Y of a topological space Ξ is *irreducible* if it cannot be expressed as the union $Y_1 \cup Y_2$ of two proper subsets, each one of which is closed in Y with the induced topology.

The empty set is *not* irreducible.

Definition 1.5.24. The *dimension* of a topological space Ξ is the supremum of all the integers i such that there exists a chain

$$Z_0 \subset Z_1 \subset \ldots \subset Z_n = \Xi$$

of distinct irreducible closed subsets.

Definition 1.5.25. The *dimension of a variety* $\mathcal{F}(\mathfrak{F})$ is the topological dimension of its point set $\mathfrak{V}(\mathfrak{F})$, when endowed with the Zariski topology.

Remark 1.5.26. The null form $0 \in \overline{R}_n(K)$ defines the projective variety

$$\mathcal{F}(0) := (\mathrm{PG}^0(n, K), \{0\}).$$

Its topological dimension is n, the same as the incidence dimension of $\mathrm{PG}(n, K)$. This is the only variety of dimension n in $\mathrm{PG}(n, K)$.

Definition 1.5.27. Let $\mathcal{F}(\mathfrak{F})$ be a variety. By

$$\mathcal{F}^r(\mathfrak{F})$$

we denote the set of all r-dimensional sub-varieties of $\mathcal{F}(\mathfrak{F})$.

Definition 1.5.28. An *hypersurface of* $\mathrm{PG}(n, K)$ is a projective variety of dimension $n-1$ in $\mathrm{PG}(n, K)$. A 3-dimensional projective variety is a *projective surface*; a 2-dimensional projective variety is a *projective curve*.

1.5.5 Non-singular varieties

Definition 1.5.29. Let $\mathfrak{F} = \{f_1, \ldots, f_k\} \subseteq \overline{R}_n(K)$. The *Jacobian matrix* associated to $\mathfrak{F}$ at a point $p \in K^{n+1}$ is the $k \times (n+1)$ matrix $J_{\mathfrak{F}}(p)$ given by

$$(J_{\mathfrak{F}}(p))_{i(j+1)} := \left.\frac{\partial F_i}{\partial X_j}\right|_p,$$

where

(i) $0 \le j \le n$;

(ii) $1 \le i \le k$;

(iii) $\partial F_i/\partial X_j$ is the formal derivative of F_i with respect to X_j.

Definition 1.5.30. A variety $\mathcal{F}(\mathfrak{F})$ is *non-singular at a point* $p \in \mathfrak{V}(\mathfrak{F})$ if the rank of its Jacobian matrix $J_{\mathfrak{F}}(p)$ at p is maximal, that is

$$\mathrm{rank} J_{\mathfrak{F}(p)} = (n - \dim \mathcal{F}(\mathfrak{F})).$$

A variety $\mathcal{F}(\mathfrak{F})$ is *non-singular* if it is non-singular at each of its points.

Definition 1.5.31. Assume $\mathbb{P}x$ to be a non-singular point of a variety $\mathcal{F}(\mathfrak{F})$. The *tangent space* to $\mathcal{F}(\mathfrak{F})$ at $\mathbb{P}x$ is the subspace of $\mathrm{PG}(n, K)$ generated by the points corresponding to the projection of the **rows** of the Jacobian matrix $J_{\mathfrak{F}}(x)$.

1.6 Unitary Groups

The results in this section are taken from [Die71] and from the notes of the 1999 Socrates Summer school [Kin99].

1.6.1 Definitions

Let V be a vector space over a field K and assume σ to be either an involution of K or the identity mapping; denote by K' the subfield of K fixed by σ.

Definition 1.6.1. A *sesquilinear form f defined on V* is a mapping $V \times V \to K$ such that, for any choice of x, x_1, x_2, y, y_1, y_2 in V and λ in K,

(i) $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$;

(ii) $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$;

(iii) $f(x\lambda, y) = \lambda^\sigma f(x, y)$;

(iv) $f(x, y\lambda) = f(x, y)\lambda$.

Definition 1.6.2. Let f and g be two sesquilinear forms which are respectively defined over the vector spaces X and Y. Then, f and g are *equivalent* if there exists an isomorphism T of X into Y such that, for any $x, y \in X$,

$$f(x, y) = g(Tx, Ty).$$

Definition 1.6.3. A sesquilinear form f defined on V is *non-degenerate* if, for any non-zero vector $x \in V$, there exists a vector $y \in V$ such that

$$f(x, y) \neq 0.$$

The form f is *reflexive* if, for any $x, y \in V$,

$$f(x, y) = 0 \iff f(y, x) = 0.$$

Definition 1.6.4. A sesquilinear form f is *Hermitian* if, for any $x, y \in V$,

$$f(x, y) = f(y, x)^\sigma.$$

From now on we assume f to be a sesquilinear form on V which is both non-degenerate and reflexive.

Definition 1.6.5. A transformation u of V *unitary with respect to the form f* is any bijective linear transformation of V which preserves f. That is, for any $x, y \in V$,

$$f(x, y) = f(u(x), u(y)).$$

Lemma 1.6.6. *The set of all transformations of V unitary with respect to the form f form a subgroup* $\mathrm{U}_f(n, K)$ *of the general linear group* $\mathrm{GL}(n, K)$.

Definition 1.6.7. Let θ be an automorphism of the field K. A *unitary semi-similarity of V (corresponding to the form f and the automorphism θ) of multiplier r_u* is a collineation $u : V \to V$ such that, for any $x, y \in V$,

$$f(u(x), u(y)) = r_u f(x, y)^{\theta}.$$

Lemma 1.6.8. *The set of all unitary semi-similarities of V forms a subgroup $\Gamma\mathrm{U}_f(n, K)$ of the group $\Gamma\mathrm{L}(n, K)$ of all collineations of V.*

Definition 1.6.9. A semi-similarity u is *linear* if the automorphism θ associated with u is the identity of K.

Lemma 1.6.10. *The set of all linear semi-similarities is a subgroup $\mathrm{GU}_f(n, K)$ of the general linear group $\mathrm{GL}(n, K)$; indeed,*

$$\mathrm{GU}_f(n, K) = \Gamma\mathrm{U}(n, K) \cap \mathrm{GL}(n, K).$$

Lemma 1.6.11. *Let f, g be two equivalent sesquilinear forms. Then, the unitary groups induced by f and g are all isomorphic; that is, $\mathrm{U}_f(n, K) \simeq \mathrm{U}_g(n, K)$, $\Gamma\mathrm{U}_f(n, K) \simeq \Gamma\mathrm{U}_g(n, K)$ and $\mathrm{GU}_f(n, K) \simeq \mathrm{GU}_g(n, K)$.*

Definition 1.6.12. Let α be in $K^\star$. The *dilation of V with coefficient α* is the mapping

$$h_\alpha : \begin{cases} V & \to & V \\ x & \to & x\alpha. \end{cases}$$

Lemma 1.6.13. *The set $H(n, K) := \{h_\alpha : \alpha \in K^\star\}$ of all dilations of V is a normal subgroup of $\Gamma\mathrm{L}(n, K)$.*

Definition 1.6.14. The group of all *projective collineations* of the projective space $\mathbb{P}V$, obtained by derivation from V, is the quotient group

$$\mathrm{P}\Gamma\mathrm{L}(n, K) := \Gamma\mathrm{L}(n, K)/H(n, K).$$

The canonical projection from $\Gamma\mathrm{L}(n, K)$ in $\mathrm{P}\Gamma\mathrm{L}(n, K)$ is denoted as

$$\mathbb{P} : \begin{cases} \Gamma\mathrm{L}(n, K) & \to & \mathrm{P}\Gamma\mathrm{L}(n, K) \\ x & \to & xH(n, K). \end{cases}$$

Definition 1.6.15. The projective collineation groups

$$\mathrm{P}\Gamma\mathrm{U}_f(n, K), \quad \mathrm{PGU}_f(n, K), \quad \mathrm{PU}_f(n, K)$$

are defined as the images in $\mathrm{P}\Gamma\mathrm{L}(n, K)$ via the projection $\mathbb{P}$ of

$$\Gamma\mathrm{U}_f(n, K), \quad \mathrm{GU}_f(n, K), \quad \mathrm{U}_f(n, K).$$

1.6.2 Subspaces and forms

Lemma 1.6.16. *A necessary and sufficient condition for the existence of a unitary transformation u, mapping a subspace $X \leq V$ into $Y \leq V$, is that the restriction of the form f to X is equivalent to the restriction of the* same *form f to Y.*

Definition 1.6.17. A subspace X of V is *orthogonal* to $Y \leq V$ *with respect to the form f* if and only if, for all $x \in X$ and $y \in Y$,

$$f(x, y) = 0.$$

The largest subspace of V orthogonal to X is denoted as

$$X^{\perp} := \{v \in V : \forall x \in X, f(v, x) = 0\}.$$

Definition 1.6.18. A space X is *isotropic* if $X \cap X^{\perp} \neq \{\underline{0}\}$; it is *totally isotropic* if $X \subseteq X^{\perp}$.

Definition 1.6.19. An *hyperbolic plane* X is a non-isotropic plane of V containing at least one isotropic vector.

Lemma 1.6.20.

(i) *If X and Y are two totally isotropic subspaces of V and* $\dim X = \dim Y$*, then there exists an $u \in \mathrm{U}_f(n, K)$, such that $u(X) = Y$.*

(ii) *There exists an integer ν such that any totally isotropic subspace of V is contained in a totally isotropic subspace of maximal dimension ν.*

Definition 1.6.21. A *quasi-symmetry* (with hyperplane H) is a unitary transformation u fixing point-wise a non-isotropic hyperplane H in V.

Definition 1.6.22. A *hyperbolic transformation* is a unitary transformation $u \in \mathrm{U}_f(n, K)$ fixing all vectors of a subspace $Y \leq V$ of dimension $n-2$ which is orthogonal to an hyperbolic plane.

Remark 1.6.23. The projective image $\mathbb{P}X$ of an hyperbolic plane X is a *hyperbolic line*. A *projective hyperbolic transformation* is, hence, a unitary transformation fixing all points belonging to a projective *hyperplane* $(\mathbb{P}X)^{\perp}$.

1.6.3 Hermitian groups

Definition 1.6.24. A Hermitian sesquilinear form g is a *trace form* if, for all $v \in V$, the element $g(v, v) \in K$ can be written as a trace over K'; that is, for any $v \in V$, there exists a $\lambda_v \in K$ such that

$$g(v, v) = \mathfrak{T}_{K/K'}(\lambda_v).$$

Lemma 1.6.25. *If the characteristic of K is not 2, then all Hermitian sesquilinear forms over K are trace forms. If K has characteristic 2, then the only trace forms are the alternating ones.*

Definition 1.6.26. The *standard Hermitian product* on the vector space V is the Hermitian sesquilinear form $\langle \cdot, \cdot \rangle$, given by

$$\langle \cdot, \cdot \rangle : \begin{cases} V \times V & \rightarrow & K \\ (u, v) & \rightarrow & \sum u_i v_i^{\sigma}. \end{cases}$$

For any Hermitian form g equivalent to the standard Hermitian product, the unitary groups $\mathrm{U}_g(n, K)$, $\mathrm{GU}_g(n, K)$, $\Gamma\mathrm{U}_g(n, K)$ and $\mathrm{PU}_g(n, K)$, $\mathrm{PGU}_g(n, K)$, $\mathrm{P}\Gamma\mathrm{U}_g(n, K)$, are denoted omitting the reference to g; that is, they are simply written as $\mathrm{U}(n, K)$, $\mathrm{GU}(n, K)$, $\Gamma\mathrm{U}(n, K)$ and $\mathrm{PU}(n, K)$, $\mathrm{PGU}(n, K)$, $\mathrm{P}\Gamma\mathrm{U}(n, K)$.

For any prime power q, the notation $\mathrm{U}(n, q) := \mathrm{U}(n, \mathrm{GF}(q))$ will be adopted as well.

1.6.4 Generators of the unitary group

Theorem 1.6.27. *Let f be a non-alternating symplectic form. Then, either the unitary group is $\mathrm{U}_f(n, K) = \mathrm{U}(2, 4)$, or $\mathrm{U}_f(n, K)$ is generated by the quasi-symmetries of $V \simeq K^n$.*

Theorem 1.6.28. *Let ν be the dimension of a maximal totally isotropic subspace X of V. Then,*

(i) *if $\nu \geq 1$, all the transformations in $\mathrm{U}_f(n, K)$ are products of hyperbolic transformations;*

(ii) *if $\nu \geq 1$ and $n \geq 3$, all non-isotropic lines are the intersection of two hyperbolic planes, except in the case where $\mathrm{U}_f(n, K)$ coincides with the orthogonal group $O(3, 3)$.*

1.6.5 Morphisms and automorphisms

Define $Z(n, K)$ as the centre of $\mathrm{GL}(n, K)$.

Lemma 1.6.29. *For any sesquilinear form f, the following isomorphism relations are satisfied:*

(i) $\mathrm{PGL}(n, K) \simeq \mathrm{GL}(n, K)/Z(n, K)$;

(ii) $\mathrm{P}\Gamma\mathrm{U}_f(n, K) \simeq \Gamma\mathrm{U}_f(n, K)/H(n, K)$;

(iii) $\mathrm{PGU}_f(n, K) \simeq \mathrm{GU}_f(n, K)/Z(n, K)$.

Theorem 1.6.30. *Suppose g to be a Hermitian form, let $n \geq 3$ and assume* char$K$ *to be odd. Then, all automorphisms of the unitary group $\mathrm{U}_g(n, K)$ can be written as*

$$\phi(u) = \chi(u) u^g,$$

where

(i) *$g \in \Gamma\mathrm{U}_g(n, K)$;*

(ii) *χ is an homomorphism of $\mathrm{U}_g(n, K)$ into its centre.*

Theorem 1.6.31 (Walter)**.** *Let K be a field of odd characteristic with more than 3 elements and assume $n \geq 5$. Then, any automorphism of the projective unitary group $\mathrm{PU}_f(n, K)$ is obtained from an automorphism of $\mathrm{U}_f(n, K)$ by way of quotienting.*

1.7 Hermitian Forms and Hermitian varieties

The main references for this section are [Seg67], [Seg65] and [Hir98b].

1.7.1 Hermitian matrices

Assume K to be a field with an involutory automorphism σ and let K' be the fixed field of σ in K.

Definition 1.7.1. Let $H \in \mathrm{Mat}(n, K)$. Then, H is

(i) *Hermitian with respect to the automorphism σ*, if

$$H^\star = H^\sigma;$$

(ii) *anti-Hermitian with respect to the automorphism σ*, if

$$H^\star = -H^\sigma;$$

(iii) *unitary with respect to the automorphism σ*, if

$$H^\sigma = (H^\star)^{-1};$$

(iv) *anti-orthogonal with respect to the automorphism σ*, if

$$H^\sigma = H^{-1}.$$

Lemma 1.7.2. *The conjugate of a Hermitian matrix via a unitary matrix is a Hermitian matrix.*

Lemma 1.7.3. *Let $H \in \mathrm{Mat}(n, K)$ be a Hermitian matrix; then, $\det H \in K'$.*

Proof. Since $\det H = \det H^\star$,

$$d := \det H = \det H^\star = \det H^\sigma = (\det H)^\sigma = d^\sigma.$$

Hence, $d \in \mathrm{Fix}_K(\sigma) = K'$. □

Definition 1.7.4. Let V be a vector space over K, and assume $H \in \mathrm{Mat}(n, K)$ to be a matrix, Hermitian with respect to the automorphism σ. The *σ-Hermitian form over V defined by H* is the form

$$h : \begin{cases} V \times V & \rightarrow & K \\ (x, y) & \rightarrow & x^\sigma H y^\star. \end{cases}$$

Lemma 1.7.5. *Assume q to be a square and let $H \in \mathrm{Mat}(n, q)$ be a Hermitian matrix. Then, αH is a Hermitian matrix for any $\alpha \in \mathrm{GF}(\sqrt{q})$.*

Definition 1.7.6. A polynomial $f(x)$ in $K[x]$ is *Hermitian* if and only if, for any integer n and any Hermitian matrix $H \in \mathrm{Mat}(n, K)$, $f(H)$ is a Hermitian matrix.

Remark 1.7.7. All polynomials with coefficients in the subfield K' of K are Hermitian.

Lemma 1.7.8. *The set of all Hermitian matrices of* $\mathrm{Mat}(n, q)$ *is a vector space of dimension* n^2 *over* $\mathrm{GF}(\sqrt{q})$.

Proof. A Hermitian H matrix can be given by providing the entries in its upper triangular part; any entry on the main diagonal, that is of the form H_{ii}, is an element of $\mathrm{GF}(\sqrt{q})$; entries above the main diagonal are elements of $\mathrm{GF}(q)$; hence, they have the form $a + \epsilon b$ with $a, b \in \mathrm{GF}(\sqrt{q})$ and ϵ a fixed element of $\mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$.

A direct count shows that exactly

$$n + 2(\frac{1}{2}n)(n-1) = n^2$$

choices of elements of $\mathrm{GF}(\sqrt{q})$ have to be made in order to determine H. □

Definition 1.7.9. Two matrices $A, B \in \mathrm{Mat}(n, K)$ are *Hermitian-equivalent* if there exists a non-singular matrix $C \in \mathrm{Mat}(n, K)$ such that

$$A = C^\sigma B C^\star.$$

Theorem 1.7.10 (Equivalence of Hermitian matrices). *Let $H \in \mathrm{Mat}(n, K)$ be a Hermitian matrix of rank $n - t$. Then, H is Hermitian-equivalent to a matrix J of the form*

$$J := \mathrm{diag}(j_0, \ldots, j_{n-t}, \underbrace{0, \ldots, 0}_{t \text{ times}}),$$

where $j_i \in K'$ for any i.

1.7.2 Hermitian forms

Lemma 1.7.11 (Representation theorem for Hermitian forms). *Let V be a vector space of dimension n over the field K and let H be a Hermitian matrix in* $\mathrm{Mat}(n, K)$. *Then, the σ-Hermitian form over V defined by H is a sesquilinear Hermitian form in the sense of Definition*

1.6.4. Conversely, given a sesquilinear Hermitian form h over a vector space V of dimension n, there exists a Hermitian matrix $H \in \mathrm{Mat}(n, K)$ such that h is the σ-Hermitian form over V defined by H.

Thanks to Lemma 1.7.11, it is possible to identify σ-Hermitian forms and sesquilinear Hermitian forms.

Remark 1.7.12. Over an arbitrary field K, there might exist different classes of Hermitian forms, depending on the involutory automorphism σ of K which has been chosen. On the other hand, if K is a finite field $\mathrm{GF}(q)$, then there is an involutory automorphism of K if and only if q is a square. In this case, the involution is unique and it is associated with the subfield of K with index 2, that is $\mathrm{GF}(\sqrt{q})$.

Let q be a prime power p^{2n}. The unique involutory automorphism σ of $\mathrm{GF}(q)$ over $\mathrm{GF}(\sqrt{q})$ will be denoted by the conjugation sign. Namely, for $x \in \mathrm{GF}(q)$:

$$\overline{x} := x^{\sigma} = x^{\sqrt{q}}.$$

Definition 1.7.13. Let $r \geq 1$ be an integer and assume V to be a vector space of dimension n over the field K. A mapping $h : V^n \to K$ is a *homogeneous polynomial mapping of degree r* if there exists a polynomial $f \in \overline{R}_n^r(K)$ such that

$$h : \begin{cases} V^n & \to \quad K \\ (p_1, p_2, \dots, p_n) & \to \quad f(p_1, p_2, \dots, p_n). \end{cases}$$

Such a polynomial f is said to *represent* the mapping h.

For a vector space V over an arbitrary field K, a σ-Hermitian form h usually cannot be represented by a polynomial mapping. For instance, there is no polynomial in $\overline{R}_{2n}(\mathbb{C})$ which represents the Hermitian form induced over the vector space $\mathbb{C}^n$ by the standard Hermitian product between complex numbers. However, if K is finite, the following theorem is true.

Theorem 1.7.14. *Let V be a vector space of dimension n over $\mathrm{GF}(q)$, with q a square, and let h be a Hermitian form defined over V. Then, there exists a polynomial $f \in \overline{R}_{2n}^{\sqrt{q}+1}$ which represents h.*

Proof. The only involution of $\mathrm{GF}(q)$ is the Frobenius automorphism $\sigma : t \to t^{\sqrt{q}}$. Theorem 1.7.11 guarantees that there exists a Hermitian matrix H such that the form h is represented by H. Then,

$$h : \begin{cases} V \times V & \to \quad K \\ (x, y) & \to \quad x^{\sqrt{q}} H y^{\star}. \end{cases}$$

By computing the expansion of the vector/matrix product, this yields

$$h(x, y) = \sum_{j=1}^{n} [y_j \sum_{i=1}^{n} x_i^{\sqrt{q}} H_{ji}],$$

whence the result. □

1.7.3 Hermitian hypersurfaces: definitions

This subsection deals only with Hermitian forms which are representable by polynomials. However, the assumption that the field K is finite is not necessary.

Definition 1.7.15. The *Hermitian hypersurface defined by the Hermitian form* h is the algebraic variety

$$\mathfrak{H}(h) := \mathcal{F}(f(x,x)),$$

where f is a polynomial representing h and $x = (X_0, \dots, X_n)$. The *Hermitian hypersurface defined by the matrix* H is the Hermitian hypersurface

$$\mathcal{H}(H) := \mathfrak{H}(h),$$

where h is the Hermitian form induced by the matrix H. The algebraic variety $\mathcal{F}(\underline{0})$, induced by the trivial Hermitian form, is *not* considered to be a Hermitian variety

Remark 1.7.16. A Hermitian form h over $\mathrm{GF}(q)$ is *not* a Hermitian form over $\mathrm{GF}(q^i)$ for $i > 1$. However it makes sense to consider the $\mathrm{GF}(q^i)$-rational points of the $\mathrm{GF}(q)$-Hermitian variety $\mathcal{H}(h)$.

Theorem 1.7.17. *The set of all Hermitian hypersurfaces of* $\mathrm{PG}(n, q)$ *can be endowed with the structure of a* $\mathrm{PG}(n^2 + 2n, \sqrt{q})$.

Proof. The correspondence in Lemma 1.7.11 allows us to identify Hermitian forms with Hermitian matrices. Let H, H' be two non-zero Hermitian matrices defining the same Hermitian hypersurface, and call f, f' the Hermitian polynomials associated with them. Since $\mathcal{F}(f(x,x)) = \mathcal{F}(f'(x,x))$, the ideals generated by $f(x,x)$ and $f'(x,x)$ have to be the same, that is

$$\mathfrak{I}(f(x,x)) = \mathfrak{I}(f'(x,x)).$$

It follows that there exists an $\alpha \in \mathrm{GF}(q)^\star$ such that

$$f(x,x) = \alpha f'(x,x).$$

Then, by construction,

$$H = \alpha H'$$

and $\alpha \in \mathrm{GF}(\sqrt{q})^\star$. An immediate computation shows the converse, namely that if $H = \alpha H'$ with $\alpha \in \mathrm{GF}(\sqrt{q})$, then $\mathcal{H}(H) = \mathcal{H}(H')$.

By Lemma 1.7.8, the Hermitian matrices in $\mathrm{Mat}(n+1, q)$ constitute a vector space V over $\mathrm{GF}(\sqrt{q})$ with dimension $(n+1)^2$.

Distinct Hermitian hypersurfaces of $\mathrm{PG}(n,q)$ are in one-to-one correspondence with elements of the set U of all Hermitian polynomials modulo $\mathrm{GF}(q)^\star$; the set U, in turn, is in one-to-one correspondence with the quotient space

$$V^\star/\,\mathrm{GF}(\sqrt{q})^\star,$$

which is isomorphic to $\mathrm{PG}(n^2+2n,\sqrt{q})$ and this proves the theorem. □

Definition 1.7.18. The *rank* of a Hermitian hypersurface

$$\mathcal{H}(H) := \mathcal{F}(\overline{x}Hx^\star)$$

is the rank of the matrix H.

Lemma 1.7.19. *A point x on a Hermitian hypersurface $\mathcal{H}(H)$ is* singular *if and only if x belongs to the null-space of H, that is*

$$\overline{x}H = \underline{0}.$$

Lemma 1.7.20. *A Hermitian hypersurface is non-singular if and only if the matrix associated with it has full rank, that is, it is a non-singular matrix.*

Lemma 1.7.21. *Let H and H' be two Hermitian-equivalent matrices. Then, the hypersurfaces $\mathcal{H}(H)$ and $\mathcal{H}(H')$ are projectively equivalent.*

Lemma 1.7.22. *For any $k \le n+1$, there exists exactly one Hermitian hypersurface in $\mathrm{PG}(n,q)$ of rank k up to projectivities.*

Proof. Theorem 1.7.10 and Lemma 1.7.21 imply that any non-singular Hermitian hypersurface in $\mathrm{PG}(n,q)$ is projectively equivalent to the one generated by the diagonal matrix

$$M := \mathrm{diag}(m_0,\ldots,m_k,0,\ldots,0),$$

where $m_0,\ldots,m_k$ are in $\mathrm{GF}(\sqrt{q})$. Since the norm from $\mathrm{GF}(q)$ onto $\mathrm{GF}(\sqrt{q})$ is surjective, there exist elements $t_i \in \mathrm{GF}(q)$, such that

$$t_i\overline{t_i} = m_i.$$

Let T be the matrix

$$T := \mathrm{diag}(t_0,\ldots,t_k,0,\ldots,0).$$

Then, M is Hermitian-equivalent via T to the block matrix

$$\mathrm{diag}(I_k,\ \underbrace{0,\ldots,0}_{n+1-k \text{ times}}\ ),$$

where I_k is the $k\times k$ identity matrix. □

Definition 1.7.23. The *canonical Hermitian hypersurface of rank k in* $\mathrm{PG}(n,q)$ is the Hermitian hypersurface

$$\Pi_{n-k-1}\mathcal{U}_{k,q}$$

induced by the matrix $\mathrm{diag}(I_{k+1},0,\ldots,0)\in\mathrm{Mat}(n+1,q)$. The *canonical non-singular Hermitian hypersurface in* $\mathrm{PG}(n,q)$ is the non-singular Hermitian hypersurface

$$\mathcal{U}_n := \Pi_{-1}\mathcal{U}_{n,q} := \mathcal{H}(I),$$

where I is the identity of $\mathrm{Mat}(n+1,q)$.

A Hermitian hypersurface which is projectively equivalent to a $\Pi_{n-1}\mathcal{U}_{0,q}$ is a hyperplane repeated $\sqrt{q}+1$ times; a Hermitian hypersurface projectively equivalent to a $\Pi_{n-k-1}\mathcal{U}_{k,q}$ is a *Hermitian cone* having as *vertex* a $\Pi_{n-k-1}\in\mathrm{PG}^{n-k-1}(n,q)$ and *base* a $\mathcal{U}_{k,q}$.

Definition 1.7.24. The *canonical Hermitian norm of rank k* in $\mathrm{PG}(n,q)$ is the form

$$h_{k,n}(x) := \sum_{i=0}^{k} x_i\overline{x}_i = \sum_{i=0}^{k} x_i^{\sqrt{q}+1}.$$

With Definition 1.7.24, we can write

(i) $\mathcal{U}_n := \mathcal{F}(h_{n,n}(x))$;

(ii) $\Pi_{n-k-1}\mathcal{U}_k := \mathcal{F}(h_{k,n}(x))$.

1.7.4 Hermitian sub-varieties and points

Lemma 1.7.25. *The intersection of a Hermitian $\mathcal{H}$ variety with a subspace $\Pi_r\in\mathrm{PG}^r(n,q)$ of dimension r not completely included in $\mathcal{H}$ is a Hermitian variety of Π_r.*

Corollary 1.7.26. *The intersection of a Hermitian variety with a line is either a line, a Baer subline or a point.*

Proof. The corollary follows by observing that Hermitian varieties in dimension 1 are either Baer sublines or lines (if completely degenerate), while a Hermitian variety in dimension 0 is a point. □

The following theorems deal with the cardinality of the set of the points of a (possibly singular) Hermitian variety $\mathcal{H}$.

Theorem 1.7.27. *The zeta function of the non-singular Hermitian curve $\mathcal{U}_{2,q}$ is*

$$\zeta_{\mathcal{U}_{2,q}}(T) = \frac{(1+\sqrt{q}T)^{q-\sqrt{q}}}{(1-T)(1-qT)}.$$

Theorem 1.7.28. *The number of* $\mathrm{GF}(q)$*-rational points of the non-singular Hermitian variety* $\mathcal{U}_{n,q}$ *is*

$$\mu(n,q) := [q^{(n+1)/2} + (-1)^n][q^{n/2} - (-1)^n]/(q-1).$$

Corollary 1.7.29.

(i) $\mu(1,q) = \sqrt{q} + 1$;

(ii) $\mu(2,q) = q\sqrt{q} + 1$;

(iii) $\mu(3,q) = (q+1)(q\sqrt{q} + 1)$.

Theorem 1.7.30. *The singular Hermitian variety* $\Pi_m \mathcal{U}_{k,q}$ *contains:*

(i) $q^m + q^{m-1} + \ldots + 1 = (q^{m+1} - 1)/(q-1)$ *singular points;*

(ii) $q^{m+1}\mu(k,q)$ *non-singular* $\mathrm{GF}(q)$*-rational points;*

(iii) $\eta(m,k,q) = (q^{m+1} - 1)/(q-1) + q^{m+1}\mu(k,q)$ *total* $\mathrm{GF}(q)$*-rational points.*

1.7.5 Hermitian varieties and unitary groups

The stabilisers of a Hermitian variety $\mathcal{U}_{n,q}$ in the collineation groups of $\mathrm{PG}(n,q)$ are unitary groups. In fact, the following lemma holds true.

Lemma 1.7.31. *The stabiliser in* $\mathrm{PGL}(n+1,q)$ *of the set of the* $\mathrm{GF}(q)$*-rational points of* $\mathcal{U}_{n,q}$ *is* $\mathrm{PGU}(n+1,q)$. *The stabiliser of the same set in* $\mathrm{P\Gamma L}(n+1,q)$ *is* $\mathrm{P\Gamma U}(n+1,q)$.

Definition 1.7.32. The group $\mathrm{P\gamma U}(n+1,q)$ is the group of all collineations of $\mathrm{PG}(n,q)$ stabilizing the point set of $\mathcal{U}_{n,q}$ which are associated either with the identity of the field $\mathrm{GF}(q)$ or with its involutory automorphism.

Lemma 1.7.33 (Orders of groups)**.** *Assume* p *be a prime, and let* $q = p^h$*, with* h *even; define*

$$\lambda_\epsilon(m,r) := r^{m(m-1)/2} \prod_{i=1}^{m} (r^i - \epsilon^i).$$

Then, the collineation groups have the following orders:

(i) $|\,\mathrm{GL}(n+1,q)| = \lambda_1(n+1,q)$;

(ii) $|\,\mathrm{PGL}(n+1,q)| = (q-1)^{-1}\lambda_1(n+1,q)$;

(iii) $\mathrm{PGU}(n+1,q) \leq \mathrm{P\gamma U}(n+1,q) \leq \mathrm{P\Gamma U}(n+1,q)$;

(iv) $|\,\mathrm{PGU}(n+1,q)| = \frac{\lambda_{-1}(n+1,\sqrt{q})}{\sqrt{q}+1}$;

(v) $\mathrm{PGU}(n+1,q) < \mathrm{P}\gamma\mathrm{U}(n+1,q) \leq \mathrm{P\Gamma U}(n+1,q)$;

(vi) $|\,\mathrm{P}\gamma\mathrm{U}(n+1,q) : \mathrm{PGU}(n+1,q)| = 2$;

(vii) $|\,\mathrm{P}\gamma\mathrm{U}(n+1,q) : \mathrm{P\Gamma U}(n+1,q)| = h/2$;

(viii) $|\,\mathrm{PGL}(n+1,q) : \mathrm{PGU}(n+1,q)| = \frac{\lambda_{-1}(n+1,\sqrt{q})}{\lambda_1(n+1,q)}(\sqrt{q}-1)$;

(ix) *If* $q = p^2$*, with* p *prime, then* $\mathrm{P}\gamma\mathrm{U}(n+1,q) = \mathrm{P\Gamma U}(n+1,q)$.

Corollary 1.7.34. *The number of distinct non-singular Hermitian hypersurfaces in* $\mathrm{PG}(n,q)$ *is*

$$\frac{\sqrt{q}^{\{n(n+1)/2\}}}{\sqrt{q}-1}\prod_{i=1}^{n+1}\frac{q^i-1}{q^{i/2}-(-1)^i}.$$

Proof. Since all non-singular Hermitian hypersurfaces are projectively equivalent, the number is the index

$$|\,\mathrm{P\Gamma L}(n+1,q) : \mathrm{P\Gamma U}(n,q)| = |\,\mathrm{PGL}(n+1,q) : \mathrm{PGU}(n+1,q)|,$$

whence the result. □

1.7.6 Polarities

References for this subsection are [BC66], [Bae52] and [Cam95].

Definition 1.7.35. The *dual* of a Desarguesian projective space $\mathfrak{P} = \mathrm{PG}(n,q)$ is the incidence structure $\mathfrak{P}^\star = (J, P, I^\star)$ defined as follows:

(i) J is the set $\mathrm{PG}^{n-1}(n,q)$ of all hyperplanes of $\mathfrak{P}$;

(ii) P is the set of the points of $\mathfrak{P}$.

(iii) for $j \in J$ and $p \in P$, j is $I^\star$-incident with p if and only if $p \in j$.

For any n, the dual of $\mathrm{PG}(n,q)$ is isomorphic to $\mathrm{PG}(n,q)$.

Definition 1.7.36. A *correlation* is an inclusion reversing permutation of the subspaces of $\mathrm{PG}(n,q)$.

Definition 1.7.37. A sesquilinear form $f(x,y)$ *represents* a correlation θ if and only if, for all $x \in \mathrm{PG}(n,q)$,

$$\theta(x) = \{y \in \mathrm{PG}(n,q) : f(x,y) = 0\}.$$

Lemma 1.7.38. *Any correlation* θ *is represented by a non-degenerate sesquilinear form* f *such that, for all* $x, y \in \mathrm{PG}(n,q)$*,*

$$f(x,y) = 0 \textit{ implies } f(y,x) = 0.$$

Definition 1.7.39. A *polarity* is a correlation of order 2.

A polarity can be seen as a collineation between the projective space $\mathrm{PG}(n,q)$ and its dual $\mathrm{PG}(n,q)^{\star}$.

Definition 1.7.40. Let θ be a polarity represented by a sesquilinear form f. Assume f to be induced by the bilinear mapping $l(x,y)$ with companion automorphism σ. Then, there are three possibilities for θ:

(i) The automorphism σ is the identity, $f(x,y) = f(y,x)$ and there exists a $z \in \mathrm{PG}(n,q)$ such that $f(z,z) \neq 0$; the polarity θ is called *orthogonal*.

(ii) The automorphism σ is the identity and $f(x,x) = 0$ for any $z \in \mathrm{PG}(n,q)$; the polarity θ is called *symplectic*.

(iii) The automorphism σ is an involution and $f(x,y) = f(y,x)^{\sigma}$; the polarity θ is called *unitary*.

Definition 1.7.41. Let ϕ be a polarity of $\mathrm{PG}(n,q)$. The *polar space* of a point $p \in \mathrm{PG}(n,q)$ is the hyperplane $\phi(p)$.

Definition 1.7.42. Two points $x, y \in \mathrm{PG}(n,q)$ are *conjugate* with respect to the polarity ϕ if and only if $x \in \phi(y)$ and *vice-versa*. A point x is *self-conjugate* or *absolute* if $x \in \phi(x)$.

Lemma 1.7.43. *Let K be a field of characteristic different from 2. Then, the non-degenerate quadrics of $\mathrm{PG}(n,K)$ are precisely the sets of absolute points with respect to the orthogonal polarities of $\mathrm{PG}(n,K)$.*

Lemma 1.7.44. *The absolute points with respect to an orthogonal polarity of $\mathrm{PG}(n,2^t)$ are precisely those of a distinguished hyperplane H. Such an hyperplane is itself absolute if and only if the dimension n is odd.*

Lemma 1.7.45. *A polarity is unitary if and only if there exists a line in $\mathrm{PG}(n,q)$ containing one non-absolute and at least 3 absolute points. The non-degenerate Hermitian hypersurfaces of $\mathrm{PG}(n,K)$ are precisely the sets of absolute points with respect to the unitary polarities of $\mathrm{PG}(n,K)$.*

Remark 1.7.46. Let f be a non-degenerate sesquilinear form. For any non-self-conjugate point $x \in \mathrm{PG}(n,q)$, it is possible to assume

$$f(x,x) = 1.$$

1.7.7 Subspaces in Hermitian varieties

Lemma 1.7.47. *Assume x and y to be two points of $\mathcal{U}_n$. The line xy is a sub-variety of $\mathcal{U}_n$ if and only if x and y are mutually conjugate.*

Corollary 1.7.48. *A necessary and sufficient condition for a t-dimensional subspace $\Pi_t \in \mathrm{PG}^t(n,q)$ to be a sub-variety of $\mathcal{U}_{n,q}$ is that all its points are mutually conjugate.*

Observe that this corollary implies that *any subspace Π completely contained in a non-singular Hermitian variety $\mathcal{U}_n$ is included in the tangent space of the variety at any of its points*.

Theorem 1.7.49. *Let n be an integer, and assume t to be the integral part of $(n-1)/2$. Then, $\mathcal{U}_n$ contains linear subspaces of dimension t and no higher.*

Theorem 1.7.50. *Let*

$$\psi(n,t,q)$$

be the number of subspaces in $\mathrm{PG}^t(n,q)$ contained in $\mathcal{U}_{n,q}$. Then,

(i) $\psi(2t+1,t,q) = \prod_{j=0}^{t}(q^{2j+1}+1)$;

(ii) $\psi(2t+2,t,q) = \prod_{j=0}^{t}(q^{2j+3}+1)$.

Corollary 1.7.51. *The number of m-dimensional projective subspaces contained in a $\mathcal{U}_{n,q}$ is*

$$N(m,\mathcal{U}_{n,q}) := \prod_{i=2m-n}^{n+1}[(\sqrt{q})^i-(-1)^i] / \prod_{i=0}^{n-m}[q^{i+1}-1].$$

1.7.8 Incidence properties

Definition 1.7.52. A *unital* in $\mathrm{PG}(2,q)$ is a set of points U such that any line of the plane meets U in either 1 or $\sqrt{q}+1$ points. A line l which intersects U in one point is *tangent* to U; if l intersects U in $\sqrt{q}+1$ points, then l is a *chord* of U.

Lemma 1.7.53. *The set of $\mathrm{GF}(q)$-rational points of a non-degenerate Hermitian curve is an unital in $\mathrm{PG}(2,q)$. This unital is called* classical.

For further information on unitals see also Chapter 12 of [Hir98b].

Chapter 2

The 2-dimensional case: Hermitian curves

In this chapter, first we introduce Kestenband's classification of point-line configurations arising from the intersection of Hermitian curves. Later, we show that these configurations are in fact projectively unique and we compute the stabiliser of each of them in the full linear collineation group $\mathrm{PGL}(3, q)$. A group theoretical characterisation of the Hermitian curve concludes the chapter.

2.1 Classification of intersections in dimension 2

In [Kes81], the possible point-line configurations arising from the intersection of two Hermitian curves in $\mathrm{PG}(2, q)$ are described. The classification is done with linear algebra techniques.

2.1.1 Incidence classification

Definition 2.1.1. Let $\mathcal{H} = \mathcal{H}(H)$ and $\mathcal{H}' = \mathcal{H}(H')$ be two distinct Hermitian varieties. The *Hermitian pencil* Γ *generated by* $\mathcal{H}$ *and* $\mathcal{H}'$ is the set

$$\Gamma := \{\mathcal{H}(\lambda H + \mu H') : \lambda, \mu \in \mathrm{GF}(\sqrt{q})\}.$$

The *base locus* of Γ is the set

$$\Gamma_\cap := \bigcap_{\mathcal{T} \in \Gamma} \mathcal{T}.$$

The result of [Kes81] is based upon the following important observation.

Lemma 2.1.2. *The intersection of any two distinct Hermitian varieties* $\mathcal{H}$ *and* $\mathcal{H}'$ *is the base locus of the Hermitian pencil* Γ *they generate.*

Proof. Let $\mathcal{E} = \mathcal{H} \cap \mathcal{H}'$ and assume $\mathcal{H} = \mathcal{H}(H)$, $\mathcal{H}' = \mathcal{H}(H')$ and $x \in \mathcal{E}$. Then,

$$\overline{x} H x^\star = \overline{x} H' x^\star = 0.$$

It follows that, for any λ, μ:

$$\overline{x}(\lambda H + \mu H')x^\star = 0;$$

hence, $\mathcal{E} \subseteq \Gamma_\cap$. Conversely, since $\mathcal{H}, \mathcal{H}' \in \Gamma$, if $x \in \Gamma_\cap$, then $x \in \mathcal{E}$ and the lemma follows. □

We may observe that the proof of Lemma 2.1.2 does not require Γ to be the $\mathrm{GF}(\sqrt{q})$-linear system generated by $\mathcal{H}$ and $\mathcal{H}'$. In fact, any linear system generated by $\mathcal{H}$ and $\mathcal{H}'$ would do; however, the $\mathrm{GF}(\sqrt{q})$-linear system is the largest linear system containing $\mathcal{H}_1$ and $\mathcal{H}_2$ whose elements are all Hermitian curves. Such a linear system can be seen as a line in the projective space $\mathrm{PG}(n^2+2n, \sqrt{q})$ considered as the set of all Hermitian varieties over $\mathrm{PG}(n,q)$.

Thanks to Lemma 2.1.2, it is sufficient to classify all Hermitian pencils in $\mathrm{PG}(n,q)$ in order to have a description of all possible incidence configurations.

For any Hermitian pencil Γ, let $r_i(\Gamma)$ be the number of Hermitian varieties in Γ of rank i. Clearly, the sum of all r_i's is $\sqrt{q}$.

Lemma 2.1.3. *The cardinality of the intersection of two Hermitian curves $\mathcal{H}_1$ and $\mathcal{H}_2$ depends only upon the indices $r_i(\Gamma)$ of the linear system they generate. The possible intersection numbers are as in Table 2.1.*

r_1	r_2	$k = \lvert\mathcal{E}\rvert$
0	3	$(\sqrt{q}+1)^2$
1	1	$\sqrt{q}+1$
0	2	$q+\sqrt{q}+1$
0	1	$q+1$
1	0	1
0	0	$q-\sqrt{q}+1$

Table 2.1: Possible intersection numbers for non-degenerate Hermitian Curves.

This lemma can be found in Kestenband [Kes81]. However, it is a special case of the general result of Theorem 4.1.26. The main result of [Kes81] is the following theorem.

Theorem 2.1.4. *Let H be a non-degenerate Hermitian matrix in $\mathrm{Mat}(3,q)$ and let $\mathcal{M}(x)$ and $\mathcal{C}(x)$ be its minimal and characteristic polynomials. Then, the intersection $\mathcal{E}$ of the canonical Hermitian curve $\mathcal{U}_2$ and $\mathcal{H}(H)$ belongs to one of the following seven classes.*

(i) **Class I***: $\mathcal{M}(x) = \mathcal{C}(x) = (x-\alpha)(x-\beta)(x-\gamma)$ with α, β, γ distinct elements of* $\mathrm{GF}(\sqrt{q})$*:*

- $\lvert\mathcal{E}\rvert = (\sqrt{q}+1)^2$*;*
- *the points are as in Figure 2.1.a;*
- $r_3(\Gamma) = \sqrt{q}-2$*;* $r_2(\Gamma) = 3$.

(ii) **Class II**: $\mathcal{M}(x) = \mathcal{H}(x) = (x-\alpha)(x-\delta)^2$ *with* α, δ *distinct elements of* $\mathrm{GF}(\sqrt{q})$:

- $|\mathcal{E}| = q + \sqrt{q} + 1$;
- *the points are as in Figure 2.1.b;*
- $r_3(\Gamma) = \sqrt{q} - 1$; $r_2(\Gamma) = 2$.

(iii) **Class III**: $\mathcal{M}(x) = \mathcal{C}(x) = (x-\alpha)p(x)$ *with* $p(x)$ *polynomial of degree* 2 *irreducible over* $\mathrm{GF}(\sqrt{q})$:

- $|\mathcal{E}| = q + 1$;
- *the points are as in Figure 2.1.c;*
- $r_3(\Gamma) = \sqrt{q}$; $r_2(\Gamma) = 1$.

(iv) **Class IV**: $\mathcal{M}(x) = \mathcal{C}(x) = (x-\lambda)^3$:

- $|\mathcal{E}| = q + 1$;
- *the points are as in Figure 2.1.d;*
- $r_3(\Gamma) = \sqrt{q}$; $r_2(\Gamma) = 1$.

(v) **Class V**: $\mathcal{M}(x) = (x-\alpha)(x-\beta)$ *with* α, β *distinct elements of* $\mathrm{GF}(\sqrt{q})$:

- $|\mathcal{E}| = \sqrt{q} + 1$;
- *the points constitute a Baer subline of* $\mathrm{PG}(2, q)$;
- $r_3(\Gamma) = \sqrt{q} - 1$; $r_2(\Gamma) = 1$.

(vi) **Class VI**: $\mathcal{M}(x) = (x-\lambda)^2$:

- $|\mathcal{E}| = 1$;
- $r_3(\Gamma) = \sqrt{q}$; $r_2(\Gamma) = 0$.

(vii) **Class VII**:

- $|\mathcal{E}| = q - \sqrt{q} + 1$;
- *no three points of* $\mathcal{E}$ *are collinear;*
- $r_3(\Gamma) = \sqrt{q} + 1$.

Observe that considering only linear systems containing the canonical Hermitian curve $\mathcal{U}_2$ does not hamper generality, since it is always possible to reduce to one of those via a projectivity.

r_1	r_2	$\mathcal{M}_H(x)$
0	3	$(x-\alpha)(x-\beta)(x-\gamma)$
1	1	$(x-\alpha)(x-\beta)$
0	2	$(x-\alpha)^2(x-\beta)$
0	1	$(x-\alpha)p(x), (x-\alpha)^3$
1	0	$(x-\alpha)^2$
0	0	$p(x)$

Table 2.2: Minimal polynomials corresponding to given rank sequences in the 2-dimensional case.

2.1.2 Outline of the proof

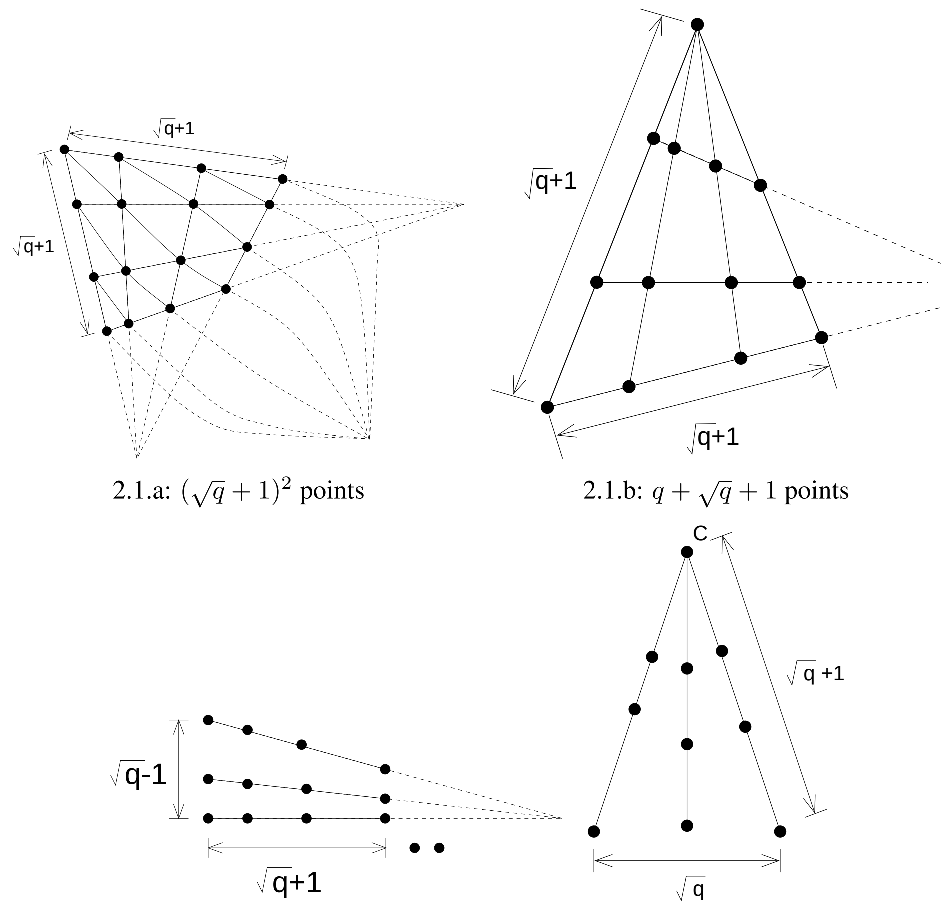
Theorem 2.1.4 is proven by constructing suitable canonical forms for Hermitian matrices in $\mathrm{Mat}(3,q)$ modulus Hermitian equivalence and considering the various cases arising individually. This is done via the following lemma, which provides 'canonical' forms for Hermitian matrices.

Lemma 2.1.5. *Let H be a Hermitian matrix in $\mathrm{Mat}(3,q)$ and assume $\mathcal{M}_H(x)$ to be its minimal polynomial. Then, H is Hermitian equivalent to one of the matrices in Table 2.3.*

$\mathcal{M}_H(x)$	conditions	canonical form
$(x-\alpha)(x-\beta)(x-\gamma)$		$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix}$
$(x-\alpha)(x-\beta)$		$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix}$
$(x-\alpha)(x-\delta)^2$	$(\beta-\gamma)^2+4a^{\sqrt{q}+1}=0$	$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & a \\ 0 & a^{\sqrt{q}} & \gamma \end{bmatrix}$
$(x-\alpha)p(x)$	$(\beta-\alpha)(\gamma-\alpha)\neq a^{\sqrt{q}+1}$	$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & a \\ 0 & a^{\sqrt{q}} & \gamma \end{bmatrix}$
$(x-\lambda)^3$	$a^{\sqrt{q}+1}+c^{\sqrt{q}+1}=0$	$\begin{bmatrix} \lambda & c^{\sqrt{q}} & 0 \\ c & \lambda & a^{\sqrt{q}} \\ 0 & a & \lambda \end{bmatrix}$

Table 2.3: Canonical forms for 3 by 3 Hermitian matrices.

In fact, the intersections might be described by just considering the position of two specially chosen curves in Γ. Since this is the basic tool for the projective classification that we present



2.1.a: $(\sqrt{q}+1)^2$ points

2.1.b: $q+\sqrt{q}+1$ points

2.1.c: $q+1$ points

2.1.d: $q+1$ points

Figure 2.1: Possible configurations for the 2-dimensional case

in the next section, it is worth to provide here a list of these suitable 'special' curves for Γ belonging to the various classes.

For any of the classes I-VII, let $\mathcal{H}$ be a curve in Γ different from $\mathcal{U}_2$. Then, $\mathcal{H}$ might be chosen as follows:

(i) **Class I**:

- $\mathcal{H}$ is a Hermitian cone with vertex not in $\mathcal{U}_2$,
- each generator of $\mathcal{H}$ is a chord of $\mathcal{U}_2$;

(ii) **Class II**:

- $\mathcal{H}$ is a Hermitian cone with vertex in $\mathcal{U}_2$,
- each generator of $\mathcal{H}$ is a chord of $\mathcal{U}_2$;

(iii) **Class III**:

- $\mathcal{H}$ is a Hermitian cone with vertex outside $\mathcal{U}_2$,
- two generators of $\mathcal{H}$ are tangent to $\mathcal{U}_2$, all the others being chords;

(iv) **Class IV**

- $\mathcal{H}$ is a Hermitian cone with vertex in $\mathcal{U}_2$,
- one generator of $\mathcal{H}$ is tangent to $\mathcal{U}_2$, all the others being chords;

(v) **Class V**

- $\mathcal{H}$ is a doubly degenerate Hermitian curve, that is a line counted $\sqrt{q}+1$ times,
- $\mathcal{H}$ is a chord of $\mathcal{U}_2$;

(vi) **Class VI**

- $\mathcal{H}$ is a doubly degenerate Hermitian curve,
- $\mathcal{H}$ is tangent to $\mathcal{U}_2$;

(vii) **Class VII**

- $\mathcal{H}$ is a non-singular Hermitian curve.

Definition 2.1.6. A point of the intersection $\mathcal{E}$ is *special* if it is either the vertex of a Hermitian cone in Γ or the only common point of $\mathcal{E}$ with a generator of a Hermitian cone in Γ.

There are

- no special points in classes I, V, VI and VII;
- one special point in classes II and IV;
- two special points in class III.

2.2 Groups of the intersection of two Hermitian curves

2.2.1 Introduction

As presented in Section 2.1, Kestenband's paper [Kes81] classifies the point-line configurations arising from the intersection of two Hermitian curves. Nothing is said about projective equivalence of the configurations in a given class nor about the linear collineation groups preserving the structures. This is the aim of the present section. This work has been submitted for publication as [Giub]. I would like to thank Professor G. Korchmáros for helpful discussions on the topic.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be Hermitian curves and denote by $\mathcal{E}$ their intersection. As before, let Γ be the $\mathrm{GF}(\sqrt{q})$-linear system generated by $\mathcal{H}_1$ and $\mathcal{H}_2$ and define for any $i = 1, 2, 3$, the set Γ_i as the subset of Γ which contains all the curves of rank i. Clearly, $r_i(\Gamma) = |\Gamma_i|$.

Our main results are the following theorems.

Theorem 2.2.1. *Each of the seven classes I-VII consists of pairwise projectively equivalent Hermitian intersections.*

Theorem 2.2.2. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *acts transitively on both the special and non-special points of* $\mathcal{E}$*. The abstract structure of* $\mathrm{Aut}(\mathcal{E})$ *depends on the class containing* $\mathcal{E}$ *and is given in Theorems 2.2.9, 2.2.15, 2.2.18, 2.2.22, 2.2.24, 2.2.26, 2.2.28.*

2.2.2 A non-canonical model of $\mathrm{PG}(2, q)$

Definition 2.2.3. For any $i \leq j$, a projective subspace Π of order p^i is in *canonical position* in $\mathrm{PG}(n, p^j)$ if and only if

$$\Pi \cap \mathrm{PG}(n, p^j) = \mathrm{PG}(n, p^i),$$

that is, Π is the subspace of $\mathrm{PG}(n, p^j)$ coordinatized over $\mathrm{GF}(p^i)$.

In order to compute the collineation group fixing a Hermitian intersection of class VII, a model of $\mathrm{PG}(2, q)$ that does not lie in canonical position in $\mathrm{PG}(2, q^3)$ is needed. The results here presented are from [CK98] and [CK97].

Let $\mathcal{F} = \mathrm{GF}(q)$, where $q = p^h$ and p is odd. Consider the field $\mathcal{G} = \mathrm{GF}(q^3)$ as a cubic extension of $\mathcal{F}$; furthermore take b as a primitive (q^2+q+1)-th root of unity over $\mathcal{G}$. The linear collineation β of $\mathrm{PG}(2, \mathcal{G})$ given by

$$\beta : \begin{cases} X \to bX \\ Y \to b^{q+1}Y \\ Z \to Z \end{cases}$$

has clearly order $q^2 + q + 1$ and fixes each vertex of the fundamental triangle $X_\infty Y_\infty Z_\infty$ of $\mathrm{PG}(2, \mathcal{G})$.

Let $\mathcal{B} = \langle \beta \rangle$; the point orbit of $E = (1, 1, 1)$ under $\mathcal{B}$ is the set

$$\Pi = \{(c, c^{q+1}, 1) : c^{q^2+q+1} = 1, c \in \mathcal{G}\}.$$

Such a set induces a subgeometry in $\mathrm{PG}(2, \mathcal{G})$, whose points are the points of Π and whose lines are the lines of $\mathrm{PG}(2, \mathcal{G})$ intersecting Π in at least 2 (and hence in $q + 1$) points. In fact, this subgeometry is a projective plane, see [CKT99] and [CK98].

Theorem 2.2.4 ([CK98], Proposition 1). *The subgeometry* Π *is isomorphic to* $\mathrm{PG}(2,\mathcal{F})$. *More precisely,* Π *is a projective subplane of* $\mathrm{PG}(2,\mathcal{E})$ *lying in non-classical position. The lines of* Π *have equation* $[tx+t^{q+1}y+z=0]$, *with* t *running on the* (q^2+q+1)*-th roots of unity and they form the line-orbit of* $[x+y+z=0]$ *under the group* $\mathcal{B}$.

It can be proven, see [CKT99], that the collineation

$$\kappa:\begin{cases} X\rightarrow bX+Y+b^{q^2+1}Z \\ Y\rightarrow b^{q^2+1}X+bY+Z \\ Z\rightarrow X+b^{q^2+1}Y+bZ \end{cases}$$

maps $\mathrm{PG}(2,q)$ into Π. Observe that β is a Singer cycle of Π which is represented in diagonal form.

In order to simplify the notation, the symbol (i) will be used to denote the point $(b^i, b^{i(q+1)}, 1)$ of Π. Similarly, $[i]$ will indicate the line of Π of equation $[b^iX+b^{i(q+1)}Y+Z=0]$.

2.2.3 Equations for the non-singular Hermitian curve

There is only one non-singular Hermitian curve up to projectivities in $\mathrm{PG}(2,q)$; however, when describing intersection configurations, it is useful to have different models for the curves. Table 2.4 presents the standard equations that will be used.

$(M1)$	$X^{\sqrt{q}+1}+Y^{\sqrt{q}+1}+Z^{\sqrt{q}+1}=0$	
$(M2)$	$X^{\sqrt{q}+1}+YZ^{\sqrt{q}}+Y^{\sqrt{q}}Z=0$	
$(M3)$	$XY^{\sqrt{q}}-X^{\sqrt{q}}Y+\omega Z^{\sqrt{q}+1}=0$	$\omega^{\sqrt{q}-1}=-1$
$(M4)$	$XY^{\sqrt{q}}+YZ^{\sqrt{q}}+ZX^{\sqrt{q}}=0$	

Table 2.4: Equations for the non-degenerate Hermitian curve

All the models (M1)-(M3) of the Hermitian curve are $\mathrm{GF}(q)$-equivalent, that is, there exists a linear transformation in $\mathrm{PGL}(3,q)$ that maps one equation into the other.

The model (M1) is the one induced by the canonical Hermitian form and corresponds to the identity matrix. Equations (M2) and (M3) allow to consider easily the affine points of the Hermitian curve $\mathcal{H}$: in (M2), the line at infinity $l_\infty : [Z=0]$ is tangent to $\mathcal{H}$ at the point $Y_\infty=(0,1,0)$; in (M3), the polar of the point $Z_\infty=(0,0,1)$ is the line l_∞ and the intersection between l_∞ and $\mathcal{H}$ is a subline belonging to $\mathrm{PG}(2,\sqrt{q})\subseteq\mathrm{PG}(2,q)$.

Let $\mathcal{H}$ be the curve in the plane Π corresponding to the equation (M4). We want to prove that $\mathcal{H}$ is a Hermitian curve.

Lemma 2.2.5. *The stabiliser of* $\mathcal{H}$ *in the group* $\mathcal{B}$ *is a subgroup* K *of order* $q-\sqrt{q}+1$ *generated by* $\beta^{(q+\sqrt{q}+1)}$.

Proof. The mapping β transforms the equation of $\mathcal{H}$

$$\mathcal{H} : XY^{\sqrt{q}} + YZ^{\sqrt{q}} + ZX^{\sqrt{q}} = 0$$

into

$$\mathcal{H}^{\beta} : (b^{q\sqrt{q}+q+2\sqrt{q}+1})[XY^{\sqrt{q}} + YZ^{\sqrt{q}} + ZX^{\sqrt{q}}] = 0;$$

hence, the group K stabilises $\mathcal{H}$. Conversely, suppose that β^l stabilises $\mathcal{H}$. Then,

$$b^{(q\sqrt{q}+q+1)l} = b^{(q+1)l} = b^{\sqrt{q}l}.$$

The result follows. □

Lemma 2.2.6. *The set $\mathcal{H}$ is a Hermitian curve of* Π.

Proof. We prove that $\mathcal{H}$ is a classical unital. First, we verify that the mapping

$$\varphi : \begin{cases} (i) & \rightarrow & [iq\sqrt{q}] \\ [i] & \rightarrow & (iq\sqrt{q}) \end{cases}$$

is a non-degenerate polarity. Since Π is a cyclic plane, it is enough to show that φ sends lines through (0) to points incident with $[0]$ and vice-versa. The line $[i]$ is incident with the point (0) if and only if $b^i + b^{i(q+1)} + 1 = 0$ that is $b^{iq\sqrt{q}} + b^{i(q+1)q\sqrt{q}} + 1 = 0$. As $(iq\sqrt{q})$ is the image point of $[i]$, the first assertion follows. A similar argument proves the converse. A direct computation shows also that the set of all self-conjugate points of φ coincides with $\mathcal{H}$. The classification of polarities of $\mathrm{PG}(2, q)$ implies that the polarity φ is either orthogonal or unitary. Hence, in order to get the result, it remains to prove that the former possibility cannot actually occur. It is well known, see Lemmas 1.7.43 and 1.7.44, that the set of all self-conjugate points of an orthogonal polarity is a (non-degenerate) conic for q odd and a line for q even. On the other hand, no collineation group preserving either a conic or a line contains a cyclic subgroup of order $q - \sqrt{q} + 1$. Hence, Lemma 2.2.5 rules out the possibility for φ not to be unitary. □

It follows that the model (M4) is not $\mathrm{GF}(q)$-equivalent to (M1); however it is $\mathrm{GF}(q^3)$-equivalent.

2.2.4 Groups preserving the intersection of two Hermitian curves

Let $\mathrm{Aut}(\mathcal{E})$ denote the linear collineation group preserving the Hermitian intersection $\mathcal{E}$ of $\mathcal{H}_1$ and $\mathcal{H}_2$. As a subgroup of $\mathrm{PGL}(3, q)$, the group $\mathrm{Aut}(\mathcal{E})$ acts in a natural way as a permutation group on the set of all Hermitian curves in the linear system Γ. More precisely, the three (possibly empty) subsets $\Gamma_i \subseteq \Gamma$ are invariant under the action of $\mathrm{Aut}(\mathcal{E})$.

Our approach to computing $\mathrm{Aut}(\mathcal{E})$ is to take $\mathcal{H}_1$ from Γ_3 and $\mathcal{H}_2$ from Γ_1 or from Γ_2, when Γ_1 is empty, and determine its subgroup G consisting of all linear collineations preserving both

$\mathcal{H}_1$ and $\mathcal{H}_2$. This will be done by using several properties of the linear collineation group $\mathrm{PSU}(3,q)$ including the classification of all maximal subgroups of $\mathrm{PSU}(3,q)$, see [Har26], [Hof72], [Mit11].

The subgroup G turns out to be quite large and always transitive on the set of all non-special points of $\mathcal{E}$. Finally, in order to obtain the whole $\mathrm{Aut}(\mathcal{E})$ we will also need some direct computations depending on the particular properties of $\mathcal{E}$ and the possible actions of $\mathrm{Aut}(\mathcal{E})$ on the pencil Γ.

Class I

Let $\mathcal{E}$ be a Hermitian intersection in class I. A non-singular Hermitian curve $\mathcal{H}_1$ in the pencil Γ can be assumed in its canonical form (M1),

$$\mathcal{H}_1 : X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0.$$

Since the collineation group preserving $\mathcal{H}_1$ acts transitively on the points outside $\mathcal{H}_1$, a Hermitian cone in Γ can be assumed to have its vertex V in the origin $O = (0,0,1)$. In particular, both $\mathcal{H}_1$ and $\mathcal{H}_2$ are associated to a diagonal matrix, and this holds true for every curve in the pencil. Under these assumptions, the three Hermitian cones in Γ are of the form

1. $\mathcal{H}_2 : \lambda X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} = 0$;
2. $\mathcal{H}_3 : (\lambda-1)Y^{\sqrt{q}+1} + \lambda Z^{\sqrt{q}+1} = 0$;
3. $\mathcal{H}_4 : (1-\lambda)X^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0$;

with $\lambda \in \mathrm{GF}(\sqrt{q})^\star \setminus \{1\}$. *A priori*, the properties of $\mathcal{E}$ may depend on λ. However, as the next Theorem 2.2.7 states, different choices of λ provide projectively equivalent Hermitian intersections.

Theorem 2.2.7. *Hermitian intersections in class I are projectively equivalent.*

Proof. Let $\lambda, \bar{\lambda} \in \mathrm{GF}(\sqrt{q})^\star \setminus \{1\}$. Then, there are elements $u, v \in \mathrm{GF}(q)^\star$ such that

$$u^{\sqrt{q}+1} = \frac{\lambda-1}{\bar{\lambda}-1}, \qquad v^{\sqrt{q}+1} = \frac{(\lambda-1)\bar{\lambda}}{(\bar{\lambda}-1)\lambda}.$$

Let γ be the linear collineation represented by the non-singular matrix

$$g = \begin{bmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The projectivity γ sends $\mathcal{H}_2$ and $\mathcal{H}_3$ to the Hermitian cones of equations $\bar{\lambda}X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} = 0$ and $(\bar{\lambda}-1)Y^{\sqrt{q}+1} + \bar{\lambda}Z^{\sqrt{q}+1} = 0$. This proves the theorem. $\square$

Our next aim is to determine the abstract structure and the action of $\mathrm{Aut}(\mathcal{E})$ on the point-set. To do this, the following lemma is needed.

Lemma 2.2.8. *The collineation group G which preserves both the curve $\mathcal{H}_1$ and the cone $\mathcal{H}_2$ consists of all collineations*

$$t(\epsilon,\eta) : (X,Y,Z) \to (\epsilon X, \eta Y, Z),$$

with $\epsilon^{\sqrt{q}+1} = \eta^{\sqrt{q}+1} = 1$. In fact,

$$G \simeq C_{\sqrt{q}+1} \times C_{\sqrt{q}+1},$$

and it acts on the point-set of $\mathcal{E}$ as a regular permutation group.

Proof. The linear collineations $t(\epsilon,\eta)$ preserve both the curves $\mathcal{H}_1$ and $\mathcal{H}_2$. In fact,

$$t(\epsilon,\eta)(\mathcal{H}_1) = \\ (\epsilon X)^{\sqrt{q}+1} + (\eta Y)^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = \\ \mathcal{H}_1;$$

likewise $t(\epsilon,\eta)(\mathcal{H}_2) = \mathcal{H}_2$. To show the converse, let γ be a linear collineation of $\mathrm{PG}(2,q)$ preserving both $\mathcal{H}_1$ and $\mathcal{H}_2$. Since γ fixes the vertex $(0,0,1)$ of the Hermitian cone $\mathcal{H}_2$, the non-singular unitary matrix associated to γ is a block diagonal matrix

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

with $b = c^{\sqrt{q}}$. Since

$$\lambda(aX+bY)^{\sqrt{q}+1} + (cX+dY)^{\sqrt{q}+1} = \\ \mathfrak{T}[(\lambda(a^{\sqrt{q}}b) + c^{\sqrt{q}}d)X^{\sqrt{q}}Y] + (\lambda b^{\sqrt{q}+1} + d^{\sqrt{q}+1})Y^{\sqrt{q}+1} + (\lambda a^{\sqrt{q}+1} + c^{\sqrt{q}+1})X^{\sqrt{q}+1},$$

the condition on γ to preserve $\mathcal{H}_2$ yields

(i) $b(\lambda a^{\sqrt{q}} + d) = 0$;

(ii) $(\lambda a^{\sqrt{q}+1} + b^{\sqrt{q}+1}) = \lambda(\lambda b^{\sqrt{q}+1} + d^{\sqrt{q}+1}) \neq 0$.

From (i), we have either $b = 0$ or $b \neq 0$ and $d = -\lambda a^{\sqrt{q}}$. In the latter case,

$$b^{\sqrt{q}+1} = -\lambda a^{\sqrt{q}+1}$$

and $\lambda a^{\sqrt{q}+1} + b^{\sqrt{q}+1} = 0$, against (ii). This shows that $b = 0$. Then, (ii) implies $a^{\sqrt{q}+1} = d^{\sqrt{q}+1}$. Also, from $c^{\sqrt{q}+1} = b = 0$ it follows that $c = 0$. Hence, the collineation γ is indeed $t(a,b)$ and $G \simeq C_{\sqrt{q}+1} \times C_{\sqrt{q}+1}$.

Note that $\mathcal{E} = \mathcal{H}_1 \cap \mathcal{H}_2$ has no point on the fundamental triangle of $\mathrm{PG}(2, q)$. On the other hand, the group G does not fix any point outside the fundamental triangle. It follows that the G-orbit of a point $P \in \mathcal{H}_1 \cap \mathcal{H}_2$ has size $(\sqrt{q}+1)^2$, the same as G and $\mathcal{E}$. Hence, since $\mathcal{E}$ is preserved by G, $\mathcal{E}$ coincides with the orbit of P under G, and G acts regularly. □

Theorem 2.2.9. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection in class I acts transitively on the points of* $\mathcal{E}$*. Furthermore,* $\mathrm{Aut}(\mathcal{E})$ *has order* $3(\sqrt{q}+1)^2$ *and*

$$\mathrm{Aut}(\mathcal{E}) \simeq (C_{\sqrt{q}+1} \times C_{\sqrt{q}+1}) \rtimes \mathrm{S}_3 \,.$$

Proof. For any $b, c, d \in \mathrm{GF}(q)$ such that

$$b^{\sqrt{q}+1} = -\frac{1}{\lambda}, \qquad c^{\sqrt{q}+1} = -\frac{(1-\lambda)^2}{\lambda}, \qquad d^{\sqrt{q}+1} = \lambda(1-\lambda),$$

the group $\Sigma \cong \mathrm{S}_3$ generated by the linear collineations

$$\sigma_1 : (X, Y, Z) \to (Z, dX, cY),$$

$$\sigma_2 : (X, Y, Z) \to (bY, b^{-1}X, Z)$$

is a subgroup of the normaliser of G in $\mathrm{Aut}(\mathcal{E})$. In fact, $\langle G, \Sigma \rangle = G \rtimes \Sigma$: all collineations in G fix the curves in the pencil Γ; hence, $G \cap \Sigma = 1$. Furthermore, Σ preserves Γ_2, that is the set $\{\mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4\}$ and, in particular, Σ is a subgroup of $\mathrm{Aut}(\mathcal{E})$. To show that $\langle G, \Sigma \rangle = \mathrm{Aut}(\mathcal{E})$, let $\tau \in \mathrm{Aut}(\mathcal{E})$. Since Σ induces the full symmetric group on Γ_2, there exists $\sigma \in \Sigma$ such that $\sigma\tau$ preserves each of the Hermitian cones $\mathcal{H}_2$, $\mathcal{H}_3$, and $\mathcal{H}_4$. By virtue of the fact that the vertices of these Hermitian cones are also the vertices of the fundamental triangle, it turns out that $\sigma\tau$ is associated to a diagonal matrix

$$\begin{bmatrix} \eta & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

As $\sigma\tau$ fixes $\mathcal{H}_2$, we have $\eta^{\sqrt{q}+1} = \mu^{\sqrt{q}+1}$. Also, $\mu^{\sqrt{q}+1} = 1$, because $\sigma\tau$ fixes $\mathcal{H}_3$ as well. This shows that $\sigma\tau \in G$, whence $\mathrm{Aut}(\mathcal{E}) = \langle G, \Sigma \rangle$. The claim now follows from the above results together with Lemma 2.2.8. □

Class II

Let $\mathcal{E}$ be a Hermitian intersection in class II. A non-singular Hermitian curve $\mathcal{H}_1$ in the pencil Γ is assumed in the canonical form (M2),

$$\mathcal{H}_1 : X^{\sqrt{q}+1} + YZ^{\sqrt{q}} + ZY^{\sqrt{q}} = 0,$$

while a Hermitian cone with vertex $Y_\infty = (0, 1, 0)$, say

$$\mathcal{H}_2 : \lambda X^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0,$$

is chosen to generate Γ together $\mathcal{H}_1$. One more Hermitian cone belongs to Γ, namely

$$\mathcal{H}_3 : \lambda Y Z^{\sqrt{q}} + \lambda Z Y^{\sqrt{q}} - Z^{\sqrt{q}+1} = 0.$$

Its vertex is the point at infinity $X_\infty = (1, 0, 0)$.

Theorem 2.2.10. *Hermitian intersections in class II are projectively equivalent.*

Proof. Let Γ and $\bar{\Gamma}$ be two pencils which define Hermitian intersections belonging to class II, and let $\Gamma = \langle \mathcal{H}_1, \mathcal{H}_2 \rangle$. Without loss of generality, we may assume that $\bar{\Gamma}$ is generated by $\mathcal{H}_1$ together with the Hermitian cone of equation

$$\bar{\lambda} X^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0,$$

where $\bar{\lambda} \in \mathrm{GF}(\sqrt{q})^\star$. Arguing as in the proof of Theorem 2.2.7, choose an element $u \in \mathrm{GF}(q)^\star$ such that $u^{\sqrt{q}+1} = \lambda/\bar{\lambda}$. The linear collineation

$$\xi : (X, Y, Z) \to (uX, u^{\sqrt{q}+1} Y, Z).$$

sends $\mathcal{H}_2$ and $\mathcal{H}_3$ to the Hermitian cones of equations $\bar{\lambda} X^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0$ and $\bar{\lambda} Y Z^{\sqrt{q}} + \bar{\lambda} Z Y^{\sqrt{q}} - Z^{\sqrt{q}+1} = 0$, whence the claim follows. □

We now determine the structure and the action on $\mathcal{E}$ of the linear collineation group $\mathrm{Aut}(\mathcal{E})$ preserving $\mathcal{E}$. By Theorem 2.2.10, we may assume without loss of generality $\lambda = -1$. Hence, the vertex of $\mathcal{H}_3$ is the point $Y_\infty = (0, 1, 0)$.

Lemma 2.2.11. *A linear collineation γ belongs to $\mathrm{Aut}(\mathcal{E})$ if and only if*

$$\gamma(a, c, d) : (X, Y, Z) \to (aX, Y + cZ, dZ),$$

with

(i) $d \in \mathrm{GF}(\sqrt{q})^\star$;

(ii) $\mathfrak{T}(c) = 1 - d$;

(iii) $\mathfrak{N}[a] = d^2$.

Proof. The collineation γ fixes the vertices $(1, 0, 0)$ and $(0, 1, 0)$ of both Hermitian cones in Γ. Hence, it is represented by a non-singular matrix of the form

$$g = \begin{bmatrix} a & 0 & b \\ 0 & 1 & c \\ 0 & 0 & d \end{bmatrix}.$$

Since γ preserves $\mathcal{H}_2$,

$$\gamma(\mathcal{H}_2) = \lambda(aX + bZ)^{\sqrt{q}+1} + (dZ)^{\sqrt{q}+1} = \lambda a^{\sqrt{q}+1} X^{\sqrt{q}+1} + (b + d)^{\sqrt{q}+1} Z^{\sqrt{q}+1} + \mathfrak{T}[a b^{\sqrt{q}} X Z^{\sqrt{q}}] = \mathcal{H}_2.$$

Hence, given that $a \neq 0$, the following are necessary conditions for g in order to represent γ:

(i) $b = 0$;

(ii) $a^{\sqrt{q}+1} = d^{\sqrt{q}+1}$.

On the other hand, the image of $\mathcal{H}_3$ under γ is

$$\gamma(\mathcal{H}_3) = \lambda[\mathfrak{T}((Y + cZ)(dZ)^{\sqrt{q}}] - (dZ)^{\sqrt{q}+1} =$$
$$\lambda\mathfrak{T}[d^{\sqrt{q}}YZ^{\sqrt{q}} + cd^{\sqrt{q}}Z^{\sqrt{q}+1}] - (dZ^{\sqrt{q}+1}) =$$
$$\lambda\mathfrak{T}[d^{\sqrt{q}}YZ^{\sqrt{q}}] + (\mathfrak{T}[cd^{\sqrt{q}}] - d^{\sqrt{q}+1})Z^{\sqrt{q}+1}.$$

Hence, $d \neq 0$ and $\gamma(\mathcal{H}_3) = \mathcal{H}_3$, which together imply $d^{\sqrt{q}} = d$, that is (i), and $d\mathfrak{T}[c] - d^2 = d$, that is (ii). □

Lemma 2.2.12. *Let G be the subgroup of $\mathrm{Aut}(\mathcal{E})$ preserving $\mathcal{H}_1$. Then, we can write $\mathrm{Aut}(\mathcal{E}) = C_{\sqrt{q}-1}G$, where $C_{\sqrt{q}-1}$ is the cyclic group consisting of all collineations*

$$\phi(d) : (X, Y, Z) \to (X, Y, dZ)$$

with $d \in \mathrm{GF}(\sqrt{q})^{\star}$.

Proof. The action on $\mathcal{H}_1$ of a collineation γ which is represented by a matrix g as in Lemma 2.2.11 is as follows:

$$\gamma(\mathcal{H}_1) = d^2X^{\sqrt{q}+1} + d\mathfrak{T}[YZ^{\sqrt{q}}] + \mathfrak{T}[c]Z^{\sqrt{q}+1}.$$

In order for the image to be $\mathcal{H}_1$, we clearly need $d = 1$ and $\mathfrak{T}[c] = 0$. The latter yields $\mathfrak{N}[a] = 1$; hence, every element in $\mathrm{Aut}(\mathcal{H})$ can be written as a the product of an element in $C_{\sqrt{q}-1}$ by an element in G. □

Lemma 2.2.13. *The group G has order $(\sqrt{q} + 1)\sqrt{q}$ and it is isomorphic to the semidirect product of an elementary Abelian normal subgroup of order $\sqrt{q}$ by a cyclic group of order $\sqrt{q} + 1$.*

Proof. The collineations $\gamma(1, c, 1)$ form an elementary Abelian subgroup $E_{\sqrt{q}}$ of order $\sqrt{q}$. Likewise, the set of the collineations of the form $\gamma(a, 0, 1)$ with $\mathfrak{N}[a] = 1$ constitutes a cyclic subgroup $C_{\sqrt{q}+1}$ of order $\sqrt{q} + 1$. The generic element of G is of the form $g(a, c, 1)$, with the before mentioned conditions on c and a. In fact,

$$g(a, c, 1) = g(1, c, 1)g(a, 0, 1),$$

which implies the result. □

Lemma 2.2.14. *The group G acts on the points of $\mathcal{E}$ distinct from $(0, 1, 0)$ as a regular permutation group.*

Proof. We keep using the notation introduced in the previous lemma. Let Δ_2 be the set of all generators of $\mathcal{H}_2$. The cyclic component $C_{\sqrt{q}+1}$ consists of elations of centre X_∞ and axis $[X = 0]$. Since $[X = 0]$ is not an element of Δ, but $C_{\sqrt{q}+1}$ preserves $\mathcal{H}_2$, we obtain that $C_{\sqrt{q}+1}$ acts in a fixed-point free manner on Δ. It follows that $C_{\sqrt{q}+1}$ is regular on the generators of $\mathcal{H}_2$. Likewise, the elementary Abelian subgroup $E_{\sqrt{q}}$ of G acts transitively on the set of all generators Δ_3 of $\mathcal{H}_3$ distinct from $[Z = 0]$. Since any point of $\mathcal{E}$ is obtained as the intersection of an element of Δ_2 with an element of Δ_3, it follows that G is transitive on the points of $\mathcal{E}$ distinct from $(0, 1, 0)$. Finally, observe that G has order $\sqrt{q}(\sqrt{q} + 1)$ which is equal to the size of $\mathcal{E} \setminus (0, 1, 0)$. □

By virtue of the above lemmas, both the abstract structure and the action of $\mathrm{Aut}(\mathcal{E})$ are completely determined.

Theorem 2.2.15. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *in class II acts transitively on the points of* $\mathcal{E}$ *distinct from the special point. Furthermore,* $\mathrm{Aut}(\mathcal{E})$ *has order* $\sqrt{q}(q - 1)$ *and*

$$\mathrm{Aut}(\mathcal{E}) \simeq C_{\sqrt{q}-1} \times (E_{\sqrt{q}} \rtimes C_{\sqrt{q}+1}).$$

Class III

Let $\mathcal{E}$ be a Hermitian intersection in class III. A non-singular Hermitian curve $\mathcal{H}_1$ in the pencil Γ is assumed to be in form (M3), that is

$$\mathcal{H}_1 : XY^{\sqrt{q}} - X^{\sqrt{q}}Y + \omega Z^{\sqrt{q}+1} = 0,$$

with $\omega^{\sqrt{q}-1} = -1$. Since the collineation group preserving $\mathcal{H}_1$ is doubly transitive on the points of $\mathcal{H}_1$, the two generators of the Hermitian cone $\mathcal{H}_2$ in $\mathcal{E}$ may be assumed to be the tangent lines to $\mathcal{H}_1$ at the points $(0, 1, 0)$ and $(1, 0, 0)$. Then, $\mathcal{H}_2$ has equation

$$\mathcal{H}_2 : XY^{\sqrt{q}} - uYX^{\sqrt{q}} = 0,$$

with $u^{\sqrt{q}+1} = 1$. Actually, $u \neq 1$. In fact, every generator of $\mathcal{H}_2$ different from the axes must be a chord of $\mathcal{H}_1$, and this occurs if and only if $u \neq 1$. Hence, in our setting, we have just $\sqrt{q}$ pairwise distinct Hermitian intersections.

Theorem 2.2.16. *Hermitian intersections in class III are projectively equivalent.*

Proof. For every $t \in GF(q)$ such that $u = t^{\sqrt{q}-1}$, define the linear collineation

$$\theta_t : (X, Y, Z) \to ((1 - t)^{-1}X, Y, Z).$$

The image of $\mathcal{H}_1$ under θ_t is

$$\theta_t(\mathcal{H}_1) = (1 - t)^{-1}XY^{\sqrt{q}} - (1 - t^{\sqrt{q}})^{-1}X^{\sqrt{q}}Y + \omega Z^{\sqrt{q}+1} := \bar{\mathcal{H}}_1.$$

Likewise,

$$\theta_t(\mathcal{H}_2) = (1-t)^{-1}XY^{\sqrt{q}} - u(1-t^{\sqrt{q}})^{-1}YX^{\sqrt{q}} = XY^{\sqrt{q}} + X^{\sqrt{q}}Y.$$

On the other hand, since $\mathcal{H}_1 = \bar{\mathcal{H}}_1 + t(t-1)^{-1}\bar{\mathcal{H}}_2$, the collineation θ_t maps $\mathcal{E}$ into the Hermitian intersection $\bar{\mathcal{E}}$ generated by $\mathcal{H}_1$ and $\bar{\mathcal{H}}_2$. For two distinct values of t, the resulting Hermitian intersections do not coincide. In fact, if $t \in \mathrm{GF}(q)$ also satisfies the above condition, that is $\bar{t}^{\sqrt{q}-1} = u$, and $(1-t)(1-t^{\sqrt{q}})^{-1} = (1-\bar{t})(1-\bar{t})^{\sqrt{q}-1}$ holds, then we have $(1-t)(1-tu)^{-1} = (1-\bar{t})(1-u\bar{t})^{-1}$, and the latter relation implies $t = \bar{t}$. This shows that the family parametrized by t consists of $\sqrt{q}-1$ pairwise distinct Hermitian intersections which are projectively equivalent to $\mathcal{E}$. None of them coincides with $\mathcal{E}$, as $(1-t)(1-t^{\sqrt{q}}) = 1$ implies $u = 1$ which is currently ruled out. Adding $\mathcal{E}$ to that family, we obtain all possible Hermitian intersections, and this completes the proof. □

To determine the abstract structure and the action of $\mathrm{Aut}(\mathcal{E})$, we need some further preliminary results.

Lemma 2.2.17. *The linear collineation group G preserving both $\mathcal{H}_1$ and $\mathcal{H}_2$ consists of all collineations*

$$\gamma(a) : (X, Y, Z) \to (a^{\sqrt{q}+1}X, Y, aZ),$$
$$\delta(a) : (X, Y, Z) \to (-a^{\sqrt{q}+1}Y, X, aZ),$$

with $a \in \mathrm{GF}(q)^\star$. The subgroup $H = \{\gamma(a) | a \in \mathrm{GF}(q)^\star\}$ is a cyclic normal subgroup of G, and it acts regularly on the points of $\mathcal{E}$ distinct from $(1,0,0)$ and $(0,1,0)$. Furthermore, if $a \in \mathrm{GF}(\sqrt{q})^\star$ and q is even, then $\delta(a)$ is an involution and $G = \langle\delta(a)\rangle \rtimes H$; if q is odd, then $\delta(a)$ has order 4 and $G = C_2 \rtimes H$.

Proof. Let g be a linear collineation preserving both $\mathcal{H}_1$ and $\mathcal{H}_2$. Then, g preserves the fundamental triangle. More precisely, g fixes the origin $Z_\infty = (0,0,1)$ and either interchanges the points $Y_\infty = (0,1,0)$ and $X_\infty = (1,0,0)$, or fixes them both. In the former case, g is represented by a diagonal non-singular matrix

$$M_1(a,b) = \begin{bmatrix} b & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{bmatrix}.$$

The collineation g preserves $\mathcal{H}_2$ if and only if $GF(\sqrt{q})^\star$ contains b. For $b \in GF(\sqrt{q})^\star$, the condition on g to preserve $\mathcal{H}_1$ is equivalent to $a^{\sqrt{q}+1} = b$. Hence, if g fixes the vertices of the fundamental triangle, then $g = \gamma(a)$ with a suitable element $a \in GF(\sqrt{q})^\star$. A similar argument shows that if g interchanges the vertices X_∞ and Y_∞, then g is represented by the non-singular matrix

$$M_2(a,b) = \begin{bmatrix} 0 & b & 0 \\ 1 & 0 & 0 \\ 0 & 0 & a \end{bmatrix},$$

and a necessary and sufficient condition for g to preserve both $\mathcal{H}_1$ and $\mathcal{H}_2$ is $b = -a^{\sqrt{q}+1}$. This completes the proof of the first statement. The group H is isomorphic to the multiplicative group of $\mathrm{GF}(q)$; hence, it is cyclic of order $q-1$. Since $\delta(b)^{-1}\gamma(a)\delta(b) = \gamma(a^{\sqrt{q}})$ for all $a, b \in GF(q)^\star$, the group H is normal in G. As no non-trivial element in the subgroup H fixes a point outside the fundamental triangle, the orbit of any point $P \in \mathcal{E}$ under H has size $q-1$, the same as $\mathcal{E}$. It follows that the orbit of a $P \in \mathcal{E}$ is the whole of $\mathcal{E}$. This completes the proof of the second statement.

By direct computation, the square of δ is

$$\delta(a)^2 : (X, Y, Z) \to (-a^{\sqrt{q}+1}X, -a^{\sqrt{q}+1}Y, a^2 Z).$$

Hence, when q is even, for any $a \in \mathrm{GF}(\sqrt{q})^\star$, the collineation $\delta(a)$ is an involution and $G = \langle\delta(a)\rangle \rtimes H$. When q is odd, $\delta(a)$ has period 4, but $\delta(a)^2 = \gamma(-1) \in H$; hence, $G = C_2 \rtimes H$. □

We are in position to prove the following theorem.

Theorem 2.2.18. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *in class III acts transitively on the points of* $\mathcal{E}$ *distinct from the two special points. Furthermore,* $\mathrm{Aut}(\mathcal{E})$ *has order* $2(q-1)$ *and*

$$\mathrm{Aut}(\mathcal{E}) \simeq C_2 \rtimes C_{q-1}.$$

Proof. We prove that every linear collineation g preserving $\mathcal{E}$ belongs to the group G introduced in the previous lemma. Actually, g preserves $\mathcal{H}_2$; hence, it suffices to prove that g also preserves $\mathcal{H}_1$. As we have already noticed in the proof of Lemma 2.2.17, the condition on g to preserve $\mathcal{H}_2$ implies that g is represented by either one of the matrices $M_1(a,b)$ or $M_2(a,b)$, with $a \in GF(q)^\star,\ b \in GF(\sqrt{q})^\star$. In the former case, g sends $\mathcal{H}_1$ to the Hermitian curve $\bar{\mathcal{H}}_1$ of equation

$$XY^{\sqrt{q}} - X^{\sqrt{q}}Y + (a^{\sqrt{q}+1}b^{-1})\omega Z^{\sqrt{q}+1} = 0.$$

On the other hand, the pencil Γ generated by $\mathcal{H}_1$ and $\mathcal{H}_2$ contains $\bar{\mathcal{H}}_2$ if and only if $a^{\sqrt{q}+1}b^{-1} = 1$. This only occurs for $b = a^{\sqrt{q}+1}$, that is for $g \in G$. A similar argument shows that the same holds when g is represented by $M_2(a,b)$. □

Class IV

Let $\mathcal{E}$ be a Hermitian intersection in class IV. The non-singular Hermitian curve

$$\mathcal{H}_1 : X^{\sqrt{q}+1} + YZ^{\sqrt{q}} + Y^{\sqrt{q}}Z = 0$$

given by the model (M2), together with the Hermitian cone $\mathcal{H}_2$ of vertex $(0,1,0)$ and equation

$$\mathcal{H}_2 : ZX^{\sqrt{q}} - \lambda XZ^{\sqrt{q}} = 0, \qquad \lambda^{\sqrt{q}+1} = 1$$

can be chosen to generate the pencil Γ.

Theorem 2.2.19. *Hermitian intersections in class IV are projectively equivalent.*

Proof. Let $\lambda, \bar{\lambda}$ be elements of $\mathrm{GF}(q)$ with $\lambda^{\sqrt{q}+1} = \bar{\lambda}^{\sqrt{q}+1} = 1$. Choose $a \in \mathrm{GF}(q)^\star$ such that $a^{\sqrt{q}-1} = (\bar{\lambda}/\lambda)$. Arguing as in the proof of Theorem 2.2.10, it suffices to check that the linear collineation

$$\gamma(a) : (X, Y, Z) \rightarrow (aX, Y, Z)$$

preserves $\mathcal{H}_1$ and sends $\mathcal{H}_2$ to the Hermitian cone $\bar{\mathcal{H}}_2$ of equation

$$\bar{\mathcal{H}}_2 : ZX^{\sqrt{q}} - \bar{\lambda}XZ^{\sqrt{q}} = 0.$$

□

The previous lemma guarantees that in order to determine $\mathrm{Aut}(\mathcal{E})$ we may assume without loss of generality $\lambda = 1$.

Lemma 2.2.20. *The collineation group G which preserves both $\mathcal{H}_1$ and $\mathcal{H}_2$ consists of all collineations*

$$t(a, c, f) : \begin{cases} X \rightarrow aX + cZ \\ Y \rightarrow -acX + a^2Y + fZ \\ Z \rightarrow Z, \end{cases}$$

with $a \in \mathrm{GF}(\sqrt{q})^\star$, $c \in \mathrm{GF}(\sqrt{q})$ and $\mathfrak{T}[f] = -\mathfrak{N}[c]$.

Proof. Via a direct computation, we have

$$t(\mathcal{H}_1) = a^2X^{\sqrt{q}+1} + a^2\mathfrak{T}[YZ^{\sqrt{q}}] + (c^2 + f)Z^{\sqrt{q}+1},$$

$$t(\mathcal{H}_2) = a\mathcal{H}_2.$$

Hence, any collineation $t(a, c, f)$ belongs to G. Conversely, let γ be a linear collineation preserving $\mathcal{H}_2$. Then, γ is an elation of centre $(0, 1, 0)$ and axis $[Z = 0]$. It follows that γ is associated to a non-singular matrix

$$\begin{bmatrix} a & 0 & c \\ d & e & f \\ 0 & 0 & 1 \end{bmatrix},$$

with $a \in \mathrm{GF}(\sqrt{q})^\star$ and $c \in \mathrm{GF}(\sqrt{q})$. Since γ preserves $\mathcal{H}_1$ as well, then $d = -ac$, $e = a^2$ and $\mathfrak{T}[f] = -\mathfrak{N}[c]$. □

Lemma 2.2.21. *The subgroup T of G consisting of all collineations of the form $t(1, 0, f)$ is elementary Abelian of order $\sqrt{q}$. In fact, $T \simeq E_{\sqrt{q}}$, and $G/T \simeq \mathrm{AGL}(1, \sqrt{q})$. The group T is the* translation subgroup *of G.*

Proof. The order of $t(1,0,f)$ is, for any suitable f, equal to the characteristic p of $\mathrm{GF}(\sqrt{q})$ and any two elements in T commute; hence, T is an elementary Abelian group. Since $\mathfrak{T}(f) = 0$ has $\sqrt{q}$ solutions, T has order $\sqrt{q}$ and $T \simeq E_{\sqrt{q}}$. Let now $\bar{G}$ be the permutation group induced by G on the set Δ of all generators of $\mathcal{H}_2$. We show that the kernel K of the permutation representation $G \to \bar{G}$ is T. It is immediate to verify that any element of T fixes all the lines through $(0,1,0)$; hence, $T \leq K$. On the other hand, the generic line through $(0,1,0)$ is of the form

$$l : [\alpha Z + X] = 0,$$

with $\alpha \in \mathrm{GF}(q) \cup \{\infty\}$. Any linear collineation t of G acts on l by transforming it into the line

$$l^t : [\frac{(\alpha + c)}{a} Z + X] = 0.$$

Hence, if $a \neq 1$ or $c \neq 0$, the collineation $t(a,c,f)$ fixes at most two generators of $\mathcal{H}_2$. It follows that T is the full kernel of the representation of G into $\bar{G}$. The proof is completed by observing that, according to Lemma 2.2.20, $\bar{G}$ acts on Δ as the group of all permutations $X \to aX + c$ with $a \neq 0$ and c ranging over $\mathrm{GF}(\sqrt{q})$. □

The abstract structure and the action of the linear collineation group $\mathrm{Aut}(\mathcal{E})$ are given in the following theorem.

Theorem 2.2.22. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *in class IV acts transitively on the points of* $\mathcal{E}$ *distinct from the special point. Furthermore,* $|\mathrm{Aut}(\mathcal{E})| = q(\sqrt{q} - 1)$ *and*

$$\mathrm{Aut}(\mathcal{E})/E_{\sqrt{q}} \simeq \mathrm{AGL}(1, \sqrt{q}).$$

Proof. The translation group T acts transitively on the common points of $\mathcal{E}$ and any affine line through $(0,1,0)$. Also, as seen in the proof of the previous lemma, G acts transitively on the generators of $\mathcal{H}_2$. This proves the transitivity of G on the points of $\mathcal{E}$ distinct from $(0,1,0)$. It remains to show that G coincides with $\mathrm{Aut}(\mathcal{E})$. Take $g \in \mathrm{Aut}(\mathcal{E})$ and let $\bar{g}$ be the permutation induced by g on the set Δ of the generators of $\mathcal{H}_2$. If g is in the kernel of the permutation representation $\mathrm{Aut}(\mathcal{E}) \to \overline{\mathrm{Aut}(\mathcal{E})}$, then g is a translation. Let $T' = \langle T, g \rangle$ be the group generated by T and g. Then, T' is again a translation group. Hence, no non-trivial element in T' fixes an affine point. On the other hand, T' preserves the set of all common points of $\mathcal{E}$ and one affine line through $(0,1,0)$. This yields that T' has order at most $\sqrt{q}$; hence $T' = T$, that is $g \in T$. The factor group $\mathrm{Aut}(\mathcal{E})/T$ induces on Δ a permutation group containing G/T. Since $\mathrm{Aut}(\mathcal{E})/T$ preserves $\mathcal{H}_2$, it follows that $\mathrm{Aut}(\mathcal{E})/T$ consists of permutations

$$X \to aX + b,$$

with $a \in \mathrm{GF}(\sqrt{q})^{\star}$, $b \in \mathrm{GF}(\sqrt{q})$. This proves that $G/T = \mathrm{Aut}(\mathcal{E})/T$ and, therefore, $G = \mathrm{Aut}(\mathcal{E})$. □

Class V

Let $\mathcal{E}$ be a Hermitian intersection in class V. The non-singular Hermitian curve

$$\mathcal{H}_1 : X^{\sqrt{q}+1} + YZ^{\sqrt{q}} + Y^{\sqrt{q}}Z = 0,$$

given by (M2), together with the totally degenerated Hermitian cone of equation

$$\mathcal{H}_2 : X^{\sqrt{q}+1} = 0$$

can be chosen to generate the pencil Γ. From Theorem 2.1.4 and Corollary 1.7.26, every Hermitian intersection in class V is a Baer subline of $\mathrm{PG}(2, q)$. Arguing as in section 2.2.4 or, alternatively, using classical results from finite geometry, see [Hir98b], the following theorems can be proved.

Theorem 2.2.23. *Hermitian intersections in class V are projectively equivalent.*

Theorem 2.2.24. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *in class V acts* 3*-transitively on the points of* $\mathcal{E}$ *and has order* $q^2\sqrt{q}(q-1)^2(q+1)$. *Let* $AG(2, q)$ *be the affine plane whose infinite line contains* $\mathcal{E}$ *and let* O *be a point of* $AG(2, q)$. *Then, the subgroup* K *of* $\mathrm{Aut}(\mathcal{E})$ *fixing* $\mathcal{E}$ *point-wise is the semidirect product of the full translation group* T *of* $AG(2, q)$ *by the group of all dilatations of* $AG(2, q)$ *with centre* O. *Furthermore,*

$$\mathrm{Aut}(\mathcal{E})/K \simeq \mathrm{PGL}(1, \sqrt{q}).$$

Class VI

Let $\mathcal{E}$ be a Hermitian intersection in class VI. The non-singular Hermitian curve

$$\mathcal{H}_1 : X^{\sqrt{q}+1} + YZ^{\sqrt{q}} + Y^{\sqrt{q}}Z = 0,$$

given by (M2), together with the totally degenerated Hermitian cone

$$\mathcal{H}_2 : Z^{\sqrt{q}+1} = 0$$

can be chosen to generate the pencil Γ. Every Hermitian intersection in class VI is reduced to a single point of $\mathrm{PG}(2, q)$. Then, the following theorems hold.

Theorem 2.2.25. *Hermitian intersections in class VI are projectively equivalent.*

Theorem 2.2.26. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *in class VI has order* $q(q+1)(q-1)^2$ *and is isomorphic to* $\mathrm{AGL}(2, q)$.

Class VII

Let $\mathcal{E}$ be a Hermitian intersection in class VII. Then, [BS86], [Cos97], [Ebe85], [FHT86] and [Kes89] have proven that $\mathcal{E}$ is the point-orbit of a Singer subgroup of order $(q-\sqrt{q}+1)$ and its points form a complete $(q-\sqrt{q}+1)$-arc in $\mathrm{PG}(2,q)$. In this case, we will use the model (M4) for $\mathcal{H}_1$:

$$\mathcal{H}_1 : XY^{\sqrt{q}} + YZ^{\sqrt{q}} + ZX^{\sqrt{q}} = 0.$$

Observe that the collineation β maps the curve $\mathcal{H}$ associated with the equation (M4) into the Hermitian curve of equation

$$\mathcal{H}_1^\beta : b^{q\sqrt{q}+1}XY^{\sqrt{q}} + b^{q-\sqrt{q}+1}YZ^{\sqrt{q}} + ZX^{\sqrt{q}} = 0.$$

Since $\mathcal{H}_1 \neq \mathcal{H}^\beta$, we may choose $\mathcal{H}^\beta$ as $\mathcal{H}_2$. The intersection $\mathcal{E} = \mathcal{H}_1 \cap \mathcal{H}_1^\beta$ consists of the points of Π that satisfy the following system of equations:

$$\begin{cases} XY^{\sqrt{q}} + YZ^{\sqrt{q}} + ZX^{\sqrt{q}} = 0 \\ (a^{q-\sqrt{q}+1} - a^{q\sqrt{q}+1})YZ^{\sqrt{q}} + (1 - a^{q\sqrt{q}+1})ZX^{\sqrt{q}} = 0 \\ Z = 1. \end{cases}$$

It follows that

$$Y = -X^{\sqrt{q}} \frac{a^{q^2+q+1} - a^{q\sqrt{q}+1}}{a^{q-\sqrt{q}+1} - a^{q\sqrt{q}+1}} = X^{\sqrt{q}} \frac{a^{q(q-\sqrt{q}+1)} - 1}{a^{\sqrt{q}(q-\sqrt{q}+1} - 1} = X^{\sqrt{q}}(a^{(q-\sqrt{q}+1} - 1)^{q-1} = X^{\sqrt{q}}.$$

Hence, $\mathcal{E}$ is represented by all the points of the form $(\epsilon, \epsilon^{\sqrt{q}}, 1)$ with $\epsilon^{q-\sqrt{q}+1} = 1$ and it is a set of cardinality $q-\sqrt{q}+1$. From 2.1.4, it follows that $\mathcal{E}$ is an arc and that the intersection of $\mathcal{H}_1$ and $\mathcal{H}_2 = \mathcal{H}_1^\beta$ is in class VII.

Theorem 2.2.27. *Hermitian intersections in class VII are projectively equivalent.*

Proof. This theorem is a corollary to the known result that any two Singer subgroups of the same order are conjugate under the full linear collineation group $\mathrm{PGL}(3,q)$ of $\mathrm{PG}(2,q)$, see [Blo67], [Har26] and [Mit11]. □

Theorem 2.2.28. *The linear collineation group* $\mathrm{Aut}(\mathcal{E})$ *preserving a Hermitian intersection* $\mathcal{E}$ *in class VII is transitive on the points of* $\mathcal{E}$*. Furthermore,* $\mathrm{Aut}(\mathcal{E})$ *contains a normal cyclic subgroup of order* $q-\sqrt{q}+1$ *acting regularly on the points of* $\mathcal{E}$ *and*

$$\mathrm{Aut}(\mathcal{E}) = C_3 \rtimes C_{q-\sqrt{q}+1}.$$

Proof. In the above model, the Singer subgroup S of order $q-\sqrt{q}+1$ generated by $\gamma = \beta^{q+\sqrt{q}+1}$ preserves $\mathcal{E}$, as it preserves both $\mathcal{H}_1$ and $\mathcal{H}_2$. The same holds true for the linear collineation group E of order 3 generated by

$$\tau : (X, Y, Z) \to (Y, Z, X).$$

Since E normalises S, the group $G = \langle E, S\rangle$ is the semidirect product of S by E. Hence, $G \simeq C_3 \rtimes C_{q-\sqrt{q}+1}$.

To prove that $\mathrm{Aut}(\mathcal{E}) = G$ it will be useful to regard $\mathcal{E}$ as a $(q-\sqrt{q}+1)$-arc. Let Λ be the algebraic envelope associated to $\mathcal{E}$, viewed as an algebraic curve in the dual plane of $\mathrm{PG}(2, q)$. Clearly, $\mathrm{Aut}(\mathcal{E})$ is an automorphism group of Λ. For q even, Λ is a projectively equivalent to a non-singular Hermitian curve $\mathcal{H}$, see [Tha87]. The same holds for q odd, provided that projective equivalence is replaced by birational equivalence, see [CK98]. In any case, $\mathrm{Aut}(\mathcal{E})$ turns out to be isomorphic to a subgroup L of $\mathrm{PGU}(3, q)$. Since $G \le \mathrm{Aut}(\mathcal{E})$, L contains a subgroup isomorphic to G. Then, the assertion follows from the classification of all maximal subgroups of $\mathrm{PGU}(3, q)$, see [Har26], [Hof72] and [Mit11]. In fact, the subgroups of $\mathrm{PGU}(3, q)$ which are the semidirect product of a cyclic group of order 3 by a cyclic group of order $q-\sqrt{q}+1$ are all maximal in $\mathrm{PGU}(3, q)$. □

2.3 A group-theoretic characterization of Hermitian curves as classical unitals

The non-canonical model presented in 2.2.2 is used in order to provide a short proof of an already known characterization of classical unitals [CEK00]. This work has been submitted for publication [Giua].

2.3.1 Introduction

We recall some basic definitions. A unital in a Desarguesian projective plane $\mathrm{PG}(2, q)$ of square order q, is a set $\mathcal{U}$ of $q\sqrt{q}+1$ points such that any line of $\mathrm{PG}(2, q)$ meets $\mathcal{U}$ in either 1 or $\sqrt{q}+1$ points. The absolute points of a unitary polarity of $\mathrm{PG}(2, q)$ form a unital which is called the *classical* (or *Hermitian*) unital. The linear collineation group of $\mathrm{PG}(2, q)$ preserving a classical unital is $\mathrm{PGU}(3, q)$. By a theorem due to Hoffer [Hof72] this group-theoretic property characterises classical unitals: if a unital $\mathcal{U}$ is preserved by a collineation group isomorphic to $\mathrm{PSU}(3, q)$, then $\mathcal{U}$ is classical. Cossidente, Ebert and Korchmáros [CEK00] showed that Hoffer's result holds true under some weaker assumption, namely for unitals preserved by a Singer subgroup of $\mathrm{PGL}(3, q)$ of order $q-\sqrt{q}+1$. Their proof heavily depends on previous results concerning cyclic partitions of $\mathrm{PG}(2, q)$ in Baer sub-planes. A different and shorter proof of this result is the purpose of the present section.

Theorem 2.3.1. *A unital $\mathcal{U}$ in $\mathrm{PG}(2, q)$ is classical if and only if it is preserved by a cyclic linear collineation group of order $q-\sqrt{q}+1$.*

2.3.2 A result on classical unitals

The following remarkable property of classical unitals is from [CEK00].

Theorem 2.3.2 (Proposition 3.2 [CEK00])**.** *Let $q = p^k$. Every unital $\mathcal{U}$ of the projective plane $\mathrm{PG}(2,q)$ meets every classical unital in $r \equiv 1 \mod p$ points.*

Proof. Let $l_1, \ldots, l_r$ be a set of lines of $\mathrm{PG}(2,q)$ and let $\bar{l}_i$ be the characteristic vector of l_i. By definition of unital, a line l intersects $\mathcal{U}$ in either 1 or $\sqrt{q}+1$ points. Let $\bar{u}$ be the characteristic vector of $\mathcal{U}$. Then, the dot product between $\bar{u}$ and any combination of lines can be evaluated as

$$\bar{u} \cdot (\bar{l}_1 + \ldots + \bar{l}_r) \equiv r \mod p.$$

A theorem due to Blokhuis, Brouwer and Wilbrink [BBW91] (see also [AK92, 6.7.1]), states that a classical unital $\mathcal{H}$ is a codeword in the $\mathrm{GF}(p)$-code generated by the lines of $\mathrm{PG}(2,q)$. This is to say that the characteristic vector $\bar{h}$ of $\mathcal{H}$ is a combination of characteristic vectors $\bar{l}_1, \ldots, \bar{l}_r$ of the lines of the projective space. Since the number of points of $\mathcal{H}$ is $q\sqrt{q}+1$, working modulus p,

$$\begin{aligned} 1 &= \bar{h} \cdot \bar{h} \\ &= \bar{h} \cdot (\bar{l}_1 + \ldots \bar{l}_r) \\ &= \bar{h} \cdot \bar{l}_1 + \ldots \bar{h} \cdot \bar{l}_r, \end{aligned}$$

and $r \equiv 1 \mod p$. Now, the dot product between $\bar{u}$ and $\bar{h}$ can be computed as

$$\bar{u} \cdot \bar{h} = \bar{u} \cdot (\bar{l}_1 + \ldots + \bar{l}_r) = \bar{u} \cdot \bar{l}_1 + \ldots + \bar{u} \cdot \bar{l}_r \equiv r \mod p.$$

The result follows. □

2.3.3 Proof of Theorem 2.3.1

Here, we consider a Singer collineation group acting on the points and lines of the non-canonical model Π of $\mathrm{PG}(2,q)$ in $\mathrm{PG}(2,q^3)$ as introduced in section 2.2.2.

Assume $\mathcal{H}$ to be the Hermitian curve of Π with equation (M4) and define K as its stabiliser in $\mathcal{B}$. Since $\mathcal{B}$ is Abelian, K is normal in $\mathcal{B}$ and it is possible to construct a quotient incidence structure Π_0 in the following way: define *thick points* as the point-orbits of Π under K, *thick lines* as the orbits of $\mathcal{H}$ under $\mathcal{B}$, and incidence as inclusion. Note that the factor group $\mathcal{B}/K$ is a Singer group for Π_0, as it acts regularly on the set of thick-points as well as on the set of thick-lines.

We need the following characterization of finite projective planes as incidence structures.

Lemma 2.3.3 (Proposition 3.2.3(m), [Dem68])**.** *An incidence structure (P, L, I) is a projective plane of order n if and only if*

(i) $|P| \leq n^2+n+1$;

(ii) $|L| \geq n^2+n+1$;

(iii) *every line in* L *contains at least* $n+1$ *points;*

(iv) *any two distinct lines of* L *meet in at most* 1 *point.*

Lemma 2.3.4. *The incidence structure* Π_0 *is a projective plane of order* $\sqrt{q}$.

Proof. Since the index $[\mathcal{B} : K]$ is equal to $q+\sqrt{q}+1$, the number of thick-points in Π_0 is $q+\sqrt{q}+1$. According to Lemma 2.2.5, the subgroup of $\mathcal{B}$ which preserves $\mathcal{H}$ is K; hence, we have $q+\sqrt{q}+1$ thick lines as well. Furthermore, every thick line is incident with $\sqrt{q}+1$ thick points, as the size of $\mathcal{H}$ is $q\sqrt{q}+1$. By Lemma 2.3.3, in order to prove that Π_0 is a projective plane of order $\sqrt{q}$, it now suffices to verify that two thick lines share at most one thick point. Since thick-lines are classical unitals, for $q > 9$ the assertion follows from the fact that the number of common points of two distinct classical unitals in Π is at most $(\sqrt{q}+1)^2$, smaller than $2(q-\sqrt{q}+1)$. For $q = 4, 9$ a direct counting argument proves the assertion. □

We are now in position to prove Theorem 2.3.1.

Proof of Theorem 2.3.1. For any $n \mid q^2+q+1$, all Singer subgroups of order n are conjugate in $PGU(3,q)$; hence, we may assume without loss of generality that $\mathcal{U}$ is a unital in Π which is preserved by K. This hypothesis implies that $\mathcal{U}$ is the union of $\sqrt{q}+1$ point-orbits under K, and hence, the unital $\mathcal{U}$ can be viewed as a set Δ of $\sqrt{q}+1$ thick points in Π_0. In order to prove Theorem 2.3.1, it remains to show that Δ is actually a thick line, or, equivalently, that $\mathcal{U}$ meets $\mathcal{H}$ and every image of $\mathcal{H}$ under the action of $\mathcal{B}$; this is a corollary of Theorem 2.3.2. □

Chapter 3

The 3-dimensional case: Hermitian surfaces

This chapter deals with the point-line-plane incidence configurations arising from the intersection of two Hermitian surfaces. First, we consider which intersections fulfill some combinatorial conditions in order to be possible. Later, we determine classes of matrices that allow us to directly construct such intersections. For the purposes of this chapter, we mean by *Hermitian cone* a degenerate Hermitian surface of rank 3.

3.1 Description of incidence configurations in dimension 3

In this section we describe the possible point-line configurations arising from the intersection of two Hermitian surfaces in $\mathrm{PG}(3,q)$. The argument here is purely combinatorial. For a description of the geometric cases which can actually be realized in $\mathrm{PG}(3,q)$ and models of the intersections, please see section 3.3.

The following result, which will be proven in Chapter 4 for dimension n, is needed.

Lemma 3.1.1. *Let $\mathcal{H}_1$, $\mathcal{H}_2$ be two distinct Hermitian surfaces; then, the size of the intersection $\mathcal{E} = \mathcal{H}_1 \cap \mathcal{H}_2$ depends only upon the number and rank of the degenerate surfaces in the linear system $\Gamma = \langle \mathcal{H}_1, \mathcal{H}_2 \rangle$. Define as r_i the number of surfaces in Γ of rank i; then, the size of $\mathcal{E}$ for the various possible values of r_i is as in Tables 3.1, 3.2 and 3.3.*

Definition 3.1.2. A linear system Γ is *non-degenerate* if it contains at least a non-degenerate Hermitian surface.

Definition 3.1.3. We say that two points are *conjugate* with respect to the linear system Γ if they are conjugate with respect to any non-degenerate surface in Γ.

r_1	r_2	r_3	$k = \|\mathcal{E}\|$
0	0	0	$(q+1)^2$
0	0	1	$(q+\sqrt{q}+1)(q-\sqrt{q}+1)$
0	0	2	(q^2+1)
0	0	3	q^2-q+1
0	0	4	$(q-1)^2$
0	1	0	$q^2+q\sqrt{q}+q+1$
0	1	1	$q^2+q\sqrt{q}+1$
0	1	2	$(\sqrt{q}+1)(q\sqrt{q}-q+1)$
0	2	0	$(\sqrt{q}+1)(q\sqrt{q}+q-\sqrt{q}+1)$
1	0	0	$q\sqrt{q}+q+1$
1	0	1	$q\sqrt{q}+1$

Table 3.1: Possible intersection numbers for Hermitian surfaces: non-degenerate pencil.

r_1	r_2	r_3	$k = \|\mathcal{E}\|$
0	0	$\sqrt{q}+1$	$q^2-q\sqrt{q}+q+1$
0	1	$\sqrt{q}$	$(q+\sqrt{q}+1)(q-\sqrt{q}+1)$
0	2	$\sqrt{q}-1$	$(\sqrt{q}+1)^2(q-\sqrt{q}+1)$
0	3	$\sqrt{q}-2$	$q^2+2q\sqrt{q}+\sqrt{q}+1$
1	0	$\sqrt{q}$	$q+1$
1	1	$\sqrt{q}-1$	$q\sqrt{q}+q+1$

Table 3.2: Possible intersection numbers for Hermitian surfaces: degenerate pencil; $r_3 \neq 0, r_4 = 0$.

r_1	r_2	$k = \|\mathcal{E}\|$
0	$\sqrt{q}+1$	$2q^2+q+1$
1	$\sqrt{q}$	q^2+q+1
2	$\sqrt{q}-1$	$q+1$

Table 3.3: Possible intersection numbers for Hermitian surfaces: degenerate pencil; $r_2 \neq 0, r_3 = r_4 = 0$.

3.1.1 Some general remarks on cones

Lemma 3.1.4. *Assume $r_3(\Gamma) \geq 1$ and $r_4(\Gamma) \geq 1$. Take a cone $\mathcal{C}$ of vertex V in Γ. Let π be the polar plane of V with respect to a non-degenerate surface $\mathcal{H} \in \Gamma$, and define $k = |\mathcal{C} \cap \mathcal{H}|$ and $h = |\mathcal{P}|$ where*

$$\mathcal{P} := \mathcal{C} \cap \mathcal{H} \cap \pi.$$

Then, if $V \notin \mathcal{H}$,

$$k = q^2 + q\sqrt{q} + \sqrt{q} + 1 - \sqrt{q}h;$$

if $V \in \mathcal{H}$,

$$k = q^2 + \sqrt{q} + 1 + (h-1)(\sqrt{q} - \frac{1}{\sqrt{q}}).$$

Proof. All tangents to the surface $\mathcal{H}$ through V are of the form VP with $P \in \pi \cap \mathcal{H}$; hence, all components of the cone $\mathcal{C}$ tangent to $\mathcal{H}$ are of the form VP' with $P' \in \mathcal{P}$, while the remaining $(q\sqrt{q} + 1 - h)$ lines are secant, that is intersecting $\mathcal{H}$ in $\sqrt{q} + 1$ distinct points.

Hence,

$$k = h + (q\sqrt{q} + 1 - h)(\sqrt{q} + 1),$$

and the first part of the lemma is proven.

Assume now that $V \in \mathcal{H}$. This implies that $V \in \pi$ and π is tangent to $\mathcal{H}$. Hence, $\pi \cap \mathcal{H}$ decomposes in $\sqrt{q} + 1$ lines. On the other hand, π intersects $\mathcal{C}$ in either one point or in a Hermitian cone, that is in $\sqrt{q} + 1$ lines. Let $j = (h-1)/q$ be the number of lines of π in common between $\mathcal{C}$ and $\mathcal{H}$. Each of these lines is fully included in $\mathcal{H} \cap \mathcal{C}$. All lines of $\mathcal{C}$ not on π are secant to $\mathcal{H}$, that is they intersect $\mathcal{H}$ in $\sqrt{q} + 1$ points, one of those is V. It follows,

$$k = \sqrt{q}(q\sqrt{q} + 1 - j) + 1 - jq,$$

that is

$$k = q^2 + \sqrt{q} + 1 + (h-1)(\sqrt{q} - \frac{1}{\sqrt{q}}).$$

□

Corollary 3.1.5. *Assume $\mathcal{C}$ to be a Hermitian cone of vertex $V \notin \mathcal{H}$ and let π be the polar plane of V. As usual, denote by r_i the number of Hermitian surfaces of rank i in the linear system Γ. Then, the intersection between $\mathcal{C}$ and $\mathcal{H}$ belongs to one of the classes presented in table 3.4.*

Proof. The proof is done directly by a counting argument. □

Corollary 3.1.6. *Assume that $r_1(\Gamma) = r_2(\Gamma) = 0$, while $r_3(\Gamma), r_4(\Gamma) \geq 1$, and let $\mathcal{C}_1$ and $\mathcal{C}_2$ be distinct cones in Γ of vertices respectively V_1 and V_2. If $V_2 \notin \mathcal{E}$, then V_1 belongs to the polar plane π of V_2 with respect to any non-degenerate surface in Γ.*

h	r_1	r_2	r_3	$\|\mathcal{U}_3 \cap \mathcal{K}\|$	(r'_1, r'_2)
$q-\sqrt{q}+1$	0	0	1	q^2+q+1	$(0,0)$
$q+1$	0	0	2	q^2+1	$(0,1)$
$q+\sqrt{q}+1$	0	0	3	q^2-q+1	$(0,2)$
$(\sqrt{q}+1)^2$	0	0	4	q^2-2q+1	$(0,3)$
1	0	1	1	$q^2+q\sqrt{q}+1$	$(1,0)$
$\sqrt{q}+1$	0	1	2	$q^2+q\sqrt{q}-q+1$	$(1,1)$
$q\sqrt{q}+1$	1	0	1	$q\sqrt{q}+1$	$N.A.$

Table 3.4: Possible intersections $\mathcal{E}$ between a cone and a non degenerate Hermitian surface; vertex not in the intersection.
The column (r'_1, r'_2) describes the type of *planar* configuration in $\mathcal{E} \cap \pi$, where π is the polar plane of the vertex of $\mathcal{C}$.

Proof. Let π be the polar plane of V_2 with respect to a non-degenerate surface $\mathcal{H} \in \Gamma$. Consider the line $l = V_1V_2$. If $V_1 \notin \pi$, then l intersects $\mathcal{E} = \mathcal{C}_1 \cap \mathcal{C}_2$ in either $\sqrt{q}+1$ or $q+1$ points, but $V_2 \notin \mathcal{E}$ implies that the intersection in $q+1$ points is not possible. On the other hand, a line through the vertex of a cone intersects the cone in either 1 or $q+1$ points – a contradiction. It follows that $V_1 \in \pi$. □

Corollary 3.1.7. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two Hermitian cones in a non-degenerate linear system Γ. Assume that the parameters of Γ are of the form $(0, r_2, r_3)$, and let π be the polar plane of the vertex of $\mathcal{C}_2$ with respect to any non-degenerate surface in Γ. Then, the intersection Σ of $\mathcal{C}_1$ with π is a curve of a class corresponding to the parameters $(r_2, r_3 - 1)$.*

Proof. The claim follows from the observation that $\pi \cap \mathcal{C}_1$ is a degenerate curve. By looking up the orders in Table 2.1 we complete the proof. □

Lemma 3.1.8. *The configurations given by Σ are uniquely determined up to projectivities by the rank sequence (r_1, r_2, r_3).*

Proof. From Theorem 2.2.1, all plane intersections determining the same point-line configuration are projectively equivalent. Furthermore, following [Kes81], we see that a point-line configuration is uniquely determined by its cardinality k except in the case $(r'_1, r'_2) = (0, 1)$, when $k = q+1$.

The case $k = q+1$, corresponds to the situation in which Γ contains a cone $\mathcal{C}$ whose vertex V does not belong to $\mathcal{E}$ and the rank sequence is $(0, 0, 2)$. *A priori*, there would be two possibilities for $\mathcal{E} \cap \pi$:

(i) the intersection consists of $\sqrt{q}-1$ sublines, all disjoint;

(ii) the intersection consists of q sublines, all with a point in common.

In both cases, the lines containing the points of the intersection belong also to the cone of the pencil whose vertex V' is in the polar plane π of V. On the other hand, in case (ii), such vertex V' has to belong to $\mathcal{H}$ as well and the size of $\mathcal{E}$ would have to be q^2+q+1, while, from Table 3.4, we already know $|\mathcal{E}| = q^2+1$; a contradiction. It follows that the surfaces intersect in π in the configuration given by (i). □

Lemma 3.1.9. *Let Γ be a non-degenerate pencil of Hermitian surfaces and assume that there is at least a cone $\mathcal{C}$ in Γ whose vertex V does not belong to the base locus $\mathcal{E}$. Then, the vertices of any other cone in Γ belong to the polar plane π of V with respect to any non-degenerate surface $\mathcal{H} \in \Gamma$.*

Proof. The intersection of $\mathcal{E}$ with π corresponds to the configuration obtained as base locus of a pencil of Hermitian curves with parameters $(r'_1, r'_2) = (r_2, r_3 - 1)$. Hence, for $r_3 \geq 2$, the section of any cone $\mathcal{C}' \in \Gamma$ different from $\mathcal{C}$ with the plane π is a set of $\sqrt{q}+1$ lines, all concurrent in a point $V' \in \pi$. It follows that V' has to be the vertex of $\mathcal{C}'$. □

3.1.2 Pencils whose degenerate surfaces have all rank 3

In this subsection we describe the possible incidence configurations $\mathcal{E}$ when the pencil Γ is assumed to contain only cones as degenerate surfaces.

The vertex of any cone $\mathcal{C}_i \in \Gamma$ is denoted with the letter V_i. By $\mathcal{H}$ we denote, as usual, a generic non-degenerate surface in Γ.

For any cone $\mathcal{C} \in \Gamma$, the indices s_i are defined in Table 3.5.

s_1	number of components of $\mathcal{C}$ which are included in $\mathcal{E}$
s_2	number of components of $\mathcal{C}$ which are chords of $\mathcal{E}$
s_3	number of components of $\mathcal{C}$ tangent to $\mathcal{E}$.

Table 3.5: Indices for the intersection of a cone and a Hermitian surface.

Lemma 3.1.10. *Assume that Γ contains 4 cones $\mathcal{C}_1, \dots, \mathcal{C}_4$. Then, for any $i = 1, \dots, 4$, $V_i \notin \mathcal{E}$; furthermore, all components of any cone $\mathcal{C}_i$ intersect $\mathcal{E}$ in $\sqrt{q}+1$ points.*

Proof. The cardinality of $\mathcal{E}$ is $(q-1)^2$. Assume that the vertex of a cone $\mathcal{C}_1$ in Γ does not belong to $\mathcal{E}$. Then, each line of $\mathcal{C}_1$ intersects $\mathcal{H}$ in either $\sqrt{q}+1$ or 1 points. Hence,

$$(q-1)^2 = s_2(\sqrt{q}+1) + (q\sqrt{q}+1-s_2);$$

this is equivalent to say that there are $s_2 = q\sqrt{q} - q - 2\sqrt{q}$ lines of $\mathcal{C}_1$ which are chords of $\mathcal{E}$ and $q + 2\sqrt{q} + 1$ lines which are tangent to $\mathcal{E}$. Furthermore, since this configuration contain no line, the vertex of none of the cones in Γ may belong to $\mathcal{E}$.

Assume now that the vertex V of $\mathcal{C}$ belongs to Γ. Then,

$$(q-1)^2 - 1 = s_1(q) + s_2(\sqrt{q}) + (q\sqrt{q} - s_1 - s_2).$$

This would yield

$$q(q-\sqrt{q}-1) = (\sqrt{q}-1)[s_1(\sqrt{q}+1) + s_2],$$

a contradiction, since s_1 and s_2 are both natural numbers and $(\sqrt{q}-1)$ does not divide $q(q-\sqrt{q}-1)$. The result follows. □

Lemma 3.1.11. *Assume that Γ contains exactly 3 distinct cones and assume also that there is at least a cone $\mathcal{C} \in \Gamma$ whose vertex V is not in $\mathcal{E}$. Then, $\sqrt{q}(q-\sqrt{q}-1)$ components of $\mathcal{C}$ are chords of $\mathcal{H}$; furthermore, any cone in Γ whose vertex is in $\mathcal{E}$ contains $q\sqrt{q}-1$ chords and 2 tangents to $\mathcal{H}$.*

Proof. Since V is not in $\mathcal{H}$, then

$$q^2 - q + 1 = s_2(\sqrt{q}+1) + (q\sqrt{q} - s_2 + 1).$$

Hence,

$$q[q-\sqrt{q}-1] = s_2(\sqrt{q})$$

and $s_2 = \sqrt{q}(q-\sqrt{q}-1)$ components of $\mathcal{C}$ are chords of $\mathcal{H}$; the remaining $q+\sqrt{q}+1$ components are tangent to the surface. On the other hand, if $\mathcal{C}'$ is a cone of Γ whose vertex belongs to $\mathcal{H}$, then

$$q^2 - q + 1 = s_1'(q) + s_2'(\sqrt{q}) + 1.$$

Hence,

$$\sqrt{q}(q-1) = (\sqrt{q})s_1' + s_2'.$$

The result follows now by observing that $V \notin \mathcal{H}$ implies $s_1' = 0$. □

Lemma 3.1.12. *Let Γ be a pencil with $r_3(\Gamma) \geq 2$. Assume that the vertices V_1, V_2 of any two cones $\mathcal{C}_1$, $\mathcal{C}_2$ in Γ belong to $\mathcal{E}$; then, the line V_1V_2 is included in $\mathcal{E}$.*

Proof. The line V_1V_2 intersects $\mathcal{E}$ in at least two points. Since Γ is generated by $\mathcal{C}_1$ and $\mathcal{C}_2$, this implies that V_1V_2 is a component of both $\mathcal{C}_1$ and $\mathcal{C}_2$. The result follows. □

Lemma 3.1.13. *Assume $r_3(\Gamma) = 3$, $r_4(\Gamma) \geq 0$. Then, either the vertex of at most one cone of Γ belongs to $\mathcal{E}$ or the vertices of all three cones in Γ lie on the same line in $\mathcal{E}$.*

Proof. Assume that the vertices V_1 and V_2 of two cones $\mathcal{C}_1$ and $\mathcal{C}_2$ of Γ are points of $\mathcal{E}$. Then, according to Lemma 3.1.12, the line V_1V_2 has to be included in $\mathcal{E}$ as well, and $s_1' = 1$. On the other hand, $\mathcal{C}_1$ and $\mathcal{C}_3$ generate Γ and the only lines completely in $\mathcal{C}_3$ are those through V_3. The lemma follows. □

Lemma 3.1.14. *Let $r_3(\Gamma) = 3$ and assume $r_4(\Gamma) \geq 0$. Then, $\mathcal{E}$ contains one line and $\sqrt{q}(q-2)$ sublines.*

Proof. From the previous lemma, $s_1' = 1$. Hence,

$$q^2 - q + 1 = (q+1) + s_2'(\sqrt{q}).$$

The result follows. □

Lemma 3.1.15. *Assume $r_3(\Gamma) = 2$. Then, one of conditions (i)-(iii) has to be satisfied.*

Proof. Let $\mathcal{C}$ be a cone of Γ with vertex V.

If $V \notin \mathcal{E}$, then

$$q^2 + 1 = s_2(\sqrt{q}+1) + (q\sqrt{q} + 1 - s_2).$$

Hence,

$$s_2 = (q\sqrt{q} - q).$$

If $V \in \mathcal{H}$, then

$$q^2 = s_1(q) + s_2(\sqrt{q}).$$

Hence,

$$s_2 = \sqrt{q}(q - s_1).$$

It follows that there are three possibilities:

(i) the vertex of both cones in Γ belongs to $\mathcal{E}$; then, $s_1 = s_1' = 1$ and $s_2' = s_2 = q\sqrt{q} - 1$;

(ii) the vertex of a cone in Γ belongs to $\mathcal{E}$, the other not; then, $s_1 = 0$, $s_2 = q(\sqrt{q} - 1)$ and $s_2' = q\sqrt{q}$;

(iii) the vertex of none of the cones in Γ belongs to $\mathcal{H}$; then, $s_2 = s_2' = q(\sqrt{q} - 1)$.

□

Lemma 3.1.16. *Assume that $r_3(\Gamma) = 1$ and let $\mathcal{C}$ be the only cone in the pencil. If the vertex V of $\mathcal{C}$ does not belong to $\mathcal{E}$, then $\sqrt{q}[q - \sqrt{q} + 1]$ lines of $\mathcal{C}$ are chords; if $V \in \mathcal{E}$, then the configuration $\mathcal{E}$ contains at least a line.*

Proof. If the vertex V of $\mathcal{C}$ does not belong to $\mathcal{H}$, then

$$q^2 + q + 1 = s_2(\sqrt{q}+1) + (q\sqrt{q} + 1 - s_2).$$

Hence,

$$s_2 = \sqrt{q}[q - \sqrt{q} + 1].$$

If the vertex V of $\mathcal{C}$ belongs to $\mathcal{H}$, then

$$q^2 + q + 1 = s_1(q) + s_2(\sqrt{q}) + 1;$$

hence, $s_2 = \sqrt{q}(q + 1 - s_1)$. Since in this case $s_2 \leq q\sqrt{q} + 1$, it follows $s_1 \geq 1$. On the other hand, since $s_1 \in \{1, \sqrt{q}+1\}$, we obtain $s_2 \in \{q\sqrt{q}, q\sqrt{q} - q\}$. □

Class	c_3	v	s'_1	s'_2	s_2	k
a	4	0	-	-	$q\sqrt{q}+1$	$(q-1)^2$
b	3	0	-	-	$\sqrt{q}(q-\sqrt{q}-1)$	q^2-q+1
c	3	1	0	$\sqrt{q}(q-1)$	$\sqrt{q}(q-\sqrt{q}-1)$	q^2-q+1
d	3	3	1	$\sqrt{q}(q-2)$	$\sqrt{q}(q-\sqrt{q}-1)$	q^2-q+1
e	2	0	-	-	$q(\sqrt{q}-1)$	q^2+1
f	2	1	0	$q\sqrt{q}$	$q(\sqrt{q}-1)$	q^2+1
g	2	2	1	$q(\sqrt{q}-1)$	-	q^2+1
h	1	0	-	-	$\sqrt{q}(q-\sqrt{q}+1)$	q^2+q+1
k-I	1	1	1	$q\sqrt{q}$	-	q^2+q+1
k-II	1	1	2	$\sqrt{q}(q-1)$	-	q^2+q+1
k-III	1	1	$\sqrt{q}+1$	$q(\sqrt{q}-1)$	-	q^2+q+1

Table 3.6: Possible incidence classes for two non-degenerate Hermitian surfaces: Γ contains degenerate surfaces of rank 3 only.

Table 3.6 presents all possible incidence configurations obtained as base locus of linear systems Γ whose only degenerate surfaces are Hermitian cones. The first column contains the total number c_3 of cones in a given configuration. The number v is the number of cones in the pencil Γ whose vertex belongs to the intersection. The numbers s_1 and s_2 are as in Table 3.5 for a cone $\mathcal{C}$ whose vertex does not belong to $\mathcal{E}$. The integers s'_1 and s'_2 are defined in the same way for a cone $\mathcal{C}'$ whose vertex is assumed to be in $\mathcal{E}$.

3.1.3 Pencils whose degenerate surfaces have all rank 2

This subsection deals with the case in which all degenerate surfaces in the linear system Γ have rank 2, that is to say $r_3(\Gamma) = r_1(\Gamma) = 0$. We recall that the *radical* of a Hermitian form h is the set of the points x of $\mathrm{PG}(n, q)$ such that for all $y \in \mathrm{PG}(n, q)$,

$$h(x, y) = 0.$$

Definition 3.1.17. The *radical* of a Hermitian surface $\mathcal{H}$ is the radical of the Hermitian form h associated with $\mathcal{H}$. We denote the radical of $\mathcal{H}$ with the symbol $\mathrm{rad}\,\mathcal{H}$.

Lemma 3.1.18. *The radical of a Hermitian variety $\mathcal{H}$ is a subspace of $\mathrm{PG}(n, q)$. Furthermore, the following equality holds:*

$$\dim \mathrm{rad}\,\mathcal{H} + \mathrm{rank}\mathcal{H} = n.$$

Proof. Consider the linear transformation ϕ induced by H. We have, $\dim\ker\phi+\dim\operatorname{Im}\phi = n$; on the other hand, $\dim\ker\phi = \dim\operatorname{rad} H$ and $\dim\operatorname{Im}\phi = \text{rank}H$. The result follows. □

Lemma 3.1.19. *Assume that the only degenerate surface $\mathcal{C}$ of Γ has rank 2; then, the radical of $\mathcal{C}$ intersects any non-degenerate surface $\mathcal{H} \in \Gamma$ in either 1, $\sqrt{q}+1$ or $q+1$ points.*

Proof. Any plane which is a component of $\mathcal{C}$, intersects $\mathcal{H}$ in either a Hermitian curve or in a degenerate Hermitian curve, that is $\sqrt{q}+1$ lines through a point. In the former case the intersection consists of $q\sqrt{q}+1$ points; in the latter of $q\sqrt{q}+q+1$. Define v_1 as the number of components of $\mathcal{C}$ which intersect $\mathcal{H}$ in a degenerate curve and let v_2 be the number of components secant to $\mathcal{H}$, that is, whose intersection is a non-singular curve. Obviously, $v_1+v_2 = \sqrt{q}+1$.

Since $\mathcal{C}$ has rank 2, its radical $l = \operatorname{rad}\mathcal{C}$ is a line of $\mathrm{PG}(3,n)$. Hence, the possible intersection numbers with $\mathcal{H}$ are 1, $\sqrt{q}+1$ or $q+1$. Let $n = |l\cap\mathcal{H}|$. We now analyse all possibilities.

Class I.a: $n = 1$. The size of $\mathcal{E}$ is

$$q^2+q\sqrt{q}+q+1 = v_1(q\sqrt{q}+q)+(\sqrt{q}+1-v_1)q\sqrt{q}+1.$$

We obtain $v_1 = 1$.

Class I.b: $n = \sqrt{q}+1$. The size of $\mathcal{E}$ is

$$q^2+q\sqrt{q}+q+1 = v_1(q\sqrt{q}+q-\sqrt{q})+(\sqrt{q}+1-v_1)(q\sqrt{q}-\sqrt{q})+\sqrt{q}+1 =$$

Hence, $v_1 = 2$.

Class I.c: $l = q+1$. The size of $\mathcal{E}$ is

$$q^2+q\sqrt{q}+q+1 = v_1(q\sqrt{q})+(\sqrt{q}+1-v_1)(q\sqrt{q}-q)+q+1.$$

Hence,

$$q^2+q\sqrt{q} = v_1q+q^2-q$$

and $v_1 = (1+\sqrt{q})$. □

Corollary 3.1.20. *Let Γ be a non-degenerate linear system of Hermitian surfaces with $r_2(\Gamma) = 2$. Assume $\mathcal{C}$ and $\mathcal{C}'$ to be the two degenerate surfaces in Γ. Then, the radicals of $\mathcal{C}$ and $\mathcal{C}'$ are skew.*

Proof. Assume V to be a point in the intersection of the radicals of $\mathcal{C}$ and $\mathcal{C}'$. Then, V is conjugate to any point of $\mathrm{PG}(3,q)$ with respect to the Hermitian form induced by a linear combination of $\mathcal{C}$ and $\mathcal{C}'$. It follows that V is in the radical of any surface of Γ, a contradiction. □

Lemma 3.1.21. *Let Γ, $\mathcal{C}$ and $\mathcal{C}'$ be as in corollary 3.1.20. Then, all components of the degenerate surfaces $\mathcal{C}$ and $\mathcal{C}'$ are secant to all the non-degenerate surfaces of Γ. Furthermore, the radical of $\mathcal{C}$ is contained in a component of $\mathcal{C}'$ and* vice-versa.

Class	c_2	v	p_1	p_2	k
I-a	1	1	1	$\sqrt{q}$	$q^2+q\sqrt{q}+q+1$
I-b	1	$\sqrt{q}+1$	2	$\sqrt{q}-1$	$q^2+q\sqrt{q}+q+1$
I-c	1	$q+1$	$\sqrt{q}+1$	0	$q^2+q\sqrt{q}+q+1$
II-c	2	$q+1$	0	$\sqrt{q}+1$	q^2+1

Table 3.7: Possible incidence classes for two non-degenerate Hermitian surfaces: Γ contains degenerate surfaces of rank 2 only.

Proof. Let n be the size of the intersection of the radical of $\mathcal{C}$ with a non-degenerate surface $\mathcal{H} \in \Gamma$. Then, n is either 1, $\sqrt{q}+1$ or $q+1$. We now analyse the different possibilities.

Class II.a: $n = 1$. Then,

$$q^2+1 = v_1 q + q^2 + q\sqrt{q} + 1 > q^2 + 1,$$

a contradiction.

Class II.b: $n = \sqrt{q}+1$. Then,

$$q^2+1 = v_1 q + (\sqrt{q}+1)(q-1)\sqrt{q} + \sqrt{q} + 1$$

a contradiction.

Class II.c: $n = q+1$. Then,

$$q^2+q = v_1 q + q(q-1) + q + 1 = v_1 + q^2 + 1.$$

This case is actually possible and yields $v_1 = 0$. It follows that all components of $\mathcal{C}$ are secant to any non-degenerate surface $\mathcal{H}$. □

Table 3.7 presents all possible incidence classes $\mathcal{E}$ for two Hermitian surfaces $\mathcal{H}_1, \mathcal{H}_2$ when the pencil they generate contains degenerate surfaces of rank 2 only.

Here, the second column contains the total number c_2 of degenerate surfaces in a given configuration; v is the number of points in common between the radical of a degenerate surface and the intersection configuration $\mathcal{E}$.

We recall that a plane π is *tangent* $\mathcal{E}$ if it is tangent to any non-degenerate surface in Γ; we say that π is *secant* (or *transversal to*) $\mathcal{E}$ if it intersects a non-degenerate surface of Γ in a non-singular Hermitian curve. By p_1, the number of planes, components of a degenerate surface in Γ, that are tangent $\mathcal{E}$ is denoted; p_2 is the number of planes in such a surface that are secant $\mathcal{E}$.

3.1.4 Pencils whose degenerate surfaces have ranks 2 and 3

This subsection describes the configurations $\mathcal{E}$ arising from the intersection of two Hermitian surfaces, when the non-degenerate pencil Γ they generate is assumed to contain both Hermitian cones and doubly-degenerate Hermitian surfaces; that is to say that both $r_2(\Gamma) \neq 0$ and $r_3(\Gamma) \neq 0$. We assume that $\mathcal{C}_1 \in \Gamma$ is a degenerate surface of rank 2 and that $\mathcal{C}_2 \in \Gamma$ has rank 3. The symbols in Table 3.8 will be used. Observe that the indices s_1, s_2 and s_3 are not independent. In fact, since $\mathcal{C}_2$ is a cone over a non-degenerate Hermitian curve, $s_1 + s_2 + s_3 = q\sqrt{q} + 1$.

s_1	components of $\mathcal{C}_2$ included in $\mathcal{E}$
s_2	components of $\mathcal{C}_2$ secant to (being chords of) $\mathcal{E}$
s_3	components of $\mathcal{C}_2$ tangent to $\mathcal{E}$
v_1	planes of $\mathcal{C}_1$ tangent to $\mathcal{E}$
v_2	planes of $\mathcal{C}_1$ secant to $\mathcal{E}$
l_1	intersection between $\operatorname{rad}\mathcal{C}_1$ and $\mathcal{C}_2$
l_2	intersection between $\operatorname{rad}\mathcal{C}_2$ and $\mathcal{C}_1$

Table 3.8: Indices for the intersection of Hermitian surfaces of rank 2 and of rank 3.

Lemma 3.1.22. *Assume that a non-degenerate linear system Γ contains a surface $\mathcal{C}_1 \in \Gamma$ of rank 2 and a surface $\mathcal{C}_2 \in \Gamma$ of rank 3. Then, the vertex of $\mathcal{C}_2$ does not belong to the radical of $\mathcal{C}_1$. Furthermore, the components of $\mathcal{C}_1$ and $\mathcal{C}_2$ intersect $\mathcal{H}$ as illustrated in Table 3.9, Class I.*

Proof. Since $\mathcal{C}_1 \neq \mathcal{C}_2$, the surfaces $\mathcal{C}_1$ and $\mathcal{C}_2$ generate the linear system Γ. On the other hand, Γ is non-degenerate by assumption; hence, the vertex of $\mathcal{C}_2$ cannot belong to the radical of $\mathcal{C}_1$. This proves the first part of the lemma.

We distinguish some different cases. First, we consider the information obtained by considering the intersection between the lines of $\mathcal{C}_2$ and $\mathcal{E}$. There are two possibilities:

Class I.a: $V_2 \notin \mathcal{E}$. Then, $s_1 = 0$ and

$$q^2 + q\sqrt{q} + 1 = s_2\sqrt{q} + q\sqrt{q} + 1.$$

Hence, $s_2 = q\sqrt{q}$ and the intersection between the polar plane of the vertex of $\mathcal{C}_2$ and $\mathcal{E} \cap \mathcal{C}_2$ consists of a single point.

Class I.b: $V_2 \in \mathcal{E}$. Then,

$$q^2 + q\sqrt{q} + 1 = s_1 q + s_2\sqrt{q} + 1.$$

Hence, $s_1\sqrt{q} + s_2 = q\sqrt{q} + q$, with $s_1 + s_2 \leq q\sqrt{q} + 1$. This implies $s_2 = \sqrt{q}(q + \sqrt{q} - s_1)$ and $q + \sqrt{q} + 1 > s_1 > \sqrt{q}$. On the other hand, the lines shared between $\mathcal{C}_2$ and $\mathcal{E}$ must lie in the tangent plane τ at V to any non-degenerate surface $\mathcal{H}$ in Γ. Hence, they lie in the intersection of the 2-dimensional cone $\mathcal{C}_2 \cap \tau$ with the cone $\mathcal{H} \cap \tau$. Such an intersection contains either 0, 1, 2 or $\sqrt{q}+1$ lines. It follows $s_1 = \sqrt{q}+1$, $s_2 = q-1$ and $s_3 = q\sqrt{q} - q - \sqrt{q} + 1$.

Now we focus on the intersection between the plane components of $\mathcal{C}_1$ and $\mathcal{H}$. Let l_1 be the cardinality of the intersection between the radical of $\mathcal{C}_1$ and $\mathcal{E}$. There are three actual possibilities:

Class I.i: $l_1 = 1$. Then,

$$q^2 + q\sqrt{q} + 1 = v_1(q\sqrt{q} + q) + (\sqrt{q} + 1 - v_1)(q\sqrt{q}) + 1.$$

Hence, $v_1 = 0$ and $v_2 = \sqrt{q}+1$, that is all the components of $\mathcal{C}_1$ are secant to any non-degenerate surface $\mathcal{H}$.

Class I.ii: $l_1 = \sqrt{q}+1$. Then,

$$q^2 + q\sqrt{q} + 1 = \sqrt{q}[v_1(q + \sqrt{q} - 1) + (\sqrt{q} + 1 - v_1)(q-1) + 1] + 1.$$

Hence, $v_1 = 1$, $v_2 = \sqrt{q}$ and one of the components of $\mathcal{C}_1$ is tangent to any non-degenerate surface $\mathcal{H}$.

Class I.iii: $l_1 = q+1$. Then,

$$q^2 + q\sqrt{q} + 1 = q[v_1(\sqrt{q}) + (\sqrt{q} + 1 - v_1)(\sqrt{q} - 1) + 1] + 1.$$

Hence, $v_1 = \sqrt{q}$ and $v_2 = 1$. □

Lemma 3.1.23. *Let Γ be a linear system of Hermitian surfaces such that $r_3(\Gamma) = 2$ and $r_2(\Gamma) = 1$. Take $\mathcal{C}_2$ and $\mathcal{C}_3$ as the Hermitian cones of Γ and assume $\mathcal{C}_1$ to be the doubly-degenerate surface in the linear system. Define r as the radical line of $\mathcal{C}_1$. Then, either the vertices of both $\mathcal{C}_2$ and $\mathcal{C}_3$ belong to $\mathcal{E}$, or none of them does.*

Proof. Let $l_1 = |\mathcal{E} \cap r|$.

There are two possible classes with respect to the components of one of the cones, say $\mathcal{C}_2$:

Class II.a: $V_2 \notin \mathcal{E}$. Then,

$$q^2 + q\sqrt{q} - q + 1 = s_2(\sqrt{q} + 1) + (q\sqrt{q} + 1 - s_2).$$

Hence, $s_2 = \sqrt{q}(q-1)$.

Class II.b: $V_2 \in \mathcal{E}$. Then,

$$q^2 + q\sqrt{q} - q + 1 = s_1 q + s_2\sqrt{q} + 1.$$

If $s_1 = 0$, then $s_2 = q\sqrt{q} + q - \sqrt{q} > q\sqrt{q} + 1$, impossible. Hence, $s_1 = 1$ and the vertex of $\mathcal{C}_3$ has to belong to $\mathcal{E}$ as well. Furthermore, $s_2 = q\sqrt{q} - \sqrt{q}$.

In fact, the intersection between the components of $\mathcal{C}_1$ and $\mathcal{E}$ can be realized in only two ways, since most of the possibilities are ruled out by considerations on the order.

Class II.i: $l_1 = 1$. Then,

$$q^2 + q\sqrt{q} - q + 1 = v_1(q\sqrt{q} + q) + (\sqrt{q} + 1 - v_1)(q\sqrt{q}) + 1;$$

hence, $v_1 = -1$, a contradiction, since $v_1 \geq 0$.

Class II.ii: $l_1 = \sqrt{q} + 1$ Then,

$$q^2 + q\sqrt{q} - q + 1 = \sqrt{q}[v_1(q + \sqrt{q} - 1) + (\sqrt{q} + 1 - v_1)(q - 1) + 1] + 1;$$

hence, $v_1 = 0$.

Class II.iii: $l_1 = q + 1$ points. Then,

$$q^2 + q\sqrt{q} - q + 1 = q[v_1(\sqrt{q}) + (\sqrt{q} + 1 - v_1)(\sqrt{q} - 1)] + 1;$$

hence, $v_1 = \sqrt{q}$ and $v_2 = 1$. □

3.1.5 Pencils with $r_1(\Gamma) \geq 1$

A Hermitian surface of rank 1 is a plane π repeated $\sqrt{q}+1$ times. The intersection configuration $\mathcal{E}$ associated to a linear system Γ with $r_1(\Gamma) = 1$ is hence planar. In fact, a plane might meet a non-degenerate Hermitian surface $\mathcal{H}$ in only two configurations:

(i) **Class III-a**: π is tangent to $\mathcal{H}$; the intersection $\mathcal{E}$ is a Hermitian cone, that is a Hermitian curve of rank 2;

(ii) **Class III-b**: π is secant to $\mathcal{H}$; the intersection $\mathcal{E}$ is a non-degenerate Hermitian curve.

From Table 3.1, we have that in Class III-a, the rank sequence (r_1, r_2, r_3) for Γ is $(1, 0, 0)$; in Class III-b, $(r_1, r_2, r_3) = (1, 0, 1)$ and there is a cone $\mathcal{C}$ in Γ whose vertex does not belong to π.

3.2 Hermitian matrices and polynomials

In this section, we provide some matrices which represent classes of Hermitian intersections. This is useful in order to construct the possible intersection configurations in dimension 3.

The results are presented in Tables 3.10, 3.11, 3.12.

Class	c_2	c_3	l_2	l_3	s_1	s_2	v_1	k
I-a-i	1	1	1	0	0	$q\sqrt{q}$	0	$q^2+q\sqrt{q}+1$
I-a-ii	1	1	$\sqrt{q}+1$	0	0	$q\sqrt{q}$	1	$q^2+q\sqrt{q}+1$
I-a-iii	1	1	$q+1$	0	0	$q\sqrt{q}$	$\sqrt{q}$	$q^2+q\sqrt{q}+1$
I-b-i	1	1	1	1	$\sqrt{q}+1$	$q-1$	0	$q^2+q\sqrt{q}+1$
I-b-ii	1	1	$\sqrt{q}+1$	1	$\sqrt{q}+1$	$q-1$	1	$q^2+q\sqrt{q}+1$
I-b-iii	1	1	$q+1$	1	$\sqrt{q}+1$	$q-1$	$\sqrt{q}$	$q^2+q\sqrt{q}+1$
II-a-ii	1	2	$\sqrt{q}+1$	0	0	$\sqrt{q}(q-1)$	1	$q^2+q\sqrt{q}-q+1$
II-a-iii	1	2	$q+1$	0	0	$\sqrt{q}(q-1)$	$\sqrt{q}$	$q^2+q\sqrt{q}-q+1$
II-b-ii	1	2	$\sqrt{q}+1$	$1+1$	1	$\sqrt{q}(q-1)$	1	$q^2+q\sqrt{q}-q+1$
II-b-iii	1	2	$q+1$	$1+1$	1	$\sqrt{q}(q-1)$	$\sqrt{q}$	$q^2+q\sqrt{q}-q+1$

Table 3.9: Possible incidence classes for two non-degenerate Hermitian surfaces: Γ contains degenerate surfaces of ranks 2 and 3.

$\mathcal{M}_H(x)$	conditions	canonical form
$(x-\alpha)(x-\beta)(x-\gamma)^2$	$(\eta-\xi)^2+4c^{\sqrt{q}+1}=0$ See Lemma 3.2.7	$\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \eta & c^{\sqrt{q}+1} \\ 0 & 0 & c & \xi \end{bmatrix}$
$(x-\alpha)(x-\beta)(x-\gamma)$		$\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{bmatrix}$
$(x-\alpha)(x-\beta)^3$	$c^{\sqrt{q}+1}+d^{\sqrt{q}+1}=0$ See Lemma 3.2.8	$\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & c & 0 \\ 0 & c^{\sqrt{q}+1} & \beta & d^{\sqrt{q}+1} \\ 0 & 0 & d & \beta \end{bmatrix}$
$(x-\alpha)^2(x-\beta)^2$	$(\lambda-\mu)^2-4b^{\sqrt{q}+1}=0$ $(\eta-\xi)^2-4d^{\sqrt{q}+1}=0$ See Lemma 3.2.9	$\begin{bmatrix} \lambda & b^{\sqrt{q}} & 0 & 0 \\ b & \mu & 0 & 0 \\ 0 & 0 & \eta & c^{\sqrt{q}} \\ 0 & 0 & c & \xi \end{bmatrix}$
$(x-\alpha)^2(x-\beta)$	$(\lambda-\mu)^2-4b^{\sqrt{q}+1}=0$ See Lemma 3.2.10	$\begin{bmatrix} \lambda & b^{\sqrt{q}} & 0 & 0 \\ b & \mu & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{bmatrix}$

Table 3.10: Canonical forms for the 3-dimensional case: $\mathcal{M}_H(x)$ splits over $\mathrm{GF}(\sqrt{q})$; 2 or 3 distinct roots.

$\mathcal{M}_H(x)$	conditions	canonical form
$(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$	See Lemma 3.2.7	$\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{bmatrix}$
$(x-\alpha)^4$	See Lemmas 3.2.11, 3.2.14 $\sigma = (ad)^{\sqrt{q}}b - (ad)b^{\sqrt{q}}$ $\mathfrak{I}[(ad)^{\sqrt{q}}b\sigma] \neq 0$	$\begin{bmatrix} \alpha & a & b & c \\ a^{\sqrt{q}} & \alpha & d & e \\ b^{\sqrt{q}} & d^{\sqrt{q}} & \alpha & f \\ c^{\sqrt{q}} & e^{\sqrt{q}} & f^{\sqrt{q}} & \alpha \end{bmatrix}$
$(x-\alpha)^3$	See Lemmas 3.2.11, 3.2.14	$\begin{bmatrix} \alpha & a & b & c \\ a^{\sqrt{q}} & \alpha & d & e \\ b^{\sqrt{q}} & d^{\sqrt{q}} & \alpha & f \\ c^{\sqrt{q}} & e^{\sqrt{q}} & f^{\sqrt{q}} & \alpha \end{bmatrix}$
$(x-\alpha)^2$	See Lemma 3.2.11	$\begin{bmatrix} \alpha & a & b & c \\ a^{\sqrt{q}} & \alpha & d & e \\ b^{\sqrt{q}} & d^{\sqrt{q}} & \alpha & f \\ c^{\sqrt{q}} & e^{\sqrt{q}} & f^{\sqrt{q}} & \alpha \end{bmatrix}$

Table 3.11: Canonical forms for the 3-dimensional case: $\mathcal{M}_H(x)$ splits over $\mathrm{GF}(\sqrt{q})$; 1 or 4 roots.

$\mathcal{M}_H(x)$	conditions	canonical form
$(x-\alpha)(x-\beta)p_2(x)$	See Lemma 3.2.16 $(\xi-\zeta)^2+4d^{\sqrt{q}+1} \in \not\square$	$\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \zeta & c \\ 0 & 0 & c^{\sqrt{q}} & \xi \end{bmatrix}$
$(x-\alpha)p_3(x)$		$\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \lambda & d & e \\ 0 & d^{\sqrt{q}} & \eta & f \\ 0 & e^{\sqrt{q}} & f^{\sqrt{q}} & \xi \end{bmatrix}$
$(x-\alpha)^2p_2(x)$	See Lemma 3.2.17 $(\lambda+\mu)^2+4c^{\sqrt{q}+1}=0$ $(\eta-\alpha)(\xi-\alpha) \neq d^{\sqrt{q}+1}$	$\begin{bmatrix} \lambda & c & 0 & 0 \\ c^{\sqrt{q}} & \mu & d & e \\ 0 & 0 & \eta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix}$
$p_2(x)q_2(x)$	See Lemma 3.2.18 $\xi^2-(\lambda+\mu)\xi+d^{\sqrt{q}+1}-c^{\sqrt{q}+1} \neq 0$	$\begin{bmatrix} \lambda & c & 0 & c \\ c^{\sqrt{q}} & \mu & d & e \\ 0 & 0 & \eta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix}$
$p_2(x)^2$		$\begin{bmatrix} \lambda & c & 0 & c \\ c^{\sqrt{q}} & \mu & d & e \\ 0 & 0 & \eta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix}$

Table 3.12: Canonical forms for the 3-dimensional case: $\mathcal{M}_H(x)$ does not split over $\mathrm{GF}(\sqrt{q})$; degree 4.

3.2.1 Some general considerations on Hermitian pencils

This subsection presents some general considerations that will be used later.

The first lemma proves that if we want to consider linear systems Σ in which any two varieties intersect in the same configuration, then the dimension of Σ is at most 1. In the second lemma, we verify that if the base locus $\mathcal{E}$ of a linear system Γ of Hermitian varieties has maximal cardinality, then Γ is a maximal set of Hermitian varieties meeting in $\mathcal{E}$. These results hold for any dimension n.

Lemma 3.2.1. *Let Σ be a linear system of Hermitian varieties. If any two distinct elements of Σ meet in the same configuration, then* $\dim \Sigma = 1$.

Proof. The set Σ is a projective subspace of $\mathrm{PG}(n^2+2n, \sqrt{q})$. Take three linearly independent Hermitian varieties $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 \in \Sigma$ and let H_1, H_2 and H_3 be corresponding Hermitian matrices. Assume also that

$$\mathcal{E} := \mathcal{H}_1 \cap \mathcal{H}_2 = \mathcal{H}_1 \cap \mathcal{H}_3 = \mathcal{H}_2 \cap \mathcal{H}_3.$$

The three varieties $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ are all different; if it were $\mathcal{H}_3 \subseteq \mathcal{H}_1 \cup \mathcal{H}_2$, then we could write

$$\mathcal{H}_3 = (\mathcal{H}_3 \cap \mathcal{H}_1) \cup (\mathcal{H}_3 \cap \mathcal{H}_2) = \mathcal{E} \cup \mathcal{E} = \mathcal{E} = \mathcal{H}_1 \cap \mathcal{H}_2.$$

This is a contradiction, since $\mathcal{H}_1 \neq \mathcal{H}_2$ and $\mathcal{E}$ is not a Hermitian variety. Then, there exists a $t \in \mathcal{H}_3 \setminus \mathcal{E}$, belonging neither to $\mathcal{H}_1$ nor to $\mathcal{H}_2$. The matrix H' given by

$$H' = H_1 - \left(\frac{\bar{t} H_1 t^\star}{\bar{t} H_2 t^\star}\right) H_2$$

identifies a Hermitian variety $\mathcal{H}' := \mathcal{H}(H')$ in the linear system Γ, defined by $\mathcal{H}_1$ and $\mathcal{H}_2$. Such variety $\mathcal{H}'$ intersects $\mathcal{H}_3$ in t. Again, from the independence of $\mathcal{H}_3$ from $\mathcal{H}_1$ and $\mathcal{H}_2$,

$$\mathcal{H}' \neq \mathcal{H}_3,$$

a contradiction. □

Corollary 3.2.2. *Let H_1, H_2 and H_3 be three independent Hermitian matrices such that*

$$\mathcal{H}(H_1) \cap \mathcal{H}(H_2) = \mathcal{H}(H_2) \cap \mathcal{H}(H_3) = \mathcal{H}(H_1) \cap \mathcal{H}(H_3).$$

Then, for any μ in $\mathrm{GF}(\sqrt{q})$,

$$\mathcal{H}(H_1) \cap \mathcal{H}(H_2) \subseteq \mathcal{H}(H_1) \cap \mathcal{H}(H_2 + \mu H_3).$$

Proof. By hypothesis, we have

$$\mathcal{H}(H_1) \cap \mathcal{H}(H_2) = \mathcal{H}(H_1) \cap \mathcal{H}(H_2) \cap \mathcal{H}(H_3).$$

On the other hand, a solution of the system of equations induced by the three Hermitian matrices H_1, H_2 and H_3 is necessarily a solution of the system determined by H_1 and $H_2 + \mu H_3$. The result follows. □

Lemma 3.2.3. *Assume that two Hermitian varieties $\mathcal{H}_1$ and $\mathcal{H}_2$ intersect in a configuration $\mathcal{E}$ of* maximal *cardinality. Then, the only Hermitian varieties intersecting $\mathcal{H}_1$ in $\mathcal{E}$ are those belonging to the linear system Γ defined by $\mathcal{H}_1$ and $\mathcal{H}_2$.*

Proof. Assume $\mathcal{H}_3$ to be a Hermitian variety intersecting $\mathcal{H}_1$ in $\mathcal{E}$. Because of the maximality of $\mathcal{E}$, it is also $\mathcal{H}_3 \cap \mathcal{H}_2 = \mathcal{E}$. Now, Corollary 3.2.2 affirms that any linear combination of $\mathcal{H}_2$ and $\mathcal{H}_3$ intersect $\mathcal{H}_1$ in a superset of $\mathcal{E}$; since $\mathcal{E}$ is maximal, such a superset has to be $\mathcal{E}$ again. By the argument used in the proof of Corollary 3.2.1, this is impossible when $\mathcal{H}_3$ does not belong to Γ, whence the result. □

Further linear algebra observations

Now we present some linear algebra results. These results are straightforward generalizations of those in [Kes81].

Lemma 3.2.4. *Let H and J be two Hermitian matrices equivalent up to unitary transformations. Then, the minimal polynomials $\mathcal{M}_H(x)$ and $\mathcal{M}_J(x)$ are the same.*

Proof. By hypothesis, there exists a matrix U such that

$$H = \overline{U} J U^\star$$

with $U^\star = \overline{U}^{-1}$. It follows that $H^n = (\overline{U}) J^n (U^\star)$. Hence, for any polynomial $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ such that $p(J) = \underline{0}$,

$$p(H) = a_0 I + a_1(\overline{U} J U^\star) + \ldots + \overline{U} J^n U^\star = \overline{U} p(J) U^\star = \overline{U}\underline{0}U^\star = \underline{0}.$$

Hence, $\mathcal{M}_H(x) \mid \mathcal{M}_J(x)$. By a similar argument, $\mathcal{M}_J(x) \mid \mathcal{M}_H(x)$ and the result follows. □

Lemma 3.2.5 ([Kes81], Lemma 3)**.** *Let H be a Hermitian matrix and suppose that its minimal polynomial $\mathcal{M}_H(x)$ has a factorisation*

$$p(x) = p_1(x) p_2(x) \ldots p_k(x)$$

in $k > 1$ factors co-prime in $\mathrm{GF}(\sqrt{q})[x]$. *Then, the null spaces corresponding to these factors are mutually conjugate.*

Proof. We work by induction on k. Observe that all $p_i(x)$ are Hermitian polynomials, since their coefficients lie in the ground field $\mathrm{GF}(\sqrt{q})$.

Case $k = 2$: since $p_1(x)$ and $p_2(x)$ are co-prime, the Chinese Remainder Theorem implies that there exist two Hermitian polynomials $r_1(x), r_2(x) \in \mathrm{GF}(\sqrt{q})[x]$ such that

$$1 = r_1(x)p_1(x) + r_2(x)p_2(x);$$

hence, the identity matrix I can be written as

$$I = r_1(H)p_1(H) + r_2(H)p_2(H).$$

Assume now $v^\star \in \mathrm{Null}_H\, p_1(x)$ and $w^\star \in \mathrm{Null}_H\, p_2(x)$. Then,

$$v = v(p_1(H)r_1(H) + p_2(H)r_2(H)) = vp_2(H)r_2(H)$$

and, likewise,

$$w^\star = r_1(H)p_1(H)w^\star + r_2(H)p_2(H)w^\star = r_1(H)p_1(H)w^\star.$$

Hence, H being Hermitian,

$$\overline{v}w^\star = w\overline{v}^\star = w(p_1(H)^\star r_1(H)^\star)\overline{v}^\star = w(\overline{r_1(H)p_1(H)})\overline{v}^\star = w\overline{r_1(H)}(\overline{p_1(H)v^\star}) = w\underline{0} = 0.$$

Induction $k \Rightarrow k+1$: Assume $p(x) = p_1(x)\dots p_{k+1}(x)$, and for any $0 < i \leq k$ define $q_i(x)$ to be $p_i(x)p_{i+1}(x)$. The polynomial $q_k(x)$ is co-prime with all the $p_i(x)$ for $i < k$, hence, by the inductive hypothesis, its null space is conjugate with all of theirs. In particular, both the null space of $p_k(x)$ and that of $p_{k+1}(x)$ are conjugate with the null space of any other $p_i(x)$, since they are contained in $\mathrm{Null}_H\, q_k(x)$. By using the same argument on the factorisation of $p(x)$ given by

$$p(x) = p_1(x)\dots p_{k-2}(x)q_{k-1}(x)p_{k+1}(x),$$

the null space of p_{k+1} is proven to be conjugate with the null space of q_{k-1}, which contains $\mathrm{Null}_H\, p_k(x)$. The result follows. □

Lemma 3.2.6. *Let H be an $n \times n$ Hermitian matrix such that*

(i) *its minimal polynomial $\mathcal{M}(x)$ has degree n;*

(ii) *$\mathcal{M}(x)$ splits in $\mathrm{GF}(\sqrt{q})[x]$;*

(iii) *$\mathcal{M}(x)$ has no double root.*

Then, H is unitarily equivalent to a diagonal matrix.

Proof. Consider the matrix U consisting of the representation of H with respect to the base formed by its normalized eigenvectors. This matrix is diagonal and, by Lemma 3.2.5, is unitarily equivalent to H, whence the result. □

We now produce some 4×4 Hermitian matrices. These matrices can be (and will be) used to construct the linear systems corresponding to the cases as presented in section 3.1. Cases I-III assume that the factorisation of the minimal polynomial splits over $\mathrm{GF}(\sqrt{q})$. Case IV considers some of the possibilities when the minimal polynomial of a matrix contains higher degree irreducible factors.

3.2.2 Case I: 3 or 4 distinct roots

Lemma 3.2.7. *Let H be a 4×4 Hermitian matrix whose minimal polynomial has either the form $\mathcal{M}_H(x) = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$ or $\mathcal{M}_H(x) = (x-\alpha)(x-\beta)(x-\gamma)$. Then, H is unitarily equivalent to a diagonal matrix.*

Proof. The first part of the lemma is a direct consequence of Lemma 3.2.6.

Consider now the case in which $\mathcal{M}_H(x)$ has degree 3 and all its roots are distinct. The characteristic polynomial $\mathcal{C}_H(x)$ has degree 4 and is divisible by the minimal polynomial of H. It follows that $\mathcal{C}_H(x)$ splits in linear factors over $\mathrm{GF}(\sqrt{q})$ as well.

Assume the roots of $\mathcal{C}_H(x)$ not to be the same as those of $\mathcal{M}_H(x)$. Then,

$$\mathcal{C}_H(x) = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta),$$

with α, β, γ and δ all distinct. Clearly, all the matrices $(H-\alpha I)$, $(H-\beta I)$, $(H-\gamma I)$ and $(H-\delta I)$ have rank 3; then, $\mathcal{M}_H(H)$ would have rank 1, a contradiction. It follows that

$$\mathcal{C}_H(x) = (x-\alpha)(x-\beta)(x-\gamma)^2.$$

Since α, β and γ are all distinct, the null spaces corresponding to $(x-\alpha)$, $(x-\beta)$ and $(x-\gamma)$ are mutually conjugate. Hence, H is unitarily equivalent to a matrix H' of the form

$$H' = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \sigma & d \\ 0 & 0 & \overline{d} & \theta \end{bmatrix},$$

where $\sigma, \theta \in \mathrm{GF}(\sqrt{q})$ and $d \in \mathrm{GF}(q)$. By a direct computation, the characteristic polynomial of H' is

$$\mathcal{C}_{H'}(x) = (x-\alpha)(x-\beta)(x^2 - (\sigma+\theta)x + \sigma\theta - d^{\sqrt{q}+1}).$$

On the other hand, $\mathcal{C}_{H'}(x) = \mathcal{C}_H(x)$; hence, the previous relation implies that

$$x^2 - (\sigma+\theta)x + \sigma\theta - d^{\sqrt{q}+1} = (x-\gamma)^2,$$

that is, the following system of equations has to be fulfilled:

$$\begin{cases} (\sigma+\theta) = 2\gamma \\ \sigma\theta - d^{\sqrt{q}+1} = \gamma^2. \end{cases}$$

This yields

$$\gamma^2 - 2\sigma\gamma + d^{\sqrt{q}+1} + \sigma^2 = 0;$$

the conclusion is that the norm of d is $d^{\sqrt{q}+1} = -(\gamma-\sigma)^2$. On the other hand, the minimal polynomial $\mathcal{M}_{H'}(x)$ coincides with the minimal polynomial of H; hence, $\mathcal{M}_H(H') = 0$. The matrix H' is block-diagonal. Assume $H' = \operatorname{diag}(\alpha, \beta, T)$ where $T \in \operatorname{Mat}(2, q)$, and define $W = \mathcal{M}_H(T)$. Then, we have the following equalities

(i) $W_{1,1} = (\gamma-\sigma)[(2\gamma-\sigma-\alpha)(2\gamma-\sigma-\beta)+d^{\sqrt{q}+1})] + d^{\sqrt{q}+1}(2\gamma-\alpha-\beta)$;

(ii) $W_{1,2} = d[(2\gamma-\sigma-\alpha)(2\gamma-\sigma-\beta) + d^{\sqrt{q}+1} + (2\gamma-\alpha-\beta)(\sigma-\gamma)]$;

(iii) $W_{2,1} = W_{1,2}^{\sqrt{q}}$;

(iv) $W_{2,2} = d^{\sqrt{q}+1}(\gamma-\alpha-\beta+\sigma) + (\sigma-\alpha)(\sigma-\beta)(\sigma-\gamma)$.

A substitution and a simplification in $W_{1,1}$ yield

$$W_{1,1} = (\gamma-\sigma)(\gamma-\beta)(\gamma-\alpha),$$

whence $\gamma = \sigma$ and, consequently, $d = 0$. It follows that H' is diagonal. □

3.2.3 Case II: 2 distinct roots

Lemma 3.2.8. *A non-degenerate 4×4 Hermitian matrix H with minimal polynomial of the form $\mathcal{M}_H(x) = (x-\alpha)(x-\lambda)^3$ is unitarily equivalent to a matrix H' of the form*

$$H' = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \lambda & c^{\sqrt{q}} & 0 \\ 0 & c & \lambda & d^{\sqrt{q}} \\ 0 & 0 & d & \lambda \end{bmatrix},$$

where $c, d \in \mathrm{GF}(q) \setminus \{0\}$ and $c^{\sqrt{q}+1} + d^{\sqrt{q}+1} = 0$.

Proof. The argument develops exactly as in [Kes81], Lemma 7. In fact, it is enough to find four non-self-conjugate, mutually conjugate vectors r, s, t, u such that

(i) $Hr = \lambda r + cs$;

(ii) $Hs = c^{\sqrt{q}} r + \lambda s + dt$;

(iii) $Ht = d^{\sqrt{q}} s + \lambda t$;

(iv) $Hu = \alpha u$.

The null space corresponding to the polynomial $(x - \alpha)$ has dimension 1 and, by Lemma 3.2.5, it is conjugate to the space corresponding to $(x - \lambda)$; hence, there exists a vector u with the required properties. In order to find r, s, and t it is now enough to consider what happens for 3×3 matrices whose minimal polynomial is of the form $(x - \lambda)^3$. The result follows directly from Table 2.3. □

Lemma 3.2.9. *A non-degenerate 4×4 Hermitian matrix H with minimal polynomial of the form $\mathcal{M}_H(x) = (x - \alpha)^2(x - \beta)^2$ is unitarily equivalent to a matrix H' of the form*

$$H' = \begin{bmatrix} \eta & c & 0 & 0 \\ c^{\sqrt{q}} & \theta & 0 & 0 \\ 0 & 0 & \zeta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix},$$

with

(i) $(\eta + \theta)^2 + 4c^{\sqrt{q}+1} = 0$;

(ii) $(\zeta + \xi)^2 + 4d^{\sqrt{q}+1} = 0$.

Proof. The two eigenspaces V_1, V_2 corresponding to the eigenvalues α and β are mutually conjugate with respect to H; hence, H admits a block diagonal representation H'. Furthermore, the characteristic polynomial of H' can be written as

$$\mathcal{C}_{H'}(x) = (x^2 - (\eta + \theta)x + \eta\theta + c^{\sqrt{q}+1})(x^2 - (\zeta + \xi)x + \zeta\xi + d^{\sqrt{q}+1}),$$

whence we deduce the relation

$$4\eta\theta - 4c^{\sqrt{q}+1} = (\eta + \theta)^2.$$

From the latter, condition (i) follows. With a similar argument, it is possible to obtain condition (ii).

An additional result is that

$$(\eta + \theta) = 2\alpha; \qquad (\zeta + \xi) = 2\beta.$$

□

Lemma 3.2.10. *A non-degenerate 4×4 Hermitian matrix H of the form*

$$\begin{bmatrix} \lambda & b & 0 & 0 \\ b^{\sqrt{q}} & \mu & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{bmatrix}$$

has minimal polynomial $\mathcal{M}_H(x) = (x - \alpha)^2(x - \beta)$ if and only if

(i) $(\lambda-\mu)^2-4b^{\sqrt{q}+1}=0$;

(ii) $\alpha=(\lambda+\mu)/2$.

Proof. Let $T=\begin{bmatrix}\lambda & b\\ b^{\sqrt{q}} & \mu\end{bmatrix}$. In order for H to have minimal polynomial $(x-\alpha)^2(x-\beta)$, it is enough to require that the minimal polynomial of T is $(x-\alpha)^2$. This is to say that:

(i) the discriminant of the equation $E(x)=0$, given by

$$E(x) := (\lambda-x)(\mu-x)-b^{\sqrt{q}+1},$$

is zero, that is $(\lambda-\mu)^2=4b^{\sqrt{q}+1}$;

(ii) $E(\alpha)=0$, that is $\alpha=(\lambda+\mu)/2$.

□

3.2.4 Case III: 1 root

Lemma 3.2.11. *A Hermitian matrix H of the form*

$$\begin{bmatrix}\lambda & a & b & c\\ a^{\sqrt{q}} & \lambda & d & e\\ b^{\sqrt{q}} & d^{\sqrt{q}} & \lambda & f\\ c^{\sqrt{q}} & e^{\sqrt{q}} & f^{\sqrt{q}} & \lambda\end{bmatrix}$$

has characteristic polynomial $(x-\lambda)^4$ if and only if its coefficients satisfy the following conditions:

(i) $a^{\sqrt{q}+1}+b^{\sqrt{q}+1}+c^{\sqrt{q}+1}+d^{\sqrt{q}+1}+e^{\sqrt{q}+1}+f^{\sqrt{q}+1}=0$;

(ii) $\mathfrak{T}[(df)^{\sqrt{q}}e+(bf)^{\sqrt{q}}c+(ad)^{\sqrt{q}}b+(ae)^{\sqrt{q}}c]=0$;

(iii) $\det(H-\lambda I)=0$, *that is,*

$$(af)^{\sqrt{q}+1}+(be)^{\sqrt{q}+1}+(cd)^{\sqrt{q}+1}=\mathfrak{T}[(bf)^{\sqrt{q}}ae+(be)^{\sqrt{q}}cd+(adf)^{\sqrt{q}}c].$$

Proof. The characteristic polynomial of H is

$\mathcal{C}_H(x)=$

$$\begin{gathered}x^4-4\lambda x^3+\\ [6\lambda^2-(a^{\sqrt{q}+1}+b^{\sqrt{q}+1}+c^{\sqrt{q}+1}+d^{\sqrt{q}+1}+e^{\sqrt{q}+1}+f^{\sqrt{q}+1})]x^2+\\ [-4\lambda^3+2\lambda(a^{\sqrt{q}+1}+b^{\sqrt{q}+1}+c^{\sqrt{q}+1}+d^{\sqrt{q}+1}+e^{\sqrt{q}+1}+f^{\sqrt{q}+1})+\\ -(\mathfrak{T}[(df)^{\sqrt{q}}e+(bf)^{\sqrt{q}}c+(ad)^{\sqrt{q}}b+(ae)^{\sqrt{q}}c])]x+\\ \lambda^4-((a^{\sqrt{q}+1}+b^{\sqrt{q}+1}+c^{\sqrt{q}+1}+d^{\sqrt{q}+1}+e^{\sqrt{q}+1}+f^{\sqrt{q}+1})\lambda^2+\\ (\mathfrak{T}[(df)^{\sqrt{q}}e+(bf)^{\sqrt{q}}c+(ad)^{\sqrt{q}}b+(ae)^{\sqrt{q}}c])\lambda+\\ [(af)^{\sqrt{q}+1}+(be)^{\sqrt{q}+1}+(cd)^{\sqrt{q}+1}-\mathfrak{T}[(bf)^{\sqrt{q}}ae+(be)^{\sqrt{q}}cd+(adf)^{\sqrt{q}}c]].\end{gathered}$$

Conditions (i), (ii) and (iii) follow by direct comparison of the coefficients of this expression with the expansion

$$(x-\lambda)^4 = x^4 - 4x^3\lambda + 6x^2\lambda^2 - 4x\lambda^3 + \lambda^4.$$

□

Lemma 3.2.12. *An Hermitian matrix H given as in Lemma 3.2.11 has to satisfy the following further conditions in order to have minimal polynomial $(x-\lambda)^2$:*

(i) $a^{\sqrt{q}+1} + b^{\sqrt{q}+1} + c^{\sqrt{q}+1} = 0$;

(ii) $a^{\sqrt{q}+1} = f^{\sqrt{q}+1}$, $b^{\sqrt{q}+1} = e^{\sqrt{q}+1}$, $c^{\sqrt{q}+1} = d^{\sqrt{q}+1}$;

(iii) $n^{(2)}_{1,2} := bd^{\sqrt{q}} + ce^{\sqrt{q}} = 0$;

(iv) $n^{(2)}_{1,3} := ad + cf^{\sqrt{q}} = 0$, $n^{(2)}_{1,4} = ae + bf = 0$;

(v) $n^{(2)}_{2,3} := a^{\sqrt{q}}b + ef^{\sqrt{q}} = 0$;

(vi) $n^{(2)}_{2,4} := a^{\sqrt{q}}c + df = 0$;

(vii) $n^{(2)}_{3,4} := b^{\sqrt{q}}c + d^{\sqrt{q}}e = 0$;

(viii) $H - \lambda I \neq \underline{0}$.

Proof. Let $N = (H - \lambda I)$. Then, N^2 is a Hermitian matrix

$$\begin{bmatrix} n^{(2)}_{1,1} & n^{(2)}_{1,2} & n^{(2)}_{1,3} & n^{(2)}_{1,4} \\ n^{(2)\sqrt{q}}_{1,2} & n_{2,2} & n^{(2)}_{2,3} & n^{(2)}_{2,4} \\ n^{(2)\sqrt{q}}_{1,3} & n^{(2)\sqrt{q}}_{2,3} & n^{(2)}_{3,3} & n^{(2)}_{3,4} \\ n^{(2)\sqrt{q}}_{1,4} & n^{(2)\sqrt{q}}_{2,4} & n^{(2)\sqrt{q}}_{3,4} & n^{(2)}_{4,4} \end{bmatrix},$$

where

(a) $n^{(2)}_{1,1} = a^{\sqrt{q}+1} + b^{\sqrt{q}+1} + c^{\sqrt{q}+1}$,

(b) $n^{(2)}_{2,2} = a^{\sqrt{q}+1} + d^{\sqrt{q}+1} + e^{\sqrt{q}+1}$,

(c) $n^{(2)}_{3,3} = b^{\sqrt{q}+1} + d^{\sqrt{q}+1} + f^{\sqrt{q}+1}$,

(d) $n^{(2)}_{4,4} = c^{\sqrt{q}+1} + e^{\sqrt{q}+1} + f^{\sqrt{q}+1}$.

For $i \neq j$, the conditions (iii)-(vii) are immediate, while the results of Lemma 3.2.11 and properties (a)-(d) yield conditions (i) and (ii). □

Lemma 3.2.13. *Let H be a 4×4 Hermitian matrix*

$$\begin{bmatrix} \alpha & b & c & d \\ b^{\sqrt{q}} & \beta & e & f \\ c^{\sqrt{q}} & e^{\sqrt{q}} & \gamma & g \\ d^{\sqrt{q}} & f^{\sqrt{q}} & g^{\sqrt{q}} & \delta \end{bmatrix}.$$

Then $H^2 = \underline{0}$ if and only if

(i) $\alpha^2 + b^{\sqrt{q}+1} + c^{\sqrt{q}+1} + d^{\sqrt{q}+1} = 0$;

(ii) $\beta^2 + b^{\sqrt{q}+1} + e^{\sqrt{q}+1} + f^{\sqrt{q}+1} = 0$;

(iii) $\gamma^2 + c^{\sqrt{q}+1} + e^{\sqrt{q}+1} + g^{\sqrt{q}+1} = 0$;

(iv) $\delta^2 + d^{\sqrt{q}+1} + f^{\sqrt{q}+1} + g^{\sqrt{q}+1} = 0$;

(v) $(\alpha + \beta)b + ce^{\sqrt{q}} + df^{\sqrt{q}} = 0$;

(vi) $(\alpha + \gamma)c + be + dg^{\sqrt{q}} = 0$;

(vii) $(\alpha + \delta)d + fb + gc = 0$;

(viii) $(\beta + \gamma)e + cb^{\sqrt{q}} + fg^{\sqrt{q}} = 0$;

(ix) $(\beta + \delta)f + db^{\sqrt{q}} + eg = 0$;

(x) $(\gamma + \delta)h + dc^{\sqrt{q}} + fe^{\sqrt{q}} = 0$;

(xi) $\mathrm{rank} H = 2$;

(xii) *if $\alpha + \beta + \gamma + \delta \neq 0$, then $cf = ed$.*

Proof. By direct computation, it is possible to obtain conditions (i)-(x). If c, f, d and e are all non-zero, then by (vi) and (ix) together,

$$-cf(\alpha + \beta + \gamma + \delta) = fbe + fdh^{\sqrt{q}} + cb^{\sqrt{q}}d + ceh,$$

while from (viii) and (v),

$$-ed(\alpha + \beta + \gamma + \delta) = efb + ehc + dcb^{\sqrt{q}} + dfh^{\sqrt{q}}.$$

It follows that either $\alpha + \beta + \gamma + \delta = 0$ or $cf = ed$.

Let Ψ be the linear transformation induced by H. Since $\Psi^2 = \underline{0}$, it follows that $\mathrm{Im}\,\Psi \subseteq \ker \Psi$. Furthermore,

$$\mathrm{Im}\,\Psi \simeq \mathrm{GF}(q)^4 / \ker \Psi;$$

it follows that $\dim \ker \Psi = \dim \mathrm{Im}\,\Psi = 2$, and that the rank of H is 2. □

Lemma 3.2.14. *In order for a Hermitian matrix H, given as in Lemma 3.2.11, to have minimal polynomial $(x-\lambda)^4$, one of the following coefficients has to be non-zero:*

(i) $n_{1,2}^{(3)} = f[d^{\sqrt{q}}cf^{\sqrt{q}-1} - f^{\sqrt{q}}a + e^{\sqrt{q}}b]$;

(ii) $n_{1,3}^{(3)} = e[dce^{\sqrt{q}-1} - e^{\sqrt{q}}b + f^{\sqrt{q}}a]$;

(iii) $n_{1,4}^{(3)} = d[bed^{\sqrt{q}-1} - d^{\sqrt{q}}c + af]$,

(iv) $n_{2,1}^{(3)} = n_{1,2}^{(3)\sqrt{q}} = f[dc^{\sqrt{q}} - (fa)^{\sqrt{q}} + eb^{\sqrt{q}}f^{\sqrt{q}-1}]$;

(v) $n_{2,3}^{(3)} = c[ebc^{\sqrt{q}-1} - c^{\sqrt{q}}d + a^{\sqrt{q}}f]$;

(vi) $n_{2,4}^{(3)} = b[dcb^{\sqrt{q}-1} - b^{\sqrt{q}}e + a^{\sqrt{q}}f]$;

(vii) $n_{3,1}^{(3)} = n_{1,3}^{(3)\sqrt{q}} = e[fa^{\sqrt{q}}e^{\sqrt{q}-1} - (eb)^{\sqrt{q}} + (dc)^{\sqrt{q}}]$;

(viii) $n_{3,2}^{(3)} = n_{2,3}^{(3)\sqrt{q}} = c[fac^{\sqrt{q}-1} - (cd)^{\sqrt{q}} + (eb)^{\sqrt{q}}]$;

(ix) $n_{3,4}^{(3)} = a[d^{\sqrt{q}}ca^{\sqrt{q}-1} - fa^{\sqrt{q}} + b^{\sqrt{q}}e]$;

(x) $n_{4,1}^{(3)} = n_{1,4}^{(3)\sqrt{q}} = d[(af)^{\sqrt{q}}d^{\sqrt{q}-1} - (cd)^{\sqrt{q}} + (be)^{\sqrt{q}}]$;

(xi) $n_{4,2}^{(3)} = n_{2,4}^{(3)\sqrt{q}} = b[f^{\sqrt{q}}ab^{\sqrt{q}-1} - (be)^{\sqrt{q}} + (dc)^{\sqrt{q}}]$;

(xii) $n_{4,3}^{(3)} = n_{3,4}^{(3)\sqrt{q}} = a[e^{\sqrt{q}}ba^{\sqrt{q}-1} - (af)^{\sqrt{q}} + dc^{\sqrt{q}}]$.

If all of the coefficients in (i)-(xii) are zero, $H \neq \lambda I$ and the conditions of Lemma 3.2.12 are not fulfilled, then $\mathcal{M}_H(x) = (x-\lambda)^3$.

Proof. Let $N = H - \lambda I$. By considering the conditions in Lemma 3.2.11,

$$N^3 = \begin{bmatrix} -\mathfrak{T}[(df)^{\sqrt{q}}e] & n_{1,2}^{(3)} & n_{1,3}^{(3)} & n_{1,4}^{(3)} \\ n_{2,1}^{(3)} & -\mathfrak{T}[(bf)^{\sqrt{q}}c] & n_{2,3}^{(3)} & n_{2,4}^{(3)} \\ n_{3,1}^{(3)} & n_{3,2}^{(3)} & -\mathfrak{T}[(ae)^{\sqrt{q}}c] & n_{3,4}^{(3)} \\ n_{4,1}^{(3)} & n_{4,2}^{(3)} & n_{4,3}^{(3)} & -\mathfrak{T}[(ad)^{\sqrt{q}}e] \end{bmatrix}.$$

The result follows. □

3.2.5 Case IV: some notes when the factorisation contains irreducibles

The symbols $p_n(x)$, $q_n(x)$ are used to denote distinct polynomials of degree n that do not split over $\mathrm{GF}(\sqrt{q})$. Observe that any polynomial of degree 2 in $\mathrm{GF}(\sqrt{q})[x]$ splits in $\mathrm{GF}(q)[x]$.

Lemma 3.2.15. *Let $p_4(x)$ be an irreducible polynomial of degree 4 over $\mathrm{GF}(\sqrt{q})$. Then, p_4 factorises into terms of degree at most 2 over $\mathrm{GF}(q)$.*

Proof. The polynomial $p_4(x)$ splits in $\mathrm{GF}(q^2)$. There are two possibilities:

(i) $p_4(x)$ has at least a root in $\mathrm{GF}(q)$;

(ii) all the roots of $p_4(x)$ are in $\mathrm{GF}(q^2)$.

In case (i), there exist $\alpha \in \mathrm{GF}(q)$ such that $p_4(\alpha) = 0$. Since, by hypothesis, $\alpha \notin \mathrm{GF}(\sqrt{q})$, we have $\alpha^{\sqrt{q}} \neq \alpha$ and $p_4(\alpha^{\sqrt{q}}) = 0$. It follows that

$$p_4(x) = (x - \alpha)(x - \alpha^{\sqrt{q}})q_2(x),$$

whence the result.

Assume now that $p_4(x)$ does not have any root in $\mathrm{GF}(q)$, and let $\beta \in \mathrm{GF}(q^2)$ be one of its roots. From Galois theory it is known that the orbit of β under the action of $\mathrm{Gal}(\mathrm{GF}(q^2) : \mathrm{GF}(\sqrt{q}))$ consists of 4 elements. Hence, the roots of p_4 are all distinct and the following factorisation can be provided:

$$p_4(x) = (x - \beta)(x - \beta^{\sqrt{q}})(x - \beta^q)(x - \beta^{q\sqrt{q}}).$$

Then, there exist two polynomials r_2 and s_2 as follows:

$$r_2(x) = (x - \beta)(x - \beta^q) = x^2 - x\mathfrak{T}_{\mathrm{GF}(q^2):\mathrm{GF}(q)}[\beta] + \mathfrak{N}_{\mathrm{GF}(q^2):\mathrm{GF}(q)}[\beta];$$

$$s_2(x) = (x - \beta^{\sqrt{q}})(x - \beta^{q\sqrt{q}}) = x^2 - x\mathfrak{T}_{\mathrm{GF}(q^2):\mathrm{GF}(q)}[\beta^{\sqrt{q}}] + \mathfrak{N}_{\mathrm{GF}(q^2):\mathrm{GF}(q)}[\beta^{\sqrt{q}}].$$

A straightforward computation shows that $p_4(x) = r_2(x)s_2(x)$ and $r_2(x), s_2(x) \in \mathrm{GF}(q)[x]$. □

Lemma 3.2.16. *Let H be a 4×4 Hermitian matrix with minimal polynomial of the form $\mathcal{M}_H(x) = (x - \alpha)(x - \beta)p_2(x)$. Then, H is unitarily equivalent to a block diagonal matrix H' of the form*

$$H' = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \zeta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix}$$

where

(i) $(\xi - \zeta)^2 + 4d^{\sqrt{q}+1}$ *is a non-square in* $\mathrm{GF}(\sqrt{q})$*;*

(ii) *there exists* $\omega \in \mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$ *such that* $\zeta\xi = \mathfrak{N}[\omega] + \mathfrak{N}[d]$ *and* $\zeta + \xi = \mathfrak{T}[\omega]$.

Proof. The null spaces corresponding to the polynomials $(x-\alpha)$, $(x-\beta)$ and $p_2(x)$ are mutually conjugate; hence, H' has a block-diagonal structure. On the other hand, a 2×2 matrix

$$T = \begin{bmatrix} \zeta & d \\ d^{\sqrt{q}} & \xi \end{bmatrix}$$

has characteristic polynomial $\mathcal{C}_T(x) = x^2 - (\zeta+\xi)x + (\zeta\xi - d^{\sqrt{q}+1})$. Since $\mathcal{C}_T(x)$ is a polynomial of degree 2 with coefficients in $\mathrm{GF}(\sqrt{q})$, it splits over $\mathrm{GF}(q)$. Assume ω to be one of its roots in $\mathrm{GF}(q)$; it follows that $\omega^{\sqrt{q}}$ is a root of $\mathcal{C}_T(x)$ as well. The condition that $\mathcal{C}_T(x)$ does not split over $\mathrm{GF}(\sqrt{q})$ is equivalent to require that

$$(\zeta+\xi)^2 - 4(\zeta\xi - d^{\sqrt{q}+1}) = (\xi-\zeta)^2 + 4d^{\sqrt{q}+1}$$

is a non-square in $\mathrm{GF}(\sqrt{q})$, whence (i). On the other hand, if $\mathcal{C}_T(x)$ is irreducible over $\mathrm{GF}(\sqrt{q})$, then $\omega \in \mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$, and $\omega \neq \omega^{\sqrt{q}}$. This implies the equality

$$\mathcal{C}_T(x) = x^2 - \mathfrak{T}[\omega]x + \mathfrak{N}[\omega],$$

that is $(\zeta+\xi) = \mathfrak{T}[\omega]$ and $(\zeta\xi - d^{\sqrt{q}+1}) = \mathfrak{N}[\omega]$.

By hypothesis, we assumed that $\mathcal{M}_T(x)$ has not degree 1; it follows that $\mathcal{M}_T(x) = \mathcal{C}_T(x)$, which is the result. □

Lemma 3.2.17. *Let H be a 4×4 Hermitian matrix with minimal polynomial of the form $\mathcal{M}_H(x) = (x-\alpha)^2 p_2(x)$. Then, H is unitarily equivalent to a block diagonal matrix H' of the form*

$$H' = \begin{bmatrix} \lambda & c & 0 & 0 \\ c^{\sqrt{q}} & \mu & 0 & 0 \\ 0 & 0 & \zeta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix}$$

with

(i) $(\lambda-\mu)^2 - 4c^{\sqrt{q}+1} = 0$*;*

(ii) $(\xi-\zeta)^2 + 4d^{\sqrt{q}+1}$ *a non-square in* $\mathrm{GF}(\sqrt{q})$.

Proof. The block form follows, as before, from the null spaces of $(x-\alpha)$ and $p_2(x)$ being mutually conjugate. Condition (i) is obtained as in Lemma 3.2.9; condition (ii) is proven as in Lemma 3.2.16. □

Lemma 3.2.18. *Let H be a 4×4 Hermitian matrix with minimal polynomial of the form $\mathcal{M}_H(x) = p_2(x)q_2(x)$, $p_2(x) \neq q_2(x)$. Then, H is unitarily equivalent to a block diagonal matrix H' of the form*

$$H' = \begin{bmatrix} \lambda & c & 0 & 0 \\ c^{\sqrt{q}} & \mu & 0 & 0 \\ 0 & 0 & \zeta & d \\ 0 & 0 & d^{\sqrt{q}} & \xi \end{bmatrix}$$

with

(i) $(\lambda-\mu)^2 + 4d^{\sqrt{q}+1}$ *a non-square in* $\mathrm{GF}(\sqrt{q})$*;*

(ii) $(\xi-\zeta)^2+4d^{\sqrt{q}+1}$ *a non-square in* $\mathrm{GF}(\sqrt{q})$*;*

(iii) $\xi^2-(\lambda+\mu)\xi+d^{\sqrt{q}+1}-c^{\sqrt{q}+1}\neq 0$.

Proof. Since the null spaces of $p_2(x)$ and $q_2(x)$ are mutually orthogonal, assertions (i) and (ii) follow as in Lemma 3.2.16.

If it were $p_2(x)=q_2(x)$, then

$$\begin{cases} \xi+\zeta=\lambda+\mu \\ \xi\zeta-d^{\sqrt{q}+1}=\lambda\mu-c^{\sqrt{q}+1}. \end{cases}$$

Condition (iii) follows. □

3.3 Construction of the incidence configurations

In this section we provide actual models which realize all Hermitian pencils which are non-degenerate among the ones introduced in section 3.1.

Usually, we shall consider linear systems Γ generated by the canonical Hermitian surface $\mathcal{U}_3$ and another non-degenerate surface $\mathcal{H}=\mathcal{H}(H)$ and assume q to be odd.

3.3.1 Pencils with degenerate surfaces of rank 3 only

Class a: The variety $\mathcal{H}=\mathcal{H}(H)$ where H is a matrix

$$H=\begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{bmatrix}$$

with $\alpha,\beta,\gamma,\delta$ distinct elements of $\mathrm{GF}(\sqrt{q})$ can be chosen to generate Γ together with $\mathcal{U}_3$. The minimal polynomial of H is $\mathcal{M}_H(x)=(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$. All surfaces in the linear system are associated with diagonal matrices.

Classes b and c: We choose a surface $\mathcal{H}(H)$ with H of the form

$$H=\begin{bmatrix} \alpha & b & 0 & 0 \\ b^{\sqrt{q}} & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{bmatrix}$$

to generate Γ together with $\mathcal{U}_3$. Since we require that there exists exactly one $\lambda\in\mathrm{GF}(\sqrt{q})$ such that the block $T=\begin{bmatrix} \alpha & b \\ b^{\sqrt{q}} & \beta \end{bmatrix}$ has rank 1, the following equation in λ has to admit only one solution:

$$(\alpha-\lambda)(\beta-\lambda)-b^{\sqrt{q}+1}=0.$$

Hence,

$$(\alpha - \beta)^2 + 4b^{\sqrt{q}+1} = 0.$$

Since T has never rank 0, necessarily $b \neq 0$. The minimal polynomial for H is $\mathcal{M}_H(x) = (x-\lambda)^2(x-\gamma)(x-\delta)$. The cone corresponding to $H - \lambda I$ has equation

$$\mathcal{C} : (\alpha - \lambda)X^{\sqrt{q}+1} + (\beta - \lambda)Y^{\sqrt{q}+1} + bXY^{\sqrt{q}} + b^{\sqrt{q}}X^{\sqrt{q}}Y + Z^{\sqrt{q}+1} + T^{\sqrt{q}+1} = 0$$

and the coordinates of its vertex V have to satisfy the following system of equations:

$$\begin{cases} (\alpha-\lambda)X^{\sqrt{q}} + bY^{\sqrt{q}} = 0 \\ (\beta-\lambda)Y^{\sqrt{q}} + b^{\sqrt{q}}X^{\sqrt{q}} = 0 \\ Z = 0 \\ T = 0. \end{cases}$$

Hence, the homogeneous coordinates for V are of the form

$$V = ((\lambda - \alpha)^{\sqrt{q}}, b^{\sqrt{q}}, 0, 0).$$

Finally, since, $\lambda = (\alpha + \beta)/2$, we can rewrite this expression using only α, β and b and

$$V = ((\beta - \alpha)/2, b^{\sqrt{q}}, 0, 0).$$

If $V \in \mathcal{U}_3$, then $((\beta-\alpha)/2)^{\sqrt{q}+1} + b^{\sqrt{q}+1} = 0$. In this case, Γ belongs to class (c); otherwise, when $((\beta-\alpha)/2)^{\sqrt{q}+1} + b^{\sqrt{q}+1} \neq 0$, Γ is of class (b).

Class d: The case corresponding to class (d) can be realized by considering the intersection between the Hermitian cones $\mathcal{C}_1 = \mathcal{H}(H_1)$ and $\mathcal{C}_2 = \mathcal{H}(H_2)$ described by the following matrices:

$$H_1 = \begin{bmatrix} 0 & a & b & 0 \\ a^{\sqrt{q}} & \alpha & c & 0 \\ b^{\sqrt{q}} & c^{\sqrt{q}} & \beta & 0 \\ 0 & 0 & & 0 \end{bmatrix}; \qquad H_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \gamma & d & a^{\sqrt{q}} \\ 0 & d^{\sqrt{q}} & \delta & b^{\sqrt{q}} \\ 0 & a & b & 0 \end{bmatrix};$$

with $a \neq b$, a and b different from 0 and

$$(\alpha + \gamma)(\beta + \delta) - \mathfrak{N}(d + c) \neq 0.$$

Classes e, f and g: We consider surfaces $\mathcal{H}(H)$ where

$$H = \begin{bmatrix} \alpha & b & 0 & 0 \\ b^{\sqrt{q}} & \beta & 0 & 0 \\ 0 & 0 & \gamma & c \\ 0 & 0 & c^{\sqrt{q}} & \delta \end{bmatrix},$$

with $(\alpha - \beta)^2 + b^{\sqrt{q}+1} = 0$ and $(\gamma - \delta)^2 + c^{\sqrt{q}+1} = 0$ to generate Γ together with $\mathcal{U}_3$. The minimal polynomial of H is of the form $\mathcal{M}_H(x) = (x - \lambda)^2(x - \mu)^2$. As before, we may compute the coordinates of the vertices of the two cones in the pencil. They are

$$V_1 = ((\beta - \alpha)/2, b^{\sqrt{q}}, 0, 0); \qquad V_2 = (0, 0, (\delta - \gamma)/2, c^{\sqrt{q}}).$$

Class (e) is realized when neither $((\beta-\alpha)/2)+b^{\sqrt{q}+1}=0$ nor $((\delta-\gamma)/2)+c^{\sqrt{q}+1}=0$; class (f) corresponds to the case where only one of these equations is satisfied; we have class (g) when both equations are satisfied.

Class h: For class (h) we shall follow a more geometrical approach: that is, we will choose suitable surfaces in $\mathrm{PG}(3,q)$ and reconstruct the pencil Γ from them.

A intersection of class (h) can be constructed as follows: let $\mathcal{H}$ be a non-degenerate Hermitian surface; take a point $V\notin\mathcal{H}$ let π be the polar plane of V with respect to $\mathcal{H}$. Take as $\mathcal{L}$ the Hermitian curve in π such that $(\mathcal{H}\cap\pi)\cap\mathcal{L}$ is the cyclic $q-\sqrt{q}+1$-arc. Then, the pencil generated by the cone $V\mathcal{L}$ and $\mathcal{H}$ belongs to class (g). As a matrix H inducing the Hermitian form associated with $P\mathcal{L}$ we may choose a block diagonal one of the form $(0,B)$ where $\langle\mathcal{H}(B),\mathcal{U}_2\rangle$ belongs to Kestenband's class VII.

Class k: Class (k) has three sub-classes. Like it has been done for class (h), we shall provide some geometric constructions for the varieties involved. We need a preliminary lemma.

Lemma 3.3.1. *Two rank-2 Hermitian curves sharing their singular point might intersect in either* 1, 2 *or* $\sqrt{q}+1$ *lines. In the latter case, they coincide.*

Proof. A rank-2 Hermitian curve is constructed as a cone over a Baer subline of any line of the plane not through its singular point. Two Baer sublines of a line in $\mathrm{PG}(2,q)$, unless they coincide, either have 1 or two points in common. This implies the result. □

In all the three cases (k-i), (k-ii) and (k-iii), the pencil Γ is generated by a non-degenerate surface $\mathcal{U}_3$ and a cone $\mathcal{C}$ whose vertex V belongs to $\mathcal{U}_3$. Let π be the tangent plane to $\mathcal{U}_3$ at V and let l be a line of π not through V. Both $\mathcal{U}_3$ and $\mathcal{C}$ intersect l in a degenerate Hermitian curve, that is sets of $\sqrt{q}+1$ lines through V. Now, Lemma 3.3.1 allows us to identify and construct the three possible situations.

3.3.2 Pencils with degenerate surfaces of rank 2 only

Class I-a: The intersection $\mathcal{E}$ belongs to class I-a if and only if the linear system Γ contains exactly one Hermitian surface $\mathcal{C}$ of rank 2. We may assume such a surface to be associated with a Hermitian matrix H' of the form

$$H'=\begin{bmatrix}\alpha & b & 0 & 0\\ b^{\sqrt{q}} & \beta & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix},$$

with $(\alpha-\beta)^2+4b^{\sqrt{q}+1}$ a non-square in $\mathrm{GF}(\sqrt{q})$. We observe that the minimal polynomial of H' is an irreducible of degree 2. The radical of $\mathcal{C}$ is the line $[Z=T=0]$. Such a line is tangent to the non-degenerate Hermitian surface given by

$$\mathcal{U}_3' : XZ^{\sqrt{q}} + XT^{\sqrt{q}} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}}X + T^{\sqrt{q}}X.$$

Class I-b Consider the surface $\mathcal{C}$ as introduced in the previous class. Its radical meets the canonical Hermitian surface $\mathcal{U}_3$ in $\sqrt{q}+1$ points. Furthermore, the minimal polynomial of any non-degenerate surface in the pencil generated by $\mathcal{U}_3$ and $\mathcal{C}$ is of the form $\mathcal{M}_H(x) = p(x)(x-\lambda)$ where $p(x)$ is irreducible over $\mathrm{GF}(\sqrt{q})$ of degree 2.

Class I-c We consider the surface $\mathcal{C}$ of class I-a together with the non-degenerate surface

$$\mathcal{U}_3'' : XZ^{\sqrt{q}} + ZX^{\sqrt{q}} + YT^{\sqrt{q}} + TY^{\sqrt{q}} = 0$$

as generators of Γ. The radical of $\mathcal{C}$ is included in $\mathcal{U}_3''$.

Class II-c: Class II can be realized by considering as generators for a linear system Γ the two singular surfaces induced by the matrices

$$H_1 = \begin{bmatrix} \alpha & b & 0 & 0 \\ b^{\sqrt{q}} & \beta & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \qquad H_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma & c \\ 0 & 0 & c^{\sqrt{q}} & \delta \end{bmatrix},$$

where we assume $(\alpha-\beta)^2+4b^{\sqrt{q}+1}$ and $(\gamma-\delta)^2+4b^{\sqrt{q}+1}$ to be non-squares in $\mathrm{GF}(\sqrt{q})$. Clearly, the minimal polynomial of any non degenerate surface in Γ is of the form $m(x) = p(x)q(x)$ with both $p(x)$ and $q(x)$ irreducibles of degree 2 over $\mathrm{GF}(\sqrt{q})$.

3.3.3 Pencils whose degenerate surfaces have rank 2 and 3

In this case, we shall consider as generators for the linear system Γ two of the degenerate surfaces in the pencil.

Class I-a A linear system in class I-a can be generated by a Hermitian cone $\mathcal{C}$ of vertex V and a rank 2 Hermitian surface $\mathcal{D}$ of radical l with $V \notin \mathcal{D}$.

In class (I-a-i), the radical l of $\mathcal{D}$ intersects $\mathcal{C}$ in exactly one point. This is to say, since $V \notin \mathcal{D}$, that l is tangent to a non-degenerate plane section of $\mathcal{C}$. Such a configuration can be realized by taking for $\mathcal{C}$ the Hermitian cone of vertex $(0,0,0,1)$ given by the equation

$$\mathcal{C} : X^{\sqrt{q}}Y + Y^{\sqrt{q}}X + Z^{\sqrt{q}+1} = 0$$

and, as $\mathcal{D}$, the surface induced by a Hermitian matrix H of the form

$$H = \begin{bmatrix} \alpha & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ b^{\sqrt{q}} & 0 & 0 & \delta \end{bmatrix},$$

with $(\alpha-\delta)^2-4b^{\sqrt{q}+1}$ a non-square in $\mathrm{GF}(\sqrt{q})$ and $\alpha\delta-b^{\sqrt{q}+1}\neq 0$. Via a direct computation, we see that the radical of $\mathcal{D}$ has equation $l:[X=T=0]$. Such a line intersects $\mathcal{C}$ only in the point $(0,1,0,0)$; hence, $\mathcal{D}$ and $\mathcal{C}$ satisfy the required conditions.

Class (I-a-ii) is realized in a similar way: this time we need as radical for $\mathcal{D}$ a line l which is intersecting $\mathcal{C}$ in $\sqrt{q}+1$ points. Consider as $\mathcal{C}$ the Hermitian cone of equation

$$\mathcal{C}: XY^{\sqrt{q}}-Y^{\sqrt{q}}X+\omega Z^{\sqrt{q}+1}=0,$$

with $\omega^{\sqrt{q}-1}=-1$. A model for $\mathcal{D}$ is provided by the Hermitian surface induced by a matrix of the form

$$H=\begin{bmatrix} 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & \gamma & c\\ 0 & 0 & c^{\sqrt{q}} & \delta \end{bmatrix},$$

with $(\alpha-\delta)^2-4b^{\sqrt{q}+1}$ a non-square in $\mathrm{GF}(\sqrt{q})$ and $\gamma\delta-c^{\sqrt{q}+1}\neq 0$. In fact, the radical of $\mathcal{D}$ is the line $l:[Z=T=0]$, which intersects $\mathcal{C}$ in points satisfying $XY^{\sqrt{q}}-YX^{\sqrt{q}}=0$, that is in the points of a subline $\mathrm{PG}(1,\sqrt{q})$.

Class (I-a-iii) is possible from the combinatorial point of view; however, it cannot be realized: the only lines completely contained in $\mathcal{C}$ are those through the vertex; hence, V should belong to $\mathcal{E}$, against the non-degeneracy hypothesis.

Class I-b: As for Class (a), we consider the pencil Γ as generated by the cone $\mathcal{C}$ and the rank 2 surface $\mathcal{D}$ of radical l; this time we assume $V\in\mathcal{D}$.

Lemma 3.3.2. *Let Γ be a linear system of Hermitian surfaces and assume that there are at least two degenerate surfaces $\mathcal{C}_1$ and $\mathcal{C}_2$ in Γ. Let $l_1=\operatorname{rad}\mathcal{C}_1$ and $l_2=\operatorname{rad}\mathcal{C}_2$. If $l_1\cap l_2\neq\emptyset$, then all surfaces in Γ are degenerate.*

Proof. Assume $P\in l_1\cap l_2$. Then, all partial derivatives of both the equation of $\mathcal{C}_1$ and the equation of $\mathcal{C}_2$ are zero in P. From the linearity of the derivative, it follows that all partial derivatives with respect to the equation of $\lambda\mathcal{C}_1+\mu\mathcal{C}_2$ are zero as well. □

Lemma 3.3.2 yields that $V\notin l$.

No non-degenerate surface belongs to a pencil of class (I-b-iii). In fact, in (I-b-iii), the radical l of $\mathcal{D}$ intersects the cone $\mathcal{C}$ in $q+1$ points; this implies that $V\in l$, in contradiction with Lemma 3.3.2.

In order to realize a pencil in class (I-b-i), we consider the Hermitian cone $\mathcal{C}$ of vertex $V=(0,0,0,1)$ and equation

$$\mathcal{C}: X^{\sqrt{q}}Y+Y^{\sqrt{q}}X+Z^{\sqrt{q}+1}=0,$$

together with the rank 2 surface $\mathcal{D}$ induced by the matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ b^{\sqrt{q}} & 0 & 0 & 0 \end{bmatrix},$$

with $b \in \mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$. Clearly, the point $(0,0,0,1)$ belongs to $\mathcal{D}$; furthermore, the radical of $\mathcal{D}$ has equation $l : [X = T = 0]$, and such a line l intersects $\mathcal{C}$ in the point $(0,1,0,0)$, different from V.

Likewise, a pencil Γ generated by the cone $\mathcal{C}'$ of equation

$$\mathcal{C}' : XY^{\sqrt{q}} - Y^{\sqrt{q}}X + \omega Z^{\sqrt{q}+1} = 0,$$

with $\omega^{\sqrt{q}-1} = -1$, and the surface $\mathcal{D}$ induced by a matrix of the form

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & c^{\sqrt{q}} & 0 \end{bmatrix},$$

with $c \in \mathrm{GF}(q) \setminus \mathrm{GF}(\sqrt{q})$, belongs to class (I-b-ii), since the intersection of the radical l with $\mathcal{C}$ is the set of points $(X,Y,0,0) \in \mathrm{PG}(2,q)$ with $X, Y \in \mathrm{GF}(\sqrt{q})$.

Class II: In classes (II-a-iii) and (II-b-iii) the radical l of $\mathcal{D}$ is a subset of $\mathcal{E}$; hence, it has to contain the vertex of any cone in the pencil Γ and, by Lemma 3.3.2, we obtain that all the surfaces in the linear system are degenerate. We now investigate classes (II-a-ii) and (II-b-ii).

A model for class (II-a-ii) can be realized by considering the linear system Γ generated by the two Hermitian cones $\mathcal{C}_1$ and $\mathcal{C}_2$ given by the following matrices H_1 and H_2:

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \beta & b & 0 \\ 0 & b^{\sqrt{q}} & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{bmatrix}; \qquad H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \beta & b & 0 \\ 0 & b^{\sqrt{q}} & \gamma & c \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

with $\beta\gamma - b^{\sqrt{q}+1} \neq 0$. Since we assume to be in odd characteristic, we see that the linear system generated by $\mathcal{C}_1$ and $\mathcal{C}_2$ is clearly non-degenerate; it contains two rank 3 and one rank 2 surface $\mathcal{D}$, given by $\mathcal{D} = \mathcal{C}_1 - \mathcal{C}_2$. Furthermore, none of the vertices of the cones belongs to the intersection $\mathcal{E}$. Hence, Γ is of class (II-a-ii).

We generate a member of class (II-b-ii) as follows. Let $\mathcal{C}_1 = \mathcal{H}(H_1)$ and $\mathcal{C}_2 = \mathcal{H}(H_2)$ be the Hermitian cones induced by the matrices:

$$H_1 = \begin{bmatrix} 0 & a & c & 0 \\ a^{\sqrt{q}} & \alpha & d & 0 \\ c^{\sqrt{q}} & d^{\sqrt{q}} & \beta & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \qquad H_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \gamma & v & a^{\sqrt{q}} \\ 0 & v^{\sqrt{q}} & \delta & c^{\sqrt{q}} \\ 0 & a & c & 0 \end{bmatrix},$$

where both H_1 and H_2 are assumed to be of rank 3. The line $[Y = Z = 0]$, joining the vertices of $\mathcal{C}_1$ and $\mathcal{C}_2$, is contained in $\mathcal{E}$. Since we want the linear system Γ generated by $\mathcal{C}_1$ and $\mathcal{C}_2$ to contain one rank 2 surface, the following further conditions, equivalent to require that $\mathcal{C}_1 + \mathcal{C}_2$ has rank 2, have to be imposed on the coefficients:

$$\begin{cases} (v+d)^{\sqrt{q}} = \frac{c^{\sqrt{q}}}{a^{\sqrt{q}}}(\alpha+\gamma) \\ (\beta+\delta) = \frac{c^{\sqrt{q}}}{a^{\sqrt{q}}}(d+v). \end{cases}$$

On the other hand, $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(\sqrt{q})$ are fixed by the Frobenius involution; hence, the first condition can be rewritten as

$$(\beta+\delta)a^{\sqrt{q}+1} = (\alpha+\gamma)c^{\sqrt{q}+1}.$$

Chapter 4

General results

The aim of this chapter is to present a formula to determine the possible sizes of the intersection of two Hermitian varieties in dimension n. Furthermore, some GAP code to work with Hermitian hypersurfaces is introduced. It is observed that most of the 'interesting' cases are out of reach for such a straightforward code and some further improvements are suggested.

4.1 The cardinality formula

In this section we want to determine the possible size of the intersection of any two Hermitian hypersurfaces in $\mathrm{PG}(n, q)$. In order to prove the result, the variety $\mathscr{H}$ of $\mathrm{PG}(n^2 + 2n, q)$ representing the singular Hermitian hypersurfaces of $\mathrm{PG}(n, q)$ will be studied. This result has been presented at the international conference "Combinatorics 2000" in Gaeta. I'm thankful to Prof. A. Cossidente and Dott. A. Siciliano for having first suggested me to investigate the properties of this remarkable object.

4.1.1 Introduction

In [CS], the geometry of Hermitian matrices of order three over a Galois field is studied; Sections 2 and 3 deal with varieties arising in $\mathrm{PG}(8, \sqrt{q})$ from rank 1 and rank 2 Hermitian matrices. More precisely, it is proven that the variety coming from rank 2 matrices is a cubic hypersurface $\mathscr{M}_3^7$ whose singular points form the variety of all rank 1 Hermitian matrices.

In our work, we shall investigate the variety of the singular Hermitian matrices of order n and use its properties in order to determine the possible intersection orders for any two Hermitian hypersurfaces.

4.1.2 Preliminaries

Definition 4.1.1. For any matrix $M \in \mathrm{Mat}(n, q)$, the symbol M_{ij} denotes the element in the i-th row and j-th column of M; the symbol M^{ij} denotes the minor of M obtained by deleting the i-th row and the j-th column.

Let L be a list of the form $L = \{i_1j_1, i_2j_2, \ldots, i_kj_k\}$. If all i_t and j_t are different, then M^L is the minor of M obtained by removing all the i_t-th columns and j_t-th rows from M; if there exist g, h such that $i_g = i_h$ or $j_g = j_h$, then M^L is the $(n-k) \times (n-k)$ null matrix; likewise we define $M_{ij}^{hk} = 0$ if $i = h$ or $j = k$.

Definition 4.1.2. Assume $\mathbb{K}$, $\mathbb{F}$ to be two fields with $[\mathbb{F} : \mathbb{K}] = 2$, $\mathbb{F} = \mathbb{K}(\epsilon)$, and let $\overline{x}$ be the image of $x \in \mathbb{F}$ under the involution fixing $\mathbb{K}$. Let

$$M := \begin{bmatrix} X_{00} & X_{01} + \epsilon\widetilde{X_{01}} & \ldots & X_{0n} + \epsilon\widetilde{X_{0n}} \\ X_{01} + \overline{\epsilon}\widetilde{X_{01}} & X_{11} & \ldots & X_{1n} + \epsilon\widetilde{X_{1n}} \\ \vdots & & & \vdots \\ X_{0n} + \overline{\epsilon}\widetilde{X_{0n}} & \ldots & & X_{nn} \end{bmatrix}$$

be a $(n+1) \times (n+1)$-Hermitian matrix over $\mathbb{F}$ with respect to the automorphism induced by the conjugation. The symbol $\mathrm{Her}_{\mathbb{K}}(n+1, \mathbb{F})$ denotes the set of all such matrices.

We introduce a mapping ξ defined as follows:

$$\xi \begin{cases} \mathrm{Her}_{\mathbb{K}}(n+1, \mathbb{F}) \to \mathbb{K}^{n^2+2n+1} \\ M \to (X_{00}, X_{01}, \widetilde{X_{01}}, X_{11}, X_{02} \ldots, X_{nn}). \end{cases}$$

Definition 4.1.3. The *determinantal polynomial* for $\mathrm{Her}_{\mathbb{K}}(n+1, \mathbb{F})$ is the polynomial P_n in $\mathbb{K}[X_{00}, X_{01}, \widetilde{X_{01}}, \ldots, X_{nn}]$ given by

$$P_n(X_{00}, X_{01}, \widetilde{X_{01}}, \ldots, X_{nn}) := \det(\xi^{-1}(M)).$$

Observe that the degree of the polynomial P_n is $n+1$. In the following theorem we compute partial derivatives of P_n with respect to X_{ij} and $\widetilde{X_{ij}}$.

Theorem 4.1.4. *With the notations of Definition 4.1.3,*

(i)

$$\frac{\partial P}{\partial X_{ii}} = \det(M^{ii});$$

(ii) *for* $i \neq j$,

$$\frac{\partial P}{\partial X_{ij}} = (-1)^{i+j}(\det(M^{ij}) + \det(M^{ji}));$$

(iii) *for* $i \neq j$,

$$\frac{\partial P}{\partial \widetilde{X_{ij}}} = (-1)^{i+j}[\epsilon \det(M^{ij}) + \overline{\epsilon}\det(M^{ji})].$$

Proof. For $i = j$, consider the expansion of P as

$$P = \sum_{t=0}^{n} (-1)^{i+t} M_{it} \det(M^{it})$$

and observe that for any i, h, k with $(h,k) \neq (i,i)$:

$$\frac{\partial \widetilde{X_{hk}}}{\partial X_{ii}} = 0.$$

Then, the formal derivative with respect to X_{ii} is

$$\frac{\partial P}{\partial X_{ii}} =$$

$$\sum_{t=0}^{n} (-1)^{i+t} \left[\frac{\partial M_{it}}{\partial X_{ii}} \det(M^{it}) + M_{it} \frac{\partial \det(M^{it})}{\partial X_{ii}} \right] =$$

$$\sum_{t=0}^{n} (-1)^{i+t} [\frac{\partial X_{it}}{\partial X_{ii}} \det(M^{it}) + \epsilon \frac{\partial \widetilde{X_{it}}}{\partial X_{ii}} \det(M^{it}) + M_{it} \frac{\partial \det(M^{it})}{\partial X_{ii}}] =$$

$$(-1)^{2i} \det(M^{ii}) + 0 + \sum_{t=0}^{n} (-1)^{i+t} M_{it} \frac{\partial \det(M^{it})}{\partial X_{ii}}.$$

On the other hand, M^{it} does not contain the term X_{ii}; hence,

$$\sum_{t=0}^{n} (-1)^{i+t} M_{it} \frac{\partial \det(M^{it})}{\partial X_{ii}} = 0$$

and (i) follows.

Now assume $i \neq j$. The determinantal polynomial P can be written as

$$P = \sum_{t=0}^{n} (-1)^{i+t} (X_{it} + \epsilon \widetilde{X_{it}}) \det(M^{it}).$$

Then, the partial derivative with respect to X_{ij} is

$$\frac{\partial P}{\partial X_{ij}} = (-1)^{i+j} \det(M^{ij}) + \sum_{t=0}^{n} (-1)^{i+t} M_{it} \frac{\partial \det(M^{it})}{\partial X_{ij}}.$$

On the other hand, the term X_{ij} appears only in the expression of M_{ij} and of M_{ji}. Hence, expanding the determinant by the j-th row and the i-th column, we obtain

$$\frac{\partial P}{\partial X_{ij}} = (-1)^{i+j} \det(M^{ji}) + \sum_{t=0}^{n} (-1)^{i+t} M_{jt} \frac{\partial \det(M^{jt})}{\partial X_{ij}}.$$

We claim that

$$\sum_{t=0}^{n} (-1)^{j+t} M_{jt} \frac{\partial \det(M^{jt})}{\partial X_{ij}} = (-1)^{i+j} \det(M^{ij}).$$

As a matter of fact,

$$\sum_{t=0}^{n}(-1)^{j+t}M_{jt}\frac{\partial\det(M^{jt})}{\partial X_{ij}} =$$
$$\sum_{t=0}^{n}(-1)^{j+t}M_{jt}\frac{\partial\sum_{k=0}^{n}(-1)^{i+k}M_{ik}^{jt}\det(M^{jt,ik})}{\partial X_{ij}} =$$
$$\sum_{t=0}^{n}\sum_{k=0}^{n}(-1)^{(i+j)+(k+t)}M_{jt}[\frac{\partial M_{ik}^{jt}}{\partial X_{ij}}\det(M^{jt,ik}) + M_{ik}^{jt}\frac{\partial\det(M^{ij,ik})}{\partial X_{ij}}] =$$
$$(-1)^{i+j}[\sum_{t=0}^{n}(-1)^{j+t}M_{jt}\det(M^{jt,ij})]+$$
$$(-1)^{i+j}[\sum_{t=0}^{n}\sum_{k=0}^{n}M_{jt}M_{ik}^{jt}\frac{\partial\det(M^{jt,ik})}{\partial X_{ij}}] = (-1)^{i+j}\det(M^{ij}) + 0,$$

since $M^{jt,ik}$ does not contain any term in X_{ij}.

Given that

$$\frac{\partial M_{ij}}{\partial\widetilde{X_{ij}}} = \overline{\left(\frac{\partial M_{ji}}{\partial\widetilde{X_{ij}}}\right)} = \epsilon,$$

it is possible to write the derivative of P with respect to $\widetilde{X_{ij}}$ as

$$\frac{\partial P}{\partial\widetilde{X_{ij}}} = (-1)^{i+j}[\epsilon\det(M^{ij}) + \sum_{t=0}^{n}(-1)^{i+t}M_{it}\frac{\partial\det(M^{it})}{\partial\widetilde{X_{ij}}}].$$

In order to prove part (iii), the main claim is

$$\sum_{t=0}^{n}(-1)^{i+t}M_{it}\frac{\partial\det(M^{it})}{\partial\widetilde{X_{ij}}} = \overline{\epsilon}\det(M^{ji}).$$

In fact, we have

$$\sum_{t=0}^{n}(-1)^{i+t}M_{it}\frac{\partial\det(M^{it})}{\partial\widetilde{X_{ij}}} =$$
$$(-1)^{i+j}[\sum_{t=0}^{n}\sum_{k=0}^{n}M_{it}\frac{\partial M_{jk}^{it}}{\partial\widetilde{X_{ij}}}\det(M^{jk,it})] =$$
$$(-1)^{i+j}[\sum_{t=0}^{n}M_{jt}\frac{\partial M_{ji}^{it}}{\partial\widetilde{X_{ij}}}\det(M^{jt,ij})] = (-1)^{i+j}\overline{\epsilon}\det(M^{ji}),$$

whence the theorem follows. □

4.1.3 The determinantal variety $\mathscr{H}$

From now on, we shall assume to be working over a finite field $\mathrm{GF}(q)$, with q square, and write $\mathrm{Her}(n+1,q)$ for $\mathrm{Her}_{\mathrm{GF}(\sqrt{q})}(n+1,\mathrm{GF}(q))$. Observe that the polynomial P_n defines an algebraic hypersurface $\mathscr{H}_{n,q}=\mathcal{F}(P_n)$ in $\mathrm{PG}(n^2+2n,\sqrt{q})$ that we may call the *determinantal variety* of $\mathrm{Her}(n+1,q)$. The name is justified by the fact that a point x is in $\mathscr{H}_{n,q}$ if and only if $\xi^{-1}(x)$ is a singular Hermitian hypersurface in $\mathrm{PG}(n,q)$ or, equivalently, the pre-images under ξ of x in $\mathrm{Her}(n+1,q)$ are singular Hermitian matrices.

We need some further notation.

Definition 4.1.5. Let $\mathscr{H}_{n,q}$ be the hypersurface in $\mathrm{PG}(n^2+2n,\sqrt{q})$ of all singular Hermitian hypersurfaces of $\mathrm{PG}(n,q)$. Denote by

(i) the symbol $\mathscr{O}_{r,n,q}:=\mathscr{O}_{r,n}$ the set of points of $\mathscr{H}_{n,q}$ corresponding to Hermitian matrices of rank r;

(ii) the symbol $\mathscr{O}^i_{n,q}:=\mathscr{O}^i_n$ the set of points of $\mathscr{H}_{n,q}$ with multiplicity i;

(iii) the symbol $\mathscr{O}_{\le r,n,q}:=\mathscr{O}_{\le r,n}$ the set of points of $\mathscr{H}_{n,q}$ corresponding to matrices of rank *at most* r;

(iv) the symbol $\mathscr{O}^{\ge i}_{n,q}:=\mathscr{O}^{\ge i}_n$ the set of points of $\mathscr{H}_{n,q}$ of multiplicity *at least* i;

(v) the symbol $\mathscr{O}^0_{n,q}$ the points of $\mathrm{PG}(n,\sqrt{q})$ not in $\mathscr{H}_{n,q}$.

Theorem 4.1.6. *The singular points of $\mathscr{H}_{n,q}$ are in 1–1 correspondence with Hermitian varieties of $\mathrm{PG}(n,q)$ having rank at most $n-1$, that is*

$$\mathscr{O}^{\ge 2}_{n,q}=\mathscr{O}_{\le(n-1),n,q}.$$

Proof. If $\mathcal{H}(H)$ is a Hermitian variety in $\mathrm{PG}(n,q)$ of rank at most $n-1$, then all its $n\times n$ minors have determinant zero. Theorem 4.1.4 guarantees that all partial derivatives of the function $\det(M)$ can be expressed as combinations of suitable determinants of $n\times n$ minors of M. It follows that all partial derivatives of $\det(M)$ are 0 at the point $\xi(H)$ of $\mathscr{H}_{n,q}$ corresponding to H; hence, the point is singular.

Consider now a singular point T on $\mathscr{H}_{n,q}$, and let $H=\xi^{-1}(T)$ be a Hermitian matrix in $\mathrm{Her}(n+1,q)$ which is the pre-image of T. Let H^{ij} be any $n\times n$ minor of H. Then,

(i) if $i=j$,

$$\det(H^{ii})=\frac{\partial P}{\partial X_{ii}}(H)=0;$$

(ii) if $i \neq j$, the linear system

$$\begin{cases} \det(H^{ij}) + \det(H^{ji}) = \frac{\partial P}{\partial X_{ij}} = 0 \\ \epsilon \det(H^{ij}) + \overline{\epsilon} \det(H^{ji}) = \frac{\partial P}{\partial \widetilde{X_{ij}}} = 0 \end{cases}$$

consists of two independent equations in $\det(H^{ij})$ and $\det(H^{ji})$; hence,

$$\det(H^{ij}) = \det(H^{ji}) = 0.$$

It follows that all $n \times n$-minors have determinant 0; hence, the rank of H is at most $n-1$. □

Lemma 4.1.7. *Let H be a singular Hermitian matrix of rank r. If $r < \sqrt{q}$, then the image of H on $\mathscr{H}_{n,q}$ is at most a $(n-r+1)$-ple point.*

Proof. If $r = n$, the result follows directly from Theorem 4.1.4.

Assume now $r < n$. Then, there exists a linear transformation ϑ such that H is equivalent to a matrix H' of the form

$$H' := \left[\begin{array}{c|c} 0_{(n-r+1)\times(n-r+1)} & \\ \hline & I_{r\times r} \end{array}\right].$$

Let σ be a primitive element of $\mathrm{GF}(\sqrt{q})^\star$ and define T as the matrix

$$T := \left[\begin{array}{c|ccc} I_{(n-r+1)\times(n-r+1)} & & & \\ \hline & \sigma & & \\ & & \cdots & \\ & & & \sigma^r \end{array}\right].$$

The linear system generated by T and H' contains, by construction, exactly one matrix of rank r, r matrices of rank n and $\sqrt{q}+1-r-1 = \sqrt{q}-r$ non-singular matrices. It follows that the line TH' of $\mathrm{PG}(n^2+2n, \sqrt{q})$ is not totally contained in $\mathscr{H}_{n,q}$. The degree of $\mathscr{H}_{n,q}$ is $n+1$; hence, Bezout's theorem guarantees that TH' intersects $\mathscr{H}_{n,q}$ in at most $n+1$ points, counted with the proper multiplicities. Since the matrices of rank n correspond to non-singular points of $\mathscr{H}_{n,q}$, it follows that

$$\mathrm{mult}(H) + r \leq n+1,$$

that is $\mathrm{mult}(H) \leq (n-r+1)$. □

Corollary 4.1.8. *If $n \leq \sqrt{q}$, then all matrices of rank $n-1$ correspond to double points of $\mathscr{H}_{n,q}$ and* vice versa. *That is,*

$$\mathscr{O}_{n-1,n,q} = \mathscr{O}^2_{n,q}.$$

Proof. From Lemma 4.1.12, matrices of rank $n-1$ correspond to points of $\mathscr{H}_{n,q}$ of multiplicity at most 2. On the other hand, all matrices of rank at most $n-1$ do correspond to singular points of $\mathscr{H}_{n,q}$; hence, their multiplicity as points is at least 2. The result follows. □

Lemma 4.1.9. *Let N be a generic matrix in $\mathrm{Mat}(n+1,q)$ define D as the polynomial*

$$D(N_{00}, N_{01}, N_{10}, \ldots, N_{nn}) := \det(N),$$

and assume

$$\mathscr{D}_{n,q} := \mathcal{F}(D).$$

Then, $\mathscr{H}_{n,q}$ is a section of $\mathscr{D}_{n,q}$ via a $\mathrm{PG}(n^2+2n, \sqrt{q})$; in fact, there exists a linear mapping ϕ such that $\mathscr{H}_{n,q}$ is the image under ϕ of the $\mathrm{GF}(\sqrt{q})$-rational points of $\mathscr{D}_{n,q}$.

Proof. Consider the determinant function $P_n(X_{00}, X_{01}, \widetilde{X_{01}}, \ldots)$ for a matrix X written as in Theorem 4.1.4. Assume that the variables do vary in $\mathrm{GF}(q)$, rather than in $\mathrm{GF}(\sqrt{q})$; this is equivalent to consider the $\mathrm{GF}(q)$-rational points of the variety $\mathscr{H}_{n,q}$. In this case, P_n can be seen as the determinant function of a matrix of the same structure as X. The two equations

$$\begin{cases} X_{01} + \epsilon \widetilde{X_{01}} = \alpha \\ X_{01} + \epsilon^{\sqrt{q}} \widetilde{X_{01}} = \beta \end{cases}$$

are independent over $\mathrm{GF}(q)$ and always admit a solution in X_{01}, $\widetilde{X_{01}}$. Hence, there exists a matrix N such that

$$P(X_{00}, X_{01}, \widetilde{X_{01}} \ldots) = D(N_{00}, N_{01}, N_{10}, \ldots).$$

On the other hand, given any matrix $N \in \mathrm{Mat}(n+1,q)$, consider the following transformation ϕ, where $i > j$:

$$\begin{array}{l} N_{ii} \to X_{ii} \\ N_{ij} - \epsilon N ji \to X_{ij} \\ N_{ji} - \epsilon^{\sqrt{q}} N_{ij} \to X_{ji}. \end{array}$$

The mapping ϕ is linear (hence rational) and transforms the polynomial $D(N)$ into $P(X)$.

It follows that the $\mathrm{GF}(\sqrt{q})$-rational points of $\mathscr{D}_{n,q}$ are transformed by ϕ into the $\mathrm{GF}(\sqrt{q})$-rational points of $\mathscr{H}_{n,q}$ and the $\mathrm{GF}(q)$-rational points of $\mathscr{H}_{n,q}$ are mapped into the $\mathrm{GF}(q)$-rational points of $\mathscr{D}_{n,q}$. The result follows. □

The result of Lemma 4.1.9 can be summarized in the following diagram.

$$\begin{array}{ccccc} \mathrm{Mat}(n+1,q) & \longrightarrow & \mathscr{D}_{n,q} & \subseteq & \mathrm{PG}(n^2+2n,q) \\ \uparrow \subseteq & & \uparrow \phi & & \\ \mathrm{Her}(n+1,q) & \longrightarrow & \mathscr{H}_{n,q} & \subseteq & \mathrm{PG}(n^2+2n,\sqrt{q}) \end{array}$$

Corollary 4.1.10. *For any $i \geq 2$, the $\mathrm{GF}(\sqrt{q}^i)$-rational points of $\mathscr{H}_{n,q}$ do correspond to the $\mathrm{GF}(\sqrt{q}^i)$-rational points of $\mathscr{D}_{n,q}$.*

Corollary 4.1.11. *For any $l > 0$, the $\mathrm{GF}(q^{2l})$-rational points of $\mathscr{H}_{n,q}$ and $\mathscr{H}_{n,q^l}$ are the same.*

We are now in position to generalise Lemma 4.1.7 to matrices of any rank r, lifting the restriction $r < q$.

Theorem 4.1.12. *Let H be a singular Hermitian matrix of rank r. Then the image of H on $\mathscr{H}_{n,q}$ is at most a $(n-r+1)$-ple point; that is,*

$$\mathscr{O}_{r,q} \subseteq \mathscr{O}_q^{\leq n-r+1}.$$

Proof. If $r \leq \sqrt{q}-1$, this is Lemma 4.1.7.

Otherwise, let k be an integer such that $\sqrt{q}^k > r$, and consider the $\mathrm{GF}(\sqrt{q}^k)$-rational points of $\mathscr{H}_{n,q}$. Every $\mathrm{GF}(\sqrt{q})$-rational point H of $\mathscr{H}_{n,q}$ is a $\mathrm{GF}(\sqrt{q}^k)$ rational point. Furthermore, the multiplicity of any point H is preserved under algebraic extensions. Let θ be a primitive element of $\mathrm{GF}(\sqrt{q}^k)^\star$. Since $\sqrt{q}^k > r$, all the powers $\theta, \theta^2, \ldots, \theta^r$ are distinct. Let P be the image via $\xi' : \mathrm{Mat}(n+1, q^k) \to \mathrm{PG}(n^2+2n, \sqrt{q}^k)$ of the matrix

$$T := \left[\begin{array}{c|ccc} I_{(n-r+1)\times(n-r+1)} & & & \\ \hline & \theta & & \\ & & \ddots & \\ & & & \theta^r \end{array}\right].$$

The line HP intersects $\mathscr{H}_{n,q}$ in H and in at least r more of its $\mathrm{GF}(\sqrt{q}^k)$ rational points; furthermore, HP is not completely included in $\mathscr{H}_{n,q}$; hence the result follows, as before, from Bezout's theorem. □

Observe that the matrix T constructed in the proof of Theorem 4.1.12 is *not* Hermitian.

Lemma 4.1.13. *Let $\mathbb{K}$ be a field, and assume $L, M \in \mathrm{Mat}(n+1, \mathbb{K})$; then, for all $a, b \in \mathbb{K}$,*

$$\mathrm{rank}(aL + bM) \leq \mathrm{rank}(L) + \mathrm{rank}(M).$$

Proof. Let θ and τ be the linear mappings induced by L and M. Since for all $x \in V = \mathbb{K}^n$

$$(a\lambda + b\mu)(x) = a\lambda(x) + b\mu(x),$$

the image of $(a\theta + b\tau)$ is included in the direct sum of the images of the spaces $\theta(V)$ and $\tau(V)$. The result follows from

$$\mathrm{rank}(L) = \dim \mathrm{Im}\, \theta; \qquad \mathrm{rank}(M) = \dim \mathrm{Im}\, \tau.$$

□

Corollary 4.1.14. *Let H_1, H_2 be two Hermitian matrices in $\mathrm{Mat}(n+1, q)$ of rank at most $n/2$. Then, the line $\xi(H_1)\xi(H_2)$ determined by the images of H_1 and H_2 is completely included in $\mathscr{H}_{n,q}$.*

Proof. From Lemma 4.1.13, for any $\lambda, \mu \in \mathrm{GF}(\sqrt{q})$,

$$\mathrm{rank}(\lambda H_1 + \mu H_2) \leq \mathrm{rank}(H_1) + \mathrm{rank}(H_2) \leq n < n + 1.$$

It follows that all matrices in the linear system Γ generated by H_1 and H_2 are singular. □

Corollary 4.1.15. *For any integer $i < n/2$, the envelope of secants to the variety $\mathscr{O}_{\leq i,n}$ is a subvariety of $\mathscr{O}_{\leq 2i,n}$.*

Lemma 4.1.16. *Let M be an $(n+1) \times (n+1)$ matrix of the form*

$$M := \left[\begin{array}{c|c} 0_{(n-r+1)\times(n-r+1)} & \\ \hline & I_{r\times r} \end{array}\right].$$

And let H be a generic $(n+1) \times (n+1)$ matrix. Then, $\mu^{n-r+1} \mid \det(\lambda M + \mu H)$.

Proof. The proof is by induction on $n - r$.

If $n - r = 0$, then the first row of M can be assumed to be the zero vector. It follows that

$$\det(\lambda M + \mu H) = \sum_{i=0}^{n} (\lambda M_{i0} + \mu H_{i0}) \det(\lambda M^{i0} + \mu H^{i0}) = \sum_{i=0}^{n} \mu H_{i0} \det(\lambda M^{i0} + \mu H^{i0}) = \mu \sum_{i=0}^{n} H_{i0} \det(\lambda M^{i0} + \mu H^{i0});$$

hence, $\mu \mid \det(\lambda M + \mu H)$.

Assume now that the lemma is true for $n-r = k$; it is claimed that it holds for $n-r = k+1$. Observe that, if M is of the form in the hypothesis with $k = n - r > 1$, then M^{i0} is a matrix satisfying the same hypothesis with difference between order and rank $k' = n - r - 1$. By inductive reasoning, it follows that

$$\mu^{n-r} | \det(\lambda M^{i0} + \mu H^{i0});$$

hence, by the same argument as in the first part of the proof,

$$\mu^{n-r+1} | \det(\lambda M + \mu H)$$

and we get the result. □

Corollary 4.1.17. *The following inclusion is true:*

$$\mathscr{O}_{r,n,q} \subseteq \mathscr{O}_{n,q}^{n-r+1}$$

Proof. The points of $\mathscr{O}_{r,n,q}$ have at least multiplicity $n-r+1$, whence

$$\mathscr{O}_{r,n,q} \subseteq \mathscr{O}_{n,q}^{\geq n-r+1}.$$

From Theorem 4.1.12,

$$\mathscr{O}_{r,n,q} \subseteq \mathscr{O}_{n,q}^{\leq n-r+1}$$

and, by definition of $\mathscr{O}$,

$$\mathscr{O}_{n,q}^{\leq n-r+1} \cap \mathscr{O}_{n,q}^{\geq n-r+1} = \mathscr{O}_{n,q}^{n-r+1}.$$

□

The main result of this subsection is the following theorem.

Theorem 4.1.18. *Let M be a Hermitian matrix of rank $r \leq n$. Then, the multiplicity of the point $\xi(M)$ of $\mathscr{H}_{n,q}$ corresponding to M is exactly $n-r+1$; furthermore,*

$$\mathscr{O}_{r,n,q} = \mathscr{O}_{n,q}^{n-r+1}.$$

Proof. From Corollary 4.1.17, we have that matrices of rank r correspond to points on $\mathscr{H}$ of multiplicity $n-r+1$.

As a matter of fact, we know that

$$\sum_{r=1}^{n} |\mathscr{O}_{r,n,q}| = \sum_{m=1}^{n} |\mathscr{O}_{n,q}^{m}| = |\mathscr{H}_{n,q}|.$$

Thanks to Corollary 4.1.17,

$$|\mathscr{O}_{n,q}^{n-r+1}| \geq |\mathscr{O}_{r,n,q}|;$$

hence, all cardinalities have to be the same and, since the sets are all finite, this yields the equality. □

4.1.4 Action of $\mathrm{PGL}(n+1,q)$ on $\mathscr{H}$

The action of any linear collineation $\sigma \in \mathrm{PGL}(n+1,q)$ can be lifted to the space $\mathrm{PG}(n^2+2n,\sqrt{q})$. For any $P \in \mathrm{PG}(n^2+2n,\sqrt{q})$, we define

$$\tau_\sigma(P) := \xi(\sigma(\xi^{-1}(P))).$$

This induces an action of $\mathrm{PGL}(n+1,q)$ on $\mathrm{PG}(n^2+2n,\sqrt{q})$. In fact, the following corollary is true.

Corollary 4.1.19. *For any i such that $0 < i < n$, the τ-action of the group $\mathrm{PGL}(n+1,q)$ on $\mathrm{PG}(n^2+2n,\sqrt{q})$ is transitive on $\mathscr{O}_{n,q}^{i}$.*

Proof. All Hermitian hypersurfaces of given rank $n-i+1$ lie in the same orbit under the action of $\mathrm{PGL}(n+1,q)$. It follows that $\mathrm{PGL}(n+1,q)$ is transitive on

$$\xi^{-1}(\mathscr{O}_{n-i+1,n,q}) = \xi^{-1}(\mathscr{O}^{i}_{n,q}),$$

whence the result. □

Lemma 4.1.20. *Let $\Gamma := \{\lambda H + \mu T\}$ be a linear pencil of $(n+1)\times(n+1)$ Hermitian varieties, and let $r_i(\Gamma)$ be the number of Hermitian varieties of rank i in Γ. Then, if $r_{n+1}(\Gamma) \neq 0$,*

$$\sum (n-i+1) r_i(\Gamma) \leq n+1.$$

Proof. If $r_{n+1}(\Gamma) \neq 0$, then the line HT is not completely included in $\mathscr{H}_{n,q}$. By Bezout's theorem, this implies that HT intersects $\mathscr{H}_{n,q}$ in at most $n+1$ points, counted with the proper multiplicities. The result follows from Theorem 4.1.18. □

Lemma 4.1.21. *For $r \leq n$, the variety $\mathscr{H}_{r,q}$ can be embedded in $\mathscr{O}_{\leq r,n}$. Furthermore, this embedding η can be realized in such a way as to have*

$$\mathscr{H}_{r,q} = \eta^{-1}(\mathscr{O}_{\leq r,n,q} \cap \mathrm{PG}(r^2+2r,\sqrt{q})).$$

Proof. Let M' be an $r \times r$ Hermitian matrix, and define M to be the $(n+1)\times(n+1)$ matrix

$$\eta(M') := M = \left[\begin{array}{c|c} M' & \\ \hline & 0_{n+1-r} \end{array}\right].$$

Then, $M \in \mathscr{O}_{\leq r,n,q} \cap \mathrm{PG}(r^2+2r,\sqrt{q})$. Observe that, from Corollary 4.1.19, any two embeddings of $\mathscr{H}_{r,q}$ in $\mathscr{O}_{\leq r,n,q}$ are equivalent. □

Corollary 4.1.22. *For any $r < n$, the canonical subspace $\mathrm{PG}(r^2+2r,\sqrt{q})$ of $\mathrm{PG}(n^2+2n,\sqrt{q})$ intersects $\mathscr{H}_{n,q}$ in a subset of its set of singular points $\mathscr{O}^{\geq n-r+1}_{n,q}$. Furthermore, such intersection has the structure of an algebraic variety of degree $r+1$ in $\mathrm{PG}(r^2+2r,\sqrt{q})$.*

Proof. The embedding η of $\mathscr{H}_{r,q}$ into $\mathscr{O}^{\geq n-r+1}_{n,q}$ is a bijection when restricted to $\mathscr{H}_{n,q} \cap \mathrm{PG}(n^2+2n,\sqrt{q})$. This proves the result. □

Theorem 4.1.23. *With the same conditions as in Corollary 4.1.20, assume that there exist an integer v such that $r_{v+1} \neq 0$, whereas for any $t > v$, $r_{t+1} = 0$. Then,*

$$\sum (v-i+1) r_i(\Gamma) \leq v+1.$$

Proof. If $v = n$, then this is Corollary 4.1.20.

Otherwise, the line HT is completely included in $\mathscr{O}^{n,q}_{\leq v+1}$. Modulus a linear transformation it is possible to assume that both H and T are of the form

$$H := \left[\begin{array}{c|c} I_v & 0 \\ \hline 0 & 0_{n+1-v} \end{array}\right] \qquad T := \left[\begin{array}{c|c} T' & 0 \\ \hline 0 & 0_{n+1-v} \end{array}\right].$$

Hence, both of them can be considered as points of $\mathscr{H}_{v,q}$, with H a non-singular point there. It is now possible to apply Lemma 4.1.20 on this variety and the the result follows. □

4.1.5 The order formula

The following lemma is from [Kes81].

Lemma 4.1.24 ([Kes81], Lemma 1)**.** *Let H_1 and H_2 be two $(n+1) \times (n+1)$ Hermitian matrices, and let $\mathcal{H}_1$, $\mathcal{H}_2$ be the corresponding Hermitian varieties. Then,*

(i) *any two varieties in the $\mathrm{GF}(\sqrt{q})$-linear system Γ generated by $\mathcal{H}_1$ and $\mathcal{H}_2$ meet in the same configuration;*

(ii) *for any p in $\mathrm{PG}(n, q)$, there exists $\mathcal{H} \in \Gamma$ such that $p \in \mathcal{H}$.*

Proof. Assume $A = r_1H_1 + r_2H_2$, $B = s_1H_1 + s_2H_2$. Then, since $(r_1, r_2) \neq \lambda(s_1, s_2)$, the linear system

$$\begin{cases} \overline{x}Ax^t = 0 \\ \overline{x}Bx^t = 0 \end{cases}$$

is equivalent to

$$\begin{cases} \overline{x}H_1x^t = 0 \\ \overline{x}H_2x^t = 0, \end{cases}$$

whence $\mathcal{H}(A) \cap \mathcal{H}(B) = \mathcal{H}_1 \cap \mathcal{H}_2$ and the first part of the lemma is done.

Assume $m_1 = \overline{p}H_1p^\star$ and $m_2 = \overline{p}H_2p^\star$. Since both H_1 and H_2 are Hermitian, $m_1, m_2 \in \mathrm{GF}(\sqrt{q})$. It follows that $\mathcal{H}(H_3) = \mathcal{H}(m_2H_1 - m_1H_2) \in \Gamma$ and

$$\overline{p}H_3p^\star = m_2\overline{p}H_1p^\star - m_1\overline{p}H_2p^\star = m_2m_1 - m_1m_2 = 0,$$

which is the expected result. □

Definition 4.1.25. Let Γ be a $\mathrm{GF}(\sqrt{q})$-linear system of Hermitian hypersurfaces in $\mathrm{PG}(n, q)$. The *rank sequence* of Γ is the list $(r_1(\Gamma), \dots, r_{n+1}(\Gamma))$ where r_i is the number of varieties of rank i in Γ.

Using Theorem 4.1.23, it is possible to describe all the allowed rank sequences for Hermitian hypersurfaces in $\mathrm{PG}(n, q)$. Thanks to the following generalization of Lemma 2, [Kes81], we are able to settle the problem of determining the list of all possible orders of intersection.

Theorem 4.1.26. *The size of the intersection of any two non-degenerate Hermitian varieties $\mathcal{H}_1$, $\mathcal{H}_2$ depends only on the rank sequence of the linear system Γ generated by them. This size is the number $\eta(\Gamma, q)$, given by*

$$\eta(\Gamma, q) := \frac{1}{\sqrt{q}(q-1)}\{(1 - q^{n+1}) + \sum_{i=1}^{n} r_i(\Gamma)[(q\mu(i-1, q) + 1)(q^{n+1-i} - 1)]\} + \frac{r_{n+1}(\Gamma)}{\sqrt{q}}\mu(n, q).$$

Proof. By Lemma 4.1.24 any two distinct elements of Γ intersect in the same configuration, say $\mathcal{E}$. Let k be the cardinality of this set.

Any point of $\mathrm{PG}(n,q)\setminus\mathcal{E}$ belongs to exactly one hypersurface in $\mathcal{H}(\Gamma)$, while the points in $\mathcal{E}$ belong to all $\sqrt{q}+1$ of them. Hence,

$$|\mathrm{PG}(n,q)| = \left(\sum_{\mathscr{X}\in\Gamma} |\mathscr{X}|\right) - \sqrt{q}|\mathcal{E}|.$$

From Theorems 1.7.28 and 1.7.30 it follows that

$$\frac{1}{q-1}\sum_{i=1}^{n} r_i(H,q)[(q\mu(i-1,q)+1)(q^{n+1-i}-1)] \\ +r_{n+1}(H,q)\mu(n,q)-\sqrt{q}k = \frac{q^{n+1}-1}{q-1},$$

whence the result. □

As an example of Theorem 4.1.26 we determine the cardinality of all possible intersections of non-degenerate Hermitian varieties up to dimension $n=4$. For $n=2$, the results might be found in Chapter 2; for $n=3$, they are in Chapter 3. For $n=4$, first, we count the number of points of a non-degenerate Hermitian hypersurface: this is

$$\mu(4,q) = (q+1)(q^2\sqrt{q}+1).$$

Then, we tabulate the results by applying the formula of 4.1.26 with all possible values of the rank sequence. The results are in Table 4.1. Observe that when $r_1 = 1$, there are only two possible intersection configurations – namely the one obtained when the rank 1 hypersurface $\mathcal{C}$ in Γ is secant to any other variety in the pencil and the one obtained when $\mathcal{C}$ is tangent to any other hypersurface. This is a general property. In fact, we prove the following corollary.

Corollary 4.1.27. *Let Γ be a non-degenerate linear system of Hermitian hypersurfaces in the projective space $\mathrm{PG}(n,q)$. Assume that $r_1(\Gamma)=1$ and let $\mathcal{C}$ be such a rank 1 hypersurface. Then, one of the following holds*

(i) *Γ contains only one the singular hypersurface $\mathcal{C}$ and $\mathcal{C}$ is tangent to all the non-degenerate hypersurfaces of Γ;*

(ii) *Γ contains also a hypersurface $\mathcal{K}$ of rank n and the base locus of Γ is a non-degenerate Hermitian hypersurface $\mathcal{U}_{n-1}$ in the hyperplane $\mathcal{C}$.*

Proof. From Theorem 4.1.23, we have that the rank sequence for the linear system Γ is either $(1,0,\dots,0,0)$ or $(1,0,\dots,0,1)$. Assume the latter; then, a straightforward computation shows that $|\mathcal{E}| = \mu(n-1,q)$. The hyperplane $\mathcal{C}$ is either tangent to any non-degenerate hypersurface $\mathcal{H}$

r_1	r_2	r_3	r_4	$k = \|\mathcal{E}\|$
0	0	0	0	$q^3 + q^2 - q\sqrt{q} + q + 1$
0	0	0	1	$q^3 + q^2 + q + 1$
0	0	0	2	$q^3 + q^2 + q\sqrt{q} + q + 1$
0	0	0	3	$q^3 + q^2 + 2q\sqrt{q} + q + 1$
0	0	0	4	$q^3 + q^2 + 3q\sqrt{q} + q + 1$
0	0	0	5	$q^3 + q^2 + 4q\sqrt{q} + q + 1$
0	0	1	0	$q^3 + q^2 + q + \sqrt{q} + 1$
0	0	1	1	$q^3 + q^2 + q\sqrt{q} + q + \sqrt{q} + 1$
0	0	1	2	$q^3 + q^2 + 2q\sqrt{q} + q + \sqrt{q} + 1$
0	0	1	3	$q^3 + q^2 + 3q\sqrt{q} + q + \sqrt{q} + 1$
0	0	2	0	$q^3 + q^2 + q\sqrt{q} + q + 2\sqrt{q} + 1$
0	0	2	1	$q^3 + q^2 + 2q\sqrt{q} + q + 2\sqrt{q} + 1$
0	1	0	0	$q^3 + q^2\sqrt{q} + q^2 + q\sqrt{q} + q + \sqrt{q} + 1$
0	1	0	1	$q^3 + q^2\sqrt{q} + q^2 + 2q\sqrt{q} + q + \sqrt{q} + 1$
0	1	0	2	$q^3 + q^2\sqrt{q} + q^2 + 3q\sqrt{q} + q + \sqrt{q} + 1$
0	1	1	0	$q^3 + q^2\sqrt{q} + q^2 + 2q\sqrt{q} + 2q + 2\sqrt{q} + 1$
1	0	0	0	$q^2\sqrt{q} + q + 1$
1	0	0	1	$q^2\sqrt{q} + q\sqrt{q} + q + 1$

Table 4.1: Intersection numbers for non-degenerate Hermitian varieties in dimension 4.

in Γ or it cuts all of them transversally. If $\mathcal{C}$ is transversal to all non-degenerate hypersurfaces, then its intersection with $\mathcal{H}$ is again a non-degenerate Hermitian surface in $\mathrm{PG}(n-1, q)$. Such a surface has size $\mu(n-1, q)$ and the rank sequence for Γ has to be $(1, 0, \dots, 0, 1)$. When the rank sequence is $(1, 0, \dots, 0)$, the other possibility for $\mathcal{C}$ happens – that is $\mathcal{C}$ is tangent to all other varieties in Γ. $\square$

4.1.6 Some further remarks on $\mathscr{H}$

For $n \leq 5$, the dimension of the subvarieties $\mathscr{O}^{\leq t}_{n,q}$ have been computed. The results are presented in table 4.2. If $n = 2$, the result is in [CS]; for $n > 2$ a direct computation with the program `Macaulay2` [GS00] has been performed. For $n > 5$, computations have been aborted after having been running for three days on a quad-Xeon 550 server.

The code that has been used is the following. It is worth to remark that defining the base field to be 9, in this case, does not hamper generality, since all the manipulations performed are formal reductions of the polynomials which are independent from the characteristic $c > 0$ of the field.

Size.m2

```
KK=GF(9)
i=KK_0
ib=i^3
```

n	$\mathscr{H}_{n,q}$	$\mathscr{O}^{\geq 2}$	$\mathscr{O}^{\geq 3}$	$\mathscr{O}^{\geq 4}$	$\mathscr{O}^{\geq 5}$
2	7	4			
3	14	11	7		
4	23	20	15	8	
5	34	31(?)	?	19	10

Table 4.2: Dimension of the varieties $\mathscr{O}^{\geq t}$ for small n

```
  R4=KK[ X00,
         X01, X01t, X11,
         X02, X02t, X12,
              X12t, X22,
         X03, X03t, X13,
              X13t, X23,
              X23t, X33,
         X04, X04t, X14,
              X14t, X24,
              X24t, X34,
              X34t, X44]
  M4=matrix(
       {
        {X00,  X01+i*X01t,  X02+i*X02t,
                  X03+i*X03t,  X04+i*X04t},
        {X01+ib*X01t, X11,  X12+i*X12t,
                  X13+i*X13t,  X14+i*X14t},
        {X02+ib*X02t, X12+ib*X12t,
                  X22,  X23+i*X23t,  X24+i*X24t},
        {X03+ib*X03t, X13+ib*X13t,
                  X23+ib*X23t, X33,  X34+i*X34t},
        {X04+ib*X04t, X14+ib*X14t,
                  X24+ib*X24t,i X34+ib*X34t,X44}
       }
HVar4= ideal (det M4)
S4Points2 = minors(M4,4)
S4Points3 = minors(M4,3)
S4Points4 = minors(M4,2)

dim S4Points2
dim S4Points3
dim S4Points4
```

We conjecture that $\dim \mathscr{H}_{n,q} - \dim \mathscr{O}^{\leq 2}_{n,q} = 3$ for all n and q.

The variety $\mathscr{O}^1_{n,q}$ has been extensively studied. In fact, it constitutes a *cap* in $\mathrm{PG}(n^2 +$

$2n, \sqrt{q})$, as is proven in the following lemmas.

Lemma 4.1.28 (Wan). *Let H be a Hermitian matrix of rank 2. Then, there exist two Hermitian matrices M_1, M_2 of rank 1 such that*

$$H = M_1 + M_2.$$

Lemma 4.1.29 (Lunardon,[Lun99]; Cossidente, Siciliano [CS]). *Take Σ as the set of all Hermitian matrices of $\mathrm{Mat}(n+1, q)$ of rank 1. Its image in $\mathrm{PG}(n^2 + 2n, \sqrt{q})$ is a cap $\mathscr{V}_{(n+1),2}$, the Hermitian Veronesian.*

In the setting of [CS], we may enunciate the following corollary.

Corollary 4.1.30. *The envelope of secants to the Hermitian Veronesian $\mathscr{V}_{(n+1),2}$ is the algebraic variety whose points correspond to all Hermitian matrices of rank at most 2.*

4.2 Explicit computations and algorithms

In this section we present some simple GAP ([GAP99]) code for the computation of the orbits of the projective unitary group $\mathrm{PU}(n + 1, q)$ in its action on $\mathrm{PG}(n, q)$.

4.2.1 The computer code: general remarks

We used the package [GS99] to model small projective spaces. In fact, quite a little part of the functionality which is provided by that code has been used.

In this section q is, as usual, assumed to be a square, and p is defined as $\sqrt{q}$. Note that p is not necessarily a prime.

The program itself has been split into several files. This has been done for two different reasons:

(1) ease the development of the code;

(2) provide a simple way to insert checkpoints in the program – in fact the output of the previous stages of a computation can be dumped to disk and reloaded later in order to resume execution with some slightly changed parameters.

Point (2) has been our main concern: GAP4 does provide a facility to save and restore its workspace; however, the command `SaveWorkspace` cannot be used inside a function or a loop.

Our code is composed of the following units: `Main`, `Param`, `Projective`, `Helpers`, `Prelim`, `Unitary`, `Orbits` and `Post-comp`.

4.2.2 Initialization: `main` and `param`

The file `main.gap` contains the core of the program and it is the one that calls all modules in the proper order.

main.gap

```
#####
# Computation of orbits of Hermitian varieties
#  under the action of the
#   Projective unitary group
#####

#--> Main file

 RequirePackage("pg");
  Read("Param.gap");
   F:=GF(q);

  Read("Projective.gap");

  Read("Helpers.gap");

  Read("Prelim1.gap");
  Read("Prelim2.gap");

  Read("Unitary.gap");

  Read("Orbits.gap");

  Read("Post-orb1.gap);
  Read("Post-orb2.gap);
  Read("Post-orb3.gap);
  Read("Post-orb4.gap);
  Read("Post-orb5.gap);
  Read("Post-orb6.gap);

 Print("\n Done\n");
```

The parameters that determine the computation, that is the dimension n of the space and the square q are defined in `Param.gap`.

4.2.3 Auxiliary functions: `Projective` and `Helpers`

Both the files `Projective.gap` and `Helpers.gap` contain functions to support the computation. The functions in the file `Projective.gap` are meant to be re-usable for general work on projective spaces; on the other hand, the code in `Helpers.gap` has been written just for this program and it makes heavy use of global variables.

While it is agreed that usually global variables are to be avoided, their choice for this very application has been dictated by our wish to simplify the syntax of some functions and increase the readability of the code. Another consideration that had to be made is that GAP transfers parameters to functions 'by value': all variables are copied whenever a function call happens. This could be (and is) quite a problem in 'memory starvation' situations, when huge amounts of data need to be transferred as arguments, as it may happen in our case.

The `Projective.gap` file is as follows.

`Projective.gap`

```


##############
# General Use Macros
##############



#General Procedures
SetMinus := function(A,B)
 local x,T,U;
 U:=A;
 T:=IntersectionSet(A,B)    ;
  #This should speed things up
 for x in T do
  RemoveSet(U,x);
 od;
 return(U);
end;;

SetMinus1 := function(A,B)
 local x,T,U;
 U:=A;
 for x in B do
  RemoveSet(U,x);
 od;
 return(U);
end;;

Prod := function (l1,l2,l3)
```

```
 local i,t,u;
 t:=0;
 u:=Length(l1);
 for i in [1..u] do
  t:=t+l1[i]*l2[i]*l3[i];
 od;
 return t;
end;;

#scalar product
Scal := function (l1,l2)
 return Prod(l1,l2,[1,1,1,1]);
end;;

#Hermitian
Herm1 := function(l1,l2,v,f)
 return(Prod(List(l1,t->t),List(l2,t->t^f),v));
end;;

HermM := function(l1,M,f)
 local l1q,idl;
 idl := List(l1,t->t^0);
 l1q := List(l1,t->t^f);
 return(Prod(l1q*M,l1,idl));
end;;

Herm := function(l1,l2,f)
 return(Herm1(l1,l2,[1,1,1,1],f));
end;;
#Forms associated to Hermitian product
HermS := function(l1,f)
 return(Herm(l1,l1,f));
end;;

HermS1 := function(l1,v,f)
 return(Herm1(l1,l1,v,f));
end;;



#####################################
# Pr Space Functions Implementation
#####################################

# Some functions have three variants:
```

```
# function(V):      Construct from vector space
# function1(n,K):  Construct the object
#                          of dim n over K
# function2(W,K):  Construct from
#                          the set W over K
##
# These functions are all quite verbose

#############################
# We want to construct a projective space P
#            as a records of the following:
# P.points
# P.lines
# P.field
# P.size
# P.order
############################

##########################################
# Function for constructing a vector space
# of dimension n over K
##########################################

#Canonical base vector
CanonicBase:= function(i,n,K)
 local k,L,gen,u,z;
 gen:=Z(Size(K));
 u:=gen^0;
 z:=gen*0;
  L:=[];
  for k in [1..n] do
   if k=i then
    Add(L,u);
   else
    Add(L,z);
   fi;
  od;
 return(L);
end;;

#Return the n dimensional vector space over K
Vsp:= function(n,K)
 local i,k,gen,u,z,L,U;
 U:=[];
 if n=0 then
```

```
  return([]);
 fi;
 for i in [1..n] do
  L:=CanonicBase(i,n,K);
  Add(U,L);
 od;
 return(VectorSpace(U,K));
end;;


#Actual construction of the projective space
#
# As point representative we assume the
#  vector in the equivalency class whose
#  first non-zero entry is 1
Norma := function(v)
 local w,u,i,j;
 u:=Length(v);
 for i in [1..u] do
  if not(v[i]-v[i]=v[i]) then
   return(List(v,x->x/v[i]));
  fi;
 od;
 return(v);
end;;

# List of the points of the projective space.
# There are different functions for this
#  task.
#
# The first one we provide is extremely
#  slow.

Alt1PrPoints := function(V)
 local W,L,U,P,G,x,y,q;
  G:=V.field;
  q:=Characteristic(G);
  W:=Set(Elements(V));
  P:=[];
  RemoveSet(W, V.zero );
  while Size(W)>0 do
   x:=Elements(W)[1];
   Add(P,Norma(x));
   Print(Norma(x),"   ",Size(W),"\n");
   U:=VectorSpace([ x ], G);
```

```
   L:=Set(Elements(U));
   # Removing the zero from L provides quite
   #  a remarkable performance improvement
   #  at the beginning of the computation.
   RemoveSet(L,U.zero);

   W:=SetMinus1(W,L);
    #Observe that we already know that
    # $W\cap L=L$.
  od;
 Print("\n P:=",Set(P),"\n");
 return(Set(P));
end;;

# This implementation is faster than the
# one above: the set command is used in
# order to reorder the list P

PrPoints := function(V)
 local W,L,U,P,G,H,x,y,q,d,l,m;
  G:=V.field;
  d:=Dimension(V);
  l:=Size(G);
  m:=(l^d-1)/(l-1);
  q:=Characteristic(G);
  W:=Set(Elements(V));
  H:=[];
  RemoveSet(W, V.zero );
  for x in W do
   Add(H,Norma(x));
   H:=Set(H);
   Print(Norma(x),"   ",Size(H),"\n");
   if Size(H)=m then
    P:=Set(H);
    Print("\n P:=",P,"\n");
    return(P);
   fi;
  od;
 P:=Set(H);
 Print("\n P:=",P,"\n");
 return(P);
end;;

%%%%%%%%%%
###########################
```

```
# When the full projective space is needed this
# is actually the best option: we do not normalize
# but just add vectors already in canonical form
# (still it takes some time to run)
############################

FullPrPoints:= function(n,K)
 local T,P,U,L,x,gen,u,z,i,y,a;
 gen:=Z(Size(K));
 u:=gen^0;
 z:=gen*0;
 P:=[];
 for x in [1..n+1] do
  if x=1 then
   L:=[u];
   Print("L:=",L,"\n");
  else
   L:=CanonicBase(x,x,K);
                              #   for a in [1..x-1] do
                              #    Add(L,z);
   # This is the old routine #   od;
                              #   Add(L,u);
                              #  fi;
  Print("L:=",L,"\n");
 fi;
  if x=n+1 then
   L:=CanonicBase(x,x,K);
   Add(P,L);
  else
  U:=Elements(Vsp(n+1-x,K));
  for y in U do
   T:=[];
   for i in L do
    Add(T,i);
   od;
   for i in y do
    Add(T,i);
   od;
   Add(P,T);
   P:=Set(P);
   Print("T=",T,"  ",Size(P),"\n");
 od;
fi;
od;
 return(Set(P));
```

```
end;;


############################################
# Now we define the lines....
# Note that we can not use the ``FullPrPoints''
# function here.
############################################

#First case: arguments=(n,K).
#Note that it is cheaper to compute
#   an intersection rather than to normalize
PrLines1 := function(n,K)
 local W,L,U,x,y;
 W:=FullPrPoints(n,K);
 L:=[];
 for x in Elements(W) do
  RemoveSet(W,x);
  for y in Elements(W) do
   U:=IntersectionSet(W,
              Set(Elements(VectorSpace([x,y],K))));
   Add(L,U);
   Print("\n Line U:=",U,"; size of L:=",
                                Size(Set(L)),"\n");
  od;
 od;
 Print("\n Set of lines L:=",Set(L),"\n");
 return(Set(L));
end;;

#Second case: the set of points is already given
PrLines2 := function(W,K)
 local L,U,x,y;
 L:=[];
 for x in Elements(W) do
  RemoveSet(W,x);
  for y in Elements(W) do
   U:=IntersectionSet(W,
           Set(Elements(VectorSpace([x,y],K))));
   Add(L,U);
   Print("\n Line U:=",U,"; size of L:=",
                             Size(Set(L)),"\n");
  od;
 od;
 Print("\n L:=",Set(L),"\n");
```

```
 return(Set(L));
end;;

#Third case: we give the vector space
PrLines := function(V)
 local W,L,K,U,x,y;
 W:=PrPoints(V);
 K:=V.field;
 L:=[];
 for x in Elements(W) do
  RemoveSet(W,x);
  for y in Elements(W) do
   U:=IntersectionSet(W,Set(VectorSpace([x,y],K)));
   Print("\n Line U:=",U,"; size of L:=",
                              Size(Set(L)),"\n");
  Add(L,U);
  od;
 od;
 Print("\n L:=",Set(L),"\n");
 return(Set(L));
end;;

# Points and lines enable us to define
#  all the subspaces of the linear structure
#  This is a recursive function and I expect
#  it to be very slow; however it is hardly
#  ever used in this form.

PrSubSpaces := function(V,n)
 local Sub,P,U,N2,K2,x,y;
 Sub:=[];
 if n=0 then
  return(PrPoints(V));
 fi;
 if n=1 then
   return(PrLines(V));
 fi;
 #We need to use PrPoints here
 P:=PrPoints(V);
 #Note that since n>1, N2 is already a list
 #                     of points
 N2:=PrSubSpaces(V,n-1);
 for x in N2 do
  U:=SetMinus(P,Set(x));
  for y in U do
```

```
   Add(x,y);
   K2:=IntersectionSet(P,
           Set(Elements(VectorSpace(x,V.field))));
   Add(Sub,K2);  #We avoid PrPoints again
   Print("Adding K2:=",K2,"\n Size of Sub:=",
                              Size(Set(Sub)),"\n");
  od;
 od;
 return(Set(Sub));
end;;

PrSubSpaces1 := function(m,K,n)
 local Sub,P,U,N2,K2,x,y;
 Sub:=[];
 if n=0 then
  return(FullPrPoints(m,K));
 fi;
 if n=1 then
   return(PrLines1(m,K));
 fi;
 P:=FullPrPoints(m,K);
 #Note that since n>1,
 #  N2 is already a list of Points....
 N2:=PrSubSpaces1(m,K,n-1);
 for x in N2 do
  U:=SetMinus(P,Set(x));
  for y in U do
   Add(x,y);
   K2:=IntersectionSet(P,
               Set(Elements(VectorSpace(x,K))));
   Add(Sub,K2);
   Print("Adding K2:=",K2,"\n Size of Sub:=",
                            Size(Set(Sub)),"\n");
  od;
 od;
 return(Set(Sub));
end;;

PrSubSpaces2 := function(W,K,n)
 local Sub,P,U,N2,K2,x,y;
 Sub:=[];
 if n=0 then
  return(W);
 fi;
 if n=1 then
```

```
   return(PrLines2(W,K));
 fi;
 P:=W;
 #Note that since n>1,
 #  N2 is already a list of Points....
 N2:=PrSubSpaces2(W,K,n-1);
 for x in N2 do
  U:=SetMinus(P,Set(x));
  for y in U do
   Add(x,y);
   K2:=Set(IntersectionSet(W,
                   Set(Elements(VectorSpace(x,K)))));
   Add(Sub,K2);
   Print("Adding K2:=",K2,"\n Size of Sub:=",
                                Size(Set(Sub)),"\n");
  od;
 od;
 return(Set(Sub));
end;;

PrSubSpaces3 := function(W,L,K,n)
 local Sub,P,U,N2,K2,x,y;
 Sub:=[];
 if n=0 then
  return(W);
 fi;
 if n=1 then
   return(L);
 fi;
 P:=W;
 N2:=PrSubSpaces2(W,K,n-1);
 for x in N2 do
  U:=SetMinus(P,Set(x));
  for y in U do
   Add(x,y);
   K2:=IntersectionSet(W,
               Set(Elements(VectorSpace(x,K))));
   Add(Sub,K2);
   Print("Adding K2:=",K2,"\n Size of Sub:=",
                           Size(Set(Sub)),"\n");
  od;
 od;
 return(Set(Sub));
end;;
```

```
#space+function
Variety1 := function(V,f)
 local U,x;
 U:=[];
 for x in V do
  if f(x)-f(x)=f(x) then
   Add(U,x);
  fi;
 od;
 return(Set(U));
end;;

#space+list of functions
Variety := function(V,F)
 local U,x,y,t,l,f;
 l:=Size(F);
 for x in V do
  y:=0;
  for t in F do
   if t(x)-t(x)=t(x) then
    y:=y+1;
   fi;
  od;
  if y=l then
   #All conditions satisfied!
   Add(U,x);
  fi;
 od;
 return(Set(U));
end;;

###############
```

This is the listing of `Helpers.gap`.

Helpers.gap

```
###########
# Helper Functions
###########
HermV := function(X, f)
 return(HermS(PtToVect(X),f));
end;;

TestHpoint := function(x,f)
```

```
 return(HermV(x,2)-HermV(x,2)=HermV(x,2));
end;;

HermVM :=function(x,M,f)
 return(HermM(PtToVect(x),M,f));
end;;

TestHMpoint := function(x,M,f)
 return(HermVM(x,M,f)-HermVM(x,M,f)=HermVM(x,M,f));
end;;

CreateHermVar := function(M,Pt,f,ind)
 local x, listH;
 listH:=[];
 for x in Pt do
 if ind=1 then
  Print(HermVM(x,M,f),"\t");
 fi;
  if (TestHMpoint(x,M,f)) then
   Add(listH,x);
  if ind=1 then
   Print(" ...OK\t"); #,x,"\n");
  fi;
  else
  if ind=1 then
   Print(" ...no\t"); #,x,"\n");
  fi;
  fi;
 od;
 return(listH);
end;;

#############
```

4.2.4 Preliminary computations: Prelim.gap

The module prelim.gap constructs some tables and functions to implement different representations for Hermitian varieties:

(i) the representation as a point of $\mathrm{PG}(n^2+2n, \sqrt{q})$,

(ii) the representation as an element of $\mathrm{Mat}(n+1, q)$ and

(iii) the presentation of the set of all $\mathrm{GF}(q)$-rational points of the variety.

The first step consists in constructing the projective space $\mathrm{PG}(n, q)$ via a library function and defining the sets associated with the canonical non-degenerate Hermitian variety `UnI`.

As seen in Theorem 1.7.17, the set of all Hermitian hypersurfaces in $\mathrm{PG}(n, q)$ is a $\mathrm{PG}(n^2 + 2n, p)$.

In order to establish a 1—1 correspondence between the set of all Hermitian varieties in $\mathrm{PG}(n, q)$ and $\mathrm{PG}(n^2 + 2n, p)$, the following algorithm is used.

Definition 4.2.1. For any point $x \in \mathrm{PG}(n, q)$. A *normalised representative* for x is a vector t in the underlying vector space V such that

(i) $\mathbb{P}t = x$;

(ii) the first non-zero component of t is 1.

We denote the normalised representative of x as $\tilde{x}$.

For any $i = 1, \dots n$, define

(i) $\alpha := [(n + 1)(n + 2)]/2$;

(ii) $\beta(i) := [(n + 1)(n + 2) - (n - i)(n - i + 1)]/2 + 1$;

(iii) $\gamma(i) := \beta + [n(n + 1) - (n - i - 1)(d - i)]$;

and assume ϵ to be a primitive element of $\mathrm{GF}(q)$ and η a primitive element of $\mathrm{GF}(p) = \mathrm{GF}(\sqrt{q})$. Consider the following mapping between $\mathrm{PG}(n^2 + 2n, p)$ and $\mathrm{Her}(n + 1, q)$:

$$\vartheta : \begin{cases} \mathrm{PG}(n^2 + 2n, p) & \rightarrow & \mathrm{Her}(n + 1, q) \\ x & \rightarrow & \rho(\tilde{x}) = M, \end{cases}$$

where the $(n + 1) \times (n + 1)$ matrix M has the following entries

(i) for $i = j$, $M_{ii} := \eta \tilde{x}_{\beta(i)}$;

(ii) for $i < j$,
$$M_{ij} := \eta \tilde{x}_{\beta(i)+j-i} + \epsilon \tilde{x}_{\alpha+\gamma(i)+j-i}$$

(iii) for $j < i$, $M_{ji} = \overline{M_{ij}}$.

It is straightforward to verify that such a mapping is a bijection and that it preserves the linear structure of $\mathrm{PG}(n^2 + 2n, p)$. The gap code to implement this correspondence is as follows.

Prelim1.gap

```
#######
# Preliminary computations
#######
```

```
Print("Start Computations\n");
S:=ProjectiveGeometry(n,q);
P:=ProjectivePoints(S);
UnI:=CreateHermVar(Z(p)*IdentityMat(n+1),P,p,1);
UnIp:=Set(List(UnI,t->PtToVect(t)));
Print("UnI is now defined\n");

########
# Construction of the set of all
# Hermitian matrices of given
# size over a field
########

# We consider all Hermitian matrices:
# they form a PG(n^2+2n,p)
#
# Encoding:
# First n*(n+1)/2 entries -> entries over
#                          the ground field;
# Remaining entries -> "complex" part.
#

Print("Take the space of all Hermitian
                   Matrices: dim=",n^2+2*n,"\n");
MatricesSpace:=ProjectiveGeometry(n^2+2*n,p);
Print("Now, the points are computed...\n");
MatricesPoints:=ProjectivePoints(MatricesSpace);
SizOfM:=Size(MatricesPoints);
MatricesSet:=[];
#
Print("Start the cycle...\n");
# Basic cycle on points
offset:=(n+1)*(n+2)/2;
for x in MatricesPoints do
 tempMatrix:=[];
 for l in [1..n+1] do
  Add(tempMatrix,[]);
 od;
 tempVect:=PtToVect(x);
#
# Actual construction of the matrix
#
 for i in [0..n] do
 #Real Entries start here!
  refpos:=(n+1)*(n+2)/2-(n-i+1)*(n-i+2)/2+1;
```

```
 #While complex ones start here!!
  refpos2:=offset+n*(n+1)/2-(n-i)*(n-i+1)/2;
 #
 # Computing the rows....
 #
  for j in [0..n] do
  # Diagonal entries are "real"...
  if i=j then
   tempMatrix[i+1][i+1]:=tempVect[refpos]*Z(p);
   Print("coord=",refpos,"--> (",i+1,",",j+1,")\t",
                            tempVect[refpos],"\n");
  fi;
  # Upper triang. part: get "real" and "complex"
  #    part for each entry
  if i<j then
    tempMatrix[j+1][i+1]:=tempVect[refpos+j-i]*Z(p)+
                          tempVect[refpos2+j-i]*Z(q);
    Print("coord=",refpos+j-i,";",refpos2+j-i,
              "--> (",i+1,",",j+1,")\t",
                         tempVect[refpos+j-i],"+",
                          tempVect[refpos2+j-i],"i\n");
  fi;
  # Obtain the lower trian. by conjugation
  if i>j then
    tempMatrix[j+1][i+1]:=(tempMatrix[i+1][j+1])^p;
  fi;
  od;
 od;
 Print(tempMatrix,"\t",Size(MatricesSet)+1,"/",
                                     SizOfM,"\n");
 Add(MatricesSet,tempMatrix);
od;
Print("List of Matrices computed\n");

##########
```

Once all Hermitian matrices in Her$(n+1, q)$ have been constructed, it is possible to produce two more lists: the list of all rational points of Hermitian varieties and the list of determinants corresponding to given varieties. Since these lists are ordered objects, functions for converting from one representation to the other are the most straightforward.

Prelim2.gap

```
#
# Create List of Hermitian Varieties
```

```
#

VarHermList := List(MatricesSet,
                    M->CreateHermVar(M,P,p,1));
DetList := List(MatricesSet,M->Determinant(M));

#
# Define functions for associating Matrices, Points
#                                   and Varieties.
# ``Helpers2.gap''
#

MatToPt := function(M)
 return(MatricesPoints[Position(MatricesSet,M)]);
end;;

PtToMat := function(V)
 return(MatricesSet[Position(MatricesPoints,V)]);
end;;

VarToMat := function(V)
 return(MatricesSet[Position(VarHermList,V)]);
end;;

MatToVar := function(V)
 return(VarHermList[Position(MatricesSet,V)]);
end;;

VarToPt := function(V)
 return(MatricesPoints[Position(VarHermList,V)]);
end;;

PtToVar := function(V)
 return(VarHermList[Position(MatricesPoints,V)]);
end;;

###########
```

4.2.5 Unitary group construction: `Unitary.gap`

The very simplest way for defining the Projective Unitary group is by considering the stabiliser of the point set `UnIp` in $\mathrm{PGL}(n+1,q)$. The group $\mathrm{PGL}(n+1,q)$ is seen as the quotient group of $\mathrm{GL}(n+1,q)$ modulus its centre. For each of the equivalence classes $\mathrm{PGL}(n+1,q)$ consists of, we choose the matrix of determinant 1 as a representative. This is what the following code aims to do. Observe that the action of $\mathrm{PGL}(n+1, q)$ on the Hermitian curve is given by the function `DoHermActPGL()`.

Unitary.gap

```
#
# Start the actual computations....
#  we want to implement PGL
#

Print("\n Take GL(",d+1,",",q,")... ");
GenL := GeneralLinearGroup(d+1,q);
Print("and get its Centre Z\n");
ZGenL:= Centre(GenL);
Print("Now define the Homomorphism
        with Z(GL(",d+1,",",q,")) as its kernel\n");
Phom := NaturalHomomorphismByNormalSubgroup(GenL,
                                             ZGenL);
Print("... and PGL is its epimorphic image\n");
PGenL:= Image(Phom);

#
# Helpers 3.
# Action of PGL on the representatives of Hermitian
#  forms
#

# canonical preimage
GetPreImg:=function(t)
 local pre1,pre2;
 pre1:=Elements(PreImages(Phom,t));
 pre2:=pre1[1]/Determinant(pre1[1]);
 return(pre2);
end;;

# action of PGL on the set of matrices by conj

DoConjFromPGL:=function(M,t)
 local pre;
 pre:=GetPreImg(t);
 return(pre^(-1)*M*pre);
end;;

# action of PGL on the set of Hermitian forms
#  as represented by Hermitian matrices
```

```
DoHermActPGL:=function(M,t)
 local pre;
 pre=GetPreImg(t);
 return(TransposedMat(pre^p)*M*pre);
end;;

# Do a copy of the set of Matrices
ListTemp := Set(ShallowCopy(MatricesSet));

#
# Some further helper functions...
#

UnitTest1:=function(t)
 return(TransposedMat(t^p)*t);
end;;

UnitTest:=function(t)
 local pre,com;
 com:=DoConjFromPGL(IdentityMat(d+1),t);
 return(Image(Phom,com));
end;;

UniHom:=GroupHomomorphismByFunction(PGenL,PGenL,
                                         UnitTest);
UniKer:=Kernel(UniHom);
PGU:=PGenL/UniKer;

#########
```

4.2.6 Orbit computation: `Orbits.gap`

The computation of the orbits under the action of the Projective Unitary Group is done via the standard library function `Orbits`.

Orb-compute.gap

```
#
# Orbits computation
#

Print("Computing Orbits.... (way too slow...)\n");
StaL:=Stabilizer(PGenL,MatricesSet,DoHermActPGL);
```

```
Orb1:=Orbits(PGenL,MatricesSet,DoHermActPGL);
Print("Orbit Computation done; renormalizing...");
Orb:=List(Orb1,
          t->IntersectionSet(Set(t),MatricesSet));
Print(" Done!\n");

#########
```

4.2.7 Intersection and results output: `Post-orb.gap`

The first element in any single orbit is chosen as representative and some cardinalities are printed out.

Post-orb1.gap

```
OrbL:=List(Orb,t->Size(t));
OrbR:=List(Orb,t->t[1]);
IdMat:=VarToMat(UnI);
for i in [1..Size(Orb)] do
 if IdMat in Orb[i] then
  OrbR[i]:=IdMat;
 fi;
od;
OrbP:=List(OrbR, t->MatToPt(t));
Print("\n --- Orbits Under the action
                   of the (P)GL group --- \n");
Print(Orb,"\n");
Print("Number of Orbits :=",Size(Orb),"\n");
Print("Size of Orbits :=",OrbL,"\n");
Print("Set of Representatives :=", OrbR, "\n");
#Now Consider linear combinations...
IdPointPos:=Position(OrbP,MatToPt(IdMat));
IdPoint:=OrbP[IdPointPos];
SameInter:=[];
Print("Classes\t\t Sizes\n");
```

Next, there is some code in order to perform a consistency check. The `MergeClass` and `TryClass` functions are used to merge all the orbits that lead to the same intersection configuration. Lemma 3.2.1 guarantees that that `MergeClass` should act as the identity on the orbits.

Post-orb2.gap

```
###                  ###
```

```
# Consistency check #
###                ###

TryClass := function( n )
 local a1, a2, a3, a4, x;
 a4:=[n];
 for x in Orb[n] do
  for lamb in GF(p) do
  a1 := lamb*IdMat+x;
  a2 := VarToMat(CreateHermVar(a1,P,p,0));
  a3 := PositionProperty(Orb,t-> a2 in t);
  Print("From class: ",n, " -> To class: ", a3, "\n");
  Add(a4,a3);
  od;
 od;
  return(Set(a4));
end;;


SameInter:=[];
for i in [1..Size(Orb)] do
 if not i=IdPointPos then
  Add(SameInter,TryClass(i));
 fi;
od;


###              ###
#  Merge Classes   #
###              ###

SameInterS:=Set(List(SameInter,t -> Set(t)));
TmpList:=[];
SameKindOfInter:=[];
for i in SameInterS do
 iPos:=Position(SameInterS,i);
 for j in SameInterS do
  jPos:=Position(SameInterS,j);
  Tmp:=IntersectionSet(i,j);
  if not Tmp=Set([]) then
    Tmp2:=Set(Union(i,j));
    SameInterS[iPos]:=Tmp2;
    SameInterS[jPos]:=Tmp2;
  fi;
 od;
```

```
od;
SameInterS:=Set(SameInterS);
Print("To Merge: ",SameInterS,"\n");
for i in SameInterS do
 TmpOrb:=Union(List(i, t->Orb[t]) );
 Add(TmpList,TmpOrb);
od;
Add(TmpList,[[IdMat]]);
```

Post-orb3.gap

```
SameKindOfInter:=Set(TmpList);
Print("Sizes of orbits  =",List(Orb,t->Size(t)),
                                              "\n");
Print("Sizes of classes =",
             List(SameKindOfInter,t->Size(t)),"\n");
```

Now, the code computes the actual intersection with `UnI` and produces a list with the possible intersection sizes.

Post-orb4.gap

```
###
# Compute Actual intersection with U
###

IntersectMatWithU:=function(M)
 local Var,Var1,t;
 if M=[ IdMat ] then
  return(UnIp);
 fi;
 Var:=MatToVar(M);
 Var1:=Set(List(Var,t->PtToVect(t)));
 return(IntersectionSet(UnIp,Var1));
end;;
SizeOfInters:=[];

# Check classes

IntWithUList:=[];
for x in SameKindOfInter do
 Print("Orbit number ",
           Position(SameKindOfInter,x),"\n");
 TmpList:=[];
 TmpWithUList:=[];
```

```
 for y in x do
  Add(TmpList,Size(IntersectMatWithU(y)));
  Add(TmpWithUList,IntersectMatWithU(y));
 od;
 Add(IntWithUList,TmpWithUList);
 Print("Sizes: ",TmpList,"\n");
 Add(SizeOfInters,Set(TmpList));
od;
DiffConfList:=List(IntWithUList,t->Set(t));

# Check if some classes yield the same intersection
# and, if the case,  merge them (ToUniteList)

TmpList:=[];
TmpList2:=[];
ToUniteListTmp:=[];
for i in DiffConfList do
 Add(TmpList,Position(DiffConfList,i));
od;
l:=Size(TmpList);
for i in [1..l] do
 for j in [0..l-1] do
  k:=Position(TmpList,i,j);
   if IsInt(k) then
    Add(TmpList2,k);
   fi;
 od;
 if not IsEmpty(TmpList2) then
  Add(ToUniteListTmp,Set(TmpList2));
 fi;
 TmpList2:=[];
od;
ToUniteList:=Set(ToUniteListTmp);
TmpList:=[];
TmpList2:=[];
for i in ToUniteList do
 TmpList2:=Union(List(i, t->SameKindOfInter[t]) );
 Add(TmpList,TmpList2);
od;
MergedIntersections:=Set(TmpList);
```

The last two modules, `Post-orb5` and `Post-orb6` deal with the output and the saving of the results. In `Post-orb5`, the program prints out a table which correlates size of orbits (intersection classes) and the intersection sizes.

Post-orb5.gap

```
Print("-------------> Table <----------------\n");
Print("Sizes of orbits    =",
                         List(Orb,t->Size(t)),"\n");
Print("Sizes of classes   =",
             List(SameKindOfInter,t->Size(t)),"\n");
Print("Corr. sizes of int =",SizeOfInters,"\n");
Print("No. of distinct conf. per class:",
                List(DiffConfList,t->Size(t)),"\n");
Print("Classes that yeld same intersections:",
                                  ToUniteList,"\n");
Print("Corr. no. of varieties =",
         List(MergedIntersections,t->Size(t)),"\n");
Print("Corr. sizes =",
      List(ToUniteList,t->SizeOfInters[t[1]]),"\n");
Print("Size of U = ",Size(Unp),"\n");
Print("---------------------------------------\n");
```

The list `Orb` contains all the representatives for each of the possible intersection classes. `Post-orb6` provides a function to dump the result of all computation on a file. The format is such as to make it simple to reload the data, if need be.

Post-orb6.gap

```
DumpInfo:=function(filenm)
 local i,j,k,t,kk;
 PrintTo(filenm,"------> Status report <------\n\n");
 AppendTo(filenm,"General Info:\n");
 AppendTo(filenm,"\t p:=",p,"\n\t q:=",q,"\n\t d:=",
                                               d,"\n");
 AppendTo(filenm,"Space:= PG(",d,",",q,")\n\n");
 AppendTo(filenm,"----> Table of sizes \n\n");
 AppendTo(filenm,"Sizes of orbits    =",
                         List(Orb,t->Size(t)),"\n");
 AppendTo(filenm,"Sizes of classes   =",
             List(SameKindOfInter,t->Size(t)),"\n");
 AppendTo(filenm,"Corr. sizes of int =",
                                  SizeOfInters,"\n");
 AppendTo(filenm,"No. of distinct conf. per class:",
                List(DiffConfList,t->Size(t)),"\n");
 AppendTo(filenm,"Classes that yield same
                  intersections:",ToUniteList,"\n");
 AppendTo(filenm,"Corr. no. of varieties  =",
          List(MergedIntersections,t->Size(t)),"\n");
```

```
 AppendTo(filenm,"Corr. sizes =",
       List(ToUniteList,t->SizeOfInters[t[1]]),"\n");
 AppendTo(filenm,"Size of U = ",Size(UnIp),"\n\n");
 AppendTo(filenm,"----> Matrices in classes");
 for i in SameKindOfInter do
  AppendTo(filenm,"Class number: ",
                 Position(SameKindOfInter,i),"\n");
  for j in i do

   AppendTo(filenm,"\t M[",Position(i,j),"]= [\n");
   for k in j do
    AppendTo(filenm,"\t\t", k,"\n");
   od;
   AppendTo(filenm,"\t]\n;");
  od;
  AppendTo(filenm,"----\n");
 od;
 AppendTo(filenm,"\n\n ---> Configurations in
                                 classes\n");
 for t in [1..Size(SameKindOfInter)] do
  i:=SameKindOfInter[t];
  AppendTo(filenm,"Class number(s): ",
                 Elements(Filtered(ToUniteList,
                          hh -> t in hh)),"\n");
  for j in i do
   AppendTo(filenm,"  Case number:",
                             Position(i,j),"\n");
   AppendTo(filenm,"   Points (");
   kk:=IntersectMatWithU(j);
   AppendTo(filenm,Size(kk),"):\n");
   for k in kk do
    AppendTo(filenm,"\t\t",k,"\n");
   od;
  AppendTo(filenm,"--\n");
  od;
   AppendTo(filenm,"------\n");
  od;
end;;

#####
```

4.2.8 Generators of the projective unitary group

Direct computation of $\mathrm{PU}(n+1,q)$ as the stabiliser of $\mathcal{U}_n$ in $\mathrm{PG}(n,q)$ proves to be highly unpractical for all but the most trivial cases. This is mostly due to the size of the objects involved and constraints on memory available on the computers. Hence, some results on generating sets for this group have been studied, in order to be able provide an explicit representation. Such results have not been implemented in the code presented before. However, some explicit computations have been carried out and we expect to use them in a new version of the program.

The results from Section 1.6 on quasi-symmetries will be used here.

Quasi-symmetries

Let $\mathcal{U}_n$ be the standard Hermitian hypersurface $\mathcal{U}_n$ in $\mathrm{PG}(n,q) = \mathbb{P}V$.

We recall that any quasi-symmetry σ of V fixes an hyperplane; hence, modulus a suitable change of coordinates, σ can be represented as a diagonal matrix

$$Q_\alpha^{(n+1)} = \mathrm{diag}(\alpha, 1, 1, \ldots, 1),$$

with $\alpha\overline{\alpha} = 1$.

On the other hand, a direct computation shows that, by conjugation of Q_α with the diagonal matrix

$$T = \mathrm{diag}(t, 1, 1, \ldots, 1),$$

we get an equivalent transformation of the projective space $\mathrm{PG}(n,q)$; this transformation is $Q_{t^2\alpha}^{(n+1)}$. It follows that there are as many distinct classes of quasi-symmetries as classes of squares in the field K the vector space V is defined on. If $K = \mathrm{GF}(q)$, this means that there are exactly two classes of quasi-symmetries.

Since $\mathrm{GF}(\sqrt{q})$ is included in the set of squares of $\mathrm{GF}(q)$, we may assume without loss of generality the following:

(i) $\alpha \in \{1, \epsilon\}$, where ϵ is a fixed element of norm 1 which is not a square in $\mathrm{GF}(q)$;

(ii) the conjugates are computed modulus transformations in the Special Linear group $\mathrm{SL}(n+1,q)$.

A direct computation for $n = 1, 2$ yields the following results.

(i) If $n = 1$ then, any quasi-symmetry is a conjugate of the diagonal matrix $D_\alpha^{(2)} = \mathrm{diag}(\alpha, 1)$; hence, for any $T \in \mathrm{SL}(2,q)$:

$$T^{-1}AT = \begin{bmatrix} t_{11}\alpha t_{22} - t_{12}t_{21} & t_{11}t_{12}(1-\alpha) \\ t_{21}t_{22}(\alpha - 1) & -t_{12}\alpha t_{21} + t_{11}t_{12} \end{bmatrix}.$$

(ii) If $n = 2$ then, the conjugate of $D_\alpha^{(3)}$ by $T \in \mathrm{SL}(3,q)$ is:

$$\begin{bmatrix} \eta_1 t_{1,1} - \eta_2 t_{2,1} + \eta_3 t_{3,1} & \eta_1 t_{1,2} - \eta_2 t_{2,2} + \eta_3 t_{3,2} & \eta_1 t_{1,3} - \eta_2 t_{3,3} + \eta_3 t_{3,3} \\ \eta_5 t_{2,1} - \eta_4 t_{1,1} - \eta_6 t_{3,1} & \eta_5 t_{2,2} - \eta_4 t_{1,2} - \eta_6 t_{3,2} & \eta_5 t_{2,3} - \eta_4 t_{1,3} - \eta_6 t_{3,3} \\ \eta_7 t_{1,1} - \eta_8 t_{2,1} + \eta_9 t_{3,1} & \eta_7 t_{1,2} - \eta_8 t_{2,2} + \eta_9 t_{3,2} & \eta_7 t_{1,3} - \eta_8 t_{2,3} + \eta_9 t_{3,3} \end{bmatrix},$$

where

$$\eta_1 = \alpha(t_{2,2}t_{3,3} - t_{2,3}t_{3,2}); \qquad \eta_2 = t_{1,2}t_{3,3} - t_{1,3}t_{3,2};$$

$$\eta_3 = t_{1,2}t_{2,3} - t_{1,3}t_{2,2}; \qquad \eta_4 = \alpha(t_{2,1}t_{3,3} - t_{2,3}t_{3,1});$$

$$\eta_5 = t_{1,1}t_{3,3} - t_{1,3}t_{3,1}; \qquad \eta_6 = t_{1,1}t_{2,3} - t_{1,3}t_{2,1};$$

$$\eta_7 = \alpha(t_{2,1}t_{3,2} - t_{2,2}t_{3,1}); \qquad \eta_8 = t_{1,1}t_{3,2} - t_{1,3}t_{3,1};$$

$$\eta_9 = t_{1,1}t_{2,2} - t_{1,2}t_{2,1}.$$

Definition 4.2.2. For any matrix $T \in \mathrm{Mat}(n, K)$ and for any $d \in K$, let $T_{(x,y)=d}$ be the matrix in which the entry t_{xy} is replaced by the value d, and let T^{xy} be the minor of T obtained by deleting the x-th row and the y-th column from T.

Lemma 4.2.3. *Let M be a conjugate of $D_\alpha^{(n+1)}$ via a matrix $T \in \mathrm{SL}(n+1, q)$. Then,*

$$M_{ij} = \det T_{(i,j)=t_{ij}\alpha}.$$

Proof. By expanding the row/column product,

(i) for $i = 1$, $(D_\alpha^{(n+1)}T)_{1j} = \alpha t_{1j}$;

(ii) for $i \neq 1$, $(D_\alpha^{(n+1)}T)_{ij} = t_{ij}$.

Since

$$(T^{-1})_{ij} = (-1)^{i+j} \det T^{ij},$$

a new computation yields

$$(T^{-1}D_\alpha^{(n+1)}T)_{ij} = \det T^{(i,1)}\alpha t_{1j} + \sum_{k=2}^{n+1}(-1)^{i+j}\det T^{ik}t_{kj} = \det(T_{(i,j)=t_{ij}\alpha}).$$

□

Ishibashi's theorem

For the odd characteristic case, it is possible to use a different result: a theorem by Ishibashi [Ish85] provides a small set of generators for the unitary group.

Let f be an unitary form over a vector space V over $\mathrm{GF}(q)$ and assume that V has hyperbolic rank at least 1. Denote by $q(x)$ the Hermitian form associated to f and decompose V in the direct product

$$V = H \perp L,$$

where H is a hyperbolic plane with isotropic base u, v. Furthermore, we may assume that

$$f(u, v) = \lambda \overline{f(v, u)},$$

and define the following five kinds of mappings:

(i) the isometry Δ that fixes L and acts on H by mapping $u \to v$, $v \to \overline{\lambda} u$;

(ii) the isometry $\phi(\epsilon)$ that, for any $\epsilon \in \mathrm{GF}(q)$, fixes L and sends $u \to \epsilon u$ and $v \to \epsilon^{-1} v$;

(iii) the *Eichler transformation* (*quasi-transvection*) $E(u, x)$, defined for any $x \in L$, that acts on $z \in V$ as

$$E(u, x) : z \to z - \lambda f(z, u)x + f(z, x)u - \lambda f(z, u)q(x)u;$$

(iv) the symmetry $\tau(x)$, given, for any $x \in V$ with $q(x) \neq 0$, by

$$\tau(x) : z \to z - f(z, x)q(x)^{-1}x;$$

(v) the permutation σ that fixes the hyperbolic plane H and permutes the vectors of a given orthogonal base $\{z_1, \ldots, z_{n-2}\}$ of L in such a way as to have

$$z_1 \to^{\sigma} z_2 \to^{\sigma} \ldots \to^{\sigma} z_{n-2},$$

where $q(z_i) = q(z_j)$ for all i, j.

Theorem 4.2.4. *For $n > 2$ odd, the group $U_f(n, q)$ is generated by three isometries, namely:*

(i) $E(u, z_1)$,

(ii) $\Delta\sigma$,

(iii) $\phi(\alpha)$, *where α is a primitive element of* $\mathrm{GF}(q)^{\star}$.

From now on, we shall assume α to be a primitive element of $\mathrm{GF}(q)^{\star}$.

Theorem 4.2.5. *Assume that the restriction* $f\mid_L$ *is equivalent to the Hermitian form induced by the identity matrix* $\operatorname{diag}(1,\ldots,1,1)$*. Then, for* $n>2$*,* n *even, the group* $U_f(n,q)$ *is generated by the three isometries*

(i) $E(u,z_1)$,

(ii) $\Delta\sigma$,

(iii) $\phi(\alpha)\tau(z_1-z_{n-2})$.

Theorem 4.2.6. *Assume that the restriction* $f|_L$ *is equivalent to the Hermitian form induced by a matrix* $\operatorname{diag}(1,\ldots,1,\alpha)$*, with* $-2^{-1}=\alpha^{2k+1}$*. Then, for* $n>2$*,* n *even, the group* $U_f(n,q)$ *is generated by the three isometries*

(i) $E(u,z_1+z_{n-2})$,

(ii) $\Delta\tau(z_1)\sigma$,

(iii) $\phi(\alpha)\tau(z_1)$.

Theorem 4.2.7. *Assume that the restriction* $f\mid_L$ *is equivalent to the Hermitian form induced by the matrix* $\operatorname{diag}(1,\ldots,1,\alpha)$*, with* $-2^{-1}=\alpha^{2k}$*. Then, for* $n>4$*,* n *even, the group* $U_f(n,q)$ *is generated by the three isometries*

(i) $E(u,z_1+z_{n-2})$,

(ii) $\Delta\tau(z_1)\sigma$,

(iii) $\phi(\alpha)\tau(z_1-z_{n-3})$.

The group $U_f(4,q)$ *is generated by*

(i) $E(u,z_1+z_2)$,

(ii) Δ,

(iii) $\phi(\alpha)\tau(z_1)$.

Remark 4.2.8. In the cases of Theorems 4.2.6 and 4.2.7, the group $U_f(n,q)$ is the same as the orthogonal group $O_f(n,q)$.

Construction of the matrices

Assume $B = \{u, v, z_1, \ldots, z_{n-2}\}$ be a fixed base of V, such that $H = \langle u, v \rangle$ is an hyperbolic plane and let U be the matrix representing the Hermitian form f with respect to B.

Then, the transformations E, Δ and σ have to satisfy the following conditions.

(i)

$$\Delta = \begin{bmatrix} 0 & 1 & & & \\ \overline{\lambda} & 0 & & & \\ & & 1 & & 0 \\ & & & \ddots & \\ & & 0 & & 1 \end{bmatrix};$$

(ii)

$$\phi(\epsilon) = \begin{bmatrix} \epsilon & 0 & & & \\ 0 & \overline{\epsilon}^{-1} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix};$$

(iii)

$$E(u, x) = I + A_1(x) - A_2(x),$$

where

$$A_1(x) = (-\lambda x \overline{u}^\star + u \overline{x}^\star)U,$$

$$A_2(x) = \lambda q(x) u \overline{u}^\star U;$$

(iv)

$$\tau(x) = I - q(x)^{-1} x \overline{x}^\star U;$$

(v)

$$\sigma = \begin{bmatrix} 1 & 0 & & & \\ 0 & 1 & & & \\ & & 0 & \ldots & 1 \\ & & 0 & \ddots & 0 \\ & & 1 & \ldots & 0 \end{bmatrix}.$$

Furthermore, since it is possible to assume without loss of generality that the matrix U is

$$U = \begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & 0 \\ & & & \ddots & \\ & & 0 & & 1 \end{bmatrix},$$

the transformation $E(u, z_1)$ can be written as

$$E(u,z_1) = \begin{bmatrix} 1 & -\frac{1}{2} & -1 & & & & \\ 0 & 1 & 0 & & & & \\ 1 & 0 & 1 & & & & \\ & & & 1 & 0 & \dots & 0 \\ & & & 0 & 1 & & \\ & & & & & \ddots & \\ & & & 0 & & & 1 \end{bmatrix}.$$

4.2.9 Concluding remarks

The code introduced in this section is able to provide useful results only for small values of q and low dimension n.

The main speed bottleneck of the program is in the computation of the orbits of the Projective Unitary Group seen acting on the set of all Hermitian matrices.

Some improvement can be attained by using the set of generators introduced in subsection 4.2 in order to define $\mathrm{PGU}(n+1, q)$, albeit the best approach is definitely by providing directly the list of the matrices in the group. However, even in this case the `orbits` function of GAP seems to be too slow for getting meaningful results.

There are two main obstacles towards the solution of the problem of intersection of Hermitian varieties in its full generality:

1. 'combinatorial explosion' of the number of possible cases, as Chapter 3 and the computation of intersection orders for Hermitian hypersurfaces in dimension 4 show;
2. lack of a general method to compute the groups except in the most simple cases.

In order to get a deeper understanding of the structures involved, it will be helpful to be able to produce some examples for the high dimensional cases. In fact, we plan to rewrite the code from scratch in C using the infrastructure provided by the `gnump` library to implement the finite fields.

Bibliography

[AK92] E.F. Assmus and J.D. Key, *Designs and their codes*, Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992.

[Bae52] R. Baer, *Linear algebra and projective geometry*, Academic Press, New York, 1952.

[BBW91] A. Blokhuis, A. Brouwer, and H. Wilbrink, *Hermitian unitals are code words*, Discrete Math. **97** (1991), 63–68.

[BC66] R.C. Bose and I.M. Chakaravarti, *Hermitian varieties in a finite projective space* $\mathrm{PG}(n, q^2)$, Canad. J. Math. **18** (1966), 1161–1182.

[Blo67] D.M. Bloom, *The subgroups of* $\mathrm{PSL}(3, q)$ *for* q *odd*, Trans. Amer. Math. Soc. **127** (1967), 150–178.

[BR98] A. Beutelspacher and U. Rosenbaum, *Projective geometry: from foundations to applications*, Cambridge University Press, Cambridge, 1998.

[BS86] E. Boros and T. Szőnyi, *On the sharpness of a theorem of B. Segre*, Combinatorica **6** (1986), 261–268.

[Cam95] P. J. Cameron, *Projective and polar spaces*, QMW Maths Notes/13, London, 1995.

[CEK00] A. Cossidente, G.L. Ebert, and G. Korchmáros, *A group–theoretic characterization of classical unitals*, Arch. Math. **74** (2000), 1–5.

[CK97] A. Cossidente and G. Korchmáros, *The Hermitian function field arising from a cyclic arc in a Galois plane*, Geometry, combinatorial designs and related structures (Cambridge) (S.S. Magliveras J.W.P. Hirschfeld and M.J. de Resmini, eds.), Cambridge University Press, 1997, pp. 63–68.

[CK98] ______, *The algebraic envelope associated to a complete arc*, Recent Progress in Geometry (E. Ballico and G. Korchmáros, eds.), III, vol. 51, Rend. Circolo Mat. Palermo, 1998, pp. 9–24.

[CKT99] A. Cossidente, G. Korchmáros, and F. Torres, *On curves covered by the Hermitian curve*, J. Algebra **216** (1999), 56–76.

[Cos97] A. Cossidente, *Addendum to: "A new proof of the existence of* (q^2-q+1)*-arcs in* $\mathrm{PG}(2,q^2)$*" [J. Geom.* **53** *(1995), no. 1-2, 37–40]*, J. Geom. **59** (1997), 32–33.

[CS] A. Cossidente and A. Siciliano, *The geometry of Hermitian matrices of order three over Galois fields*, submitted.

[Dem68] P. Dembowski, *Finite geometries*, Springer–Verlag, Berlin, 1968.

[Die71] J. Dieudonné, *La geometrie des groupes classiques*, 3rd ed., Springer–Verlag, New York, 1971.

[Ebe85] G.L. Ebert, *Partitioning projective geometries into caps*, Canad. J. Math. **37** (1985), 1163–1175.

[FHT86] J.C. Fisher, J.W.P. Hirschfeld, and J.A. Thas, *Complete arcs in planes of square orders*, Ann. Discrete Math. **30** (1986), 243–250.

[Ful69] W. Fulton, *Algebraic curves*, The Benjamin/Cummings Publishing Company, Reading, Massachusetts, 1969.

[GAP99] The GAP Group, Aachen, St Andrews, *GAP – Groups, Algorithms, and Programming, Version 4.1*, 1999, (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[Giua] L. Giuzzi, *A characterization of classical unitals*, submitted.

[Giub] ______, *Groups of the intersection of two hermitian curves*, submitted.

[GS99] P. Govaerts and L. Storme, *Projective geometry 'pg1.0'*, Department of Pure Mathematics and Computer Algebra, University of Ghent, 1999.

[GS00] D.R. Grayson and M.E. Stillman, *Macaulay 2 version 0.8.60*, 2000, (`http://www.math.uiuc.edu/Macaulay2`).

[Har26] R.W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in* $\mathrm{GF}(2^n)$, Ann. of Math. **27** (1926), 140–158.

[HH70] B. Hartley and T.O. Hawkes, *Rings, modules and linear algebra*, Chapman and Hall, London, 1970.

[Hir98a] J.W.P. Hirschfeld, *Algebraic geometry over a field of positive characteristic*, 1998, Notes edited by L. Giuzzi.

[Hir98b] ______, *Projective geometry over finite fields*, 2nd ed., Oxford Science Pubblications, Oxford, 1998.

[Hof72] A.R. Hoffer, *On unitary collineation groups*, J. Algebra **22** (1972), 211–218.

[Ish85] H. Ishibashi, *Small systems of generators of isotropic unitary groups over finite fields of characteristic not two*, J. Algebra **93** (1985), 324–331.

[Kes81] B.C. Kestenband, *Unital intersections in finite projective planes*, Geom. Dedicata **11** (1981), no. 1, 107–117.

[Kes89] ______, *A family of complete arcs in finite projective planes*, Colloq. Math. **17** (1989), 59–67.

[Kin99] O.H. King, *Classical groups*, Notes of the Socrates intensive programme, Potenza, 1999.

[KSW73] H. Karzel, K. Sörensen, and D. Windelberg, *Einführung in die Geometrie*, Vandenhoeck and Ruprecht, Göttingen, 1973.

[Lan80] S. Lang, *Linear algebra*, Addison Wesley, Reading, Massachusetts, 1980.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[Lun99] G. Lunardon, *Normal spreads*, Geom. Dedicata **75** (1999), no. 3, 245–261.

[Mit11] H.H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911), 207–242.

[Rob80] D.J.S. Robinson, *A course in the theory of groups*, Springer–Verlag, New York, 1980.

[Seg65] B. Segre, *Forme e geometrie hermitiane con particolare riguardo al caso finito*, Ann. Mat. Pura Appl. **70** (1965), 1–201.

[Seg67] ______, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I **Mem. 8** (1967), 133–236.

[Sin38] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.

[Tec87] H. Tecklenburg, *A proof of the theorem of Pappus in finite Desarguesian affine planes*, J. Geom. **30** (1987), 172–181.

[Tha87] J.A. Thas, *Complete arcs and algebraic curves in* $\mathrm{PG}(2,q)$, J. Algebra **106** (1987), 457–464.

[WC76] I. Walton and C. Cotton, *The compleat angler*, 5th ed., Richard Marriott, London, 1676.

[Wie64] H. Wielandt, *Finite permutation groups*, Academic Press, New York and London, 1964.