

TRUNCATED QUADRICS AND ELLIPTIC CURVES

by

Stephen C. Flink

B.S., University of Colorado at Denver, 2000

M.S., University of Colorado at Denver, 2004

A thesis submitted to the
University of Colorado Denver
in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Applied Mathematics
2009

This thesis for the Doctor of Philosophy

degree by

Stephen C. Flink

has been approved

by

Stanley E. Payne

William E. Cherowitzo

Ellen Gethner

Sylvia A. Hobart

Michael S. Jacobson

Date

Flink, Stephen C. (Ph.D., Applied Mathematics)

Truncated Quadrics and Elliptic Curves

Thesis directed by Professor Stanley E. Payne

ABSTRACT

Let p be an odd prime and let $q = p^e$. Let \mathcal{E} be an elliptic quadric in $PG(3, q)$. The quadric \mathcal{E} carries the structure of the projective line $PG(1, q^2)$, and the points of \mathcal{E} may be put in a one-to-one correspondence with the points of $PG(1, q^2)$ in a manner that preserves the structure of the quadric, in terms of the respective automorphism groups. In this thesis, we consider the geometric properties of the subset \mathcal{E}_\square of \mathcal{E} whose points correspond in this way to the nonzero squares in the Galois Field \mathbb{F}_{q^2} . In the course of determining the number of points of \mathcal{E}_\square on certain hyperplanes of $PG(3, q)$, there arise two families of elliptic curves. The Hasse-Weil theorem is invoked to give bounds on the cardinalities of plane intersections with \mathcal{E}_\square . Empirical results for small values of q show that these bounds are the best possible. The theory of elliptic curves over finite fields is used to establish proofs of other properties of the plane sections of \mathcal{E} .

A substructure \mathcal{H}_\square of the hyperbolic quadric \mathcal{H} in $PG(3, q)$ is defined and studied. \mathcal{H}_\square is analogous to and has geometric properties very similar to those of \mathcal{E}_\square . As with our examination of \mathcal{E}_\square , there arise two families of elliptic curves, and

the Hasse-Weil theorem implies bounds on the cardinalities of plane intersections with \mathcal{H}_\square . We find that the two families of curves which arise in the study of \mathcal{H}_\square are identical with the two families of elliptic curves from the study of \mathcal{E}_\square . We call these families of curves $\mathbf{E}_\mathcal{E}^\square$, parameterized by \mathbb{F}_q^* , and $\mathbf{E}_\mathcal{E}'^\square$, parameterized by $\mathbb{F}_q \setminus \{0, 1, -1\}$.

Assume now that q is not a power of 3. We show that the set of curves $\mathbf{E}_\mathcal{E}^\square$ is symmetric in the sense that the curves in this set with $q + 1 + t$ points are in one-to-one correspondence with the curves in this set with $q + 1 - t$ points. When $q \equiv 3 \pmod{4}$, the set of curves $\mathbf{E}_\mathcal{E}'^\square$ exhibits the same symmetry.

This abstract accurately represents the content of the candidate's thesis. I recommend its publication.

Signed _____
Stanley E. Payne

DEDICATION

For Greg

ACKNOWLEDGMENT

This thesis would not have been possible without the assistance of the George Galloway trust. I would also like to thank the mathematics faculty at CU Denver for awarding me a Lynn Bateman Memorial Teaching Award for the Fall semester of 2006.

Many people have provided encouragement and useful advice. Their influence may have been inadvertent and seemed small at the time and may have come in the course of working together or from offhand conversations. Thank you to John Wilson, Leanne Holder, Mark Miller, Janice Dugger, Art Busch, Oscar Jenkins, Dave Brown, Frank Thraxton, Sandy Barrett, Victoria Naman, Georgia Meginity, Shannon Raptis and Francis Conry. Special thanks to Rob Rostermundt for our many conversations and for being the designated driver after I completed my comprehensive exam. From the distant past, I need to thank Leona Jackson, Bill Blair, Rick Schmidt, James Plastino and Mark Chamberlin.

In no particular order, math courses from Dave Wilson, Hugh Bradley, Tom Kammerling, Markus Emsermann, Rich Lundgen, Dave Fisher, Tom Russell, Bill Cherowitzo, Bruce MacMillan, and Brooks Reid have been particularly enlightening. Thanks again to Bruce MacMillan for allowing me to sit in on his Calculus courses during the 2004-05 academic year.

I would like to thank the members of my thesis committee for taking the time to examine this work and for their helpful feedback. Thank you in particular to Stan Payne for his guidance in my research.

Most of all, I would like to thank Yongxia for her love, support and patience.

CONTENTS

Figures	ix
Tables	x
<u>Chapter</u>	
1. Introduction	1
2. Two Quadrics in $PG(3, q)$	8
2.1 Definitions and Preliminaries	8
2.2 An Elliptic Quadric	11
2.3 A Ruled Quadric in $PG(3, q)$	17
3. The Actions of Two-Point Stabilizers	19
3.1 The Stabilizer of Two Points of \mathcal{E}	19
3.2 Orbits of Planes Under G_l	21
3.3 The Group Stabilizing Two Points of \mathcal{H}	23
3.4 Point Sets Associated with Squares	28
3.4.1 The Square Points of \mathcal{E}	28
3.4.3 The Square Points of \mathcal{H}	32
4. Truncated Quadrics and Elliptic Curves	37
4.1 Point Counts on Planes Meeting \mathcal{E}_\square	37
4.2 Some Background on Elliptic Curves	41
4.3 Birational Transformations Between Quartics and Cubics	43
4.3.1 Elliptic Curves From Orbits $\mathcal{O}_{\mathcal{E}_\square}^\cap$	43

4.3.3	Elliptic Curves From Orbits $\mathcal{O}_{\mathcal{E}\square}^{\not\cap}$	47
4.3.4	Elliptic Curves from Orbits $\mathcal{O}_{\mathcal{H}\square}^{\cap}$	48
4.3.5	Elliptic Curves from Orbits $\mathcal{O}_{\mathcal{H}\square}^{\not\cap}$	50
4.3.6	Families of Curves	51
4.4	Summary of Plane Intersections with Truncated Quadrics	52
4.4.1	Other Plane Orbit Types	52
4.4.2	Summary of Plane Intersections for Truncated Quadrics	53
4.5	Sums of Point Counts	56
4.6	The Invariant j and Symmetry of Incidences	58
4.6.1	Admissible Changes of Variables	59
4.6.4	The Invariant j	61
<u>Appendix</u>		
A.	Additional Results	66
A.1	$q - 1$ Elliptic Quadrics Intersecting in 2 Points	66
A.2	Addition on the Curves	67
B.	Tables of Elliptic Curves	69
B.1	Tables for Elliptic Curves	69
C.	Programs	98
C.1	C++ Programs	98
C.2	Sage Programs	104
<u>References</u>		105

FIGURES

Figure

2.1	Tangent planes to \mathcal{E} and the lines l and l^\perp	15
3.1	A diagram of the elliptic quadric from the point of view of the stabilizer of two points.	31
3.2	A diagram of the hyperbolic quadric from the point of view of the stabilizer of two points not on any line of the quadric.	35

TABLES

Table

4.1	Intersection numbers of \mathcal{E}_\square with planes in $\mathcal{P}_\mathcal{E}^\square$ for $q = 263$	38
4.2	The number of \mathbb{F}_q -rational points on elliptic curves $E = E_\mathcal{E}^{\omega^\square}$ for $\omega \in \mathbb{F}_{263}$, their j -invariants and multiplicities in $\mathbf{E}_\mathcal{E}^\square$	65
B.1	Point counts and j -invariants for curves over \mathbb{F}_3	70
B.2	Point counts and j -invariants for curves over \mathbb{F}_5	70
B.3	Point counts and j -invariants for curves over \mathbb{F}_7	70
B.4	Point counts and j -invariants for curves over \mathbb{F}_{11}	70
B.5	Point counts and j -invariants for curves over \mathbb{F}_{13}	71
B.6	Point counts and j -invariants for curves over \mathbb{F}_{17}	71
B.7	Point counts and j -invariants for curves over \mathbb{F}_{19}	71
B.8	Point counts and j -invariants for curves over \mathbb{F}_{23}	72
B.9	Point counts and j -invariants for curves over \mathbb{F}_{29}	72
B.10	Point counts and j -invariants for curves over \mathbb{F}_{31}	72
B.11	Point counts and j -invariants for curves over \mathbb{F}_{37}	73
B.12	Point counts and j -invariants for curves over \mathbb{F}_{41}	73
B.13	Point counts and j -invariants for curves over \mathbb{F}_{43}	73
B.14	Point counts and j -invariants for curves over \mathbb{F}_{47}	74
B.15	Point counts and j -invariants for curves over \mathbb{F}_{53}	74
B.16	Point counts and j -invariants for curves over \mathbb{F}_{59}	74

B.17	Point counts and j -invariants for curves over \mathbb{F}_{61}	75
B.18	Point counts and j -invariants for curves over \mathbb{F}_{67}	75
B.19	Point counts and j -invariants for curves over \mathbb{F}_{71}	76
B.20	Point counts and j -invariants for curves over \mathbb{F}_{73}	76
B.21	Point counts and j -invariants for curves over \mathbb{F}_{79}	77
B.22	Point counts and j -invariants for curves over \mathbb{F}_{83}	77
B.23	Point counts and j -invariants for curves over \mathbb{F}_{89}	78
B.24	Point counts and j -invariants for curves over \mathbb{F}_{97}	78
B.25	Point counts and j -invariants for curves over \mathbb{F}_{101}	79
B.26	Point counts and j -invariants for curves over \mathbb{F}_{103}	79
B.27	Point counts and j -invariants for curves over \mathbb{F}_{107}	80
B.28	Point counts and j -invariants for curves over \mathbb{F}_{109}	80
B.29	Point counts and j -invariants for curves over \mathbb{F}_{113}	81
B.30	Point counts and j -invariants for curves over \mathbb{F}_{127}	82
B.31	Point counts and j -invariants for curves over \mathbb{F}_{131}	83
B.32	Point counts and j -invariants for curves over \mathbb{F}_{137}	84
B.33	Point counts and j -invariants for curves over \mathbb{F}_{139}	85
B.34	Point counts and j -invariants for curves over \mathbb{F}_{149}	86
B.35	Point counts and j -invariants for curves over \mathbb{F}_{151}	87
B.36	Point counts and j -invariants for curves over \mathbb{F}_{157}	88
B.37	Point counts and j -invariants for curves over \mathbb{F}_{163}	89
B.38	Point counts and j -invariants for curves over \mathbb{F}_{167}	90
B.39	Point counts and j -invariants for curves over \mathbb{F}_{173}	91
B.40	Point counts and j -invariants for curves over \mathbb{F}_{179}	92

B.41	Point counts and j -invariants for curves over \mathbb{F}_{181}	93
B.42	Point counts and j -invariants for curves over \mathbb{F}_{191}	94
B.43	Point counts and j -invariants for curves over \mathbb{F}_{193}	95
B.44	Point counts and j -invariants for curves over \mathbb{F}_{197}	96
B.45	Point counts and j -invariants for curves over \mathbb{F}_{199}	97

1. Introduction

The focus of this dissertation is on a question in three-dimensional projective geometry, $PG(3, q)$, when \mathbb{F}_q is an arbitrary finite field of odd order. Our principal problem is to determine geometric properties of an object with a natural algebraic definition, but whose geometric structure is not obvious. We begin with a nondegenerate quadric \mathcal{Q} in $PG(3, q)$. We partition the points of \mathcal{Q} so that the partite classes correspond in a natural way with the elements of the extended field $\tilde{\mathbb{F}}_q = \mathbb{F}_q \cup \{\infty\}$. We study the geometry of \mathcal{Q}_\square , the set of points associated with the nonzero squares in \mathbb{F}_q under this partition. We call \mathcal{Q}_\square a *truncated quadric*. Our problem is to describe \mathcal{Q}_\square in terms of plane intersections. The first step is to classify all orbits of planes under the action of the group stabilizing our partition. We find that the most interesting orbits fall into two classes for each of the two types of quadric under consideration. Counting points of \mathcal{Q}_\square on planes in these orbits is shown to be equivalent to counting points on certain nonsingular elliptic curves. These are algebraic curves of genus 1, for which there exists a large and rich theory. We apply the Hasse-Weil Theorem, a deep result which gives bounds on the number of points on algebraic curves over finite fields. This theorem, in turn, gives us bounds on the cardinalities of plane intersections with the truncated quadrics. We present numerical results establishing the tightness of these bounds. We give a simple characterization of the families of elliptic curves which arise when considering each type of orbit. Finally, we explain a symmetry of incidence numbers which occurs in certain

families of orbits of planes, which have the property that for every plane meeting the truncated quadric in $\frac{q+1}{2} + t$ points, there is a plane in the same family meeting it in $\frac{q+1}{2} - t$ points.

In Chapter 2, we recall basic notions from projective geometry over finite fields. We review results which establish that the elliptic quadric is the unique example of an ovoid in $PG(3, q)$ when q is odd. The points of an elliptic quadric in $PG(3, q)$ may be put in one-to-one correspondence with the points of the projective line $PG(1, q^2)$ so that each reflects the structural properties of the other. We point out that this is analogous to the identification of the points of the extended complex plane with the unit sphere via stereographic projection.

Choosing a specific elliptic quadric \mathcal{E} , we show how to make the correspondence between the points of \mathcal{E} and $PG(1, q^2)$ explicit. We find that the norm map from $\mathbb{F}_{q^2}^*$ to \mathbb{F}_q^* partitions the points of $\mathcal{E} \setminus \{0, \infty\}$ into $q - 1$ disjoint ovals. This partition is the same as the partition induced by a certain flock of \mathcal{E} . Fix the points 0 and ∞ of \mathcal{E} , and define the line to be the line of intersection of the tangent planes to \mathcal{E} at 0 and ∞ . For each of the $q - 1$ non-tangent planes on l^\perp , we choose representative vectors parameterized by the nonzero elements of \mathbb{F}_q . This choice of representatives is such that for each value $a \in \mathbb{F}_q^*$, the points of \mathcal{E} on the plane with representative a are the elements of $\mathbb{F}_{q^2}^*$ with norm a .

In Section 2.3, we choose a specific hyperbolic quadric \mathcal{H} in $PG(3, q)$ whose algebraic form bears a strong resemblance with the form chosen for the elliptic quadric \mathcal{E} . In \mathcal{E} , the points corresponding to $\mathbb{F}_q \cup \infty$ form an oval o , and $\mathcal{E} \cap \mathcal{H} = o$. If we remove a certain pair of points from \mathcal{H} , the remaining points may be partitioned into $q + 1$ subsets. In fact, the set of $q + 1$ planes we used

to partition \mathcal{E} are used to partition the points of \mathcal{H} , in a manner different from but analogous to the partition for \mathcal{E} . We find that a subset of the points of \mathcal{H} has a natural partition into $q - 1$ arcs of size $q - 1$.

In Chapter 3, we examine the actions of the stabilizers of the elliptic and hyperbolic quadrics on lines and planes in $PG(3, q)$. Recall our identification of the points of the elliptic quadric \mathcal{E} with the points of the projective line $PG(1, q^2)$, and so with the set $\tilde{\mathbb{F}}_{q^2} = \mathbb{F}_{q^2} \cup \infty$. We are interested in the action of the group G_l stabilizing the points 0 and ∞ of the quadric, as this is the group stabilizing our partition.

In Section 3.2, Theorem 3.2.1 describes the orbits of all planes of $PG(3, q)$ under the action of G_l . In section 3.3, we describe the geometry of the hyperbolic quadric \mathcal{H} and the action of the stabilizer H_l of 0 and ∞ in a manner analogous to the work in Sections 3.1 and 3.2 for \mathcal{E} . Theorem 3.3.1 describes all orbits of planes under the action of H_l .

In section 3.4, we define our truncated quadrics \mathcal{E}_\square and \mathcal{H}_\square . These are the subsets of \mathcal{E} and \mathcal{H} which correspond to squares in \mathbb{F}_q under the respective partitions of the quadrics described in Chapter 2. The truncated elliptic quadric \mathcal{E}_\square is stabilized by G_{l_\square} , a group of index 2 in G_l . The truncated hyperbolic quadric \mathcal{H}_\square is stabilized by a group H_{l_\square} of index 2 in H_l . Having described the actions of G_l and H_l , it is straightforward to describe the actions of G_{l_\square} and H_{l_\square} on the planes of $PG(3, q)$. We do so in Theorems 3.4.2 and 3.4.4.

For each of the stabilizing groups G_{l_\square} and H_{l_\square} , there are orbits of planes whose intersections with the truncated quadric are easily described. For example, when $q - 1$ of the $q + 1$ planes on a line are all in the same orbit, the planes

are known to partition a point set of a certain size (say $\frac{1}{2}(q^2 - 1)$), and so must each contain $\frac{1}{2}(q+1)$ points of the truncated quadric. Define an *interesting* orbit of planes (under the action of G_{l_\square} or H_{l_\square}) to be one whose intersection numbers with their respective truncated quadric are not immediately obtained by application of the orbit-stabilizer theorem. We find that it is sufficient to consider two families of interesting orbits for each of the truncated quadrics: $\{\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap} : \omega \in \mathbb{F}_q^*\}$ and $\{\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap} : \omega \in \mathbb{F}_q^* \setminus \{2, -2\}\}$ for \mathcal{E}_\square and $\{\mathcal{O}_{\mathcal{H}_\square}^{\omega \cap} : \omega \in \mathbb{F}_q^* \setminus \{2, -2\}\}$, and $\{\mathcal{O}_{\mathcal{H}_\square}^{\omega \cap} : \omega \in \mathbb{F}_q^*\}$ for \mathcal{H}_\square . These interesting orbits of planes have the property that no more than two planes in such an orbit meet in the same line. For each family of orbits, we choose a line such that each orbit of planes in the family has 2 representatives in the set of planes on that line. In the remainder of the thesis, we describe the intersection of planes from these classes with our truncated quadrics and examine some of the consequences of that description.

In Section 4.1, we offer a summary of results from algebraic geometry in general and from the theory of elliptic curves in particular, which we will use in subsequent proofs. Most important for us is the Hasse-Weil theorem, stated in Theorem 4.2.2, which gives bounds on the number of points on an elliptic curve. Also important is Theorem 4.2.1, which states that every curve is birationally equivalent to a unique nonsingular curve. In Section 4.2, we begin with a plane α_ω in an interesting orbit $\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap}$ under G_{l_\square} . Some algebra on the equations describing the intersection of α_ω with \mathcal{E}_\square yields a plane curve \mathcal{C}_F whose \mathbb{F}_q -rational points are in 2:1 proportion with the points of $\alpha_\omega \cap \mathcal{E}_\square$. The equation for the curve \mathcal{C}_F is of the form $s^2 = g(a)$, where g is a quartic in x without repeated roots. In Section 4.3, we show that this curve is birationally equivalent to a

curve whose equation is of the form $y^2 = f(x)$, where f is a cubic in x without repeated roots. This is a standard form for an elliptic curve, and we may bring to bear upon our problem substantial theoretical machinery. In Theorem 4.3.1, an application of the Hasse-Weil theorem, we find that

$$\frac{q-1}{2} - \sqrt{q} \leq |\alpha_\omega \cap \mathcal{E}_\square| \leq \frac{q-1}{2} + \sqrt{q}.$$

In section 4.4, we consider intersections of truncated quadrics with representative planes from our other interesting orbits under G_{l_\square} and H_{l_\square} . We again obtain elliptic curves from the equations for plane intersections and again apply the Hasse-Weil theorem.

Also in Section 4.3, we show that the two families of curves which arise from \mathcal{E}_\square are identical to the two families of curves which arise from \mathcal{H}_\square . In Section 4.4, we use our use results from Sections 4.2 and 4.3 to describe bounds of point counts on planes in other orbits. The idea here is that G_{l_\square} stabilizes both \mathcal{E}_\square and $\mathcal{E}_{\not\square} = \mathcal{E} \setminus (\mathcal{E}_\square \cup \{0, \infty\})$, and we are able to find an element φ of G_l which interchange \mathcal{E}_\square and $\mathcal{E}_{\not\square}$. Then φ also interchanges α_ω with a plane with the property that $|\alpha_\omega \cap \mathcal{E}_\square| + |\varphi(\alpha_\omega) \cap \mathcal{E}_\square| = q + 1$. The situation is again similar for \mathcal{H}_\square . We summarize point counts of plane intersections with the truncated quadrics in Theorems 4.4.3 and 4.4.4.

In section 4.5, we explain a property of some of the families of orbits of planes under G_{l_\square} . The property occurs for families of interesting orbits whenever $q \equiv 3 \pmod{4}$ and in certain cases when $q \equiv 1 \pmod{4}$. Let \mathcal{P} be such a family of orbits. Then whenever there is an orbit $\mathcal{O} \in \mathcal{P}$ whose planes meet \mathcal{E}_\square in $\frac{q+1}{2} + t$ points, there is a different orbit $\mathcal{O}' \in \mathcal{P}$ whose planes meet \mathcal{E}_\square in $\frac{q+1}{2} - t$ points. The proof that these planes come in these complementary pairs is accomplished

using properties of a numeric invariant of the associate elliptic curves.

Appendix A.1 contains a minor result which is not used in the main part of the thesis, but which might be of independent interest. Here we describe a set of $q - 1$ elliptic quadrics whose pairwise intersection is $\{0, \infty\}$, all of which are stabilized by G_l . A description of an analogous family of hyperbolic quadrics whose pairwise intersection is a set of four points of $PG(3, q)$ not all in one plane is given in Section 6.1 of [20].

Appendix B contains tables of elliptic curves for each of the two families described in Theorem 4.4.3, for odd primes $q < 200$. For a given q and for each of the two families of curves, the table gives the j -invariant of each curve, the number of F_q -rational points on the curve, and the number of times the curve occurs in that family. Appendix C.1 contains a program in C++ written to produce the tables in Appendix B. Appendix C.2 contains a short program in SAGE which uses some built-in elliptic curve functions. This program was written to verify the accuracy of the C++ program in section C.1.

The work presented in this thesis originated with an attempt to construct sets of points in $PG(n, q)$ with the property that the cardinalities of hyperplane intersections with the set take on relatively few values. We see from Theorems 4.5.1 and 4.5.2 and from the tables in Appendix B that the truncated quadrics are highly irregular with respect to plane intersections. Let S be a subset of $PG(n, q)$ such that the cardinalities of hyperplane intersections with S take on few values. If these cardinalities take on k values, we call S a k -intersection set. Nondegenerate quadrics provide examples of 2-intersection sets in $PG(n, q)$ when n is odd. Some of our early motivation came from the construction of Brouwer

in [2], which yields 2-intersection sets by removing points from nondegenerate quadrics in odd-dimensional projective space. Another important work on 2-intersection sets is [4], which lists all such sets known at that time and explains how 2-intersection sets may be used to construct strongly regular graphs and 2-weight codes.

The literature on quadrics in finite projective space is large and varied. We acknowledge the influence of several works whose results and terminology did not directly come into play in the final version of this thesis. Elliptic and hyperbolic quadrics give examples of finite circle planes. A standard reference on the circle planes associated with elliptic quadrics is Chapter 6 of [11]. The Ph.D. thesis of Orr [19], as reworked in [20], and the paper [3] by Bruck helped us to find a proper frame of reference and to steer clear of some false conjectures.

2. Two Quadrics in $PG(3, q)$

2.1 Definitions and Preliminaries

In this section, we give a brief review of some relevant results from finite projective geometry. We follow Stan Payne's book [20] for theorems and notation. Much of what we describe here may be found in [7], which is a good introductory text on projective geometry.

Let V be a vector space of dimension $n + 1$, for some $0 < n < \infty$ over a field \mathbb{F} . The projective geometry $\mathcal{P}(V)$ is the geometry whose r -dimensional subspaces are defined to be the $r+1$ -dimensional subspaces of V , for $r = 0, \dots, n$. Incidence in $\mathcal{P}(V)$ is defined by subspace containment in V . We call the 0-, 1- and 2-dimensional subspaces of $\mathcal{P}(V)$ the *points*, *lines* and *planes* of the geometry, and an $(n - 1)$ -dimensional subspace is a *hyperplane*. When \mathbb{F} is a field with q elements, we write $PG(n, q)$ to denote $\mathcal{P}(V)$. For our purposes, the term projective plane will refer to $PG(2, q)$, although there exist other examples of projective planes. We refer the reader to the early chapters of [20] and to Chapter 1 of [7] for an axiomatic approach to projective geometry.

In $PG(n, q)$, we use a row vector $\mathbf{x} = (x_0, x_1, \dots, x_n)$ to represent a point and a column vector $\pi = [y_0, y_1, \dots, y_n]^T$ a hyperplane in $PG(n, q)$, with the understanding that for the vector representing a point or hyperplane, we may substitute any nonzero scalar multiple of that vector. The vector representing π generates the null space of all the points incident with π . That is, the point \mathbf{x} is incident with the hyperplane π whenever $\mathbf{x}\pi = 0$.

When q is the power of an odd prime, $\frac{q-1}{2}$ of the nonzero elements of the Galois field \mathbb{F}_q are squares and $\frac{q-1}{2}$ are nonsquares. We will let \square and $\not\square$ respectively denote the set of nonzero squares and the set of nonsquares in \mathbb{F}_q . Throughout the main text of this thesis, we use η to denote a fixed but arbitrary nonsquare in \mathbb{F}_q .

An *oval* in a projective plane π of order q is a set of $q + 1$ points, no three collinear. Let P be a point on an oval o . Of the $q + 1$ lines through P , q are *secant* lines, meeting o in exactly one other point. The remaining line through P is the *tangent* line to o at P . It can be shown that when q is odd, each point of $\pi \setminus o$ is on 0 or 2 tangent lines. When q is even, one may show that there is a point N such that all tangent lines to o meet at N . That is, when q is even, an oval may be extended to a *hyperoval*, a set of $q + 2$ points, no three on a line.

A *quadric* \mathcal{Q} in $PG(n, q)$ is a set of points $\mathbf{x} = (x_0, x_1, \dots, x_n)$ satisfying a homogeneous quadratic equation

$$f(x_0, \dots, x_n) = \sum_{i=0}^n \sum_{j=i}^n a_{ij} x_i x_j = 0$$

for some $a_{ij} \in \mathbb{F}_q$ not all zero. Let $A = (a_{ij})$ be the upper triangular matrix such that $f(x_0, \dots, x_n) = \mathbf{x}A\mathbf{x}^T$, and let $B = A + A^T$. A point of \mathcal{Q} is a *singular point* provided $B\mathbf{x}^T = 0$ and $\mathbf{x}A\mathbf{x}^T = 0$. We say that the quadric \mathcal{Q} is *degenerate* (or singular) if it has a singular point.

In $PG(2, q)$, a nondegenerate quadric is a *conic*. Every conic is an example of an oval. When q is odd, the converse is true as well.

Theorem 2.1.1 (Segre) *Every oval in $PG(2, q)$, q odd, is a conic.*

Our primary interest is in quadrics in $PG(3, q)$. For a point \mathbf{x} on a nonsingular quadric \mathcal{Q} , define the *tangent hyperplane* to \mathcal{Q} at \mathbf{x} to be the hyperplane $\mathbf{x}^\perp := B\mathbf{x}^T$. It can be shown that in $PG(3, q)$, there are exactly two nonisomorphic nonsingular quadrics. When for all $\mathbf{x} \in \mathcal{Q}$, \mathbf{x}^\perp intersects \mathcal{Q} in more than just \mathbf{x} , it happens that $\mathbf{x}^\perp \cap \mathcal{Q}$ is the union of two lines which meet at \mathbf{x} . In this case, \mathcal{Q} is a *hyperbolic quadric*. The quadric \mathcal{Q} is an *elliptic quadric* if for each $\mathbf{x} \in \mathcal{Q}$, $\mathcal{Q} \cap \mathbf{x}^\perp = \mathbf{x}$. In this case, for each point \mathbf{x} of \mathcal{Q} , every line meeting \mathbf{x} and not contained in \mathbf{x}^\perp meets $\mathcal{Q} \setminus \{\mathbf{x}\}$ in exactly one point.

A set \mathcal{S} of points of $PG(3, q)$ is called an *ovoid* if it satisfies the following:

1. Each line meets \mathcal{S} in at most 2 points.
2. Each point of \mathcal{S} lies on exactly $q + 1$ tangent lines, all of which lie on a plane.

Let P be a point on an ovoid \mathcal{S} . Since P is on exactly $q + 1$ tangent lines, the remaining q^2 lines through P must meet \mathcal{S} in exactly one other point. Thus \mathcal{S} has exactly $q^2 + 1$ points.

A *k-cap* in $PG(3, q)$ is a set K of k points, no three on a line. We can think of *k-caps* as the convex objects in $PG(3, q)$. We can show that ovoids are examples of maximal *k-caps*.

Lemma 2.1.2 *If q is odd and K is a k -cap in $PG(3, q)$, then $k \leq q^2 + 1$.*

Proof: Let P and Q be points of K and consider a plane π on the line PQ . We claim that $|\pi \cap K| \leq q + 1$. The $q + 1$ lines of π meeting P each meet K in at most one other point, so $|\pi \cap K| \leq q + 2$. Suppose $|\pi \cap K| = q + 2$. If R

is a point of π not on K , then each line in π through R must meet K in 0 or 2 points. But this is not possible, since $q + 2$ is odd. Thus $|\pi \cap K| \leq q + 1$. Thus the planes on PQ contain at most $(q + 1)(q - 1) + 2$ points of K . ■

One may show that every $q^2 + 1$ -cap K has the property that for every point P of K there is a unique plane π_P such that $\pi_P \cap K = P$. That is, every $q^2 + 1$ -cap is an ovoid. We see from the definition that every elliptic quadric is an ovoid. When q is odd, the converse is true as well.

Theorem 2.1.3 (Barlotti, Panella) *When q is odd, every ovoid in $PG(3, q)$ is an elliptic quadric.*

Hence in $PG(3, q)$, q odd, the study of ovoids and of k -caps of maximum size is reduced to the study of elliptic quadrics. Further, all elliptic quadrics in $PG(3, q)$ are projectively equivalent. See Theorem 5.4.4 in [20] for proof of this fact. Thus the study of ovoids is reduced to the study of an essentially unique object for each odd prime power q .

2.2 An Elliptic Quadric

Let η be a nonsquare in \mathbb{F}_q , q odd, and let

$$E = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2\eta \end{bmatrix}.$$

Then

$$\mathcal{E} = \{\mathbf{x} = (x_0, x_1, x_2, x_3) : \mathbf{x}E\mathbf{x}^T = 0\}$$

is an elliptic quadric. An explicit representation of the points is

$$\mathcal{E} = \{(1, s^2 - \eta t^2, s, t) : s, t \in \mathbb{F}_q\} \cup \{(0, 1, 0, 0)\}.$$

For a point \mathbf{x} , the unique tangent plane to \mathcal{E} at \mathbf{x} is the plane $E\mathbf{x}^T$.

Using the explicit form, we may define addition and multiplication on the points of $\mathcal{E} \setminus \{(0, 1, 0, 0)\}$ by

$$(1, s^2 - \eta t^2, s, t) + (1, u^2 - \eta v^2, u, v) = (1, (s + u)^2 - \eta(t + v)^2, s + u, t + v) \quad (2.1)$$

and

$$(1, s^2 - \eta t^2, s, t)(1, u^2 - \eta v^2, u, v) = (1, (s^2 - \eta t^2)(u^2 - \eta v^2), su + \eta tv, sv + tu). \quad (2.2)$$

Note that $\{1, \sqrt{\eta}\}$ are a basis for \mathbb{F}_{q^2} over \mathbb{F}_q , that is, we may represent $\mathbb{F}_{q^2} = \{s + \sqrt{\eta}t : s, t \in \mathbb{F}_q\}$ and it is easy to show that

$$\theta : \mathbb{F}_{q^2} \rightarrow \mathcal{E} \setminus \{(0, 1, 0, 0)\}$$

$$\theta : s + \sqrt{\eta}t \mapsto (1, s^2 - \eta t^2, s, t)$$

is a field isomorphism, using operations defined above.

We claim that $\sqrt{\eta}^q = -\sqrt{\eta}$. The map $r \mapsto r^q$ on \mathbb{F}_{q^2} is a field automorphism fixing only $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$. Then $(s^2 - \eta t^2)^q = (s + \sqrt{\eta}^q t)(s - \sqrt{\eta}^q t)$. Thus $s^2 - \eta t^2 = \mathbb{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(s + \sqrt{\eta}t)$, where $\mathbb{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ is the relative norm from \mathbb{F}_{q^2} to \mathbb{F}_q . Given a fixed basis for the vector space \mathbb{F}_q^2 underlying $PG(1, q^2)$, we choose representatives for the points of the projective line so that $PG(1, q^2) = \{(1, a) : a \in \mathbb{F}_{q^2}\} \cup \{(0, 1)\}$.

We identify the points of \mathcal{E} with the points of $PG(1, q^2)$ by

$$(1, s^2 - \eta t^2, s, t) \leftrightarrow (1, s + \sqrt{\eta}t) \quad (2.3)$$

and

$$(0, 1, 0, 0) \leftrightarrow (0, 1) = (\infty). \quad (2.4)$$

Note that $s^2 - \eta t^2$ is a square in \mathbb{F}_q if and only if $s + \sqrt{\eta}t$ is a square in \mathbb{F}_q . To see this, let α be a primitive element of \mathbb{F}_{q^2} . Then α^{q+1} generates $\mathbb{F}_q^* \subseteq \mathbb{F}_{q^2}^*$. Suppose $s + \sqrt{\eta}t = \alpha^n$. Then $s^2 - \eta t^2 = (s + \sqrt{\eta}t)(s - \sqrt{\eta}t) = (\alpha^{q+1})^n$.

We will say that a point $P = (1, s^2 - \eta t^2, s, t)$ of \mathcal{E} is *square* if $s^2 - \eta t^2 \in \square$ and that P is a *nonsquare* if $s^2 - \eta t^2 \in \not\square$. We label the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$ with 0 and ∞ , respectively. Define

$$\mathcal{E}_{\square} = \{(1, s^2 - \eta t^2, s, t) : s^2 - \eta t^2 \in \square\} \quad (2.5)$$

and

$$\mathcal{E}_{\not\square} = \{(1, s^2 - \eta t^2, s, t) : s^2 - \eta t^2 \in \not\square\} \quad (2.6)$$

To better motivate our definition of \mathcal{E}_{\square} , consider the sphere \mathcal{Z} of radius 1 whose center is at the origin in \mathbb{R}^3 . Let $P = (0, 0, 1)$ and let Π be the plane $z = 0$. Define the map taking a point $Q = (x, y, z)$ on \mathcal{Z} to the

$$\begin{aligned} \rho : \mathcal{Z} \setminus \{P\} &\rightarrow \Pi \\ \rho : (x, y, z) &\mapsto \left(\frac{x}{1-z}, \frac{y}{1-z}, 0 \right). \end{aligned}$$

This is *stereographic projection* of $\mathcal{Z} \setminus \{P\}$ onto the xy plane. If we identify each point $(x, y, 0)$ with the complex number $x + yi$, we have identified the points of $\mathcal{Z} \setminus \{P\}$ with the complex numbers. Let

$$P\mathbb{C} = \{(1, \zeta) : \zeta \in \mathbb{C}\} \cup \{(0, 1)\}$$

be the complex projective line. Then the map

$$\begin{aligned}\bar{\rho} : \mathcal{Z} \setminus \{P\} &\rightarrow PC \\ \bar{\rho} : (x, y, z) &\mapsto \left(1, \frac{x}{1-z} + \frac{y}{1-z}i\right) \text{ for } z \neq 1 \\ \bar{\rho} : (0, 0, 1) &\mapsto (0, 1) = \infty\end{aligned}$$

identifies the points of \mathcal{Z} with the points of the complex projective line. The unit sphere, so identified with the extended complex numbers $\mathbb{C} \cup \infty$ is the *Riemann sphere*. The map $\bar{\rho}$ is analogous to our identification of the points of \mathcal{E} with the projective line $PG(1, q^2)$. Then the set of points

$$\mathcal{Z}_{\square} = \{(x, y, z) \in \mathcal{Z} \setminus \{P\} : z > 0\} \quad (2.7)$$

is analogous to \mathcal{E}_{\square} .

Although we will not require it later, we may make explicit the correspondence between the points of $\mathcal{E} \setminus \{\infty\}$ and the points of an affine plane. We project from $\infty = (0, 1, 0, 0)$ through the remaining points of \mathcal{E} to the plane $\pi = [0, 1, 0, 0]^T$. The line $\langle(0, 1, 0, 0), (1, s^2 - \eta t^2, s, t)\rangle$ meets π in the point $(1, 0, s, t)$. No points of \mathcal{E} are mapped to the line at infinity $\langle(0, 0, 1, 0), (0, 0, 0, 1)\rangle$ of π .

Let $l = \langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$. The tangent planes to \mathcal{E} at the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$ are $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$ respectively, which meet in the line $l^{\perp} = \langle(0, 0, 0, 1), (0, 0, 1, 0)\rangle$. The planes on l^{\perp} different from the tangents $[1, 0, 0, 0]^T$ and $[0, 1, 0, 0]^T$ are

$$V_{\mathcal{E}} = \{\pi_c = [1, -c^{-1}, 0, 0]^T : c \in \mathbb{F}_q^*\} \quad (2.8)$$

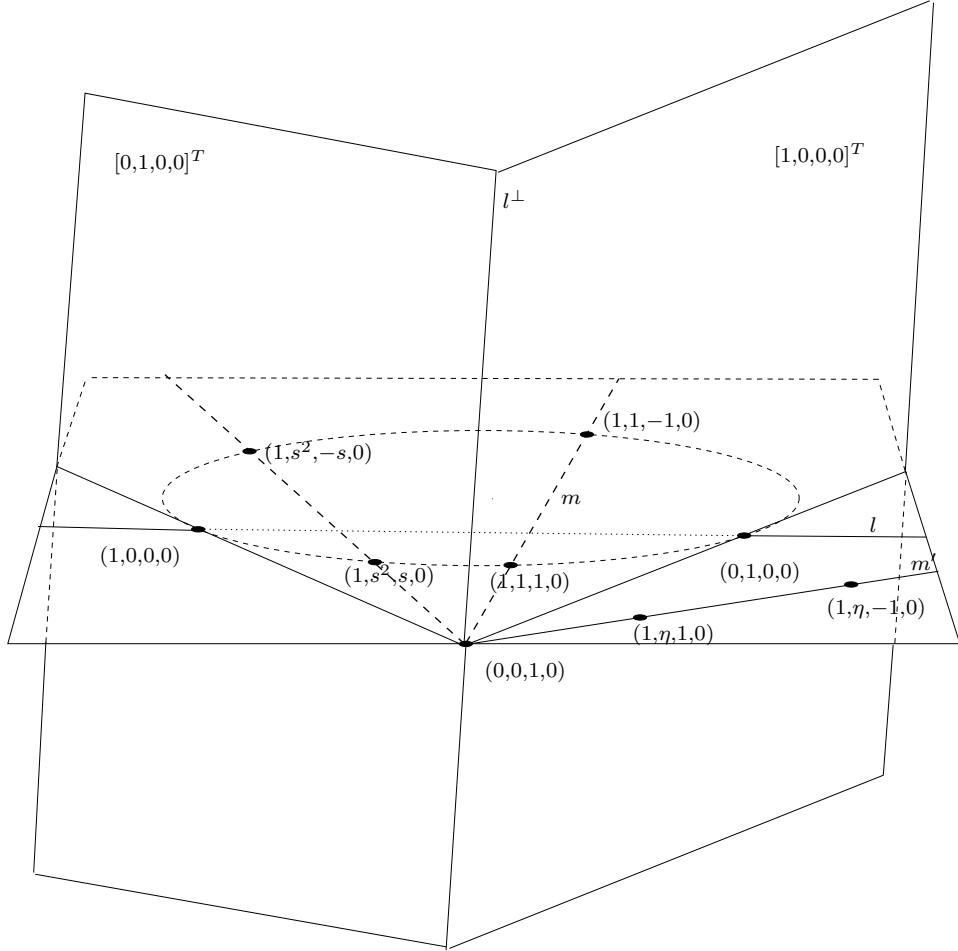


Figure 2.1: Tangent planes to \mathcal{E} and to \mathcal{H} at the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$ are the planes $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$, respectively. The oval $o = \{(1, s^2, s, 0) : s \in \mathbb{F}_q\} \cup \{(0, 1, 0, 0)\}$ in the plane $[0, 0, 0, 1]^T$ is the intersection of our chosen elliptic quadric \mathcal{E} with our chosen hyperbolic quadric \mathcal{H} . The lines l and l^\perp are both fixed by G_l . The planes in $V_{\mathcal{E}}$ all meet in the line l^\perp and the planes in $F_{\mathcal{E}}$ all meet in l .

each of which meets \mathcal{E} in the oval $\{(1, s^2 - \eta t^2, s, t) : s^2 - \eta t^2 = c\}$. This implies that for $c \in \mathbb{F}_q^*$, there are $q + 1$ pairs (u, v) such that $u^2 - \eta v^2 = c$. For future reference, define

$$V_{\mathcal{E}\square} = \{[1, -c^{-1}, 0, 0]^T : c \in \square\}$$

and

$$V_{\mathcal{E}\emptyset} = \{[1, -c^{-1}, 0, 0]^T : c \in \emptyset\}.$$

The planes on l are

$$F_{\mathcal{E}} = \{\alpha_a = [0, 0, 1, a]^T : a \in \mathbb{F}_q\} \cup \{\alpha_\infty = [0, 0, 0, 1]^T\}.$$

The plane α_∞ meets \mathcal{E} in the oval

$$o = \{(1, s^2, s, 0) : s \in \mathbb{F}_q\} \cup \{(0, 1, 0, 0)\} \quad (2.9)$$

and for the remaining planes in $F_{\mathcal{E}}$,

$$\alpha_a \cap \mathcal{E} = \{(1, s^2 - \eta t^2, s, t) : s = -ta\} \cup \{(0, 1, 0, 0)\}. \quad (2.10)$$

Note that if $(-ta)^2 - \eta t^2 = r^2$ then $(-vta)^2 - \eta(vt)^2 = (vr)^2$ and that both $(1, (-ta)^2 - \eta t^2, -ta, t)$ and $(1, (-vta)^2 - \eta(vt)^2, -vta, vt)$ are on α_a . It follows that, for $b \in \mathbb{F}_q$, the points of $\mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ on α_b are either all square or all nonsquare. As with $V_{\mathcal{E}}$, define a partition of $F_{\mathcal{E}}$ by

$$F_{\mathcal{E}\square} = \{\alpha_a : \alpha_a \cap \mathcal{E}\square \neq \emptyset\} \text{ and } F_{\mathcal{E}\emptyset} = \{\alpha_a : \alpha_a \cap \mathcal{E}\emptyset \neq \emptyset\}.$$

We refer to Figure 2.1 for a schematic of the relationship between the points of \mathcal{E} , $V_{\mathcal{E}}$, and $F_{\mathcal{E}}$.

2.3 A Ruled Quadric in $PG(3, q)$

We describe a particular hyperbolic quadric \mathcal{H} in $PG(3, q)$, with an emphasis on the geometric similarities \mathcal{H} has with \mathcal{E} . For a more complete description of hyperbolic quadrics in $PG(3, q)$, we refer to sections 6.1 and 6.2 of [20].

Put

$$H = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

and let

$$\mathcal{H} = \{\mathbf{x} : \mathbf{x}H\mathbf{x}^T = 0\} = \{\mathbf{x} : x_0x_1 - x_2^2 + x_3^2 = 0\}$$

The points may be described explicitly:

$$\begin{aligned} \mathcal{H} = & \{(1, s^2 - t^2, s, t) : s, t \in \mathbb{F}_q\} \cup \{(0, 1, s, s) : s \in \mathbb{F}_q^*\} \\ & \cup \{(0, 1, s, -s) : s \in \mathbb{F}_q^*\} \\ & \cup \{(0, 0, 1, 1), (0, 0, 1, -1), (0, 1, 0, 0)\}. \end{aligned}$$

\mathcal{H} contains the oval $o = \{(1, s^2, s, 0) : s \in \mathbb{F}_q\} \cup \{(0, 1, 0, 0)\}$ in the plane $[0, 0, 0, 1]^T$, in common with \mathcal{E} and indeed $\mathcal{H} \cap \mathcal{E} = o$. Let $l = \langle (1, 0, 0, 0), (0, 1, 0, 0) \rangle$ as in our description of \mathcal{E} . The line $l^\perp = \langle (0, 0, 1, 0), (0, 0, 0, 1) \rangle$ meets \mathcal{H} in the points $(0, 0, 1, 1)$ and $(0, 0, 1, -1)$, and the planes $[1, 0, 0, 0]^T$ and $[0, 1, 0, 0]^T$ on l^\perp are tangent at the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$ respectively. The remaining planes on l^\perp are $V_{\mathcal{H}} = \{\pi_c = [1, -c^{-1}, 0, 0]^T : c \in \mathbb{F}_q^*\}$, each of which meet \mathcal{H} in the $q + 1$ points of an oval. In particular,

$$\mathcal{H} \cap \pi_c = \{(1, s^2 - t^2, s, t) : s^2 - t^2 = c\} \cup \{(0, 0, 1, 1), (0, 0, 1, -1)\}. \quad (2.11)$$

Let P be a point of \mathcal{H} that is not on $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$. Then P has the form $(1, a^2 - b^2, a, b)$ for some $a, b \in \mathbb{F}_q$, $a \neq \pm b$. We say that P is *square* if $a^2 - b^2 \in \square$, and *nonsquare* if $a^2 - b^2 \in \not\square$. Now define partitions of $V_{\mathcal{H}}$ and $F_{\mathcal{H}}$ by

$$V_{\mathcal{H}\square} = \{[1, -c^{-1}, 0, 0]^T : c \in \square\} \text{ and } V_{\mathcal{H}\not\square} = \{[1, -c^{-1}, 0, 0]^T : c \in \not\square\}.$$

and

$$\mathbb{F}_{\mathcal{H}\square} = \{\alpha_a : \alpha_a \cap \mathcal{H}\square \neq \emptyset\} \text{ and } \mathbb{F}_{\mathcal{H}\not\square} = \{\alpha_a : \alpha_a \cap \mathcal{H}\not\square \neq \emptyset\}.$$

Then the square points of \mathcal{H} are all on the planes of $V_{\mathcal{H}\square}$ and are all on the planes of $F_{\mathcal{H}\square}$ and the nonsquare points of \mathcal{H} are all on the planes of $V_{\mathcal{H}\not\square}$ and are all on the planes of $F_{\mathcal{H}\not\square}$. The reasoning is the same as with that for \mathcal{E} in the previous section.

3. The Actions of Two-Point Stabilizers

In this chapter, we will determine the actions of the stabilizers of the truncated quadrics \mathcal{E}_\square and \mathcal{H}_\square on the planes of $PG(3, q)$. This will reduce our problem of finding cardinalities of plane intersections with the quadrics to one involving relatively few orbit types.

3.1 The Stabilizer of Two Points of \mathcal{E}

In section 6.4 of [20], the stabilizer in $GL(4, q)$ of the elliptic quadric \mathcal{E} is found to be the group G generated by

$$\{[\tau_{a,b}]\} = \left\{ \left[\begin{array}{cccc} 1 & a^2 - \eta b^2 & a & b \\ 0 & 1 & 0 & 0 \\ 0 & 2a & 1 & 0 \\ 0 & -2\eta b & 0 & 1 \end{array} \right] : a, b \in \mathbb{F}_q \right\}$$

$$\{[\varphi_{a,b}]\} = \left\{ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & a^2 - \eta b^2 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & \eta b & a \end{array} \right] : a, b \in \mathbb{F}_q, (a, b) \neq (0, 0) \right\},$$

$$N = \left[\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \quad M = \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{array} \right].$$

Recall the identification of the points of \mathcal{E} with the points of $PG(1, q^2)$ given in equations 2.3 and 2.4. We note simply that the set $\{[\tau_{a,b}]\}$ is a group isomorphic to the additive group of \mathbb{F}_{q^2} fixing $(0, 1, 0, 0) = (\infty)$, and $\{[\varphi_{a,b}]\}$ is a group isomorphic to the multiplicative group of \mathbb{F}_{q^2} fixing $(1, 0, 0, 0) = 0$ and $(0, 1, 0, 0)$. The element N interchanges 0 and (∞) , and it is easy to show that G is 3-transitive on the points of \mathcal{E} . It is possible to show that G' , the commutator subgroup of G is isomorphic to $PSL(2, q^2)$. We refer to Chapter 12 of [24] for details.

Henceforth, we drop the brackets and write $\varphi_{a,b}$ for the matrix $[\varphi_{a,b}]$.

The stabilizer of the pair of points $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ is the group G_l generated by M, N and $\{\varphi_{a,b}\}$. Note that the points of $\mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ are the nonzero elements of \mathbb{F}_{q^2} under the isomorphism θ . The group G stabilizing the elliptic quadric contains $PSL(2, q^2)$ as a subgroup. See p. 190 of [24] for a proof.

Observe that $\{\varphi_{a,b}\}$ and $M\{\varphi_{a,b}\}M$ form distinct subgroups of G_l , each of order $q^2 - 1$ and which intersect in $\{\varphi_{a,b} : a^2 - \eta b^2 = 1\}$, a subgroup of order $q + 1$. Thus $\langle \{\varphi_{a,b}\}, M\{\varphi_{a,b}\}M \rangle$ is a group of order $\frac{(q^2-1)^2}{q+1} = (q+1)(q-1)^2$. The element N normalizes $\langle \{\varphi_{a,b}\}, M\{\varphi_{s,t}\}M \rangle$ and thus G_l is a group of order $2(q+1)(q-1)^2$. Note that $A = \{a^2 I : a \in \mathbb{F}_q^*\}$ is a subgroup of G_l fixing all points. Consider the line $m = \langle (1, 1, 1, 0), (1, 1, -1, 0) \rangle$ secant to \mathcal{E} . The element $\varphi_{s,t}$ takes m to $\langle (1, s^2 - \eta t^2, s, t), (1, s^2 - \eta t^2, -s, -t) \rangle$, so the orbit of m under G_l has order at least $\frac{q^2-1}{2}$. On the other hand, m is stabilized by $G_m = \langle M, N, A, \varphi_{-1,0} \rangle \leq G_l$, a group of order $4(q-1)$, so $\{(1, s^2 - \eta t^2, s, t), (1, s^2 - \eta t^2, -s, -t) : (s, t) \neq (0, 0)\}$ constitutes the entire

orbit of $\{(1, 1, 1, 0), (1, 1, -1, 0)\}$, under the action of G_l .

Similarly, we see that the line $m' = \langle (1, \eta, 1, 0), (1, \eta, -1, 0) \rangle$ is exterior to \mathcal{E} and is in an orbit of size $\frac{q^2-1}{2}$ under G_l .

3.2 Orbits of Planes Under G_l

Let $\mathcal{L}_\mathcal{E}^\cap$ be the set of lines in the orbit of m under G_l and let $\mathcal{L}_\mathcal{E}^\not\cap$ be the orbit of m' under G_l . Choose $\omega \neq 0$ and consider the plane $[1, -1, 0, \omega]^T$ containing m . It is easy to check that under the stabilizer in G_l of m , the orbit of $[1, -1, 0, \omega]^T$ is $\{[1, -1, 0, \pm\omega]^T\}$, and that the orbit under the action of the stabilizer of m' of $[1, -\eta^{-1}, 0, \omega]^T$ is $\{[1, -\eta^{-1}, 0, \pm\omega]^T\}$. Define $\mathcal{T}_\mathcal{E}$ to be the set of lines generated by one of $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ and a point of l^\perp . It is straightforward to show that G_l acts transitively on the points of l^\perp , and that l^\perp is fixed by G_l . Because $N \in G_l$ interchanges $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$, it follows that $\mathcal{T}_\mathcal{E}$ is a single orbit of lines under G_l .

Theorem 3.2.1 *The orbits of planes of $PG(3, q)$ under the action of G_l , the stabilizer of $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ are as follows:*

1. *The two tangent planes $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$ to \mathcal{E} at $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$, respectively.*
2. *The set of $q^2 - 1$ planes tangent to $\mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$.*
3. *The $q - 1$ planes $V_\mathcal{E} = \{\pi_c = [1, -c^{-1}, 0, 0]^T : c \in \mathbb{F}_q^*\}$.*
4. *The $q + 1$ planes $F_\mathcal{E} = \{\gamma_{a,b} = [0, 0, a, b]^T : a, b \in \mathbb{F}_q\}^1$.*

¹ *We shall see that this is a useful way to represent these planes*

5. The planes not tangent to \mathcal{E} and meeting \mathcal{E} in exactly one of $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ form an orbit of size $2(q^2 - 1)$. These are the planes which are not tangent to \mathcal{E} and not in $F_{\mathcal{E}}$ and which contain a line of $\mathcal{T}_{\mathcal{E}}$. Call this orbit $\mathcal{O}_{\mathcal{E}}^*$.
6. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{E}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ of size $q^2 - 1$ such that $[1, -1, 0, \omega]^T \in \mathcal{O}_{\mathcal{E}}^{\omega \cap}$. These are the planes not in $F_{\mathcal{E}}$ or $V_{\mathcal{E}}$ containing a single line of $\mathcal{L}_{\mathcal{E}}^{\cap}$. Call this orbit $\mathcal{O}_{\mathcal{E}l}$.
7. The $\frac{q-3}{2}$ orbits $\mathcal{O}_{\mathcal{E}}^{\omega \cap'}$, $\omega \in \mathbb{F}_q^*$ of size $q^2 - 1$ such that $[1, -\eta^{-1}, 0, \omega]^T \in \mathcal{O}_{\mathcal{E}}^{\omega \cap'}$, $\omega \neq \pm 2$. These are the planes not in $F_{\mathcal{E}}$ or $V_{\mathcal{E}}$ and not tangent to \mathcal{E} which contain a single line of $\mathcal{L}_{\mathcal{E}}^{\cap'}$.

Proof: The stabilizer G_l of $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ is transitive on

$$\mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$$

and therefore on the tangent planes to the points different from $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ as well. The lines $l = \langle (1, 0, 0, 0), (0, 1, 0, 0) \rangle$ and $l^\perp = \langle (0, 0, 1, 0), (0, 0, 0, 1) \rangle$ are fixed by G_l and it is easy to check that the group is transitive on the sets $V_{\mathcal{E}}$ and $F_{\mathcal{E}}$.

The subgroup of G_l fixing $(0, 1, 0, 0)$ is generated by M and $\{\varphi_{a,b}\}$ and is seen to be transitive on the points of l^\perp . The stabilizer in $\langle M, \{\varpi_{a,b}\} \rangle$ of the plane $[0, 0, 0, 1]^T$ contains all elements $[\varphi_{s,0}]$, $s \in \mathbb{F}_q^*$, and $[\varphi_{s,0}][1, 0, 0, c]^T = [1, 0, 0, sc]^T$, so G_l is transitive on planes of the set $\mathcal{O}_{\mathcal{E}}^*$ which contain $(0, 1, 0, 0)$. Finally, N interchanges $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$, so the planes in $\mathcal{O}_{\mathcal{E}}^*$ form a single orbit.

Each line of $\mathcal{L}_{\mathcal{E}}^{\cap}$ is in exactly one plane of $F_{\mathcal{E}}$ and in exactly one plane of $V_{\mathcal{E}}$. The matrix M stabilizes m and interchanges $[1, -1, 0, \omega]^T$ and $[1, -1, 0, -\omega]^T$.

Since G_l is transitive on $\mathcal{L}_\mathcal{E}^\cap$, $\mathcal{O}_\mathcal{E}^{\omega^\cap}$ has order at least $q^2 - 1$. The stabilizer of m contains A , the matrix MN and $[\varphi_{-1,0}]$ which generate a group of order $2(q-1)$ which fixes $[1, -1, 0, \omega]^T$. Thus $\mathcal{O}_\mathcal{E}^{\omega^\cap}$ is an orbit of size $q^2 - 1$ and there are $\frac{q-1}{2}$ such orbits.

Similarly, the orbit $\mathcal{L}_\mathcal{E}^{\cap'}$ under G_l of m' gives $\frac{q-1}{2}$ orbits of size $q^2 - 1$. We check whether a plane in an orbit $\mathcal{O}_\mathcal{E}^{\omega^{\cap'}}$ can be a tangent plane, that is, whether $(1, -\eta^{-1}, 0, \omega)E \in \mathcal{E}$. We find that when $\omega = \pm 2$, the planes are tangent to the respective points $(1, -\eta, 0, \pm 1)$. The remaining $\frac{q-3}{2}$ orbits are each of size $q^2 - 1$.

The total number of planes accounted for by the union of these orbits is $q^3 + q^2 + q + 1$ which is all of the planes in $PG(3, q)$. ■

3.3 The Group Stabilizing Two Points of \mathcal{H}

We turn now to the hyperbolic quadric \mathcal{H} defined in Section 2.3. We seek similarities between \mathcal{H} and \mathcal{E} in terms of the stabilizers in each case of the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$.

The stabilizer in $PGO^+(4, q)$ of the pair $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ contains the group generated by the matrices

$$N = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

and the set

$$\{\varpi_{a,b}\} = \left\{ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & a^2 - b^2 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & b & a \end{array} \right] : a^2 - b^2 \neq 0 \right\}.$$

Let $K = \langle \{\varpi_{a,b}\} \rangle$. Note first that $|\{\varpi_{a,b}\}| = (q-1)^2$ and that N does not normalize K , and the intersection of K and NKN consists of the $\varpi_{a,b}$ such that $a^2 - b^2 = 1$. We see that the plane π_1 meets \mathcal{H} in the oval $\{(1, a^2 - b^2, a, b) : a^2 - b^2 = 1\} \cup \{(0, 0, 1, 1), (0, 0, 1, -1)\}$, which implies that $a^2 - b^2 = 1$ has $q-1$ solutions (a, b) . Thus the group $H_K = \langle K, NKN \rangle$ has order $\frac{(q-1)^2(q-1)^2}{q-1} = (q-1)^3$, and $|\langle N, K, NKN \rangle| = 2(q-1)^3$. The group H_K is normalized by the matrix M , so that $\langle M, N, K \rangle$ is a matrix group of order $4(q-1)^3$, and H_K contains the scalar matrices a^2I and Na^2I , $a \in \mathbb{F}_q^*$, and these are the only elements of this group which act as the identity on all points of π_1 . Thus the group of homographies in $PGL(3, q)$ fixing \mathcal{H} and stabilizing $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ has at least $4(q-1)^2$ elements. In chapter 6, section 1 of [20], it is shown that the complete group of homographies of the hyperbolic quadric in $PG(3, q)$, denoted $PGO^+(4, q)$, has order $2(q^3 - q)^2$, so we wish to show that the orbit of $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ has order $\frac{1}{2}(q+1)^2q^2$. The stabilizer in $PGO^+(4, q)$ of the point $(0, 1, 0, 0)$ contains a subgroup generated by matrices

$$\{B_a\} = \left\{ \left[\begin{array}{cccc} 1 & 0 & \frac{a}{2} & \frac{a}{2} \\ 0 & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & -a & 0 & 1 \end{array} \right] : a \in \mathbb{F}_q \right\}$$

and

$$\{C_a\} = \left\{ \begin{bmatrix} 1 & 0 & \frac{a}{2} & -\frac{a}{2} \\ 0 & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & a & 0 & 1 \end{bmatrix} : a \in \mathbb{F}_q \right\}$$

which contains $\{\varpi_{a,b}\}$ and is seen to be transitive on points of \mathcal{H} not on the tangent plane $(0, 1, 0, 0)^\perp$. The matrix N interchanges $(0, 1, 0, 0)$ and $(1, 0, 0, 0)$ and we find that $PGO^+(4, q)$ acts transitively on points of \mathcal{H} and on pairs $\{P, Q\}$ of points such that $P \notin Q^\perp$. There are $\frac{1}{2}(q+1)^2q^2$ such pairs, and we conclude that the complete stabilizer of two points of \mathcal{H} not on a line contained in \mathcal{H} has order $4(q-1)^2$. Thus, when working with the stabilizer of $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$, it is sufficient to use the matrix group of order $4(q-1)^3$ generated by M , N and $\{\varpi_{a,b}\}$. Call this group H_l .

Now consider the line $m = \langle(1, 1, 1, 0), (1, 1, -1, 0)\rangle$ secant to \mathcal{H} . The element $\varpi_{a,b}$ takes m to $\langle(1, a^2-b^2, a, b), (1, a^2-b^2, -a, -b)\rangle$. Let $\mathcal{L}_{\mathcal{H}}^\cap$ be the lines in the orbit of m under H_l . Let $\mathcal{L}_{\mathcal{H}}^\cap$ be the orbit of $m' = \langle(1, \eta, 1, 0), (1, \eta, -1, 0)\rangle$. The lines in $\mathcal{L}_{\mathcal{H}}^\cap$ and $\mathcal{L}_{\mathcal{H}}^\cap$ are those on the intersections of planes in $F_{\mathcal{H}}$ with some plane of $V_{\mathcal{H}}$. Let $\mathcal{T}_{\mathcal{H}}$ be the lines on one of $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$ and on a point of $l^\perp \setminus \{(0, 0, 1, 1), (0, 0, 1, -1)\}$. Let $\mathcal{T}_{\mathcal{H}}^\perp$ be the set of lines generated by one of $(0, 0, 1, 1)$ or $(0, 0, 1, -1)$ and a point of $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$. Our next theorem describes the action of H_l on the planes of $PG(3, q)$.

Theorem 3.3.1 *The orbits of planes under the action of H_l are as follows:*

1. The tangent planes $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$ to \mathcal{H} at the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$, respectively, form an orbit of size 2.
2. The tangent planes $[0, 0, 1, -1]^T$ and $[0, 0, 1, 1]^T$ to \mathcal{H} at the points $(0, 0, 1, 1)$ and $(0, 0, 1, -1)$, respectively, form an orbit of size 2.
3. The planes $V_{\mathcal{H}} = \{\pi_c\} = \{[1, -c^{-1}, 0, 0]^T : c \in \mathbb{F}_q^*\}$, form an orbit of size $q - 1$.
4. The planes $F_{\mathcal{H}}$ on the line $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$ distinct from $[0, 0, 1, 1]^T$ and $[0, 0, 1, -1]^T$ form an orbit of size $q - 1$.
5. The planes containing exactly one line of $\mathcal{T}_{\mathcal{H}}$ form a single orbit of size $2(q - 1)^2$. Call this orbit $\mathcal{O}_{\mathcal{H}d}$.
6. The planes containing exactly one line of $\mathcal{T}_{\mathcal{H}}^\perp$ form a single orbit of size $2(q - 1)^2$. Call this orbit $\mathcal{O}_{\mathcal{H}d}^\perp$.
7. The planes on exactly one of the lines $\langle(1, 0, 0, 0), (0, 0, 1, 1)\rangle$, $\langle(0, 1, 0, 0), (0, 0, 1, 1)\rangle$, $\langle(0, 1, 0, 0), (0, 0, 1, -1)\rangle$, or $\langle(1, 0, 0, 0), (0, 0, 1, -1)\rangle$ form an orbit $\mathcal{O}_{\mathcal{H}c}^\circ$ of size $4(q - 1)$.
8. The single orbit $\mathcal{O}_{\mathcal{H}c}^{2\cap}$ of tangent planes to points of \mathcal{H} not on $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$.
9. The $\frac{q-3}{2}$ orbits $\mathcal{O}_{\mathcal{H}c}^{\omega\cap}$, $\omega \in \mathbb{F}_q^*$, $\omega \neq \pm 2$, of size $(q - 1)^2$ such that $[1, -1, 0, \omega] \in \mathcal{O}_{\mathcal{H}c}^{\omega\cap}$.
10. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{H}c}^{\omega\cap'}$, $\omega \in \mathbb{F}_q^*$ of size $(q - 1)^2$ such that $[1, -\eta^{-1}, 0, \omega] \in \mathcal{O}_{\mathcal{H}c}^{\omega\cap'}$.

Proof: H_l stabilizes both l and l^\perp , so the first four sets are seen to be orbits, as H_l is transitive on each of these sets. For items 5 and 6, we need to show that H_l acts transitively on the indicated sets of planes. For item 5, note that $\{\varpi_{a,b}\}$ fixes $(1, 0, 0, 0)$ and is transitive on points of $l^\perp \setminus \{(0, 0, 1, 1), (0, 0, 1, -1)\}$. Then we see that $\varpi_{\delta^{-1}, 0}$ takes the plane $[0, 1, 1, 0]^T$ on $\langle(1, 0, 0, 0), (0, 0, 0, 1)\rangle$ to $[0, 1, \delta, 0]$. Thus the planes containing exactly one line of $\mathcal{T}_{\mathcal{H}}$ form a single orbit. Item 6 is handled similarly.

For the orbit $\mathcal{O}_{\mathcal{H}}^\circ$, observe that H_l is transitive on the 4 lines described and since the pairs $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ and $\{(0, 0, 1, 1), (0, 0, 1, -1)\}$ each are orbits, these 4 lines form a single orbit. Note that $\varpi_{\delta^{-1}, 0}$ takes the plane $[0, 1, 1, -1]^T$ on $\langle(1, 0, 0, 0), (0, 0, 1, 1)\rangle$ to $[0, 1, \delta, -\delta]^T$. Thus H_l is transitive on all planes in the set $\mathcal{O}_{\mathcal{H}}^\circ$, and the remaining planes on the 4 lines in the statement are tangents to \mathcal{H} whose orbits are described in 1 and 2, so $\mathcal{O}_{\mathcal{H}}^\circ$ is a single orbit.

For the orbits in 9, recall that H_l is transitive on lines $\langle(1, a^2 - b^2, a, b), (1, a^2 - b^2, -a, -b)\rangle$, $(a, b) \neq (0, 0)$ and that the stabilizer of $\langle(1, 1, 1, 0), (1, 1, -1, 0)\rangle$ is generated by $M, N, \varpi_{-1, 0}$ and A and so the orbit under this group of a representative plane, say $[1, -1, 0, \omega]^T$, $\omega \neq 0$ contains only itself and $[1, -1, 0, -\omega]^T$, giving the stated orbit size. Now check that $(1, -1, 0, \omega)H = (1, -1, 0, -2\omega)$ is a point on \mathcal{H} iff $\omega = \pm \frac{1}{2}$.

As H_l acts transitively on the points of $\mathcal{H} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$, it also acts transitively on the corresponding tangent planes.

The lines $\mathcal{L}_{\mathcal{H}}^{\not\circ}$ form a single orbit under H_l , as $\{(0, 0, 1, 1), (0, 0, 1, -1)\}$ and the points of $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ form orbits of points, and the stabilizer of $(0, 0, 1, 1)$ contains the set $\{\varpi_{a,b}\}$, which is transitive on the

points of $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$. It is straightforward to check that for each $c \in \mathbb{F}_q^*$, the set $\{\varpi_{a,b} : a^2 - b^2 = 1\}$ contains an element $\varpi_{a,b}$ such that $a - b = c$, so that this set is transitive on planes $[0, 1, \omega, -\omega]^T$ on the line $\langle(1, 0, 0, 0), (0, 0, 1, 1)\rangle$. \blacksquare

3.4 Point Sets Associated with Squares

In this section, we define the subsets of the points of \mathcal{E} and \mathcal{H} corresponding under the partitions induced by the planes in $V_{\mathcal{E}}$ and $V_{\mathcal{H}}$ which correspond to the nonzero squares in \mathbb{F}_q . These subsets are the truncated quadrics \mathcal{E}_{\square} and \mathcal{H}_{\square} .

3.4.1 The Square Points of \mathcal{E}

The group G_l contains a subgroup $G_{l_{\square}}$ of index 2 generated by M , N and $\{[\varphi_{a,b}] : a^2 - \eta b^2 \in \square\}$. Choose $\varphi_{c,d}$ such that $c^2 - \eta d^2 = \eta$, and note that $G_l = G_{l_{\square}} \cup \varphi_{c,d} G_{l_{\square}}$. We will be interested in a set of points stabilized by $G_{l_{\square}}$ and acted regularly upon by $\{\varphi_{a,b} : a^2 - \eta b^2 \in \square\}$, namely

$$\mathcal{E}_{\square} = \{(1, s^2 - \eta t^2, s, t) : s^2 - \eta t^2 \in \square\}. \quad (3.1)$$

We can view a point $(1, s^2 - \eta t^2, s, t) \in \mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ as being either *square* or *nonsquare* depending upon whether $s^2 - \eta t^2$ is square or nonsquare. Similarly, a line $\langle(1, s^2 - \eta t^2, s, t), (1, s^2 - \eta t^2, -s, -t)\rangle \in \mathcal{L}_{\mathcal{E}}$ in the orbit of m meets \mathcal{E} in two points, both of which are either square or nonsquare. The lines in the orbit of m are all the secant lines to \mathcal{E} which contain a single point of l^{\perp} .

A plane $[0, 0, a, b]^T \in F_{\mathcal{E}}$ meets \mathcal{E} in the $q + 1$ points

$$\{(1, u, c, d) : u = c^2 - \eta d^2 \text{ and } c/d = -b/a\} \cup \{(1, 0, 0, 0), (0, 1, 0, 0)\}$$

and we see that for a particular choice of plane in $F_{\mathcal{E}}$, u is either always a square or always a nonsquare, so there are two orbits of planes in $\mathbb{F}_{\mathcal{E}}$ under $G_{l_{\square}}$. Each plane of $F_{\mathcal{E}}$ meets l^{\perp} in a single point, so there are two orbits of points of l^{\perp} under $G_{l_{\square}}$ as well. It is also easy to show that there are two orbits of planes in $V_{\mathcal{E}}$ under $G_{l_{\square}}$ and since each plane of $V_{\mathcal{E}}$ meets l in a unique point, there are 3 orbits of points of l , including $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$. The orbit $\mathcal{L}_{\mathcal{E}}^{\square}$ of m under G_l splits into two orbits $\mathcal{L}_{\mathcal{E}_{\square}}^{\square}$ and $\mathcal{L}_{\mathcal{E}_{\square}}^{\square}$ under the action of $G_{l_{\square}}$. Similarly, the orbit $\mathcal{L}_{\mathcal{E}}^{\square}$ splits into two orbits $\mathcal{L}_{\mathcal{E}_{\square}}^{\square}$ and $\mathcal{L}_{\mathcal{E}_{\square}}^{\square}$. Let $F_{\mathcal{E}}$ be as defined in Theorem 3.2.1. Each plane $[0, 0, a, b]^T \in F_{\mathcal{E}}$ contains $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ and the $q - 1$ points $\{(1, c^2 - \eta d^2, c, d) : ca + bd = 0\}$ of \mathcal{E} . Because $c^2 - \eta d^2 \in \square$ iff $(rc)^2 - \eta(rd)^2 \in \square$, we see that a plane in $F_{\mathcal{E}}$ meets \mathcal{E}_{\square} in $q - 1$ points, or it meets $\mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ in $q - 1$ points. Call a plane of $F_{\mathcal{E}}$ square if it meets \mathcal{E}_{\square} and nonsquare otherwise. That is, put $F_{\mathcal{E}_{\square}} = \{\alpha \in F_{\mathcal{E}_{\square}} : \alpha \cap \mathcal{E}_{\square} \neq \emptyset\}$ and $F_{\mathcal{E}_{\square}} = \{\alpha \in F : \alpha \cap \mathcal{E}_{\square} = \emptyset\}$. The orbits of planes of $PG(3, q)$ are bipartitions of the orbits under G_l , with the exception of $\{[1, 0, 0, 0]^T, [0, 1, 0, 0]^T\}$, which remains an orbit under the action of $G_{l_{\square}}$.

Theorem 3.4.2 *The orbits of planes of $PG(3, q)$ under the action of $G_{l_{\square}}$ are as follows:*

1. *The tangent planes $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$ to $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$ form an orbit of size 2.*
2. *The set of $\frac{q^2-1}{2}$ tangent planes to \mathcal{E}_{\square} form a single orbit.*
3. *The set of $\frac{q^2-1}{2}$ tangent planes to \mathcal{E}_{\square} form a single orbit.*

4. The planes $V_{\mathcal{E}\square} = \{[1, -c^{-1}, 0, 0]^T : c \in \square \in \mathbb{F}_q^*\}$ form an orbit of size $\frac{q-1}{2}$.
5. The planes $V_{\mathcal{E}\varnothing} = \{[1, -c^{-1}, 0, 0]^T : c \in \varnothing \in \mathbb{F}_q^*\}$ form an orbit of size $\frac{q-1}{2}$.
6. $F_{\mathcal{E}\square}$, the $\frac{q+1}{2}$ square planes of $F_{\mathcal{E}}$ form a single orbit.
7. $F_{\mathcal{E}\varnothing}$, the $\frac{q+1}{2}$ nonsquare planes of $F_{\mathcal{E}}$ form a single orbit.
8. The planes not tangent to \mathcal{E} and meeting \mathcal{E} in exactly one of $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ and containing a line in a plane of $F_{\mathcal{E}\square}$ form an orbit of size $q^2 - 1$. Call this orbit $\mathcal{O}_{\mathcal{E}\square}$.
9. The planes not tangent to \mathcal{E} and meeting \mathcal{E} in exactly one of $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ and containing a line in a plane of $F_{\mathcal{E}\varnothing}$ form an orbit of size $q^2 - 1$. Call this orbit $\mathcal{O}_{\mathcal{E}\varnothing}$.
10. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$, for some $\omega \in \mathbb{F}_q^*$ of size $\frac{q^2-1}{2}$ such that

$$\alpha_{\omega} = [1, -1, 0, \omega]^T \in \mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$$

and is on a line of $\mathcal{L}_{\mathcal{E}}^{\cap}$ in a plane of $F_{\mathcal{E}\square}$. From the $q-1$ planes on a line in $\mathcal{L}_{\mathcal{E}\square}^{\cap}$ and not in $V_{\mathcal{E}}$ or $F_{\mathcal{E}}$, one may choose 2 representatives of each orbit.

11. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$, for some $\omega \in \mathbb{F}_q^*$ of size $\frac{q^2-1}{2}$ which consist of planes containing one line in $\mathcal{L}_{\mathcal{E}\square}^{\cap}$. From the $q-1$ planes on a line in $\mathcal{L}_{\mathcal{E}\square}^{\cap}$ and not in $V_{\mathcal{E}}$ or $F_{\mathcal{E}}$, one may choose 2 representatives of each orbit.
12. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{E}\varnothing}^{\omega\cap}$, for some $\omega \in \mathbb{F}_q^*$ of size $\frac{q^2-1}{2}$ which consist of planes containing one line in $\mathcal{L}_{\mathcal{E}\varnothing}^{\cap}$. From the $q-1$ planes on a line in $\mathcal{L}_{\mathcal{E}\varnothing}^{\cap}$ and not in $V_{\mathcal{E}}$ or $F_{\mathcal{E}}$, one may choose 2 representatives of each orbit.

13. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{E}\square}^{\omega\eta}$, for some $\omega \in \mathbb{F}_q^*$ of size $\frac{q^2-1}{2}$ which consist of planes containing one line in $\mathcal{L}_{\mathcal{E}\square}^{\eta}$. From the $q-1$ planes on a line in $\mathcal{L}_{\mathcal{E}\square}^{\eta}$ and not in $V_{\mathcal{E}}$ or $F_{\mathcal{E}}$, one may choose 2 representatives of each orbit.

Proof: Based on Theorem 3.2.1 and the discussion preceding the statement of the theorem, it is straightforward to verify the assertions. ■

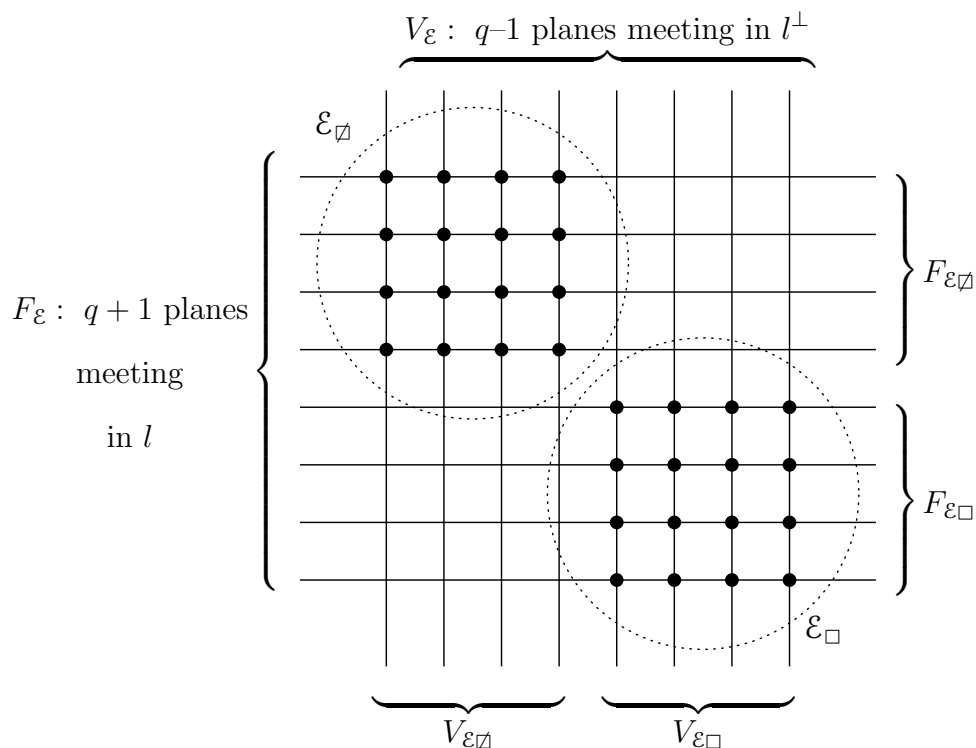


Figure 3.1: A diagram of the elliptic quadric from the point of view of the stabilizer of two points.

Figure 3.1 is a diagram of \mathcal{E} from the point of view of the stabilizer G_l of $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$. The horizontal lines represent planes in $F_{\mathcal{E}}$, and the vertical lines represent planes in $V_{\mathcal{E}}$. The planes $V_{\mathcal{E}}$ meet in $l^{\perp} = \langle (0, 0, 1, 1), (0, 0, 1, -1) \rangle$ and the planes $F_{\mathcal{E}}$ meet in $l = \langle (1, 0, 0, 0), (0, 1, 0, 0) \rangle$. The points of $\mathcal{E} \setminus \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ are on the lines in orbits $\mathcal{L}_{\mathcal{E}}^{\eta} = V_{\mathcal{E}\square} \cap F_{\mathcal{E}\square}$

and $\mathcal{L}_{\mathcal{E}}^{\not\cap} = V_{\mathcal{E}\not\cap} \cap F_{\mathcal{E}\not\cap}$ under the action of $G_{l_{\square}}$. Each dot represents a line of $\mathcal{L}_{\mathcal{E}}^{\cap}$ containing a pair of points $(1, a^2 - \eta b^2, a, b)$, $(1, a^2 - \eta b^2, -a, -b)$, $(a, b) \neq (0, 0)$. The intersections without dots represent the lines in the orbit of $m' = \langle (1, \eta, 1, 0), (1, \eta, -1, 0) \rangle$, $\mathcal{L}_{\mathcal{E}}^{\not\cap}$ under G_l . Under the action of $G_{l_{\square}}$, the four quadrants of the grid each represent an orbit of lines. Each of these four orbits of lines carries orbits of planes distinct from $F_{\mathcal{E}}$ and $V_{\mathcal{E}}$. In the next chapter, we will study how the planes in an orbit carried by an orbit of lines in a quadrant of the grid meet \mathcal{E}_{\square} . We will see that it is sufficient to study planes in orbits of the type $\mathcal{O}_{\mathcal{E}_{\square}}^{\omega\cap}$ and in orbits of the type $\mathcal{O}_{\mathcal{E}_{\square}}^{\omega\not\cap}$.

3.4.3 The Square Points of \mathcal{H}

Let $\mathcal{H}_{\square} = \{(1, s^2 - t^2, s, t) : s^2 - t^2 \in \square\}$, the subset of \mathcal{H} analogous to $\mathcal{E}_{\square} \subseteq \mathcal{E}$. That is, \mathcal{H}_{\square} is the set of points of \mathcal{H} corresponding to the set of all (a, b) such that $a^2 - b^2$ is a nonzero square. The group $H_{l_{\square}}$ stabilizing \mathcal{H}_{\square} is generated by $\{\varpi_{a,b} : a^2 - b^2 \in \square\}$, M and N and $[H_l : H_{l_{\square}}] = 2$. It is straightforward to show that, under the action of $H_{l_{\square}}$, the points on l are in three orbits:

$$\{(1, 0, 0, 0), (0, 1, 0, 0)\}, \{(1, s^2, 0, 0) : s \in \mathbb{F}_q^*\} \text{ and } \{(1, \eta s^2, 0, 0) : s \in \mathbb{F}_q^*\}.$$

Similarly, there are three orbits of points on l^{\perp} :

$$\{(0, 0, 1, 1), (0, 0, 1, -1)\}, \{(0, 0, a, b) : a^2 - b^2 \in \square\} \text{ and } \{(0, 0, a, b) : a^2 - b^2 \in \not\cap\}.$$

The orbit under H_l , $\mathcal{L}_{\mathcal{H}}^{\cap}$ splits into two orbits under $H_{l_{\square}}$: $\mathcal{L}_{\mathcal{H}_{\square}}^{\cap}$ and $\mathcal{L}_{\mathcal{H}\not\cap}^{\cap}$, which contain the points of \mathcal{H}_{\square} and $\mathcal{H}\not\cap$, respectively. Similarly, the orbit of lines $\mathcal{L}_{\mathcal{H}}^{\not\cap}$ splits into the two orbits $\mathcal{L}_{\mathcal{H}_{\square}}^{\not\cap}$ and $\mathcal{L}_{\mathcal{H}\not\cap}^{\not\cap}$ under the action of $H_{l_{\square}}$.

Theorem 3.4.4 *The orbits of planes under the action of H_{I_\square} are as follows:*

1. *The tangent planes $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$ to the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$, respectively form an orbit of size 2.*
2. *The tangent planes $[0, 0, 1, -1]^T$ and $[0, 0, 1, 1]^T$ to the points $(0, 0, 1, 1)$ and $(0, 0, 1, -1)$, respectively form an orbit of size 2.*
3. *The planes $V_{\mathfrak{H}_\square} = \{\pi_{c_\square}\} = \{[1, -c^{-1}, 0, 0]^T : c \in \square\}$, form an orbit of size $q - 1$.*
4. *The planes $V_{\mathfrak{H}_\varnothing} = \{\pi_{c_\varnothing}\} = \{[1, -c^{-1}, 0, 0]^T : c \in \varnothing\}$, form an orbit of size $q - 1$.*
5. *The planes $F_{\mathfrak{H}_\square} = \{\gamma_{a,b} = [0, 0, a, b]^T\}$ on the line $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$ such that $\alpha_{a,b} \cap \mathfrak{H}_\square = \{(1, s^2 - t^2, s, t) : s^2 - t^2 \in \square \text{ and } sa + tb = 0\} \cup \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ form an orbit of size $\frac{q-1}{2}$.*
6. *The planes $F_{\mathfrak{H}_\square} = \{\gamma_{a,b} = [0, 0, a, b]^T\}$ on the line $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$ such that $\alpha_{a,b} \cap \mathfrak{H} = \{(1, s^2 - t^2, s, t) : s^2 - t^2 \in \square \text{ and } sa + tb = 0\} \cup \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ form an orbit of size $\frac{q-1}{2}$.*
7. *The planes $F_{\mathfrak{H}_\varnothing} = \{\gamma_{a,b} = [0, 0, a, b]^T\}$ on the line $\langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$ such that $\alpha_{a,b} \cap \mathfrak{H}_\square = \{(1, s^2 - t^2, s, t) : s^2 - t^2 \in \varnothing \text{ and } sa + tb = 0\} \cup \{(1, 0, 0, 0), (0, 1, 0, 0)\}$ form an orbit of size $\frac{q-1}{2}$.*
8. *The planes meeting exactly one of $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$ and one point on $\langle(0, 0, 1, 1), (0, 0, 1, -1)\rangle \setminus \{(0, 0, 1, 1), (0, 0, 1, -1)\} \cap \gamma_{a,b}$ for some $\gamma_{a,b} \in F_{\mathfrak{H}_\square}$ form a single orbit of size $(q - 1)^2$.*

9. The planes meeting exactly one of $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$ and one point on $\langle(0, 0, 1, 1), (0, 0, 1, -1)\rangle \setminus \{(0, 0, 1, 1), (0, 0, 1, -1)\} \cap \gamma_{a,b}$ for some $\gamma_{a,b} \in F_{\mathcal{H}\square}$ form a single orbit of size $(q-1)^2$.
10. The planes on exactly one of the lines $\langle(1, 0, 0, 0), (0, 0, 1, 1)\rangle$, $\langle(0, 1, 0, 0), (0, 0, 1, 1)\rangle$, $\langle(0, 1, 0, 0), (0, 0, 1, -1)\rangle$, or $\langle(1, 0, 0, 0), (0, 0, 1, -1)\rangle$ form an orbit of size $4(q-1)$.
11. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$, $\omega \in \mathbb{F}_q^*$ of size $\frac{(q-1)^2}{2}$ such that $[1, -1, 0, \omega] \in \mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$. This includes a single orbit $\mathcal{O}_{\mathcal{H}\square}^{2\cap}$ of tangent planes to points of \mathcal{H} not on $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$. The tangent planes are the orbit $\mathcal{O}_{\mathcal{H}\square}^{2\cap}$ and are tangent to points of $\mathcal{H}\square$ when $q \equiv 3 \pmod{4}$ and are tangent to points of $\mathcal{H}\square$ when $q \equiv 1 \pmod{4}$.
12. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$, $\omega \in \mathbb{F}_q^*$ of size $\frac{(q-1)^2}{2}$. These are orbits of planes meeting a single line of $\mathcal{L}_{\mathcal{H}\square}^{\cap}$. This includes a single orbit of tangent planes to points of \mathcal{H} not on $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$. The tangent planes are tangent to points of $\mathcal{H}\square$ when $q \equiv 1 \pmod{4}$ and are tangent to points of $\mathcal{H}\square$ when $q \equiv 1 \pmod{4}$.
13. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$, $\omega \in \mathbb{F}_q^*$ of size $\frac{(q-1)^2}{2}$ such that $[1, -\eta^{-1}, 0, \omega] \in \mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$. These are orbits of planes containing a single line of $\mathcal{L}_{\mathcal{H}\square}^{\cap}$.
14. The $\frac{q-1}{2}$ orbits $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$, $\omega \in \mathbb{F}_q^*$ of size $\frac{(q-1)^2}{2}$. These are orbits of planes containing a single line of $\mathcal{L}_{\mathcal{H}\square}^{\cap}$.

Proof: We can check that $H_{I\square}$ is transitive on the four lines in the statement of number 9, via the action of $\langle M, N \rangle$. Consider the action of $\{\varpi_{a,b} : a^2 - b^2 =$

$1\} \subseteq \mathcal{H}_{l^{\square}}$ on planes on any of these lines, say $\beta = [0, 1, \omega, -\omega]^T$ for some $\omega \neq 0$ on $\langle (1, 0, 0, 0), (0, 0, 1, 1) \rangle$. $\beta \cap [0, 0, 0, 1]$. If $\varpi_{a,b}\beta = \varpi_{c,d}\beta$ for some $a^2 - b^2 = c^2 - d^2 = 1$ then we must have $a - b = c - d$, whence $a + b = c + d$ and hence $a = c$ and $b = d$. As there are $q - 1$ representations $a^2 - b^2$ of 1, the orbit of β includes all planes on $\langle (1, 0, 0, 0), (0, 0, 1, 1) \rangle$ which are not tangent to \mathcal{H} . Thus the orbit of β has size $4(q - 1)$.

It is straightforward, if occasionally tedious, to verify the remaining statements. ■

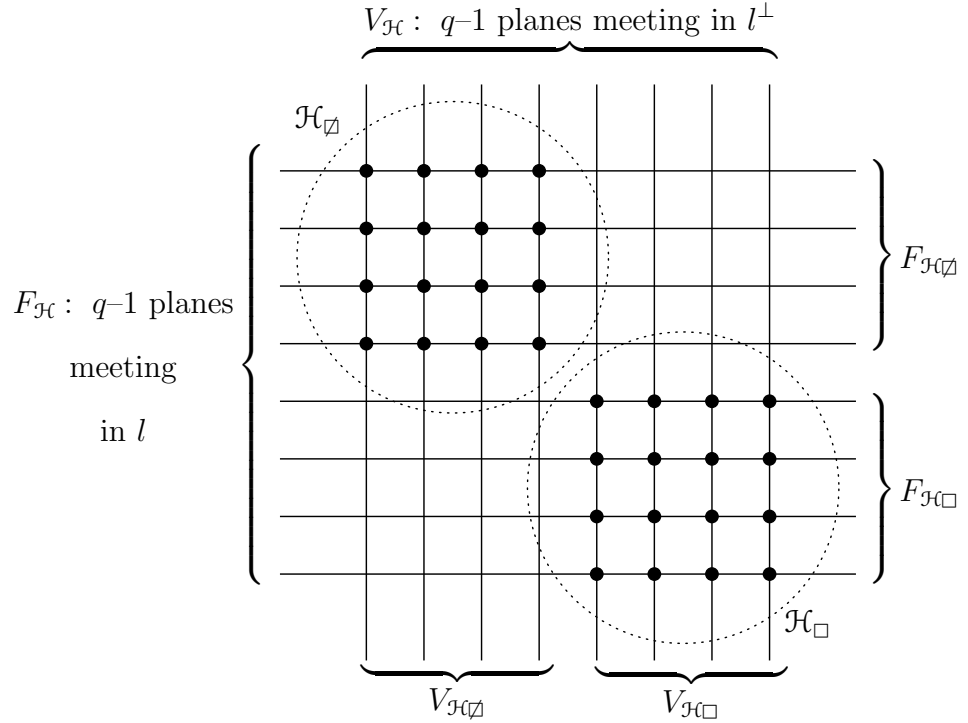


Figure 3.2: A diagram of the hyperbolic quadric from the point of view of the stabilizer of two points not on any line of the quadric.

The action of the stabilizer of two points of \mathcal{H} not on a line of the quadric is similar to the action of G_l on \mathcal{E} . Figure 3.2 is a diagram of \mathcal{H} from the point of view of the stabilizer H_l of $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$. The planes $V_{\mathcal{H}}$ meet in $l^{\perp} =$

$\langle(0, 0, 1, 1), (0, 0, 1, -1)\rangle$ and the planes $F_{\mathcal{H}}$ meet in $l = \langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$. The points of \mathcal{H} not contained in either of the planes $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$ are on the lines in orbits $\mathcal{L}_{\mathcal{H}}^{\cap} = V_{\mathcal{H}\square} \cap F_{\mathcal{H}\square}$ and $\mathcal{L}_{\mathcal{H}}^{\not\cap} = V_{\mathcal{H}\not\square} \cap F_{\mathcal{H}\not\square}$ under the action of $H_{l\square}$. Each dot represents a line of $\mathcal{L}_{\mathcal{H}}^{\cap}$ containing a pair of points $(1, a^2 - b^2, a, b)$, $(1, a^2 - b^2, -a, -b)$, $a^2 \neq b^2$. The intersections without dots represent the lines in the orbit of $m' = \langle(1, \eta, 1, 0), (1, \eta, -1, 0)\rangle$, $\mathcal{L}_{\mathcal{H}}^{\not\cap}$ under H_l . Under the action of $H_{l\square}$, the four quadrants of the grid each represent an orbit of lines. Each of these four orbits of lines carries orbits of planes distinct from $F_{\mathcal{H}}$ and $V_{\mathcal{H}}$. We will see that, for our purposes, it is sufficient to study planes in the $\frac{q-3}{2}$ orbits of the type $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$ and in the $\frac{q-1}{2}$ orbits of the type $\mathcal{O}_{\mathcal{H}\square}^{\omega\not\cap}$.

4. Truncated Quadrics and Elliptic Curves

4.1 Point Counts on Planes Meeting \mathcal{E}_\square

In view of Theorem 3.4.2, it is a simple matter to count the points of \mathcal{E}_\square on planes in certain orbits under $G_{l,\square}$. The planes in $F_{\mathcal{E}_\square}$ each meet \mathcal{E}_\square in $q - 1$ points and the planes in $F_{\mathcal{E}_\square^c}$ do not meet \mathcal{E}_\square . The planes in $V_{\mathcal{E}_\square}$ each meet \mathcal{E}_\square in $q + 1$ points and the planes in $V_{\mathcal{E}_\square^c}$ miss \mathcal{E}_\square . Each plane of $\mathcal{O}_{\mathcal{E}_\square}$ lies on a line n tangent to either $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$ and in a single plane of $F_{\mathcal{E}_\square}$. Thus the $q - 1$ planes on n each meet $\frac{q-1}{2}$ of the remaining $\frac{q^2-1}{2} - (q - 1)$ points of \mathcal{E}_\square . Similarly, the planes in $\mathcal{O}_{\mathcal{E}_\square^c}$ each meet \mathcal{E}_\square in $\frac{q+1}{2}$ points. The tangents to \mathcal{E}_\square meet \mathcal{E}_\square in either 0 or 1 point. Counting the number of points of \mathcal{E}_\square on planes in orbits of type $\mathcal{O}_{\mathcal{E}_\square}^{\omega\cap}$, $\mathcal{O}_{\mathcal{E}_\square^c}^{\omega\cap}$, $\mathcal{O}_{\mathcal{E}_\square}^{\omega\cap'}$ and $\mathcal{O}_{\mathcal{E}_\square^c}^{\omega\cap'}$ will take considerably more work.

In our discussion of the orbits of planes under the action of G_l , we found that for the $\frac{q-1}{2}$ orbits of type $\mathcal{O}_{\mathcal{E}_\square}^{\omega\cap}$, the planes on the line m include 2 representatives of each of these orbits. Similarly, the planes on the line m' include 2 representatives of the $\frac{q-3}{2}$ orbits of type $\mathcal{O}_{\mathcal{E}_\square}^{\omega\cap'}$.

In order to get a feel for the shape of \mathcal{E}_\square , we checked, for small prime values q , the intersection numbers of some planes with \mathcal{E}_\square . Consider the planes on $\langle (1, 1, 1, 0), (1, 1, -1, 0) \rangle$ distinct from $[0, 0, 0, 1]^T \in F$ and $[1, -1, 0, 0]^T \in V$, i.e., the set

$$\mathcal{P}_{\mathcal{E}}^\cap = \{\alpha_\omega = [1, -1, 0, \omega]^T : \omega \in \mathbb{F}_q^*\}.$$

Note that $\mathcal{P}_{\mathcal{E}}^\cap$ contains two representatives, α_ω and $\alpha_{-\omega}$, from each orbit $\mathcal{O}_{\mathcal{E}_\square}^{\omega\cap}$. As an example, in table 4.1 we have the intersection numbers of this family

Table 4.1: Intersection numbers of \mathcal{E}_\square with planes in $\mathcal{P}_\mathcal{E}^\square$ for $q = 263$

N	Planes meeting \mathcal{E}_\square in N points
116	**
118	*****
120	*****
122	*****
124	*****
126	*****
128	*****
130	*****
132	*****
134	*****
136	*****
138	*****
140	*****
142	*****
144	*****
146	*****
148	**

of planes for $q = 263$. We notice that Table 4.1 is symmetric with respect to $\frac{q-1}{2} = 132$, that each plane meets \mathcal{E}_\square in an even number of points and that the number of points per plane is relatively near 132. For odd primes $p < 300$, it was observed that these characteristics hold in general.

Lemma 4.1.1 *Let \mathcal{E}_\square and $\mathcal{P}_\mathcal{E}^\square$ be described as above. Then*

- 1 *Each plane in $\mathcal{P}_\mathcal{E}^\square$ meets \mathcal{E}_\square in an even number of points.*
- 2 *For any N , there are an even number of planes of $\mathcal{P}_\mathcal{E}^\square$ meeting \mathcal{E}_\square in N points.*

Proof: Suppose a point of \mathcal{E}_\square is incident with a plane $\alpha_\omega = [1, -1, 0, \omega]^T$ of $\mathcal{P}_\mathcal{E}^\square$, that is

$$(1, s^2 - \eta t^2, s, t)[1, -1, 0, \omega]^T = 1 - s^2 + \eta t^2 + \omega t = 0. \tag{4.1}$$

If $s \neq 0$ then $(1, s^2 - \eta t^2, -s, t)$ is also on α_ω . If $s = 0$, solve the quadratic in t and note that the discriminant $\omega^2 - 4\eta$ is nonzero and the roots are distinct. Check also that these roots can never be zero. This proves 1. For 2, simply note that $(1, s^2 - \eta t^2, s, t) \in \alpha_\omega$ if and only if $(1, s^2 - \eta t^2, s, -t) \in \alpha_{-\omega}$, and that each α_ω meets the oval $\{(1, s^2, s, 0) : s \in \mathbb{F}\} \cup (0, 1, 0, 0)$ in the points $(1, 1, 1, 0)$ and $(1, 1, -1, 0)$. ■

The remainder of this chapter will be concerned primarily with the proof of the following statements, and corresponding statements for the families of orbits of planes $\mathcal{O}_{\mathcal{E}\square}^{\omega\eta}$, $\mathcal{O}_{\mathcal{H}\square}^{\omega\eta}$, and $\mathcal{O}_{\mathcal{H}\square}^{\omega\eta}$.

1. If a plane of $\mathcal{P}_{\mathcal{E}}^\square$ meets \mathcal{E}_\square in N points, then $\frac{q+1}{2} - \sqrt{q} \leq N \leq \frac{q+1}{2} + \sqrt{q}$.
2. If there is a plane of $\mathcal{P}_{\mathcal{E}}^\square$ meeting \mathcal{E}_\square in $\frac{q+1}{2} - t$ points for some integer t , then there exists a plane of $\mathcal{P}_{\mathcal{E}}^\square$ which meets \mathcal{E}_\square in $\frac{q+1}{2} + t$ points.

We will see that the second statement, and the corresponding statements for planes meeting the hyperbolic quadric \mathcal{H} do not hold for all q .

Consider the plane $\alpha_\omega = [1, -1, 0, \omega]^T$, $\omega \in \mathbb{F}_q^*$ secant to \mathcal{E} and containing the points $(1, 1, 1, 0)$ and $(1, 1, -1, 0)$. Asking if a point of \mathcal{E}_\square is on α_ω , there arises the system of equations

$$(1, s^2 - \eta t^2, s, t)[1, -1, 0, \omega]^T = 1 - s^2 + \eta t^2 + \omega t = 0 \quad (4.2)$$

$$s^2 - \eta t^2 - a^2 = 0. \quad (4.3)$$

We may convert these to the homogeneous polynomials

$$f(x, s, t, a) = x^2 - s^2 + \eta t^2 + \omega x t \quad (4.4)$$

$$g(x, s, t, a) = s^2 - \eta t^2 - a^2. \quad (4.5)$$

This allows us to interpret solutions $X = (x, s, t, a)$ to $f(X) = g(X) = 0$ as points in projective space $PG(3, q)$. Because η is a nonsquare, $s^2 - \eta t^2 = 0$ has no solution, so $f(0, s, t, a) = 0$ has no solution and a point P satisfying $f(P) = g(P) = 0$ may be assumed to have the form $P = (1, s, t, a)$. If $P = (1, s, t, a)$ is a solution to this system, then so is $(1, s, t, -a)$, and these two points correspond to the single point $(1, s^2 - \eta t^2, s, t)$ on \mathcal{E}_\square with $s^2 - \eta t^2 = a^2$. That is, if there are N points satisfying $f(X) = g(X) = 0$, there are $\frac{N}{2}$ points of \mathcal{E}_\square on the plane $[1, -1, 0, \omega]^T$. Each of f and g is a degenerate quadratic form over \mathbb{F}_q in variables x, s, t, a with respective matrices M_f and M_g ,

$$M_f = \begin{bmatrix} 1 & 0 & \frac{\omega}{2} & 0 \\ 0 & -1 & 0 & 0 \\ \frac{\omega}{2} & 0 & \eta & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad M_g = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\eta & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Let \mathcal{C}_f and \mathcal{C}_g be the corresponding quadrics in $PG(3, q)$. Then \mathcal{C}_f is a quadratic cone with vertex $(0, 0, 0, 1)$ and a convenient carrier plane is $[0, 0, 0, 1]^T$. The quadric \mathcal{C}_g is a quadratic cone with vertex $(1, 0, 0, 0)$ and carrier plane $[1, 0, 0, 0]$. Note that neither of the vertices is a point on the other cone, so the cones do not share a linear component. With this choice of carrier planes, the vertex of each cone is on the carrier plane of the other.

We postpone the continuation of this discussion in order to outline some relevant results from algebraic geometry and the general theory of elliptic curves.

4.2 Some Background on Elliptic Curves

This section collects basic results from algebraic geometry from [21] and [15] and on elliptic curves in particular from [22], [16], and [25] which is necessary to justify the manipulations in coming sections. The first chapter of Shafarevich [21] is particularly illuminating.

Let f_1 and f_2 be homogeneous polynomials over an algebraically closed field \overline{K} and let \mathcal{C}_1 and \mathcal{C}_2 be projective plane curves defined by $\mathcal{C}_i = \{\mathbf{x} \in PG(2, q) : f_i(\mathbf{x}) = 0\}$ for $i = 1, 2$. A rational map from \mathcal{C}_1 to \mathcal{C}_2 is a collection of rational functions ϕ_1, ϕ_2, ϕ_3 such that for $\mathbf{x} \in \mathcal{C}_1$, $\Phi(\mathbf{x}) = (\phi_1(x_1), \phi_2(x_2), \phi_3(x_3)) \in \mathcal{C}_2$. The map Φ is a *birational equivalence* if the functions ϕ_j are invertible, that is, if there exist functions $\psi_j, j = 1, 2, 3$ such that $\phi_j \circ \psi_j$ and $\psi_j \circ \phi_j$ are the identity on the points where the maps are defined. The following theorem is central to our investigations. A proof and discussion may be found in Hartshorne [15], chapter 6.

Theorem 4.2.1 *Every curve is birationally equivalent to a nonsingular projective curve which is unique up to isomorphism.*

The genus of an algebraic curve is a nonnegative integer associated with the curve which is invariant under birational transformation. Conics, for example, are curves of genus $g = 0$. For curves over arbitrary fields, genus may be defined algebraically via the Riemann-Roch theorem. We again refer to Chapter 2 of [22]. An *elliptic curve* is an algebraic curve of genus 1.

It can be shown (Silverman [22], Chapter 2) that any elliptic curve is isomorphic to an affine curve E , together with a point (∞) whose points (x, y)

satisfy an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (4.6)$$

an equation in Weierstrass form, with coefficients in a field K . Any such curve is isomorphic to a curve in the projective plane with an equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

via the map

$$(x, y) \rightarrow [1, x, y], \quad (\infty) \rightarrow [0, 1, 0]$$

and conversely that any nonsingular curve given by a Weierstrass equation is an elliptic curve.

Any isomorphism between curves with equations of the form 4.6 is given by a change of variables

$$x = t^2x' + u \quad (4.7)$$

$$y = t^3y' + vx' + s \quad (4.8)$$

with $s, t, u, v \in \overline{K}$ and $t \neq 0$, where \overline{K} is the algebraic closure of K . See [16], Chapter 3 for proof. We call this an admissible change of variables. If the characteristic of K is not 2 or 3, equation 4.6 can always be transformed to an equation of the form

$$y^2 = x^3 + Ax^2 + Bx + C \quad (4.9)$$

via an admissible change of variables. An elliptic curve is necessarily nonsingular, that is, it has no points (x, y) at which both partial derivatives vanish.

For a curve with equation $y^2 = f(x)$ as in equation 4.9, this is equivalent to $f(x)$ having distinct roots. We define an elliptic curve to be a nonsingular affine curve whose points satisfy an equation of the form 4.9 together with a point ∞ .

We now state the Hasse-Weil Theorem, which is essential to our progress. For a curve E , let $\#E(\mathbb{F}_q)$ denote the number of \mathbb{F}_q -rational points of E .

Theorem 4.2.2 (Hasse-Weil) *Let E be a projective curve of genus g defined over a finite field \mathbb{F}_q . Then*

$$q + 1 - 2g\sqrt{q} \leq N \leq q + 1 + 2g\sqrt{q}. \quad (4.10)$$

We refer to [16] or [22] for a proof when $g = 1$ and [15] for the more difficult result when g is arbitrary.

4.3 Birational Transformations Between Quartics and Cubics

In this section, we carry out algebraic transformations on equations of curves whose points correspond to the points on the intersections of planes with the truncated quadrics. The resulting equations are of the form 4.9, and we apply the Hasse-Weil Theorem with $g = 1$.

4.3.1 Elliptic Curves From Orbits $\mathcal{O}_{\mathcal{E}\square}^\cap$

We return to the equations 4.4 and 4.5 from section 4.1. These equations arose from considering the intersection of a plane $\pi_\omega = [1, -1, 0, \omega]^T$ with \mathcal{E} . From $g(x, s, t, a) = 0$ we have $s^2 - \eta t^2 = a^2$, which we substitute into equation 4.4 to get $x^2 - a^2 + \omega t = 0$. We may assume that $x \neq 0$, since no point on $\mathcal{C}_f \cap \mathcal{C}_g$ is of the form $(0, s, t, a)$. We solve for t

$$t = \frac{a^2 - x^2}{\omega x}$$

and substitute into $g(x, s, t, a) = 0$ to obtain, after simplification

$$F(x, s, a) = \eta x^2 + (\omega^2 - 2\eta)x^2 a^2 + \eta a^2 - \omega x^2 s^2 \quad (4.11)$$

and we let $\mathcal{C}_F = \{(x, s, a) \in PG(2, q) | F(x, s, a) = 0\}$ be the corresponding plane curve. When $x = 0$, there is the unique solution $(0, 1, 0)$. Put $x = 1$ in $F(x, s, a) = 0$ to obtain the equation

$$\omega^2 s^2 = \eta a^4 + (\omega^2 - 2\eta)a^2 + \eta, \quad (4.12)$$

the affine part of \mathcal{C}_F .

We will show that equation 4.12 is birationally equivalent to an equation for an elliptic curve in Weierstrass form, that is, an equation of the form 4.9. Our hypothesis that \mathbb{F}_q is an arbitrary finite field of odd order does not change. In particular, these manipulations are justified when \mathbb{F}_q has characteristic 3.

Our method follows one outlined in chapter 8 of Cassels [8]. Note that the point $(a, s) = (1, 1)$ satisfies equation 4.12. Put¹ $u = \frac{1}{a-1}$, to obtain (after dividing through by ω^2)

$$s^2 = \frac{\eta}{\omega^2} \left(\frac{1}{u} + 1\right)^4 + \frac{(\omega^2 - 2\eta)}{\omega^2} \left(\frac{1}{u} + 1\right)^2 + \frac{\eta}{\omega^2}$$

which leads to

$$u^4 s^2 = u^4 + 2u^3 + \frac{\omega^2 - 2\eta}{\omega^2} u^2 + \frac{4\eta}{\omega^2} u + \frac{\eta}{\omega^2}.$$

Put $v = su^2$ and write the right hand side as $G(u)^2 + H(u)$, where

$$G(u) = u^2 + g_1 u + g_0 \text{ and}$$

¹The first step has the effect of moving the rational point $(1, 1)$ to ∞ on the resulting elliptic curve and is not absolutely essential.

$$H(u) = h_1 u + h_0.$$

solving for coefficients we find $g_1 = 1$, $g_0 = \frac{2\eta}{\omega^2}$, $h_1 = 0$ and $h_0 = \frac{\eta}{\omega^2} - \frac{4\eta^2}{\omega^4}$. Now $v^2 = G(u)^2 + H(u)$, so

$$(v + G(u))(v - G(u)) = H(u).$$

Put $v + G(u) = t$, whence $v - G(u) = \frac{H(u)}{t}$ and then $2G(u) = t - \frac{H(u)}{t}$.

Multiply through by $4t^2$ to obtain

$$4u^2 t^2 + 4ut^2 + \frac{2\eta}{\omega^2} t^2 = 2t^3 - 2 \left(\frac{\eta}{\omega^2} - \frac{4\eta^2}{\omega^4} \right) t.$$

Let $d = ut$, so that

$$4d^2 + 4dt + \frac{2\eta}{\omega^2} t^2 = 2t^3 - 2 \left(\frac{\eta}{\omega^2} - \frac{4\eta^2}{\omega^4} \right) t$$

and then let $r = 2d + t$, so that $d = \frac{r-t}{2}$ and after simplification

$$r^2 = 2t^3 + \left(1 - 8\frac{\eta}{\omega^2} \right) t^2 - 2 \left(\frac{\eta}{\omega^2} - 4\frac{\eta^2}{\omega^4} \right) t.$$

Finally put $y = 2r$ and $x = 2t$ to put our equation into a rather nice form:

$$\begin{aligned} y^2 &= x^3 + \left(1 - 8\frac{\eta}{\omega^2} \right) x^2 + \left(\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2} \right) x \\ y^2 &= x \left(x - \frac{4\eta}{\omega^2} \right) \left(x - \frac{4\eta - \omega^2}{\omega^2} \right) \end{aligned} \tag{4.13}$$

and let $E_{\xi_{\square}}^{\omega}$, together with ∞ , be the elliptic curve whose points satisfy this equation. Tracing through the various transformations, we find that the rational maps

$$a = \frac{2x}{y-x} + 1 \tag{4.14}$$

$$s = \frac{2x^3 + (1 - 8\frac{\eta}{\omega^2})x^2 - y^2}{(y - x)^2} \quad (4.15)$$

with inverse maps

$$x = \frac{4\eta a^2 + 2(\omega^2 - 4\eta)a + 4\eta + 2\omega^2 s}{\omega^2(a - 1)^2} \quad (4.16)$$

$$y = \frac{4\eta a^3 + 2(\omega^2 - 2\eta)a^2 + 2(\omega^2(s + 1) - 2\eta)a + 2(2\eta + \omega^2 s)}{(a - 1)^3 \omega^2} \quad (4.17)$$

map the curve with equation 4.12 to the affine part of $E = E_{\mathcal{E}_\square}^\omega$. The functions from E to \mathcal{C}_F are undefined only when $a = 1$, and the inverse functions are undefined only when $x = y$. If we put $y = x$ in equation 4.13, we find that for $x \neq 0$, the discriminant of the resulting quadratic is $\frac{16\eta}{\omega^2}$, which is never a square in \mathbb{F}_q . Thus the only point on 4.13 with $x = y$ is $(0, 0)$ and so the only rational points of E on which the maps 4.16 and 4.17 are undefined are $(0, 0)$ and ∞ . The two points of \mathcal{C}_F for which $a = 1$ are $(1, 1)$ and $(1, -1)$. We extend the rational maps between \mathcal{C}_F and E by $(1, 1) \leftrightarrow \infty$ and $(1, -1) \leftrightarrow (0, 0)$. Thus augmented, the rational maps 4.14 and 4.15 and their inverses 4.16 and 4.17 give a bijection between the points of E (including ∞) and the nonsingular points of the projective curve \mathcal{C}_F that is, the points of \mathcal{C}_F different from $(0, 1, 0)$.

Two nonsingular points (s, a) , $(s, -a)$ on \mathcal{C}_F correspond to the single point $(1, s^2 - \eta t^2, s, t)$ with $s^2 - \eta t^2 = a^2$ on $\alpha_\omega \cap \mathcal{E}_\square$, where $t = \frac{a^2 - 1}{\omega}$. Thus the map from the points of the elliptic curve E to the points on $\alpha_\omega \cap \mathcal{E}_\square$ is 2:1, and by the Hasse-Weil Theorem we have the following result.

Theorem 4.3.2 *Let $\alpha_\omega, \omega \in \mathbb{F}_q^*$ be a plane in the orbit $\mathcal{O}_{\mathcal{E}_\square}^\omega$ and let $N_\omega = |\alpha_\omega \cap \mathcal{E}_\square|$. Then N_ω is even and*

$$\frac{q+1}{2} - \sqrt{q} \leq N_\omega \leq \frac{q+1}{2} + \sqrt{q}. \quad (4.18)$$

Let $E_{\mathcal{E}\square}^{\omega\cap}$ denote the elliptic curve with equation 4.13 and $\mathbf{E}_{\mathcal{E}\square}^{\cap} = \{E_{\mathcal{E}\square}^{\omega\cap}\}_{\omega \in \mathbb{F}_q^*}$.

In our example $q = 263$ in Figure 4.1, we find $\lfloor 264 + 2\sqrt{263} \rfloor = 296 = 2(148)$ which shows that the bounds of 4.18 are as close as possible without some further restriction.

4.3.3 Elliptic Curves From Orbits $\mathcal{O}_{\mathcal{E}\square}^{\cap}$

Let $\mathcal{P}_{\mathcal{E}}^{\cap} = \{[1, -\eta^{-1}, 0, \omega]^T : \omega \in \mathbb{F}_q \setminus \{0, 2, -2\}\}$. We choose a representative plane $\alpha_{\omega} = [1, -\eta, 0, \omega]^T$ in the orbit $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$. Note that $[1, -\eta^{-1}, 0, \pm 2]^T$ are tangent planes to \mathcal{E} at the points $(1, -\eta, 0, \pm 1)$, hence the restriction. From the equations

$$(1, s^2 - \eta t^2, s, t)[1, -\eta, 0, \omega]^T = 1 - \eta(s^2 - \eta t^2) + \omega t = 0$$

$$s^2 - \eta t^2 - a^2 = 0$$

we obtain the equation

$$\eta\omega^2 s^2 = a^4 + \eta(\omega - 2)a^2 + \eta^2. \quad (4.19)$$

The substitution

$$a = \frac{\sqrt{\eta}x}{y} \quad (4.20)$$

$$s = \frac{\sqrt{\eta}(4x^3 + x^2(2 - \omega^2) - 2y^2)}{2\omega y^2} \quad (4.21)$$

transforms 4.19 to

$$y^2 = x^3 + \frac{2 - \omega^2}{2}x^2 + \left(\frac{\omega^4}{16} - \frac{\omega^2}{4}\right)x$$

$$= x \left(x - \frac{\omega^2}{4}\right) \left(x - \left(\frac{\omega^2}{4} - 1\right)\right) \quad (4.22)$$

which is nonsingular whenever $\omega \neq \pm 2$. The inverse rational maps are

$$x = \frac{-2a^2 + 2\eta + 2\eta\omega s + \omega^2 a^2}{4a^2} \text{ and} \quad (4.23)$$

$$y = \frac{-2a^2\sqrt{\eta} + \eta^{\frac{3}{2}} + 2\eta\omega s + \sqrt{\eta}\omega^2 a^2}{4a^3}. \quad (4.24)$$

Again we apply the Hasse-Weil theorem and find that for $N_\omega = |\alpha_\omega \cap \mathcal{E}_\square|$, $\omega \neq \pm 2$

$$\frac{q+1}{2} - \sqrt{q} \leq N_\omega \leq \frac{q+1}{2} + \sqrt{q}. \quad (4.25)$$

When $\omega = \pm 2$, the equation 4.22 is singular and the curves correspond to the planes tangent at the points $(1, -\eta, 0, \pm 1)$. When $q \equiv 3 \pmod{4}$, $-\eta$ is a square and the points $(1, -\eta, 0, \pm 1)$ are on \mathcal{E}_\square , while when $q \equiv 1 \pmod{4}$ they are on \mathcal{E}_{\square} . The total number of points of \mathcal{E}_\square on the planes α_ω , $\omega \in \mathbb{F}_q \setminus \{0, 2, -2\}$ is therefore $\frac{(q-1)^2}{2}$ when $q \equiv 1 \pmod{4}$ and $\frac{q^2-2q-3}{2}$ when $q \equiv 3 \pmod{4}$.

4.3.4 Elliptic Curves from Orbits $\mathcal{O}_{\mathcal{H}_\square}^\cap$

Now consider \mathcal{H}_\square , a subset of the hyperbolic quadric \mathcal{H} defined in Section 3.5 and stabilized by the group H_{l_\square} . We look first at planes in the orbits $\mathcal{O}_{\mathcal{H}_\square}^\cap$. Similar to the situation with planes in orbits $\mathcal{O}_{\mathcal{E}_\square}^\cap$ when $\omega = \pm 2$, the planes are tangent to \mathcal{H} at the points $(1, -1, 0, \pm 1)$. These points are on \mathcal{H}_\square when $q \equiv 3 \pmod{4}$ and on \mathcal{H}_{\square} when $q \equiv 1 \pmod{4}$. From the system of equations

$$\begin{aligned} (1, s^2 - t^2, s, t)[1, -1, 0, \omega]^T &= 1 - s^2 + t^2 + \omega t = 0 \\ s^2 - t^2 - a^2 &= 0 \end{aligned} \quad (4.26)$$

we obtain the quartic

$$\omega^2 s^2 = a^4 + (\omega^2 - 2)a^2 + 1 \quad (4.27)$$

which is equal to 4.19 if we set $\eta = 1$ in that equation. We adapt the birational maps from the discussion of planes in $\mathcal{O}_{\mathcal{E}}^{\cap}$. The rational maps

$$\begin{aligned} a &= \frac{x}{y} \\ s &= \frac{(4x^3 + x^2(2 - \omega^2) - 2y^2)}{2\omega y^2} \end{aligned} \quad (4.28)$$

take 4.27 to

$$y^2 = x^3 + \frac{2 - \omega^2}{2}x^2 + \left(\frac{\omega^4}{16} - \frac{\omega^2}{4}\right)x \quad (4.29)$$

$$= x \left(x - \frac{\omega^2}{4}\right) \left(x - \left(\frac{\omega^2}{4} - 1\right)\right) \quad (4.30)$$

which is identical to equation 4.22. The inverse maps are

$$x = \frac{-2a^2 + 2 + 2\omega s + \omega^2 a^2}{4a^2} \quad (4.31)$$

$$y = \frac{-2a^2 + 1 + 2\omega s + \omega^2 a^2}{4a^3}. \quad (4.32)$$

Although the curves that arise here are isomorphic to those from orbits $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$, the point counts on planes are slightly different. Note that the plane $[1, -1, 0, \omega]^T$ meets \mathcal{H} in the four points $(1, 0, \pm\omega^{-1}, -\omega^{-1})$ and $(0, 1, \pm\omega^{-1}, \omega^{-1})$ which are not in \mathcal{H}_{\square} . These pairs of points lie on the planes $[0, 1, 0, 0]^T$ and $[1, 0, 0, 0]^T$ tangent to \mathcal{H} at $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$, respectively.

Let β_{ω} be a plane in the orbit $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$, and $N_{\omega} = |\beta_{\omega} \cap \mathcal{H}_{\square}|$. Then

$$\frac{q-3}{2} - \sqrt{q} \leq N_{\omega} \leq \frac{q-3}{2} + \sqrt{q} \quad (4.33)$$

by the Hasse-Weil Theorem.

4.3.5 Elliptic Curves from Orbits $\mathcal{O}_{\mathcal{H}\square}^{\cap}$

Consider an orbit $\mathcal{O}_{\mathcal{H}\square}^{\omega\eta}$, which contains the planes $[1, -\eta, 0, \pm\omega]^T$ on the line $\langle(1, \eta^{-1}, 1, 0), (1, \eta^{-1}, -1, 0)\rangle$. Note that for all $\omega \in \mathbb{F}_q^*$, these planes are secant to \mathcal{H} . From the system

$$\begin{aligned} (1, s^2 - t^2, s, t)[1, -\eta, 0, \omega]^T &= 1 - \eta(s^2 - t^2) + \omega t = 0 \\ s^2 - t^2 - a^2 &= 0 \end{aligned} \tag{4.34}$$

we obtain the quartic

$$\left(\frac{\omega s}{\eta}\right)^2 = a^4 + \frac{\omega^2 - 2\eta}{\eta^2}a^2 + \frac{1}{\eta^2} \tag{4.35}$$

which we transform to the cubic

$$\begin{aligned} y^2 &= x^3 + \frac{2\eta - \omega^2}{2\eta^2}x^2 + \frac{\omega^4 - 4\eta\omega^2}{16\eta^4}x \\ &= x\left(x - \frac{\omega^2}{4\eta^2}\right)\left(x - \frac{\omega^2 - 4\eta}{4\eta^2}\right) \end{aligned} \tag{4.36}$$

using the technique from Section 4.3.1. Let $E_{\mathcal{H}\square}^{\omega\eta}$ be the curve with equation 4.36 and $\mathbf{E}_{\mathcal{H}\square}^{\eta} = \{E_{\mathcal{H}\square}^{\omega\eta} : \omega \in \mathbb{F}_q^*\}$. The plane $\alpha_\omega = [1, -\eta, 0, \omega]^T$ meets the plane $[0, 1, 0, 0]^T$ at the points $(1, 0, \pm\omega^{-1}, -\omega^{-1})$ and $(0, 1, -\omega^{-1}, -\omega^{-1})$ of \mathcal{H} , which are not points of \mathcal{H}_\square . The points $(1, 0, \pm\omega^{-1}, -\omega^{-1})$ give two solutions $(s, t, a) = (-\omega^{-1}, \pm\omega^{-1}, 0)$ to the system 4.34. Thus the number of solutions (s, t, a) to 4.34 is two more than $|\alpha_\omega \cap \mathcal{H}_\square|$.

To reiterate, let α_ω be a plane in the orbit $\mathcal{O}_{\mathcal{H}\square}^{\omega\eta}$, and $N_\omega = |\alpha_\omega \cap \mathcal{H}_\square|$. Then by the Hasse-Weil Theorem,

$$\frac{q-3}{2} - \sqrt{q} \leq N_\omega \leq \frac{q-3}{2} + \sqrt{q}. \tag{4.37}$$

4.3.6 Families of Curves

Return now to equation 4.36 and make the substitution $x \mapsto x + \frac{\omega^2 - 4\eta}{4\eta^2}$. Multiply both sides of the result by $\left(\frac{2\eta}{\omega}\right)^6$ and make the substitutions $y \mapsto \left(\frac{\omega}{2\eta}\right)^3 y$ and $x \mapsto \left(\frac{\omega}{2\eta}\right)^2 x$, to obtain

$$y^2 = x \left(x - \frac{4\eta}{\omega^2} \right) \left(x - \frac{4\eta - \omega^2}{\omega^2} \right) \quad (4.38)$$

which is identical to equation 4.13. That is, the families of curves $\mathbf{E}_{\mathcal{E}\square}^\square$ and $\mathbf{E}_{\mathcal{H}\square}^\square$ are the same.

To reiterate the relationship between curves from \mathcal{H}_\square and from \mathcal{E}_\square , we state the following theorem.

Theorem 4.3.7 *The set of elliptic curves $\mathbf{E}_{\mathcal{E}}^\square$ that arise from considering the intersections of planes in $\mathcal{P}_{\mathcal{E}}^\square$ with \mathcal{E}_\square is identical with the set of elliptic curves $\mathbf{E}_{\mathcal{H}}^\square$ which arise from considering the intersections of planes in $\mathcal{P}_{\mathcal{H}}^\square$ with \mathcal{H}_\square . The set of elliptic curves $\mathbf{E}_{\mathcal{E}}^\square$ that arise from considering the intersections of planes in $\mathcal{P}_{\mathcal{E}}^\square$ with \mathcal{E}_\square is identical with the set of elliptic curves $\mathbf{E}_{\mathcal{H}}^\square$ which arise from considering the intersections of planes in $\mathcal{P}_{\mathcal{H}}^\square$ with \mathcal{H}_\square .*

Thus we have two families of elliptic curves to consider, and they take surprisingly simple forms. Make the substitution $a = \frac{2}{\omega}$ into equation 4.13, and write

$$\mathbf{E}_{\mathcal{E}}^\square = \{y^2 = x(x - \eta a^2)(x - (\eta a^2 - 1)) : a \in \mathbb{F}_q^*\}. \quad (4.39)$$

From equation 4.22, we obtain, via the substitution $a = \frac{\omega}{2}$, the set of curves

$$\mathbf{E}_{\mathcal{E}}^\square = \{y^2 = x(x - a^2)(x - (a^2 - 1)) : a \in \mathbb{F}_q \setminus \{0, 1, -1\}\}. \quad (4.40)$$

4.4 Summary of Plane Intersections with Truncated Quadrics

In this section, we give a complete summary of plane intersections with \mathcal{E}_\square and \mathcal{H}_\square in terms of exact counts or bounds given by the Hasse-Weil Theorem. We first explain how the bounds we have found give bounds on orbits we have not yet considered.

4.4.1 Other Plane Orbit Types

We turn now to the orbits of planes $\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap}$, $\mathcal{O}_{\mathcal{E}_\square}^{\omega \not\cap}$, $\mathcal{O}_{\mathcal{H}_\square}^{\omega \cap}$, and $\mathcal{O}_{\mathcal{H}_\square}^{\omega \not\cap}$ and their intersections with \mathcal{E}_\square and \mathcal{H}_\square . These orbits have the same relationship with \mathcal{E}_\square and \mathcal{H}_\square as the orbits we have already considered have with \mathcal{E}_\square and \mathcal{H}_\square , and the point counts of the intersections are easily calculated.

Choose $a, b \in \mathbb{F}_q$ such that $a^2 - \eta b^2 = \eta$. Then $\varphi_{a,b} \in G_l$ interchanges \mathcal{E}_\square with \mathcal{E}_\square and in particular, $(1, 1, 1, 0)\varphi_{a,b} = (1, \eta, a, b)$ and $(1, 1, -1, 0)\varphi_{a,b} = (1, \eta, -a, -b)$, so the set $\mathcal{P}_{\mathcal{E}_\square}$ is exchanged with a set of representatives for orbits $\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap}$. As each non-tangent plane of $PG(3, q)$ meets \mathcal{E} in $q+1$ points, the number $N_{\mathcal{E}_\square}^\omega$ of points of \mathcal{E}_\square on the plane

$$[1, -\eta^{-1}, -\omega b \eta^{-1}, \omega a \eta^{-1}]^T \in \mathcal{O}_{\mathcal{E}_\square}^{\omega \cap}$$

is equal to the number of points of \mathcal{E}_\square on $[1, -1, 0, \omega]^T$. By our application of the Hasse-Weil Theorem to the number of points on planes in $\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap}$, we have

$$\frac{q+1}{2} - \sqrt{q} \leq N_{\mathcal{E}_\square}^\omega \leq \frac{q+1}{2} + \sqrt{q}.$$

We obtain the same bounds on the number of points of \mathcal{E}_\square on planes in orbits of type $\mathcal{O}_{\mathcal{E}_\square}^{\omega \not\cap}$ by counting the number of points of \mathcal{E}_\square on planes in orbits $\mathcal{O}_{\mathcal{E}_\square}^{\omega \not\cap}$ and mapping $\mathcal{O}_{\mathcal{E}_\square}^{\omega \not\cap}$ to $\mathcal{O}_{\mathcal{E}_\square}^{\omega \not\cap}$ with $\varphi_{a,b}$, which simultaneously interchanges \mathcal{E}_\square and

\mathcal{E}_{\square} . Thus if a plane π of $PG(3, q)$ meets \mathcal{E} in $q + 1$ points of which $\frac{q+1}{2} + t$ are points of \mathcal{E}_{\square} , then an element of G_l taking \mathcal{E}_{\square} to \mathcal{E}_{\square} (such as $\varphi_{a,b}$ as defined previously) takes π to a plane $\varphi_{a,b}\pi$ meeting \mathcal{E}_{\square} in $\frac{q+1}{2} + t$ points, so $\varphi_{a,b}\pi$ meets \mathcal{E}_{\square} in $\frac{q+1}{2} - t$ points. We call this a *complementarity property*.

Similarly, if we choose c and $d \in \mathbb{F}_q$ such that $c^2 - d^2 = \eta$, then $\varpi_{c,d} \in H_l$ interchanges the points of \mathcal{H}_{\square} with the points of \mathcal{H}_{\square} , and takes orbits $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega}$ and $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega\eta}$ to orbits $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega}$ and $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega\eta}$, respectively. We may choose as a representative plane in an orbit of type $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega}$ the plane $\pi_{\omega} = [1, -1, 0, \omega]$ for some $\omega \neq 0$. Then π_{ω} contains the points $(1, 0, \omega^{-1}, \pm\omega^{-1})$ and $(0, 1, \pm\omega^{-1}, \omega^{-1})$ of \mathcal{H} and so meets $\mathcal{H}_{\square} \cup \mathcal{H}_{\square}$ in $q - 3$ points. Thus a complementarity property holds for \mathcal{H} as well.

4.4.2 Summary of Plane Intersections for Truncated Quadrics

We summarize our results on the plane intersection numbers for \mathcal{E}_{\square} and for \mathcal{H}_{\square} in two theorems.

Theorem 4.4.3 *Let $\mathcal{E}_{\square} = \{(1, s^2 - \eta t^2, s, t) : s^2 - \eta t^2 \in \square\}$ and let the orbits of planes under $G_{l_{\square}}$ be as stated in Theorem 3.4.2.*

1. *The $\frac{q^2-1}{2}$ tangent planes to \mathcal{E}_{\square} each meet \mathcal{E}_{\square} in a single point.*
2. *The $\frac{q^2+3}{2}$ tangent planes to $\mathcal{E} \setminus \mathcal{E}_{\square}$ do not meet \mathcal{E}_{\square} .*
3. *The $\frac{q-1}{2}$ planes $V_{\mathcal{E}_{\square}}$ do not meet \mathcal{E}_{\square} .*
4. *The $\frac{q-1}{2}$ planes $V_{\mathcal{E}_{\square}}$ each meet \mathcal{E}_{\square} in $q + 1$ points.*
5. *The planes in $F_{\mathcal{E}_{\square}}$ each meet \mathcal{E}_{\square} in $q - 1$ points.*

6. The planes in $F_{\mathcal{E}_{\square}}$ do not meet \mathcal{E}_{\square} .
7. The planes in $\mathcal{O}_{\mathcal{E}_{\square}}$ each meet \mathcal{E}_{\square} in $\frac{q-1}{2}$ points.
8. The planes in $\mathcal{O}_{\mathcal{E}_{\square}}$ each meet \mathcal{E}_{\square} in $\frac{q+1}{2}$ points.
9. Each plane in an orbit $\mathcal{O}_{\mathcal{E}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ each meets \mathcal{E}_{\square} in N points, where N is even and satisfies $|\frac{q+1}{2} - N| \leq \sqrt{q}$.
10. Each plane in an orbit $\mathcal{O}_{\mathcal{E}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ meets \mathcal{E}_{\square} in N points, where N is even and satisfies $|\frac{q+1}{2} - N| \leq \sqrt{q}$.
11. Each plane in an orbit $\mathcal{O}_{\mathcal{E}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ meets \mathcal{E}_{\square} in N points, where N is even and satisfies $|\frac{q+1}{2} - N| \leq \sqrt{q}$.
12. Each plane in an orbit $\mathcal{O}_{\mathcal{E}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ meets \mathcal{E}_{\square} in N points, where N is even and satisfies $|\frac{q+1}{2} - N| \leq \sqrt{q}$.

Proof: When we are able to give an exact value, the number is at most a consequence of the orbit-stabilizer theorem. The bounds given in statements 9 and 10 are consequences of our application of the Hasse-Weil Theorem, and the bounds in statements 11 and 12 are arrived at via the complementarity property discussed prior to the theorem statement. ■

The structure of \mathcal{H}_{\square} is slightly more complicated than that of \mathcal{E}_{\square} , and there are several more orbit types.

Theorem 4.4.4 *Let $\mathcal{H} = \{1, s^2 - t^2, s, t\} : s^2 - t^2 \in \square\}$ and let the orbits of planes under H_{\square} be as stated in Theorem 3.4.4.*

1. The $\frac{(q-1)^2}{2}$ tangent planes to \mathcal{H}_{\square} each meet \mathcal{H}_{\square} in $q - 1$ points.

2. The $\frac{(q-1)^2}{2}$ tangent planes to \mathcal{H}_{\square} each meet \mathcal{H}_{\square} in $q - 2$ points.
3. The planes $V_{\mathcal{H}_{\square}}$ each meet \mathcal{H}_{\square} in $q - 1$ points.
4. The planes $V_{\mathcal{H}_{\square}}$ do not meet \mathcal{H}_{\square} .
5. The planes $F_{\mathcal{H}_{\square}}$ each meet \mathcal{H}_{\square} in $q - 1$ points.
6. The planes $F_{\mathcal{H}_{\square}}$ do not meet \mathcal{H}_{\square} .
7. The planes meeting exactly one of $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$ and one point x on $\langle (0, 0, 1, 1), (0, 0, 1, -1) \rangle \setminus \{(0, 0, 1, 1), (0, 0, 1, -1)\}$ such that x is on a plane of $F_{\mathcal{H}_{\square}}$ each meet \mathcal{H}_{\square} in $\frac{q-3}{2}$ points.
8. The planes meeting exactly one of $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$ and one point x on $\langle (0, 0, 1, 1), (0, 0, 1, -1) \rangle \setminus \{(0, 0, 1, 1), (0, 0, 1, -1)\}$ such that x is on a plane of $F_{\mathcal{H}_{\square}}$ each meet \mathcal{H}_{\square} in $\frac{q-1}{2}$ points.
9. The planes on exactly one of the lines $\langle (1, 0, 0, 0), (0, 0, 1, 1) \rangle$, $\langle (0, 1, 0, 0), (0, 0, 1, 1) \rangle$, $\langle (0, 1, 0, 0), (0, 0, 1, -1) \rangle$, or $\langle (1, 0, 0, 0), (0, 0, 1, -1) \rangle$ each meet \mathcal{H}_{\square} in $\frac{q-1}{2}$ points.
10. Planes in an orbit $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^* \setminus \{2, -2\}$ each meet \mathcal{H}_{\square} in N points for some N satisfying $|\frac{q-3}{2} - N| \leq \sqrt{q}$.
11. Planes in an orbit $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ each meet \mathcal{H}_{\square} in N points for some N satisfying $|\frac{q-3}{2} - N| \leq \sqrt{q}$.
12. Planes in an orbit $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega \cap}$, $\omega \in \mathbb{F}_q^*$ each meet \mathcal{H}_{\square} in N points for some N satisfying $|\frac{q-3}{2} - N| \leq \sqrt{q}$.

13. Planes in an orbit $\mathcal{O}_{\mathcal{H}(\square)}^{\omega \not\parallel}$, $\omega \in \mathbb{F}_q^*$ each meet \mathcal{H}_{\square} in N points for some N satisfying $|\frac{q-3}{2} - N| \leq \sqrt{q}$.
14. Planes in the orbit $\mathcal{O}_{\mathcal{H}(\square)}^{2\cap}$ of tangent planes to points of \mathcal{H} not on $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$ each meet \mathcal{H}_{\square} in q points when $q \equiv 1 \pmod{4}$ and in $q - 1$ points when $q \equiv 3 \pmod{4}$.
15. Planes in the orbit $\mathcal{O}_{\mathcal{H}(\not\parallel)}^{2\cap}$ of tangent planes to points of \mathcal{H} not on $[1, 0, 0, 0]^T$ or $[0, 1, 0, 0]^T$ each meet \mathcal{H}_{\square} in $q - 1$ points when $q \equiv 1 \pmod{4}$ and in q points when $q \equiv 3 \pmod{4}$.

Proof: Because $H_{l_{\square}}$ is transitive on the points of \mathcal{H}_{\square} , and hence on the tangent planes to \mathcal{H}_{\square} , it is sufficient for 1 to consider the tangent plane $[1, 1, -2, 0]^T$ to the point $(1, 1, 1, 0)$. This plane contains $2q + 1$ points of \mathcal{H} , including $(1, 1, 1, 0)$ and the four points $(1, 0, 2^{-1}, \pm 2^{-1})$ and $(0, 1, 2^{-1}, \pm 2^{-1})$. Any element $\varpi_{a,b}$ of H_l such that $a^2 - b^2 \in \not\parallel$ interchanges \mathcal{H}_{\square} and $\mathcal{H}_{\not\parallel}$, and so the points of \mathcal{H}_{\square} distinct from $(1, 1, 1, 0)$ on $[1, 1, -2, 0]^T$ are equal in number to the points of $\mathcal{H}_{\not\parallel}$ on $[1, 1, -2, 0]^T$. The reasoning for 2 is similar.

The other exact counts are either immediate or are a consequence of the orbit-stabilizer theorem. The planes in orbits of type $\mathcal{O}_{\mathcal{H}(\square)}^{\cap}$ and $\mathcal{O}_{\mathcal{H}(\square)}^{\not\parallel}$ were handled in Sections 4.3 and 4.4. The bounds given in statements 11 and 13 follow by our application of the Hasse-Weil Theorem and the complementarity property.

■

4.5 Sums of Point Counts

In this section, we use our knowledge of the number of incidences of sets of representatives of plane orbits with the truncated quadrics to find the total

number of points in the elliptic curve families given in equations 4.39 and 4.40.

The planes

$$\mathcal{P}_{\mathcal{E}}^{\cap} = \{\alpha_{\omega}\} = \{[1, -1, 0, \omega]^T : \omega \in \mathbb{F}_q^*\}$$

all meet in the line $\langle(1, 1, 1, 0), (1, 1, -1, 0)\rangle$ and partition the points of \mathcal{E}_{\square} which do not lie on either $[0, 0, 0, 1]^T$ or $[1, -1, 0, 0]^T$. Thus the number of incidences of $\{\alpha_{\omega}\} \cap \mathcal{E}_{\square}$ is seen to be $\frac{q^2-1}{2}$. As the map taking points of $\mathcal{E}_{\square} \cap \alpha_{\omega}$ to points on the associated elliptic curve is $1 : 2$, the total number of points on the family of curves $\mathbf{E} = \{E_{\mathcal{E}_{\square}}^{\omega \cap}\}$ is $q^2 - 1$, including multiplicities.

Now we have the problem of finding how the points of \mathcal{H}_{\square} are partitioned by the set of planes on a single line in an orbit $\mathcal{L}_{\mathcal{H}_{\square}}^{\omega \cap}$ or $\mathcal{L}_{\mathcal{H}_{\square}}^{\omega \not\cap}$. On the line $\langle(1, 1, 1, 0), (1, 1, -1, 0)\rangle \in \mathcal{L}_{\mathcal{H}_{\square}}$, each pair of planes $[1, -1, 0, \pm\omega]$, $\omega \in \mathbb{F}_q^*$ are in a distinct orbit $\mathcal{O}_{\mathcal{H}_{\square}}^{\omega \cap}$. We will write $\alpha_{\omega} = [1, -1, 0, \omega]^T$. When $\omega = \pm 2$, the planes α_{ω} are the tangents to \mathcal{H} at the points $(1, -1, 0, 1)$ and $(1, -1, 0, -1)$. In $[1, -1, 0, -2]^T$, the plane tangent at $(1, -1, 0, 1)$, the tangent lines to \mathcal{H} may be written $n_1 = \{(1, 1 + 2\lambda, 1 + \lambda, -\lambda) : \lambda \in \mathbb{F}_q\} \cup \{(0, 2, 1, -1)\}$ and $n_{-1} = \{(1, 1 + 2\lambda, -1 - \lambda, -\lambda) : \lambda \in \mathbb{F}_q\} \cup \{(0, 2, -1, -1)\}$. The points $(0, 2, \pm 1, -1)$ are on the plane $[1, 0, 0, 0]^T$ tangent at $(0, 1, 0, 0)$. The points $(1, 1 + 2\lambda, 1 + \lambda, \lambda)$ and $(1, 1 + 2\lambda, -1 - \lambda, -\lambda)$ are the unique points of n_1 and n_{-1} on the plane $[1, -(1 + 2\lambda)^{-1}, 0, 0] \in V_{\mathcal{H}}$. Thus $[1, -1, 0, -2]^T$ meets \mathcal{H}_{\square} in q points when -1 is a square in \mathbb{F}_q and in $q - 1$ points when -1 is a nonsquare. In this way we find the same counts for points of \mathcal{H}_{\square} on the plane $[1, -1, 0, 2]^T$.² Let N be the set of points of \mathcal{H}_{\square} on one of the planes $[0, 0, 0, 1]^T$, $[1, -1, 0, 2]^T$ or $[1, -1, 0, -2]^T$. The planes in the set $\mathcal{P}_{\mathcal{H}}^{\cap} = \{\alpha_{\omega} = [1, -1, 0, \omega]^T : \omega \neq 0, 2, -2\}$ each contain

²It is possible that we could have made a more geometric argument here.

$(1, 1, 1, 0)$ and $(1, 1, -1, 0)$ and each of the $\frac{q^2-4q+6-4d}{2}$ points of $\mathcal{H}_\square \setminus N$ are on exactly one of these planes, where $d = q - 1$ when $q \equiv 3 \pmod{4}$ and $d = q$ when $q \equiv 1 \pmod{4}$. Each plane in $\mathcal{P}_{\mathcal{H}}^\square$ contains $(1, 1, 1, 0)$ and $(1, 1, -1, 0)$ and meets 2 points of $\mathcal{H} \cap [1, 0, 0, 0]^T$. In particular, $\alpha_\omega = [1, -1, 0, \omega]$ contains the points $(0, 1, \omega^{-1}, \omega^{-1})$ and $(0, 1, -\omega^{-1}, \omega^{-1})$. Thus the planes of $\mathcal{P}_{\mathcal{H}}^\square$ have a total of $\frac{q^2-6q+9}{2}$ incidences with points of $\mathcal{H}_\square \cap ([1, 0, 0, 0]^T \cup \mathcal{H})$, counting the $2(q-3)$ incidences from $\{\alpha_\omega\}$ meeting $(1, 1, 1, 0)$ and $(1, 1, -1, 0)$. Each such incidence yields 2 points on the curve with equation 4.29. Each curve also has 4 points corresponding to the 2 points on the intersection $\alpha_\omega \cap \mathcal{H} \cap [0, 1, 0, 0]^T$. This proves the following theorem.

Theorem 4.5.1 *The family of elliptic curves*

$$\mathbf{E}_\mathcal{E}^\square = \{y^2 = x^3 + (1 - 8\frac{\eta}{\omega^2})x^2 + \left(\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2}\right)x : \omega \in \mathbb{F}_q^*\}$$

contains a total of $q^2 - 1$ \mathbb{F}_q -rational points. The family of elliptic curves

$$\mathbf{E}_\mathcal{E}^\square = \{y^2 = x^3 + \frac{2 - \omega^2}{2}x^2 + \left(\frac{\omega^4}{16} - \frac{\omega^4}{4}\right)x : \omega \in \mathbb{F}_q \setminus \{0, 2, -2\}\}$$

contains a total of $q^2 - 2q - 3$ \mathbb{F}_q -rational points.

4.6 The Invariant j and Symmetry of Incidences

In this section, we show that for the family of planes $\mathcal{P}_\mathcal{E}^\square = \{\alpha_\omega\} = \{[1, -1, 0, \omega]^T\}$, $\omega \in \mathbb{F}_q^*$, the planes meeting \mathcal{E}_\square in $\frac{q+1}{2} + t$ points are in one-to-one correspondence with the planes in $\mathcal{P}_\mathcal{E}^\square$ meeting \mathcal{E}_\square in $\frac{q+1}{2} - t$ points. To prove this result, we require more elementary properties of elliptic curves. Proofs and further discussion of these results may be found in [16] and [22]. For our

results in Section 4.6.2 and beyond, we find it necessary to restrict ourselves to finite fields \mathbb{F}_q where $q = p^e$ and $p > 3$.

4.6.1 Admissible Changes of Variables

For the finite field \mathbb{F}_q , let $\overline{\mathbb{F}}_q$ denote the algebraic closure of \mathbb{F}_q . As usual, $\omega \in \mathbb{F}_q^*$ and η is a nonsquare in \mathbb{F}_q . Two elliptic curves with Weierstrass equations $y_1^2 = f(x_1)$ and $y_2^2 = g(x_2)$ with coefficients in \mathbb{F}_q are isomorphic over $\overline{\mathbb{F}}_q$ if and only if there exists a linear change of variables of the form

$$\begin{aligned} x_1 &= u^2 x_2 + r \\ y_1 &= u^3 y_2 + s u^2 x_2 + t \end{aligned} \tag{4.41}$$

where $r, s, t \in \overline{\mathbb{F}}_q$ and $u \in \overline{\mathbb{F}}_q^*$. The curves

$$E = \{(x, y) : y^2 = x^3 + ax^2 + bx + c\} \cup \{(\infty)\}$$

and

$$E^\eta = \{(x, y) : \eta y^2 = x^3 + ax^2 + bx + c\} \cup \{(\infty)\}$$

are seen to be isomorphic over $\overline{\mathbb{F}}_q$, via the substitution $y \mapsto \sqrt{\eta}^{-1}y$. In this case we say that E^η is a *twist* of E by η . E and E^η are isomorphic over F_{q^2} , and since any nonsquare $\beta \in \mathbb{F}_q$ may be written $\beta = \eta\alpha^2$ for some $\alpha \in \mathbb{F}_q$, the twist of E is unique up to isomorphism.

Proposition 4.6.2 *Let E and E^η be elliptic curves given by $y^2 = f(x)$ and $\eta y^2 = f(x)$, respectively, where $f(x) = x^3 + ax^2 + bx + c$ and let $\#E$ be the number of points on E over \mathbb{F}_q . Then $\#E + \#E^\eta = 2(q + 1)$.*

Proof: For each zero x of f , the point $(x, 0)$ is on both E and E^η . Say f has m zeros. Then for each of the remaining $q - m$ elements x of \mathbb{F}_q , $f(x)$ is either

square or nonsquare, yielding two points on either E or E^η . The two points at infinity give the desired sum. \blacksquare

Recall that the curve E_ω from the plane π_ω in orbit $\mathcal{O}_{\mathcal{E}_\square}^{\omega \cap}$ has k points if and only if the plane α_ω meets \mathcal{E}_\square in exactly $\frac{k}{2}$ points. To show that the symmetry of incidences observed in Section 4.1 holds for all q , by Proposition 4.6.2 it will be sufficient to show that for $\omega \neq 0$, the elliptic curve $E_\omega = \{(x, y) : y^2 = x^3 + (1 - 8\frac{\eta}{\omega^2})x^2 + (\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2})x\} \cup \{(\infty)\}$ has as a twist the curve E_δ for some $\delta \neq 0$. Consider the twist $E_\omega^{\eta^{-1}}$

$$\eta^{-1}y^2 = x^3 + \left(1 - 8\frac{\eta}{\omega^2}\right)x^2 + \left(\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2}\right)x$$

and make the substitutions $x \mapsto a^{-2}\eta^{-1}x + r$ and $y \mapsto a^{-3}\eta^{-1}y$, yielding

$$y^2 = x^3 + \frac{a^2\eta(\omega^2(3r+1) - 8\eta)}{\omega^2}x^2 + \frac{a^4\eta^2(16\eta^2 - 4\eta\omega^2(4r+1) + r\omega^4(3r+2))}{\omega^4}x + \frac{a^6\eta^3r(16\eta^2 - 4\eta\omega^2(2r+1) + r\omega^4(r+1))}{\omega^4}$$

after clearing denominators. Put $r = \frac{4\eta - \omega^2}{\omega^2}$ and $a = \frac{\omega}{2\eta}$ to obtain, after simplification

$$y^2 = x^3 + \frac{2\eta - \omega^2}{2\eta}x^2 + \frac{\omega^4 - 4\eta\omega^2}{16\eta^2}x.$$

Multiply the numerator and denominator of the coefficient on x^2 by $(\frac{4\eta}{\omega})^2 \frac{1}{2\eta}$, and multiply the numerator and denominator of the coefficient on x by $(\frac{4\eta}{\omega^2})^2$, whence

$$y^2 = x^3 + \left(1 - 8\frac{\eta}{(\frac{4\eta}{\omega})^2}\right)x^2 + \left(\frac{16\eta^2}{(\frac{4\eta}{\omega})^4} - \frac{4\eta}{(\frac{4\eta}{\omega})^2}\right)x.$$

So the curve E_δ is a twist of E_ω when $\delta = \frac{4\eta}{\omega}$. Note that $\frac{4\eta}{\omega} = \omega$ implies $\eta = \left(\frac{\omega}{2}\right)^2$, contrary to the assumption that η is a nonsquare, so $\delta \neq \omega$. Thus for each E_ω in $\mathbf{E}_\mathcal{E}^\square$ with $q + 1 + t$ points, there is a different curve E_δ in $\mathbf{E}_\mathcal{E}^\square$ with $q + 1 - t$ points. This proves the following theorem.

Theorem 4.6.3 *In the family of elliptic curves over \mathbb{F}_q*

$$\mathbf{E}_\mathcal{E}^\square = \left\{ y^2 = x^3 + \left(1 - 8\frac{\eta}{\omega^2}\right)x^2 + \left(\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2}\right)x : \omega \in \mathbb{F}_q^* \right\},$$

if E_ω is a curve in $\mathbf{E}_\mathcal{E}^\square$ then E_ω^η is in $\mathbf{E}_\mathcal{E}^\square$ as well. Further, if a particular curve E_ω is represented k times in $\mathbf{E}_\mathcal{E}^\square$ then E_ω^η is represented k times in $\mathbf{E}_\mathcal{E}^\square$.

We can restate this in terms of the plane intersections $\alpha_\omega \cap \mathcal{E}_\square$. If α_ω meets \mathcal{E}_\square in $\frac{q+1}{2} + \frac{t}{2}$ points, then α_δ meets \mathcal{E}_\square in $\frac{q+1}{2} - \frac{t}{2}$ points, where $\delta = \frac{4\eta}{\omega}$. The statement of the relevant theorem for plane intersections is part of Theorem 4.6.6.

We might ask how often these complementary pairs of planes (and complementary pairs of elliptic curves) occur in our various families. To find an answer to this, we invoke more of the theory of elliptic curves. For the remainder of this section, assume that we are working over a finite field \mathbb{F}_q , where $q = p^e$ for some positive integer e and for a prime $p > 3$.

4.6.4 The Invariant j

To an elliptic curve given by a Weierstrass equation with coefficients in a field \mathbb{F} , it is possible to associate a value $j \in \mathbb{F}$, the j -invariant of the curve that is invariant under an admissible change of variables, 4.41. Thus any two curves with the same j -invariant are isomorphic over the algebraic closure of \mathbb{F} . For curves with Weierstrass equation $y^2 = x^3 + ax^2 + bx$, the j -invariant is given by

$$j = \frac{256(a^2 - 3b)^3}{b^2(a^2 - 4b)}. \quad (4.42)$$

For details of the derivation and properties of j , see Chapter 3, section 3 of [16]. The curves given by equation 4.13 for $\omega \in \mathbb{F}_q^*$ are the curves $\mathbf{E}_\mathcal{E}^\square$ and were shown to be isomorphic, as a set, to the curves $\mathbf{E}_{\mathcal{J}\mathcal{C}}^\square$. Further, we found that whenever a curve E_ω is in the set

$$\mathbf{E}_\mathcal{E}^\square = \left\{ y^2 = x^3 + \left(1 - 8\frac{\eta}{\omega^2}\right)x^2 + \left(\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2}\right)x : \omega \in \mathbb{F}_q^* \right\} \quad (4.43)$$

a quadratic twist E_ω^η of that curve is also in $\mathbf{E}_\mathcal{E}^\square$, and that a curve and its twist occur the same number of times. From formula 4.42, the j invariants for this family of curves are

$$j = \frac{16(16\eta^2 - 4\eta\omega^2 + \omega^4)}{\eta^2\omega^4(4\eta - \omega^2)^2} \quad (4.44)$$

for $\omega \in \mathbb{F}_q^*$. We have already seen that the curves E_ω and $E_{\frac{4\eta}{\omega}}$ are proper twists of one another, (and so are isomorphic over \mathbb{F}_{q^2} but not necessarily isomorphic over \mathbb{F}_q) and that E_ω and $E_{-\omega}$ are isomorphic over \mathbb{F}_q . Solving

$$\frac{16(16\eta^2 - 4\eta\delta^2 + \delta^4)}{\eta^2\delta^4(4\eta - \delta^2)^2} = \frac{16(16\eta^2 - 4\eta\omega^2 + \omega^4)}{\eta^2\omega^4(4\eta - \omega^2)^2} \quad (4.45)$$

for δ , the solution set is

$$\left\{ \pm\omega, \pm\frac{4\eta}{\omega}, \pm\frac{4\eta}{\sqrt{4\eta - \omega^2}}, \pm\sqrt{4\eta - \omega^2}, \pm\frac{2\sqrt{\eta\omega}}{\sqrt{\omega^2 - 4\eta}}, \pm\frac{2\sqrt{\eta\omega^2 - 4\eta^2}}{\omega} \right\}$$

and we find that there are at most 12 values of δ such that $E_\omega \cong E_\delta$ over \mathbb{F}_q .

For the curves

$$\mathbf{E}_\mathcal{E}^\square = \left\{ y^2 = x^3 + \frac{2 - \omega^2}{2}x^2 + \left(\frac{\omega^4}{16} - \frac{\omega^2}{4}\right)x : \omega \in \mathbb{F}_q^*, \omega \neq \pm 2 \right\}$$

the j -invariants are

$$j = \frac{16(\omega^4 - 4\omega^2 + 16)^3}{\omega^4(\omega^2 - 4)^2} \quad \omega \in \mathbb{F}_q^* \setminus \{2, -2\}$$

and in this case the values of δ such that $E_\omega \cong E_\delta$ are

$$\delta \in \left\{ \pm\omega, \pm\frac{4}{\omega}, \pm\frac{4}{\sqrt{4-\omega^2}}, \pm\sqrt{4-\omega^2}, \pm\frac{2\omega}{\sqrt{\omega^2-4}}, \pm\frac{2\sqrt{\omega^2-4}}{\omega} \right\}. \quad (4.46)$$

The curves E_ω and $E_{\frac{4}{\omega}}$ are easily seen to be isomorphic over \mathbb{F}_q . When $q \equiv 1 \pmod{4}$, $\omega^2 - 4$ and $4 - \omega^2$ are either both square or both nonsquare. A simple count shows that for some values of ω , both $\omega^2 - 4$ and $4 - \omega^2$ are nonsquare. Thus it is possible that the family of curves $\mathbf{E}_\mathcal{E}^\eta$ does not contain a proper twist of E_ω for every $\omega \in \mathbb{F}_q^*$. When $q \equiv 3 \pmod{4}$, exactly one of $\omega^2 - 4$ or $4 - \omega^2$ is a square, and it is straightforward to check that for each $\omega \in \mathbb{F}_q$, at least one value of δ in 4.46 gives a twist of E_ω by -1 . We interpret this result in terms of plane intersections with \mathcal{E}_\square and \mathcal{H}_\square .

Theorem 4.6.5 *Assume that $q \equiv 3 \pmod{4}$. Let $\mathcal{P}_{\mathcal{H}}^\square = \mathcal{P}_\mathcal{E}^\square = \{[1, -1, 0, \omega] : \omega \in \mathbb{F}_q^*, \omega \neq \pm 2\}$ and $\mathcal{P}_{\mathcal{H}}^\eta = \mathcal{P}_\mathcal{E}^\eta = \{[1, -\eta^{-1}, 0, \omega] : \omega \in \mathbb{F}_q^*, \omega \neq \pm 2\}$. Then for each plane in $\mathcal{P}_{\mathcal{H}}^\square$ meeting \mathcal{H}_\square in $\frac{q-3}{2} + t$ points for some integer t , there is a plane in $\mathcal{P}_{\mathcal{H}}^\square$ meeting \mathcal{H}_\square in $\frac{q-3}{2} - t$ points. If there is a plane in $\mathcal{P}_{\mathcal{E}}^\eta$ meeting \mathcal{E}_\square in $\frac{q+1}{2} + t$ points for some integer t , then there is a plane in $\mathcal{P}_{\mathcal{E}}^\eta$ meeting \mathcal{E}_\square in $\frac{q+1}{2} - t$ points.*

We restate our theorems on the symmetry of families of elliptic curves in terms of symmetries of families of orbits of planes under the actions of G_{l_\square} and H_{l_\square} .

Theorem 4.6.6 *Let $q = p^e$ be a prime power with $p > 3$, and let $\{\mathcal{O}_{\mathcal{E}_\square}^{\omega \square}\}_{\omega \in \mathbb{F}_q^*}$, $\{\mathcal{O}_{\mathcal{E}_\square}^{\omega \eta}\}_{\omega \in \mathbb{F}_q^*}$, $\{\mathcal{O}_{\mathcal{H}_\square}^{\omega \square}\}_{\omega \in \mathbb{F}_q^*}$, and $\{\mathcal{O}_{\mathcal{H}_\square}^{\omega \eta}\}_{\omega \in \mathbb{F}_q^*}$ be families of orbits of planes as described in Theorems 3.4.2 and 3.4.4.*

1. For each orbit in $\{\mathcal{O}_{\mathcal{E}_{\square}}^{\omega \cap}\}_{\omega \in \mathbb{F}_q^*}$ whose planes meet \mathcal{E}_{\square} in $\frac{q+1}{2} + t$ points, there is an orbit whose planes meet \mathcal{E}_{\square} in $\frac{q+1}{2} - t$ points.
2. For each orbit in $\{\mathcal{O}_{\mathcal{H}_{\square}}^{\omega \cap}\}_{\omega \in \mathbb{F}_q^*}$ whose planes meet \mathcal{H}_{\square} in $\frac{q-3}{2} + t$ points, there is an orbit whose planes meet \mathcal{H}_{\square} in $\frac{q-3}{2} - t$ points.
3. When $q \equiv 3 \pmod{4}$, for each orbit in $\{\mathcal{O}_{\mathcal{E}_{\square}}^{\omega \cap}\}_{\omega \in \mathbb{F}_q^*}$ whose planes meet \mathcal{E}_{\square} in $\frac{q+1}{2} + t$ points, there is an orbit whose planes meet \mathcal{E}_{\square} in $\frac{q+1}{2} - t$ points.
4. When $q \equiv 3 \pmod{4}$, for each orbit in $\{\mathcal{O}_{\mathcal{H}_{\square}}^{\omega \cap}\}_{\omega \in \mathbb{F}_q^*}$ whose planes meet \mathcal{H}_{\square} in $\frac{q-3}{2} + t$ points, there is an orbit whose planes meet \mathcal{H}_{\square} in $\frac{q-3}{2} - t$ points.

Proof: These statements are an immediate consequence of Theorem 4.6.5 and the correspondences between points of the truncated quadrics on planes of the stated orbits and their associated elliptic curves. ■

Appendix B contains tables for the number of points on the two families of elliptic curves which we have studied for primes $q < 200$. Table 4.2 is an example and may be viewed as a refinement of Figure 4.1. The first column states the number N of points on a curve and the second column states the j -invariants of the curves which occur having N points, followed in parentheses by the number of times that particular curve occurs. Referring to Table 4.2, we see in this example that there are 2 curves with 232 points having j -invariant 44. This agrees with the first row of Figure 4.1, which shows 2 planes of $\mathcal{P}_{\mathcal{E}}^{\square}$ meet \mathcal{E}_{\square} in exactly 116 points.

Table 4.2: The number of \mathbb{F}_q -rational points on elliptic curves $E = E_{\mathcal{E}}^{\omega}$ for $\omega \in \mathbb{F}_{263}$, their j -invariants and multiplicities in $\mathbf{E}_{\mathcal{E}}^{\cap}$.

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
232	44(2)
236	153(6)
240	60(2) 93(2) 109(2) 143(2) 159(2) 163(2) 168(2) 189(2) 212(2) 245(2)
244	20(6)
248	23(2) 30(2) 35(2) 156(2) 166(2) 211(2) 218(2) 242(2) 261(2)
252	94(6) 103(6) 120(6) 162(6) 193(6)
256	129(2) 161(2) 175(2) 199(2) 239(2) 253(2)
260	15(6) 71(6) 187(6) 225(6)
264	31(4) 37(4) 85(4) 108(4) 110(4) 150(2) 184(4)
268	15(6) 71(6) 187(6) 225(6)
272	129(2) 161(2) 175(2) 199(2) 239(2) 253(2)
276	94(6) 103(6) 120(6) 162(6) 193(6)
280	23(2) 30(2) 35(2) 156(2) 166(2) 211(2) 218(2) 242(2) 261(2)
284	20(6)
288	60(2) 93(2) 109(2) 143(2) 159(2) 163(2) 168(2) 189(2) 212(2) 245(2)
292	153(6)
296	44(2)

Appendix A. Additional Results

The results given in this appendix are not used elsewhere in this thesis. The logical place for Appendix A.1 is after Section 3.1, and we adopt the notation and perspective taken up through that point.

In Appendix A.2, we give equations for application of the chord-tangent group law on an elliptic curve from the family $\mathbf{E}_{\mathcal{E}}^{\square}$.

A.1 $q - 1$ Elliptic Quadrics Intersecting in 2 Points

We take a moment to show that the orbits under G_l of the lines $m = \langle (1, 1, 1, 0), (1, 1, -1, 0) \rangle$ and $m' = \langle (1, \eta, 1, 0), (1, \eta, -1, 0) \rangle$ carry the points of a number of elliptic quadrics, any two of which meet in the points $(1, 0, 0, 0)$ and $(0, 1, 0, 0)$. The orbit of the point $(1, \eta, 1, 0)$ under G_l , together with $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$ form the elliptic quadric $\mathcal{E}_1 = \{\mathbf{x} : \mathbf{x}E_1\mathbf{x}^T = 0\}$ where

$$E_1 = \begin{bmatrix} 0 & \frac{\eta}{2} & 0 & 0 \\ \frac{\eta}{2} & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2\eta \end{bmatrix}.$$

Choose η to be a primitive element of \mathbb{F}_q , and for $1 \leq n \leq q - 1$, put

$$\overline{E}_n = \begin{bmatrix} 0 & \frac{\eta^n}{2} & 0 & 0 \\ \frac{\eta^n}{2} & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2\eta \end{bmatrix}.$$

Then each $\mathcal{E}_n = \{\mathbf{x} : \mathbf{x} \overline{E}_n \mathbf{x}^T = 0\}$ is an elliptic quadric, and $\{\mathcal{E}_n\}_{n=1}^{q-1}$ is a family of $q-1$ elliptic quadrics pairwise intersecting only in $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$. An alternative description is

$$\mathcal{E}_n = \{(1, \eta^n(s^2 - \eta t^2), s, t) : s, t \in \mathbb{F}_q\} \cup \{(0, 1, 0, 0)\}. \quad (\text{A.1})$$

Each \mathcal{E}_n is stabilized by G_l , and $\mathcal{E} = \mathcal{E}_k$, where $\eta^k = 2$. Let $D = \text{diag}[1, \eta, 1, 1]$. Then $\langle D \rangle$ permutes $\{\mathcal{E}_n\}$ in a cycle. Each \mathcal{E}_n , $1 \leq n \leq q-1$ is stabilized by matrices of the form

$$[\tau_{a,b}^n] = \begin{bmatrix} 1 & \eta^n(a^2 - \eta b^2) & a & b \\ 0 & 1 & 0 & 0 \\ 0 & 2a & 1 & 0 \\ 0 & -2\eta b & 0 & 1 \end{bmatrix}.$$

and we find that the complete group of \mathcal{E}_n is generated by the set of all such $[\tau_{a,b}^n]$ and G_l . Note that n here is not an exponent, merely a superscript on $[\tau_{a,b}^n]$. Thus the group that stabilizes the set $\{\mathcal{E}_n\}$ of $q-1$ quadrics is generated by G_l and D .

A.2 Addition on the Curves

It is well known that the rational points of an elliptic curve, together with a point ∞ form a group with identity ∞ under a law of composition derived from the construction of chords and tangents to the curve. See Chapter 2 of [25] for proof and a discussion. For the sake of completeness, we include the addition formulae for the elliptic curve E_ω whose equation is

$$y^2 = x^3 + \left(1 - 8\frac{\eta}{\omega^2}\right)x^2 + \left(\frac{16\eta^2}{\omega^4} - \frac{4\eta}{\omega^2}\right)x.$$

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on \mathcal{C} . If $P \neq Q$ then $P+Q = (x_3, y_3)$ is given by

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 + 8 \frac{\eta}{\omega^2} - 1 - x_1 - x_2$$

$$y_3 = \frac{y_1 - y_2}{x_2 - x_1} x_3 + \frac{x_1 y_2 - x_2 y_1}{x_2 - x_1}.$$

If $P = (x_1, 0)$, then $2P = (\infty)$. Otherwise, to find $2P$, let

$$m = \frac{1}{2y_1} \left(3x_1^2 + 2 \left(1 - 8 \frac{\eta}{\omega^2} \right) x_1 + 4 \left(\frac{4\eta^2}{\omega^4} - \frac{\eta}{\omega^2} \right) \right).$$

Then

$$x_3 = m^2 + 8 \frac{\eta}{\omega^2} - 1 - 2x_1$$

$$y_3 = m(x_3 - x_1) + y_1.$$

Each point $(x, 0)$ on the curve is an element of order 2, so the order of the group of the curve is divisible by 4.

We may use the birational transformations 4.16 and 4.17 to obtain formulae for addition on the nonsingular points of the curve \mathcal{C}_F with equation 4.12. The resulting equations are quite messy and we will not reproduce them here.

Appendix B. Tables of Elliptic Curves

B.1 Tables for Elliptic Curves

In Theorem 4.3.7, it was shown that in the analysis of certain plane intersections with the point sets \mathcal{E}_\square and \mathcal{H}_\square , there arise two families of elliptic curves, which we call $\mathbf{E}_\mathcal{E}^\cap$ and $\mathbf{E}_\mathcal{E}^\not\cap$. In keeping with the remainder of this thesis, q is a power of an odd prime, and η is a fixed nonsquare element in \mathbb{F}_q . We restate equations 4.39 and 4.40. Our families of curves are

$$\mathbf{E}_\mathcal{E}^\not\cap = \{y^2 = x(x - a^2)(x - (a^2 - 1)) : a \in \mathbb{F}_q^* \setminus \{1, -1\}\} \quad (\text{B.1})$$

and

$$\mathbf{E}_\mathcal{E}^\cap = \{y^2 = x(x - \eta a^2)(x - (\eta a^2 - 1)) : a \in \mathbb{F}_q^*\}. \quad (\text{B.2})$$

In this appendix, we present tables for the families of curves which arise from truncated quadrics when $q < 200$ is an odd prime. Recall from Section 4.6.4 that two elliptic curves are isomorphic over the algebraic closure of \mathbb{F}_q if and only if their j -invariants are equal. Each table lists in the first column N , the number of points on a curve E in that family, and in the second column are given the j -invariants of the curves that arise with N points, followed in parenthesis by the number of curves in the family with that j -invariant and N points. For example, when $q = 7$, the family of curves $\mathbf{E}_\mathcal{E}^\cap$ contains 2 curves with 4 points and j -invariant 0, 2 curves with 8 points and j -invariant 6, and 2 curves with 12 points and j -invariant 0. The family $\mathbf{E}_\mathcal{E}^\not\cap$ contains 4 curves with j -invariant 6. Recall that $\mathbf{E}_\mathcal{E}^\not\cap$ contains 2 fewer curves because the line which carries the corresponding planes is the intersection of two tangent planes.

Table B.1: Point counts and j -invariants for curves over \mathbb{F}_3

$\mathbf{E}_\varepsilon^\square$	
$ E $	j-invariant (number of curves)
4	0(2)

$\mathbf{E}_\varepsilon^\triangleright$	
$ E $	j-invariant (number of curves)
	(0)

Table B.2: Point counts and j -invariants for curves over \mathbb{F}_5

$\mathbf{E}_\varepsilon^\square$	
$ E $	j-invariant (number of curves)
4	3(2)
8	3(2)

$\mathbf{E}_\varepsilon^\triangleright$	
$ E $	j-invariant (number of curves)
8	3(2)

Table B.3: Point counts and j -invariants for curves over \mathbb{F}_7

$\mathbf{E}_\varepsilon^\square$	
$ E $	j-invariant (number of curves)
4	0(2)
8	6(2)
12	0(2)

$\mathbf{E}_\varepsilon^\triangleright$	
$ E $	j-invariant (number of curves)
8	6(4)

Table B.4: Point counts and j -invariants for curves over \mathbb{F}_{11}

$\mathbf{E}_\varepsilon^\square$	
$ E $	j-invariant (number of curves)
8	2(2)
12	1(6)
16	2(2)

$\mathbf{E}_\varepsilon^\triangleright$	
$ E $	j-invariant (number of curves)
8	2(4)
16	2(4)

Table B.5: Point counts and j -invariants for curves over \mathbb{F}_{13}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
8	12(2)
12	11(4)
16	11(4)
20	12(2)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j-invariant (number of curves)
8	12(2)
16	0(4) 11(4)

Table B.6: Point counts and j -invariants for curves over \mathbb{F}_{17}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
12	10(4)
16	9(4)
20	9(4)
24	10(4)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j-invariant (number of curves)
16	9(4) 11(6)
24	10(4)

Table B.7: Point counts and j -invariants for curves over \mathbb{F}_{19}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
12	0(2)
16	5(2) 15(2)
20	18(6)
24	5(2) 15(2)
28	0(2)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j-invariant (number of curves)
16	5(4) 15(4)
24	5(4) 15(4)

Table B.8: Point counts and j -invariants for curves over \mathbb{F}_{23}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j -invariant (number of curves)
16	6(2)
20	5(6)
24	3(2) 19(4)
28	5(6)
32	6(2)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j -invariant (number of curves)
16	6(4)
24	3(4) 19(8)
32	6(4)

Table B.9: Point counts and j -invariants for curves over \mathbb{F}_{29}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j -invariant (number of curves)
20	17(2)
24	12(4) 23(4)
28	16(4)
32	16(4)
36	12(4) 23(4)
40	17(2)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j -invariant (number of curves)
24	12(4) 23(4)
32	16(4) 18(12)
40	17(2)

Table B.10: Point counts and j -invariants for curves over \mathbb{F}_{31}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j -invariant (number of curves)
24	11(2) 17(2)
28	0(2) 28(6)
32	2(4) 23(2)
36	0(2) 28(6)
40	11(2) 17(2)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j -invariant (number of curves)
24	11(4) 17(4)
32	2(8) 23(4)
40	11(4) 17(4)

Table B.11: Point counts and j -invariants for curves over \mathbb{F}_{37}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
28	17(4)
32	10(4)
36	15(4) 26(2) 30(4)
40	15(4) 26(2) 30(4)
44	10(4)
48	17(4)

$\mathbf{E}_{\mathcal{E}}^{\nabla}$	
$ E $	j -invariant (number of curves)
32	10(4) 29(12)
40	15(4) 26(2) 30(4)
48	0(4) 17(4)

Table B.12: Point counts and j -invariants for curves over \mathbb{F}_{41}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
32	4(4)
36	22(4) 29(4)
40	11(4) 39(4)
44	11(4) 39(4)
48	22(4) 29(4)
52	4(4)

$\mathbf{E}_{\mathcal{E}}^{\nabla}$	
$ E $	j -invariant (number of curves)
32	4(4) 6(6)
40	11(4) 39(4)
48	5(12) 22(4) 29(4)

Table B.13: Point counts and j -invariants for curves over \mathbb{F}_{43}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
32	22(2)
36	0(2) 24(6)
40	9(2) 12(2) 29(2) 31(2)
44	8(6)
48	9(2) 12(2) 29(2) 31(2)
52	0(2) 24(6)
56	22(2)

$\mathbf{E}_{\mathcal{E}}^{\nabla}$	
$ E $	j -invariant (number of curves)
32	22(4)
40	9(4) 12(4) 29(4) 31(4)
48	9(4) 12(4) 29(4) 31(4)
56	22(4)

Table B.14: Point counts and j -invariants for curves over \mathbb{F}_{47}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
36	38(6)
40	16(2) 25(2) 26(2)
44	37(6)
48	10(4) 36(2) 44(4)
52	37(6)
56	16(2) 25(2) 26(2)
60	38(6)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j -invariant (number of curves)
40	16(4) 25(4) 26(4)
48	10(8) 36(4) 44(8)
56	16(4) 25(4) 26(4)

Table B.15: Point counts and j -invariants for curves over \mathbb{F}_{53}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
40	32(2)
44	7(4)
48	8(4) 22(4) 42(4)
52	25(4) 45(4)
56	25(4) 45(4)
60	8(4) 22(4) 42(4)
64	7(4)
68	32(2)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j -invariant (number of curves)
40	32(2)
48	8(4) 22(4) 39(12) 42(4)
56	25(4) 45(4)
64	7(4) 17(12)

Table B.16: Point counts and j -invariants for curves over \mathbb{F}_{59}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
48	20(2) 42(2) 44(2)
52	34(6)
56	7(2) 38(2) 43(2) 53(2)
60	15(12) 17(6)
64	7(2) 38(2) 43(2) 53(2)
68	34(6)
72	20(2) 42(2) 44(2)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j -invariant (number of curves)
48	20(4) 42(4) 44(4)
56	7(4) 38(4) 43(4) 53(4)
64	7(4) 38(4) 43(4) 53(4)
72	20(4) 42(4) 44(4)

Table B.17: Point counts and j -invariants for curves over \mathbb{F}_{61}

\mathbf{E}_{ξ}^{\cap}	
$ E $	j -invariant (number of curves)
48	15(4)
52	20(2) 35(4) 40(4)
56	1(4) 33(4)
60	4(4) 6(4)
64	4(4) 6(4)
68	1(4) 33(4)
72	20(2) 35(4) 40(4)
76	15(4)

$\mathbf{E}_{\xi}^{\cap'}$	
$ E $	j -invariant (number of curves)
48	0(4) 15(4)
56	1(4) 33(4)
64	4(4) 6(4) 32(12) 56(12)
72	20(2) 35(4) 40(4)

Table B.18: Point counts and j -invariants for curves over \mathbb{F}_{67}

\mathbf{E}_{ξ}^{\cap}	
$ E $	j -invariant (number of curves)
52	0(2)
56	3(2) 9(2) 22(2)
60	12(6) 23(6)
64	33(2) 35(2) 42(2) 51(2) 57(2)
68	53(6)
72	33(2) 35(2) 42(2) 51(2) 57(2)
76	12(6) 23(6)
80	3(2) 9(2) 22(2)
84	0(2)

$\mathbf{E}_{\xi}^{\cap'}$	
$ E $	j -invariant (number of curves)
56	3(4) 9(4) 22(4)
64	33(4) 35(4) 42(4) 51(4) 57(4)
72	33(4) 35(4) 42(4) 51(4) 57(4)
80	3(4) 9(4) 22(4)

Table B.19: Point counts and j -invariants for curves over \mathbb{F}_{71}

$\mathbf{E}_{\xi}^{\square}$	
$ E $	j -invariant (number of curves)
56	33(2)
60	25(6) 42(6)
64	7(2) 11(2) 56(2) 60(2)
68	32(6)
72	17(4) 24(2) 40(4) 48(4)
76	32(6)
80	7(2) 11(2) 56(2) 60(2)
84	25(6) 42(6)
88	33(2)

$\mathbf{E}_{\xi}^{\triangleright}$	
$ E $	j -invariant (number of curves)
56	33(4)
64	7(4) 11(4) 56(4) 60(4)
72	17(8) 24(4) 40(8) 48(8)
80	7(4) 11(4) 56(4) 60(4)
88	33(4)

Table B.20: Point counts and j -invariants for curves over \mathbb{F}_{73}

$\mathbf{E}_{\xi}^{\square}$	
$ E $	j -invariant (number of curves)
60	26(4) 55(4)
64	47(4) 50(4)
68	52(4) 72(4)
72	25(4) 41(4) 43(4)
76	25(4) 41(4) 43(4)
80	52(4) 72(4)
84	47(4) 50(4)
88	26(4) 55(4)

$\mathbf{E}_{\xi}^{\triangleright}$	
$ E $	j -invariant (number of curves)
64	0(4) 47(4) 50(4) 53(12)
72	25(4) 41(4) 43(4)
80	22(12) 49(6) 52(4) 72(4)
88	26(4) 55(4)

Table B.21: Point counts and j -invariants for curves over \mathbb{F}_{79}

$\mathbf{E}_{\xi}^{\square}$	
$ E $	j -invariant (number of curves)
64	3(2) 73(2)
68	10(6)
72	22(2) 26(2) 42(2) 74(2) 77(2)
76	0(2) 34(6) 63(6)
80	15(4) 21(4) 69(2)
84	0(2) 34(6) 63(6)
88	22(2) 26(2) 42(2) 74(2) 77(2)
92	10(6)
96	3(2) 73(2)

$\mathbf{E}_{\xi}^{\triangleright}$	
$ E $	j -invariant (number of curves)
64	3(4) 73(4)
72	22(4) 26(4) 42(4) 74(4) 77(4)
80	15(8) 21(8) 69(4)
88	22(4) 26(4) 42(4) 74(4) 77(4)
96	3(4) 73(4)

Table B.22: Point counts and j -invariants for curves over \mathbb{F}_{83}

$\mathbf{E}_{\xi}^{\square}$	
$ E $	j -invariant (number of curves)
68	44(6)
72	2(2) 11(2) 49(2) 53(2) 69(2)
76	66(6)
80	8(2) 14(2) 16(2) 78(2) 80(2)
84	50(12) 68(6)
88	8(2) 14(2) 16(2) 78(2) 80(2)
92	66(6)
96	2(2) 11(2) 49(2) 53(2) 69(2)
100	44(6)

$\mathbf{E}_{\xi}^{\triangleright}$	
$ E $	j -invariant (number of curves)
72	2(4) 11(4) 49(4) 53(4) 69(4)
80	8(4) 14(4) 16(4) 78(4) 80(4)
88	8(4) 14(4) 16(4) 78(4) 80(4)
96	2(4) 11(4) 49(4) 53(4) 69(4)

Table B.23: Point counts and j -invariants for curves over \mathbb{F}_{89}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
72	79(4)
76	42(4) 62(4)
80	17(4) 46(4)
84	41(4) 54(4) 55(4) 59(4)
88	29(4) 39(4)
92	29(4) 39(4)
96	41(4) 54(4) 55(4) 59(4)
100	17(4) 46(4)
104	42(4) 62(4)
108	79(4)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
72	79(4)
80	17(4) 26(12) 37(6) 46(4)
88	29(4) 39(4)
96	1(12) 21(12) 41(4) 54(4) 55(4) 59(4)
104	42(4) 62(4)

Table B.24: Point counts and j -invariants for curves over \mathbb{F}_{97}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
80	85(4)
84	76(4) 83(4)
88	44(4) 46(4) 80(4)
92	63(4) 78(4)
96	6(4) 31(4) 36(4) 48(4)
100	6(4) 31(4) 36(4) 48(4)
104	63(4) 78(4)
108	44(4) 46(4) 80(4)
112	76(4) 83(4)
116	85(4)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
80	79(6) 85(4)
88	44(4) 46(4) 80(4)
96	6(4) 15(12) 31(4) 36(4) 48(4) 61(12)
104	63(4) 78(4)
112	0(4) 68(12) 76(4) 83(4)

Table B.25: Point counts and j -invariants for curves over \mathbb{F}_{101}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
84	7(4) 79(4)
88	6(4) 54(4)
92	41(4) 81(4) 88(4)
96	27(4) 60(4) 98(4)
100	11(2) 42(4) 69(4)
104	11(2) 42(4) 69(4)
108	27(4) 60(4) 98(4)
112	41(4) 81(4) 88(4)
116	6(4) 54(4)
120	7(4) 79(4)

$\mathbf{E}_{\mathcal{E}}^{\not\square}$	
$ E $	j-invariant (number of curves)
88	6(4) 54(4)
96	27(4) 28(12) 30(12) 60(4) 65(12) 98(4)
104	11(2) 42(4) 69(4)
112	24(12) 41(4) 81(4) 88(4)
120	7(4) 79(4)

Table B.26: Point counts and j -invariants for curves over \mathbb{F}_{103}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
84	0(2)
88	40(2) 49(2) 84(2) 99(2)
92	93(6)
96	5(2) 29(2) 32(2) 43(2) 60(2) 70(2)
100	58(6) 89(6) 97(6)
104	23(4) 69(4) 80(2)
108	58(6) 89(6) 97(6)
112	5(2) 29(2) 32(2) 43(2) 60(2) 70(2)
116	93(6)
120	40(2) 49(2) 84(2) 99(2)
124	0(2)

$\mathbf{E}_{\mathcal{E}}^{\not\square}$	
$ E $	j-invariant (number of curves)
88	40(4) 49(4) 84(4) 99(4)
96	5(4) 29(4) 32(4) 43(4) 60(4) 70(4)
104	23(8) 69(8) 80(4)
112	5(4) 29(4) 32(4) 43(4) 60(4) 70(4)
120	40(4) 49(4) 84(4) 99(4)

Table B.27: Point counts and j -invariants for curves over \mathbb{F}_{107}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
88	49(2)
92	27(6)
96	19(2) 30(2) 46(2) 57(2) 63(2) 64(2) 77(2)
100	32(6) 103(6)
104	26(2) 39(2) 43(2) 69(2) 97(2)
108	16(6) 72(12)
112	26(2) 39(2) 43(2) 69(2) 97(2)
116	32(6) 103(6)
120	19(2) 30(2) 46(2) 57(2) 63(2) 64(2) 77(2)
124	27(6)
128	49(2)

$\mathbf{E}_{\mathcal{E}}^{\not\square}$	
$ E $	j-invariant (number of curves)
88	49(4)
96	19(4) 30(4) 46(4) 57(4) 63(4) 64(4) 77(4)
104	26(4) 39(4) 43(4) 69(4) 97(4)
112	26(4) 39(4) 43(4) 69(4) 97(4)
120	19(4) 30(4) 46(4) 57(4) 63(4) 64(4) 77(4)
128	49(4)

Table B.28: Point counts and j -invariants for curves over \mathbb{F}_{109}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
92	77(4)
96	29(4) 67(4)
100	10(4) 15(4) 58(4) 84(4)
104	19(4) 86(4) 93(2)
108	22(4) 45(4) 65(4) 94(4)
112	22(4) 45(4) 65(4) 94(4)
116	19(4) 86(4) 93(2)
120	10(4) 15(4) 58(4) 84(4)
124	29(4) 67(4)
128	77(4)

$\mathbf{E}_{\mathcal{E}}^{\not\square}$	
$ E $	j-invariant (number of curves)
96	29(4) 67(4) 72(12) 89(12)
104	19(4) 86(4) 93(2)
112	0(4) 6(12) 22(4) 45(4) 65(4) 94(4)
120	10(4) 15(4) 58(4) 84(4)
128	4(12) 77(4)

Table B.29: Point counts and j -invariants for curves over \mathbb{F}_{113}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
96	1(4) 42(4)
100	5(4) 40(4)
104	20(4) 25(4)
108	11(4) 29(4) 49(4) 64(4) 95(4) 97(4)
112	41(4) 59(4)
116	41(4) 59(4)
120	11(4) 29(4) 49(4) 64(4) 95(4) 97(4)
124	20(4) 25(4)
128	5(4) 40(4)
132	1(4) 42(4)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j-invariant (number of curves)
96	1(4) 42(4) 90(12)
104	20(4) 25(4)
112	15(12) 41(4) 59(4) 94(12)
120	11(4) 29(4) 49(4) 64(4) 95(4) 97(4)
128	5(4) 24(12) 33(6) 40(4)

Table B.30: Point counts and j -invariants for curves over \mathbb{F}_{127}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
108	0(2) 12(6)
112	18(2) 54(2) 71(2) 78(2) 81(2)
116	19(6) 63(6)
120	14(2) 37(2) 67(2) 72(2) 90(2) 98(2) 113(2) 124(2)
124	85(6) 103(6)
128	77(2) 95(4) 126(4)
132	85(6) 103(6)
136	14(2) 37(2) 67(2) 72(2) 90(2) 98(2) 113(2) 124(2)
140	19(6) 63(6)
144	18(2) 54(2) 71(2) 78(2) 81(2)
148	0(2) 12(6)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
112	18(4) 54(4) 71(4) 78(4) 81(4)
120	14(4) 37(4) 67(4) 72(4) 90(4) 98(4) 113(4) 124(4)
128	77(4) 95(8) 126(8)
136	14(4) 37(4) 67(4) 72(4) 90(4) 98(4) 113(4) 124(4)
144	18(4) 54(4) 71(4) 78(4) 81(4)

Table B.31: Point counts and j -invariants for curves over \mathbb{F}_{131}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j -invariant (number of curves)
112	32(2) 74(2) 109(2)
116	59(6)
120	3(2) 6(2) 8(2) 29(2) 53(2) 66(2) 69(2) 83(2)
124	2(6) 73(6)
128	1(2) 15(2) 34(2) 52(2) 130(2)
132	25(6) 28(12) 50(12)
136	1(2) 15(2) 34(2) 52(2) 130(2)
140	2(6) 73(6)
144	3(2) 6(2) 8(2) 29(2) 53(2) 66(2) 69(2) 83(2)
148	59(6)
152	32(2) 74(2) 109(2)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j -invariant (number of curves)
112	32(4) 74(4) 109(4)
120	3(4) 6(4) 8(4) 29(4) 53(4) 66(4) 69(4) 83(4)
128	1(4) 15(4) 34(4) 52(4) 130(4)
136	1(4) 15(4) 34(4) 52(4) 130(4)
144	3(4) 6(4) 8(4) 29(4) 53(4) 66(4) 69(4) 83(4)
152	32(4) 74(4) 109(4)

Table B.32: Point counts and j -invariants for curves over \mathbb{F}_{137}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
116	70(4)
120	34(4) 68(4) 82(4) 123(4)
124	86(4) 99(4)
128	16(4) 47(4)
132	3(4) 12(4) 67(4) 85(4)
136	19(4) 88(4) 116(4) 118(4)
140	19(4) 88(4) 116(4) 118(4)
144	3(4) 12(4) 67(4) 85(4)
148	16(4) 47(4)
152	86(4) 99(4)
156	34(4) 68(4) 82(4) 123(4)
160	70(4)

$\mathbf{E}_{\mathcal{E}}^{\square'}$	
$ E $	j-invariant (number of curves)
120	34(4) 68(4) 82(4) 123(4)
128	16(4) 47(4) 50(12) 128(12)
136	19(4) 88(4) 116(4) 118(4)
144	3(4) 12(4) 45(12) 54(12) 67(4) 73(12) 85(4)
152	86(4) 99(4)
160	70(4) 84(6)

Table B.33: Point counts and j -invariants for curves over \mathbb{F}_{139}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
120	41(2) 90(2) 107(2) 124(2)
124	0(2) 114(6) 123(6)
128	27(2) 34(2) 39(2) 91(2) 106(2)
132	115(6) 137(6)
136	12(2) 37(2) 38(2) 48(2) 52(2) 73(2) 85(2) 102(2)
140	60(6) 65(12)
144	12(2) 37(2) 38(2) 48(2) 52(2) 73(2) 85(2) 102(2)
148	115(6) 137(6)
152	27(2) 34(2) 39(2) 91(2) 106(2)
156	0(2) 114(6) 123(6)
160	41(2) 90(2) 107(2) 124(2)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j-invariant (number of curves)
120	41(4) 90(4) 107(4) 124(4)
128	27(4) 34(4) 39(4) 91(4) 106(4)
136	12(4) 37(4) 38(4) 48(4) 52(4) 73(4) 85(4) 102(4)
144	12(4) 37(4) 38(4) 48(4) 52(4) 73(4) 85(4) 102(4)
152	27(4) 34(4) 39(4) 91(4) 106(4)
160	41(4) 90(4) 107(4) 124(4)

Table B.34: Point counts and j -invariants for curves over \mathbb{F}_{149}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
128	59(4)
132	22(4) 85(4) 111(4) 128(4)
136	89(2) 98(4) 124(4)
140	53(4) 72(4) 138(4)
144	7(4) 35(4) 36(4) 84(4) 114(4) 118(4)
148	42(4) 94(4)
152	42(4) 94(4)
156	7(4) 35(4) 36(4) 84(4) 114(4) 118(4)
160	53(4) 72(4) 138(4)
164	89(2) 98(4) 124(4)
168	22(4) 85(4) 111(4) 128(4)
172	59(4)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j -invariant (number of curves)
128	52(12) 59(4)
136	89(2) 98(4) 124(4)
144	7(4) 35(4) 36(4) 56(12) 83(12) 84(4) 114(4) 118(4)
152	42(4) 94(4)
160	53(4) 63(12) 64(12) 72(4) 122(12) 138(4)
168	22(4) 85(4) 111(4) 128(4)

Table B.35: Point counts and j -invariants for curves over \mathbb{F}_{151}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j -invariant (number of curves)
128	98(2)
132	34(6) 136(6)
136	6(2) 21(2) 32(2) 71(2) 114(2) 129(2)
140	87(6) 107(6)
144	10(2) 19(2) 37(2) 69(2) 85(2) 88(2) 122(2) 126(2)
148	0(2) 13(6) 104(6)
152	67(2) 101(4) 143(4) 148(4)
156	0(2) 13(6) 104(6)
160	10(2) 19(2) 37(2) 69(2) 85(2) 88(2) 122(2) 126(2)
164	87(6) 107(6)
168	6(2) 21(2) 32(2) 71(2) 114(2) 129(2)
172	34(6) 136(6)
176	98(2)

$\mathbf{E}_{\mathcal{E}}^{\square'}$	
$ E $	j -invariant (number of curves)
128	98(4)
136	6(4) 21(4) 32(4) 71(4) 114(4) 129(4)
144	10(4) 19(4) 37(4) 69(4) 85(4) 88(4) 122(4) 126(4)
152	67(4) 101(8) 143(8) 148(8)
160	10(4) 19(4) 37(4) 69(4) 85(4) 88(4) 122(4) 126(4)
168	6(4) 21(4) 32(4) 71(4) 114(4) 129(4)
176	98(4)

Table B.36: Point counts and j -invariants for curves over \mathbb{F}_{157}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j -invariant (number of curves)
136	1(2) 48(4) 50(4)
140	2(4) 49(4) 128(4)
144	37(4) 72(4) 100(4) 149(4)
148	10(4) 31(4) 119(4) 148(4)
152	41(4) 90(4)
156	5(4) 47(4) 123(4) 142(4)
160	5(4) 47(4) 123(4) 142(4)
164	41(4) 90(4)
168	10(4) 31(4) 119(4) 148(4)
172	37(4) 72(4) 100(4) 149(4)
176	2(4) 49(4) 128(4)
180	1(2) 48(4) 50(4)

$\mathbf{E}_{\mathcal{E}}^{\cap'}$	
$ E $	j -invariant (number of curves)
136	1(2) 48(4) 50(4)
144	0(4) 37(4) 72(4) 76(12) 100(4) 149(4)
152	41(4) 90(4)
160	5(4) 36(12) 47(4) 68(12) 69(12) 107(12) 123(4) 142(4)
168	10(4) 31(4) 119(4) 148(4)
176	2(4) 49(4) 116(12) 128(4)

Table B.37: Point counts and j -invariants for curves over \mathbb{F}_{163}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
140	28(6)
144	26(2) 48(2) 66(2) 91(2) 108(2)
148	46(6) 71(6) 158(6)
152	22(2) 23(2) 30(2) 85(2) 99(2)
156	0(2) 20(6) 145(6)
160	19(2) 87(2) 95(2) 96(2) 113(2) 114(2) 122(2) 137(2) 139(2) 152(2)
164	98(6)
168	19(2) 87(2) 95(2) 96(2) 113(2) 114(2) 122(2) 137(2) 139(2) 152(2)
172	0(2) 20(6) 145(6)
176	22(2) 23(2) 30(2) 85(2) 99(2)
180	46(6) 71(6) 158(6)
184	26(2) 48(2) 66(2) 91(2) 108(2)
188	28(6)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j-invariant (number of curves)
144	26(4) 48(4) 66(4) 91(4) 108(4)
152	22(4) 23(4) 30(4) 85(4) 99(4)
160	19(4) 87(4) 95(4) 96(4) 113(4) 114(4) 122(4) 137(4) 139(4) 152(4)
168	19(4) 87(4) 95(4) 96(4) 113(4) 114(4) 122(4) 137(4) 139(4) 152(4)
176	22(4) 23(4) 30(4) 85(4) 99(4)
184	26(4) 48(4) 66(4) 91(4) 108(4)

Table B.38: Point counts and j -invariants for curves over \mathbb{F}_{167}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j -invariant (number of curves)
144	82(2) 139(2) 166(2)
148	121(6)
152	6(2) 45(2) 70(2) 77(2) 142(2)
156	19(6) 62(6) 69(6) 76(6) 122(6)
160	48(2) 64(2) 91(2) 106(2) 115(2) 116(2) 165(2)
164	60(6)
168	15(4) 58(2) 59(4) 89(4) 112(4) 151(4)
172	60(6)
176	48(2) 64(2) 91(2) 106(2) 115(2) 116(2) 165(2)
180	19(6) 62(6) 69(6) 76(6) 122(6)
184	6(2) 45(2) 70(2) 77(2) 142(2)
188	121(6)
192	82(2) 139(2) 166(2)

$\mathbf{E}_{\mathcal{E}}^{\square'}$	
$ E $	j -invariant (number of curves)
144	82(4) 139(4) 166(4)
152	6(4) 45(4) 70(4) 77(4) 142(4)
160	48(4) 64(4) 91(4) 106(4) 115(4) 116(4) 165(4)
168	15(8) 58(4) 59(8) 89(8) 112(8) 151(8)
176	48(4) 64(4) 91(4) 106(4) 115(4) 116(4) 165(4)
184	6(4) 45(4) 70(4) 77(4) 142(4)
192	82(4) 139(4) 166(4)

Table B.39: Point counts and j -invariants for curves over \mathbb{F}_{173}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
148	171(2)
152	90(4) 149(4)
156	53(4) 128(4) 148(4)
160	12(4) 135(4) 157(4)
164	65(4) 107(4)
168	52(4) 75(4) 87(4) 94(4) 119(4) 122(4) 138(4) 146(4)
172	34(4) 83(4) 156(4)
176	34(4) 83(4) 156(4)
180	52(4) 75(4) 87(4) 94(4) 119(4) 122(4) 138(4) 146(4)
184	65(4) 107(4)
188	12(4) 135(4) 157(4)
192	53(4) 128(4) 148(4)
196	90(4) 149(4)
200	171(2)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
152	90(4) 149(4)
160	12(4) 58(12) 79(12) 131(12) 135(4) 157(4)
168	52(4) 75(4) 87(4) 94(4) 119(4) 122(4) 138(4) 146(4)
176	13(12) 34(4) 83(4) 156(4)
184	65(4) 107(4)
192	14(12) 23(12) 45(12) 53(4) 128(4) 148(4)
200	171(2)

Table B.40: Point counts and j -invariants for curves over \mathbb{F}_{179}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
156	55(6) 83(6)
160	39(2) 63(2) 99(2) 118(2) 176(2)
164	76(6) 137(6)
168	19(2) 23(2) 31(2) 80(2) 107(2) 110(2) 126(2) 132(2) 156(2) 166(2)
172	4(6)
176	25(2) 26(2) 27(2) 79(2) 115(2) 162(2) 164(2)
180	117(6) 120(12) 121(12)
184	25(2) 26(2) 27(2) 79(2) 115(2) 162(2) 164(2)
188	4(6)
192	19(2) 23(2) 31(2) 80(2) 107(2) 110(2) 126(2) 132(2) 156(2) 166(2)
196	76(6) 137(6)
200	39(2) 63(2) 99(2) 118(2) 176(2)
204	55(6) 83(6)

$\mathbf{E}_{\mathcal{E}}^{\triangleright}$	
$ E $	j-invariant (number of curves)
160	39(4) 63(4) 99(4) 118(4) 176(4)
168	19(4) 23(4) 31(4) 80(4) 107(4) 110(4) 126(4) 132(4) 156(4) 166(4)
176	25(4) 26(4) 27(4) 79(4) 115(4) 162(4) 164(4)
184	25(4) 26(4) 27(4) 79(4) 115(4) 162(4) 164(4)
192	19(4) 23(4) 31(4) 80(4) 107(4) 110(4) 126(4) 132(4) 156(4) 166(4)
200	39(4) 63(4) 99(4) 118(4) 176(4)

Table B.41: Point counts and j -invariants for curves over \mathbb{F}_{181}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
156	62(4)
160	104(4) 142(4)
164	99(2) 135(4) 155(4)
168	20(4) 24(4) 70(4) 148(4)
172	12(4) 32(4) 50(4) 66(4)
176	19(4) 56(4) 132(4)
180	17(4) 26(4) 34(4) 51(4) 87(4) 128(4)
184	17(4) 26(4) 34(4) 51(4) 87(4) 128(4)
188	19(4) 56(4) 132(4)
192	12(4) 32(4) 50(4) 66(4)
196	20(4) 24(4) 70(4) 148(4)
200	99(2) 135(4) 155(4)
204	104(4) 142(4)
208	62(4)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
160	54(12) 57(12) 104(4) 142(4)
168	20(4) 24(4) 70(4) 148(4)
176	19(4) 56(4) 132(4) 145(12)
184	17(4) 26(4) 34(4) 51(4) 87(4) 128(4)
192	12(4) 32(4) 50(4) 55(12) 66(4) 111(12) 163(12) 164(12)
200	99(2) 135(4) 155(4)
208	0(4) 62(4)

Table B.42: Point counts and j -invariants for curves over \mathbb{F}_{191}

$\mathbf{E}_{\mathcal{E}}^{\square}$	
$ E $	j-invariant (number of curves)
168	49(2) 58(2) 59(2) 90(2) 112(2)
172	156(6) 181(6)
176	21(2) 25(2) 89(2) 95(2) 159(2)
180	10(6) 68(6) 101(6) 143(6)
184	18(2) 26(2) 54(2) 63(2) 113(2) 127(2) 134(2)
188	45(6) 88(6)
192	9(2) 41(4) 55(4) 106(4) 107(4) 138(4) 169(4)
196	45(6) 88(6)
200	18(2) 26(2) 54(2) 63(2) 113(2) 127(2) 134(2)
204	10(6) 68(6) 101(6) 143(6)
208	21(2) 25(2) 89(2) 95(2) 159(2)
212	156(6) 181(6)
216	49(2) 58(2) 59(2) 90(2) 112(2)

$\mathbf{E}_{\mathcal{E}}^{\prime\prime}$	
$ E $	j-invariant (number of curves)
168	49(4) 58(4) 59(4) 90(4) 112(4)
176	21(4) 25(4) 89(4) 95(4) 159(4)
184	18(4) 26(4) 54(4) 63(4) 113(4) 127(4) 134(4)
192	9(4) 41(8) 55(8) 106(8) 107(8) 138(8) 169(8)
200	18(4) 26(4) 54(4) 63(4) 113(4) 127(4) 134(4)
208	21(4) 25(4) 89(4) 95(4) 159(4)
216	49(4) 58(4) 59(4) 90(4) 112(4)

Table B.43: Point counts and j -invariants for curves over \mathbb{F}_{193}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
168	103(4) 191(4)
172	15(4) 87(4) 159(4)
176	27(4) 129(4)
180	40(4) 83(4) 119(4) 148(4) 183(4)
184	12(4) 138(4) 142(4) 186(4)
188	14(4) 50(4) 88(4) 112(4)
192	22(4) 58(4) 128(4) 175(4)
196	22(4) 58(4) 128(4) 175(4)
200	14(4) 50(4) 88(4) 112(4)
204	12(4) 138(4) 142(4) 186(4)
208	40(4) 83(4) 119(4) 148(4) 183(4)
212	27(4) 129(4)
216	15(4) 87(4) 159(4)
220	103(4) 191(4)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
168	103(4) 191(4)
176	27(4) 99(12) 129(4) 166(12)
184	12(4) 138(4) 142(4) 186(4)
192	0(4) 22(4) 37(12) 58(4) 128(4) 153(12) 168(12) 175(4)
200	14(4) 50(4) 88(4) 112(4)
208	40(4) 83(4) 115(12) 119(4) 148(4) 172(12) 183(4) 184(6)
216	15(4) 87(4) 159(4)

Table B.44: Point counts and j -invariants for curves over \mathbb{F}_{197}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
172	82(4)
176	92(4) 97(4) 151(4)
180	2(4) 19(4) 40(4) 112(4) 119(4) 159(4)
184	109(4) 128(4)
188	43(4) 67(4) 194(4)
192	69(4) 87(4) 126(4) 133(4) 186(4)
196	88(4) 136(4) 152(2) 158(4) 185(4)
200	88(4) 136(4) 152(2) 158(4) 185(4)
204	69(4) 87(4) 126(4) 133(4) 186(4)
208	43(4) 67(4) 194(4)
212	109(4) 128(4)
216	2(4) 19(4) 40(4) 112(4) 119(4) 159(4)
220	92(4) 97(4) 151(4)
224	82(4)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
176	92(4) 97(4) 151(4) 188(12)
184	109(4) 128(4)
192	17(12) 31(12) 69(4) 87(4) 105(12) 118(12) 126(4) 133(4) 137(12) 186(4)
200	88(4) 136(4) 152(2) 158(4) 185(4)
208	43(4) 62(12) 67(4) 194(4)
216	2(4) 19(4) 40(4) 112(4) 119(4) 159(4)
224	82(4) 171(12)

Table B.45: Point counts and j -invariants for curves over \mathbb{F}_{199}

$\mathbf{E}_{\mathcal{E}}^{\cap}$	
$ E $	j-invariant (number of curves)
172	0(2)
176	82(2) 92(2) 137(2) 171(2)
180	67(6) 69(6) 115(6)
184	76(2) 119(2) 130(2) 138(2) 152(2) 162(2) 169(2) 183(2)
188	125(6)
192	3(2) 53(2) 58(2) 99(2) 154(2) 164(2) 165(2) 186(2)
196	29(6) 31(6) 43(6) 146(6)
200	40(4) 61(4) 98(4) 136(2) 140(4)
204	29(6) 31(6) 43(6) 146(6)
208	3(2) 53(2) 58(2) 99(2) 154(2) 164(2) 165(2) 186(2)
212	125(6)
216	76(2) 119(2) 130(2) 138(2) 152(2) 162(2) 169(2) 183(2)
220	67(6) 69(6) 115(6)
224	82(2) 92(2) 137(2) 171(2)
228	0(2)

$\mathbf{E}_{\mathcal{E}}^{\not\cap}$	
$ E $	j-invariant (number of curves)
176	82(4) 92(4) 137(4) 171(4)
184	76(4) 119(4) 130(4) 138(4) 152(4) 162(4) 169(4) 183(4)
192	3(4) 53(4) 58(4) 99(4) 154(4) 164(4) 165(4) 186(4)
200	40(8) 61(8) 98(8) 136(4) 140(8)
208	3(4) 53(4) 58(4) 99(4) 154(4) 164(4) 165(4) 186(4)
216	76(4) 119(4) 130(4) 138(4) 152(4) 162(4) 169(4) 183(4)
224	82(4) 92(4) 137(4) 171(4)

Appendix C. Programs

C.1 C++ Programs

The following program was used to generate the tables in B.1, the tables for elliptic curves which arise from the intersections of planes in the orbits $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$, $\mathcal{O}_{\mathcal{E}\square}^{\omega\neg\cap}$, $\mathcal{O}_{\mathcal{H}\square}^{\omega\cap}$ and $\mathcal{O}_{\mathcal{H}\square}^{\omega\neg\cap}$. As shown in Chapter 3, there arise only two classes of curves and it is sufficient to consider planes in orbits $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$ and $\mathcal{O}_{\mathcal{E}\square}^{\omega\neg\cap}$. This program was initially written to count points on the intersections of planes in these orbits with $\mathcal{E}\square$ or $\mathcal{H}\square$. The program uses the C++ modulo operator and does not build fields and so only produces tables for (odd) primes q .

We outline the operation of the program. A prime q is entered manually. An array is created of the nonzero squares modulo q . The variable eta is the smallest nonsquare modulo q . The main loop iterates over all nonzero elements w in the field. For the family of curves being tested, the j -invariant ‘Jinv’ is calculated for w and stored in the $[w][0]$ place in ‘allcounter’. The variable ‘plane’ is set equal to the vector $\alpha_w = [1, -1, 0, w]$ for a plane in $\mathcal{O}_{\mathcal{E}\square}^{\omega\cap}$ and to $[1, -eta, 0, w]$ for a plane in $\mathcal{O}_{\mathcal{E}\square}^{\omega\neg\cap}$. The variable ‘point’ is set equal to $(1, s^2 - (eta)t^2, s, t)$ and the procedure ‘dotprod’ returns 1 if ‘point’ is incident with ‘plane’ and 0 otherwise. The total number of points on α_w is recorded in the $[w]$ place of ‘counter’ and in the $[w][1]$ place of ‘allcounter’. This double recording is a carryover from an earlier version of the program. The information is then transferred to the $q \times q$ array ‘allcountercounter’ whose $[i][j]$ entry will be the number of planes α_w with i points and whose corresponding curve has j -invariant j . We use the

fact that there are twice as many points on the elliptic curve E_ω as there are on the corresponding plane α_ω . The nonzero entries in ‘allcountercounter’ are then printed in tabular form with all of the curves with $N > 0$ points listed in a row, together with their j -invariant and the number of times a curve with each value the j -invariant occurs.

```

// program to count points on the subset of
// the elliptic quadric in PG(3,q) associated with
// the squares in Fq for odd primes q
// Steve Flink
// 7-14-08

#include <iostream>
#include <math.h>
#include <fstream>
using namespace std;
/*****/
int issquare(int x, int squares[], int sqrs, int q)
{
    x = x%q;
    while (x<0)
    {
        x=x+q;
    }
    for (int i=0; i<sqrs; i++)
    {
        if (x == squares[i])
        {
            return 1;
        }
    }
    return 0;
}
/*****/
int findeta(int squares[],int sqrs, int q)
{
    for(int i=2; i<q; i++)
    {
        if(issquare(i, squares, sqrs, q)==0)
        {
            return i;
        }
    }
}
/*****/
int psqrt (int x, int squares[], int sqrs, int q)
{
    int root = 0;
    if (issquare(x, squares, sqrs, q)==1)
    {
        for (int i=0; i<sqrs; i++)
        {
            if (x == squares[i])
                return (i+1)%q;
        }
    }
    return 0;
}
/*****/
int nsqrt (int x, int squares[], int sqrs, int q)
{
    int root = 0;
    if (issquare(x, squares, sqrs, q)==1)
    {
        for (int i=0; i<sqrs; i++)
        {
            if (x == squares[i])
            {
                root = (-1*(i+1))%q;
                while (root<= 0)
                {
                    root =root + q;
                }
                return root;
            }
        }
    }
    return 0;
}
/*****/
int inv (int a, int q) /*uses extended euclidean algorithm to find mod inverse*/
{
    int qq = q;
    int x = 0;
    int lastx = 1;
    int y = 1;
    int lasty = 0;
    int temp = 0;
    int quotient = 0;
    while (q != 0)
    {
        temp = q;
        quotient = a/q;
        q = a %q;
        a = temp;
        temp = x;
        x = lastx-quotient*x;
        lastx = temp;
        temp = y;
        y = lasty-quotient*y;
        lasty = temp;
    }
    while (lastx <0)
    {

```

```

        lastx = lastx + qq;
    }
    return lastx;
}
/*****/
int dotprod(int vec1[], int vec2[], int q)
{
    int sum = 0;
    for (int i=0; i<4; i++)
    {
        sum = sum + (vec1[i]*vec2[i]);
    }
    sum = sum %q;
    while(sum < 0)
    {
        sum = sum +q;
    }
    return sum;
}
/*****/
void printvec(int vec[], ofstream& data)
{
    cout<<" ";
    data<<" ";
    for (int i=0; i<3; i++)
    {
        cout<<vec[i]<<" ";
        data<<vec[i]<<" ";
    }
    cout<<vec[3]<<" ";
    data<<vec[3]<<" ";
}
/*****/
int main()
{
    int q=199;
    int eta;
    /*
    const int sqrs = static_cast<int>((q-1)/2);*/
    int sqrs;
    int counts[200]= {0};
    int countscounter[200][2]= {0};
    int allcounter[200][2] ={0};
    int allcountercounter[200][200]={0};
    int squares[200]={0};
    int Jcounter[200][2]={0};
    int point[4] = {1, 0, 0, 0};
    int plane[4] = {1, -1, 0, 0};
    int c, d, m, a, s, t, u, v, w, s2, t2, a2;
    long temp, temp2, temp3;
    int delta;
    int sum = 0;
    long jnum, jdenom;

    int Jinv = 0;

    char wait = 'y';
    sqrs = q;
    ofstream outData;
    outData.open("singlelaguerretable.out");
    while (wait == 'y')
    {
        for(int i=0; i<=q; i++)
        {
            for (int j=0; j<2; j++)
            {
                countscounter[i][j]=0;
            }
        }

        for (int i=0; i<q; i++)
        {
            for (int j=0; j<q; j++)
            {
                allcountercounter[i][j]=0;
            }
        }

        for (int i=0; i<2; i++)
        {
            counts[i]=0;
        }
        for (int i=0; i<=q; i++)
        {
            squares[i]=0;
        }
        for (int m=0; m<2; m++)
        {
            for (int i=0; i<q; i++)
            {
                Jcounter[i][m]=0;
            }
        }
        for (int i=1; i<=sqrs; i++)
        {
            squares[i-1] = (i*i)%q;
        }
    }
}

```



```

}
/*
for(int j=0; j<countscounter[i][1]; j++)
{
    cout<<"*\\\!";
    outData<<"$\blacksquare$\!";
}
*/
if (countscounter[i][1]!=0)
{
    cout<<" & ";
    outData<<" & ";
}
for (int n=0; n<q; n++)
{
    if (allcountercounter[i][n]!=0 && countscounter[i][1]!=0)
    {
        cout<<" "<< n <<"("<<allcountercounter[i][n]<<"\\s";
        outData<<" "<< n <<"("<<allcountercounter[i][n]<<"\\s";
    }
}
cout<<endl;
/*for (int i=0; i<q; i++)
{
    for (int j=0; j<q; j++)
    {
        if (allcountercounter[i][j]!=0)
        {
            cout<<"There are "<< allcountercounter[i][j] <<" curves with "<< i;
            cout<<" points and j-invariant "<< j <<".<<endl;
        }
    }
}
*/
for (int i=0; i<q; i++)
{
    if (Jcounter[i][0]!=0)
    {
        cout<<"J = "<<i<<" occurs "<<Jcounter[i][0]<<" times "<<endl;
    }
}
*/
outData<<endl<<" \\\\ \hline \\end{tabular}"<<endl;
cout<<endl<<" \\\\ \hline \\end{tabular}"<<endl;
cout<<endl<<endl<< "Again? ";
cin >> wait;
} //end of main
outData.close();
return 0;
}

```

C.2 Sage Programs

From the Sage website (<http://www.sagemath.org/>):

Sage is a free mathematics software system licensed under the GPL.

It combines the power of many existing open-source packages into a common Python-based interface.

Sage has built-in functions for elliptic curves, including functions to calculate the group on the points of the curve and the j -invariant. For the research in this thesis, the following program was used to verify the values for point counts and j -invariants obtained with the C++ program in the first section of this appendix.

In this program, $n = \eta$ and $w = \omega$.

```
w=1
n=5
a=1
b=1
k=1
s=1
r=1
m=1
p = 47
print "p = ", p
m = RDF(2*sqrt(p))
r = m.integer_part()
s=p+1-r
print "bounds: "
print s
s=p+1+r
print s
print "1728 = ", 1728%p
print "....."
while w<=(p-1)/2:
    k=w^2%p
    d=k^2%p
    c=n^2%p
    f=w^-1%p
    a=((2-k*n)/2)%p
    b=(d*c/16-k*n/4)%p
    E = EllipticCurve(GF(p), [0,a,0,b,0])
    print "omega: ", w
    print "cardinality: ", E.cardinality()
    print "factors of cardinality: ", factor(E.cardinality())
    print "factors of p-1: ", factor(p-1)
    print "j-invariant: ", E.j_invariant()
    print "group: ", E.abelian_group(),E
    #E.points()
    print "-----"
    w=w+1
```

REFERENCES

- [1] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design Theory*. Cambridge University Press, Cambridge, UK, second edition, 1999.
- [2] A. E. Brouwer. Some new two-weight codes and strongly regular graphs. *Discrete Applied Mathematics*, 10:111–114, 1985.
- [3] R. H. Bruck. Construction problems of finite projective planes. *Proc. Conf. Combinatorics*, 1967.
- [4] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18:97–122, 1986.
- [5] P. J. Cameron and J. H. van Lint. *Designs, Graphs, Codes and their Links*. Cambridge University Press, Cambridge, first edition, 1996.
- [6] C. Carathéodory. *Theory of Functions of a Complex Variable*. Chelsea, New York, second english edition edition, 1958.
- [7] Rey Casse. *Projective Geometry: An Introduction*. Oxford University Press, New York, first edition, 2006.
- [8] J. W. S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, Cambridge, UK, first edition, 1991.
- [9] Henri Cohen and Gerhard Frey. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall, Boca Raton, FL, first edition, 2006.
- [10] I. Connell. Lecture notes on elliptic curves. <http://www.math.mcgill.ca/connell/public/ECH1>.
- [11] Peter Dembowski. *Finite Geometries*. Springer-Verlag, Berlin, first edition, 1997 Reprint of the 1968 edition.
- [12] Eugene Dickson. *Linear Groups*. B. G. Teubner, Leipzig, first edition, 1901.
- [13] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., New York, NY, second edition, 1999.

- [14] Larry C. Grove. *Classical Groups and Geometric Algebra*. The American Mathematical Society, Graduate Studies in Mathematics, Volume 39, Providence, Rhode Island, first edition, 2002.
- [15] Robin Hartshorne. *Algebraic Geometry*. Springer Verlag, New York, NY, first edition, 1977.
- [16] Dale Husemöller. *Elliptic Curves*. Springer, New York, NY, second edition, 2004.
- [17] Henry McKean and Victor Moll. *Elliptic Curves: Function Theory, Geometry, Arithmetic*. Cambridge University Press, Cambridge, UK, first edition, 1997.
- [18] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley and Sons, New York, NY, fifth edition, 1991.
- [19] W. F. Orr. *The Miquellian inversive plane $IP(q)$ and the associated projective planes*. PhD thesis, University of Wisconsin, 1973.
- [20] Stanley Payne. *Topics in Finite Geometry: Ovals, Ovoids and Generalized Quadrangles*. UCD Course Notes, 2009.
<http://www-math.cudenver.edu/~spayne/classnotes/topics.pdf>.
- [21] Igor R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, Berlin, first edition, 1994.
- [22] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, New York, NY, first edition, 1986.
- [23] William Stein and David Joyner. Sage: System for algebra and geometry experimentation. <http://sage.sourceforge.net/>.
- [24] Donald E. Taylor. *The Geometry of the Classical Groups*. Heldermann Verlag, Berlin, first edition, 1992.
- [25] Lawrence C. Washington. *Elliptic Curves: number theory and cryptography*. CRC Press, Boca Raton, FL, first edition, 2003.