

Coding and Cryptography with Hyperovals of $PG(2, 2^s)$

*An undergraduate research project under
the direction of Dr. Keith E. Mellinger
at the University of Mary Washington*

Catherine Castleberry Katie Hunsberger

August 1, 2008

Contents

1	Introduction	3
2	Preliminaries	4
2.1	Finite Projective Planes - <i>a synthetic approach</i>	4
2.2	Finite Projective Planes - <i>an algebraic approach</i>	8
2.3	Connections to Coding	14
2.4	Additional Preliminaries for Finite Fields	15
3	Applications to Cryptography	18
3.1	Additional Geometric Properties	19
3.2	Secret Sharing Scenarios	22
3.3	Security of our Secret Sharing Schemes	23
4	Applications to Coding	25
4.1	Skew Lines and Non-Hyperoval Points, \mathcal{C}_{SkNH}	27
4.2	Secant Lines and All Points, \mathcal{C}_{SeA}	32
4.3	Secant Lines and Non-Hyperoval Points, \mathcal{C}_{SeNH}	35
4.4	Summary of Code Properties	38
5	Conclusion	38

List of Figures

1	Secant and skew lines	7
2	Nucleus of the form (f, e, d)	12
3	A dual conic when $q = 4$	13
4	Five points determine a unique conic	20
5	Two tangents and three points determine a conic	21
6	Representing a codeword as a collection of points	26

List of Tables

1	Properties of points and lines of π	7
2	Properties of secant and skew lines	8
3	Code parameters for \mathcal{C}_{SkNH}	27
4	Code parameters for \mathcal{C}_{SeA}	32
5	Code parameters for \mathcal{C}_{SeNH}	35
6	Summary of code parameters	38

1 Introduction

The field of information theory consists of two main branches of study: cryptology and coding theory, also known as the theory of error-correcting codes. Cryptology is the science of cryptography, the art of encrypting a message, and cryptanalysis, the art of breaking an encryption technique. In coding theory, by contrast, we are not interested in hiding anything. Rather, coding theory looks at the reliability of a transmitted message and attempts to improve this reliability mathematically. Our goal is to make a contribution to both of these areas.

Cryptography, the study and practice of hiding information, underwent a transformation in the twentieth century, shifting focus from linguistic patterns to various fields of mathematics. An interesting concept in cryptography is that of a *secret sharing scheme*. A secret sharing scheme is a method for distributing a secret piece of information among a number of participants. The secret is divided and doled out to the individuals in such a way that the entire secret can only be recovered when the participants combine their shares of information; no single participant can recover the entire secret on their own.

A simple example of a secret sharing scheme is a company producing a “top secret” recipe for baked beans. The C.E.O. of the company needs to be able to access the recipe at any time, but in the event of his absence, any five of the twenty-five company board members should be able to recover the recipe together. This scenario can be accomplished with a secret sharing scheme in which each board member receives one share of information while the C.E.O. receives five.

The theory of error-correcting codes came to fruition in the late twentieth century. Coding theory developed as a result of Claude Shannon’s famous 1948 paper “A Mathematical Theory of Communication.” The idea behind coding theory is to detect and, hopefully, correct any errors that might occur during the transmission of a given message. Binary linear codes, wherein the message is a string of zeros and ones, are used in various forms of data transmission, from wireless communication to compact disks.

Binary linear coding transforms a message into a *codeword*, which is simply a vector in a vector space. Through the process of encoding, the original message is lengthened to include some additional error-correcting information so that the receiver will (hopefully) be able to detect and possibly correct any errors that occurred during transmission. Following transmission, a decoding process takes place. A fundamental issue in coding theory is to find so-called “optimal” codes, or codes which have maximal error-correction capability.

Utilizing various properties of finite projective planes, our goal is to first devise various secret sharing schemes,

and second, to generate several classes of binary linear codes.

2 Preliminaries

As our work relies heavily on the structure of the classical finite projective plane, and some substructures therein, we start with a look at the basics. We will begin with a synthetic approach.

2.1 Finite Projective Planes - *a synthetic approach*

Just about every object in finite geometry can be described completely using synthetic definitions. This usually involves only the notions of two objects, *points* and *lines*, and certain incidences between them. We start with the basic building block, the finite projective plane. Much more information, including certain applications, can be found in [1]. Another good, albeit more advanced reference, is [6].

Definition 2.1. *A finite projective plane π is a set of points along with a set of subsets of these points, known as lines, satisfying the following axioms:*

1. *two distinct points determine a unique line,*
2. *two distinct lines determine a unique point, and*
3. *there exist four points, no three of which are collinear.*

One can now use elementary counting techniques to determine many properties of such a plane. Let π be an arbitrary finite projective plane.

Proposition 2.2. *Every line in π contains the same number of points.*

Proof. Consider two distinct lines, l_1 and l_2 , in the projective plane π . By axiom 2, these two lines must meet in some point P . By axiom 3, it follows that there is some point Q not on l_1 or l_2 . By axiom 2, every line through Q must intersect both l_1 and l_2 , and similarly, by axiom 1, every point on l_1 and l_2 must lie on some line running through Q . In this manner, we establish a one-to-one correspondence between the points on l_1 and the points on l_2 . Therefore they contain the same number of points. Because l_1 and l_2 are arbitrary lines in π , it follows that every line in π contains the same number of points. \square

Definition 2.3. *Let $q + 1$ denote the number of points on any given line in π . The integer q is called the order of π .*

For the remainder of this section, we let π be a finite projective plane of order q .

Proposition 2.4. *Any point in π has $q + 1$ lines running through it.*

Proof. Consider an arbitrary point P in π . By axiom 3, it follows that there is some line l not containing P . By axiom 2, every line running through P must intersect l , and by axiom 1, every point on l determines a unique line with P . In this manner, we establish a one-to-one correspondence between the lines running through P and the points on l . Since there are $q + 1$ points on l , every point has $q + 1$ lines running through it. \square

We can now count the number of points and lines in π .

Proposition 2.5. *A finite projective plane π of order q contains $q^2 + q + 1$ points.*

Proof. Consider an arbitrary point P in π . By axiom 1, every two points determine a line, so every other point in π lies on some line running through P . There are $q + 1$ lines running through P , and each of these lines contains q points, excluding the point P . Hence we can express the number of points in π by $q(q + 1) + 1 = q^2 + q + 1$. \square

Proposition 2.6. *A finite projective plane π of order q contains $q^2 + q + 1$ lines.*

Proof. By axiom 1 every two points determine a unique line. Also, note that the number of ways you can choose two distinct points from the $q^2 + q + 1$ points is $\binom{q^2 + q + 1}{2}$. However, every two of the $q + 1$ points on any given line count the same line. Hence, every line is counted $\binom{q + 1}{2}$ times. Thus, the total number of lines in π can be expressed by

$$\frac{\binom{q^2 + q + 1}{2}}{\binom{q + 1}{2}} = \frac{(q^2 + q + 1)(q^2 + q)}{(q^2 + q)} = q^2 + q + 1 .$$

\square

We now want to look at some arrangements of points of π . Our goal is to use certain substructures to approach some problems in coding theory and cryptography. Before looking at the applications, we will introduce the notion of an *arc* in a finite projective plane and determine some properties of arcs.

Definition 2.7. *In a finite projective plane π , an arc A is a set of points, no three of which are collinear.*

Proposition 2.8. *If A is an arc in a finite projective plane π of order q , then A contains at most $q + 2$ points.*

Proof. Consider an arbitrary point P in A as well as all of the lines that pass through P . Note that each of these lines meets A in at most one additional point. Thus, A has at most $(q + 1) + 1$ points, or $q + 2$ points. \square

Proposition 2.9. *If A contains $q + 2$ points, then q is even.*

Proof. Choose an arbitrary point P on A . Consider all the lines that pass through P . If there are $q + 1$ other points on A , then every line through P meets A in a second point. Because P was an arbitrary point, no line meets A in exactly one point. Now choose a point Q not on A and consider all the lines through Q . Each of these lines must meet A in zero or two points (zero when the line is skew and two when the line is secant). Thus, the points of A occur in pairs and so the number of points in A must be even. Because $q + 2$ is even, q is even. \square

Corollary 2.10. *In a finite projective plane π of odd order q , the maximum number of points an arc A can contain is $q + 1$.*

We have shown that when q is odd, the maximum number of points in an arc is $q + 1$. Such a maximum set is called an *oval*. When q is even, a maximal set of such points could have size $q + 2$.

Definition 2.11. *In a finite projective plane of order q , q even, a set of $q + 2$ points, no three of which are collinear, is called a *hyperoval*.*

We will show in the following section that $(q + 1)$ -arcs (arcs containing $q + 1$ points) are easy to construct. When q is even, one can always extend a $(q + 1)$ -arc to a $(q + 2)$ -arc.

Theorem 2.12. *Let A be a $(q + 1)$ -arc of a finite projective plane π of even order q . Then the $q + 1$ lines that are tangent to A are concurrent.*

Proof. Consider a secant line l to the arc A . Let P be an arbitrary point on l and consider the lines through P . Because q is even, A contains an odd number of points. Hence, some line through P must be tangent to A . But P was chosen as an arbitrary point, and thus every point on l has a tangent through it. There are $q + 1$ points on l each corresponding to one of $q + 1$ lines tangent to A , and so there is a one-to-one correspondence between the points on l and the lines tangent to A . As l was arbitrary, it follows that no two tangent lines can intersect at a point lying on a secant line. By axiom 2, the tangent lines must meet each other in some point. We conclude that the tangent lines must all pass through a common point. \square

Definition 2.13. *The point of concurrency of the tangent lines to a $(q + 1)$ -arc A is called the *nucleus*.*

When considering a $(q + 1)$ -arc that has been extended to a hyperoval H by adding the nucleus, all lines are either *skew*, meeting H in zero points, or *secant*, meeting H in two points, as shown below in Figure 1. It is easy to determine the number of lines of each type. Any two of the $q + 2$ points of H will determine a unique secant line. Hence, there are $\binom{q + 2}{2} = \frac{q^2 + 3q + 2}{2}$ lines secant to H . Since π contains $q^2 + q + 1$ lines total, there are $\frac{q^2 - q}{2}$ skew lines. It is also straight-forward to count the number of secant and skew lines that pass through any point off the hyperoval. For any point off H , the secant lines through H necessarily pair up the points of H . Hence, there must be $\frac{q+2}{2}$ secant lines through such a point. As there are $q + 1$ lines through a point, there must be $\frac{q}{2}$ skew lines through any point off H .

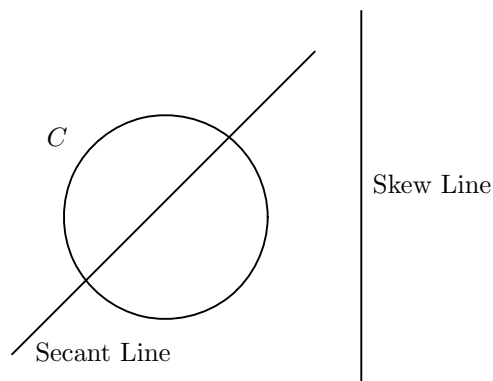


Figure 1: Secant and skew lines

We have proven a considerable number of things about finite projective planes. The following tables recap the properties we have proven about a finite projective plane π of order q , together with the properties of the lines defined by a hyperoval.

Number of points	$q^2 + q + 1$
Number of lines	$q^2 + q + 1$
Number of points on a line	$q + 1$
Number of lines through a point	$q + 1$
Maximum size of arc, q even	$q + 2$
Maximum size of arc, q odd	$q + 1$

Table 1: Properties of points and lines of π

We are now ready to introduce some algebra into the mix. Just as objects like circles and parabolas can be defined synthetically, they can also be defined algebraically. For instance, in the Euclidean plane, a circle

Number of secants	$\frac{(q+2)(q+1)}{2}$
Number of skews	$\frac{q^2-q}{2}$
Number of secants through P	$\frac{q}{2} + 1, P \notin H$ $q + 1, P \in H$
Number of skews through P	$\frac{q}{2}, P \notin H$ $0, P \in H$

Table 2: Properties of secant and skew lines

is the collection of points equidistance from a fixed point. But a circle is also the set of points satisfying a certain quadratic equation in the coordinates x and y .

2.2 Finite Projective Planes - *an algebraic approach*

We can construct finite projective planes using vector spaces and finite fields. A *finite field* is an algebraic structure wherein two operations are carried out on a finite number of elements. These two operations correspond to the usual addition and multiplication operations, as in the real field \mathbb{R} . A finite field of order q is denoted $GF(q)$, and it can be shown that q is either a prime or a prime power. In $GF(q)$, all operations are carried out modulo p , where $q = p^t$ and p is prime. For example, if we choose $q = 7$, we obtain the field with elements $\{0, 1, 2, 3, 4, 5, 6\}$, and all arithmetic is carried out modulo 7. For instance, $4 + 5 = 2$ and $3 \cdot 4 = 5$. We further discuss the properties of finite fields that are relevant to our work in Section 2.4, and much more detailed information can be found in [9].

Using finite fields, we can construct an example of a projective plane. Let V be a three-dimensional vector space of the finite field $GF(q)$. We can define points as the one-dimensional subspaces of V and lines as the two-dimensional subspaces of V . This vector space model provides us with a finite projective space of dimension two and order q , denoted $PG(2, q)$, and it is straightforward to check that the axioms of a finite projective plane are satisfied.

This brings us to the concept of *homogeneous coordinates*. Because we have defined points as the one-dimensional subspaces of V , a given point can be represented by any scalar multiple of a given vector. For example, the vectors $(1, 2, 3)$ and $(3, 6, 2)$ in the three-dimensional vector space over $GF(7)$ represent the same projective point in $PG(2, 7)$. In order to control for this variability, we often “normalize” vectors by scalar multiplying so that the first nonzero coordinate from the left is a 1. Therefore, the points of the projective plane $PG(2, q)$ are uniquely represented as $\{(1, a, b) : a, b \in GF(q)\} \cup \{(0, 1, a) : a \in GF(q)\} \cup$

$\{(0, 0, 1)\}$.

Since we have defined lines as the two-dimensional subspaces of V , we can utilize the orthogonal complement to represent them. The set of vectors orthogonal to the non-zero vector (a, b, c) spans a two-dimensional subspace. Therefore we can represent lines as three-dimensional vectors, normalized in the same manner as points to ensure uniqueness of representation. Because points *and* lines are represented as three-dimensional vectors, we will distinguish between the two by using parentheses, like (a, b, c) , to represent points, and square brackets, like $[x, y, z]$, to represent lines. A point (a, b, c) is on the line $[x, y, z]$ if and only if $(a, b, c) \cdot [x, y, z] = 0$, or if $ax + by + cz = 0$.

We can use the cross product, a straightforward algebraic operation, to determine the point of intersection of two lines, as well as the line running through two points. The *cross product* of two vectors \mathbf{a} and \mathbf{b} , denoted $\mathbf{a} \times \mathbf{b}$, is defined as the vector \mathbf{c} which is orthogonal to both \mathbf{a} and \mathbf{b} . In terms of a projective plane, the cross product of two lines $[x_1, y_1, z_1]$ and $[x_2, y_2, z_2]$ is the point at which the two lines meet. Similarly, the cross product of two points (a_1, b_1, c_1) and (a_2, b_2, c_2) is the line on which both points lie.

For example, consider the lines $l_1 = [1, 1, 1]$ and $l_2 = [0, 1, 0]$ in $PG(2, 4)$. The cross product of l_1 and l_2 is $(1, 0, 1)$, which is precisely the intersection of these two lines.

We can now use homogeneous coordinates to construct a $(q + 1)$ -arc.

Definition 2.14. *A conic C is a set of points whose coordinates satisfy the quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$, for some $a, b, c, d, e, f \in GF(q)$.*

Depending on the coefficients, some quadratic forms will yield degenerate conics. For instance, $x^2 = 0$ gives a set of points forming a line. We are only interested in nondegenerate examples. It can be shown that all nondegenerate cases are equivalent to the one determined by the form $y^2 = xz$. This consists of the $q + 1$ points $\{(1, k, k^2) : k \in GF(q)\} \cup \{(0, 0, 1)\}$.

It is well known [5] that the points satisfying the quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$ in a projective plane constitute one of four possible geometric structures: a single line, a pair of distinct lines, a single point, or a nondegenerate conic (as described above). Given a conic C in π , it is easy to check whether this conic is in fact nondegenerate. First, we count the points of C . If C contains $q + 1$ points, then the possibility that the points of C lie on two distinct lines (with $2q + 1$ points), as well as the possibility that C is a single point, are both eliminated. Once it is established that C contains $q + 1$ points, all that remains to be shown is the non-collinearity of these points. To do this, we simply take three of the points and use the cross product to check that they do not all lie on the same line.

Our work will rely solely on the nondegenerate conics. Hence, from this point on, when we refer to a conic C we specifically mean a nondegenerate conic.

Proposition 2.15. *Every conic is an arc.*

Proof. As mentioned above, it is known [5] that every nondegenerate conic of $PG(2, q)$ is the same as, or projectively equivalent to any other conic. More technically, for any conic C_1 , there is always an automorphism of the plane that will send C_1 to the conic C described above. Hence, if we can show that C is an arc, it will follow that every conic is an arc. To this end, suppose to the contrary that three points of the conic C are collinear.

Case 1: First we examine the case where one of these three points is $(0,0,1)$. Consider three distinct points: $P_1 = (0, 0, 1)$, $P_2 = (1, a, a^2)$, and $P_3 = (1, b, b^2)$. If these points are collinear, then a linear combination of two should yield the third. So we have

$$\begin{aligned} k_1P_1 + k_2P_2 &= P_3 \\ (0, 0, k_1) + (k_2, k_2a, k_2a^2) &= (1, b, b^2) \\ (k_2, k_2a, k_1 + k_2a^2) &= (1, b, b^2) \end{aligned}$$

Without loss of generality, we can assume $k_2 = 1$. But if $ak_2 = b$, then $a = b$. This contradicts the assumption that P_2 and P_3 are distinct points.

Case 2: Now we examine the case where none of these three points is $(0,0,1)$. Consider three distinct points: $P_1 = (1, a, a^2)$, $P_2 = (1, b, b^2)$, and $P_3 = (1, c, c^2)$. If these points are collinear, then a linear combination of two should yield the third. So we have

$$\begin{aligned} k_1P_1 + k_2P_2 &= P_3 \\ k_1(1, a, a^2) + k_2(1, b, b^2) &= (1, c, c^2) \end{aligned}$$

Again, without loss of generality, we can assume that $k_1 + k_2 = 1$, and we can eliminate a variable since $k_2 = 1 - k_1$. Next, we know that (1) $ak_1 + b(1 - k_1) = c$ and (2) $a^2k_1 + b^2(1 - k_1) = c^2$. By squaring (1), we obtain

$$a^2k_1^2 + 2abk_1(1 - k_1) + b^2(1 - k_1)^2 = c^2 .$$

Setting this equal to (2), we eliminate the variable c , obtaining

$$\begin{aligned} a^2k_1^2 + 2abk_1(1 - k_1) + b^2(1 - k_1)^2 &= a^2k_1 + b^2(1 - k_1) \\ a^2k_1(k_1 - 1) - 2abk_1(k_1 - 1) + b^2k_1(k_1 - 1) &= 0 \\ k_1(k_1 - 1)(a - b)^2 &= 0 . \end{aligned}$$

This implies that either $k_1 = 0$, $k_1 = 1$, or $a - b = 0$. If $k_1 = 0$, then $k_2 = 1$, implying that $b = c$. This contradicts the assumption that P_2 and P_3 are distinct. If $k_1 = 1$, then $k_2 = 0$, implying that $a = c$. This contradicts the assumption that P_1 and P_3 are distinct. If $a - b = 0$, then $a = b$. This contradicts the assumption that P_1 and P_2 are distinct. Hence, all 3 possibilities yield a contradiction. Therefore, no three points of a conic are collinear, and hence every conic is an arc. \square

Now, in a projective plane π of even order q , every point on a nondegenerate conic C has a unique tangent. This follows from the fact that such conics are $(q + 1)$ -arcs. By Theorem 2.12, when q is even, the tangents to a conic C all meet in a common point called the *nucleus*.

Theorem 2.16. *Let C be a nondegenerate conic in $PG(2, q)$, q even, satisfying $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$. Then the nucleus for C is of the form (f, e, d) .*

Proof. We give a proof for the standard conic only. Consider the standard conic defined by $y^2 + xz = 0$. In this case, $a = 0$, $b = 1$, $c = 0$, $d = 0$, $e = 1$, and $f = 0$. The points that satisfy this quadratic form are $(0, 0, 1)$ and all points of the form $(1, x, x^2)$, where $x \in GF(q)$. The line tangent to the point $(0, 0, 1)$ is $[1, 0, 0]$. (Note that we know this because the dot product of $(0, 0, 1)$ and $[1, 0, 0]$ is equal to 0 and the dot product of $(1, x, x^2)$ and $[1, 0, 0]$ is not equal to 0.) The lines tangent to the points $(1, x, x^2)$ are of the form $[x^2, 0, 1]$. (Note that we know this again because the dot product of $(1, x, x^2)$ and $[x^2, 0, 1]$ is equal to 0 precisely when $x = a$, and the dot product of $(0, 0, 1)$ and $[x^2, 0, 1]$ is not equal to 0.) The point $(0, 1, 0)$ lies on the tangent lines $[1, 0, 0]$ and those of the form $[x^2, 0, 1]$, and hence $(0, 1, 0)$ is the nucleus of the conic. Note that this point is of the form (f, e, d) . \square

In general, it can be shown that the nucleus of any conic satisfying the quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$ is of the form (f, e, d) as shown in Figure 2. For a complete proof, see [5].

The $q + 1$ points of a conic together with its nucleus constitute a *hyperoval* (Definition 2.11). Note that this is not the only instance of a set of $q + 2$ points in a finite projective plane such that no three are collinear.

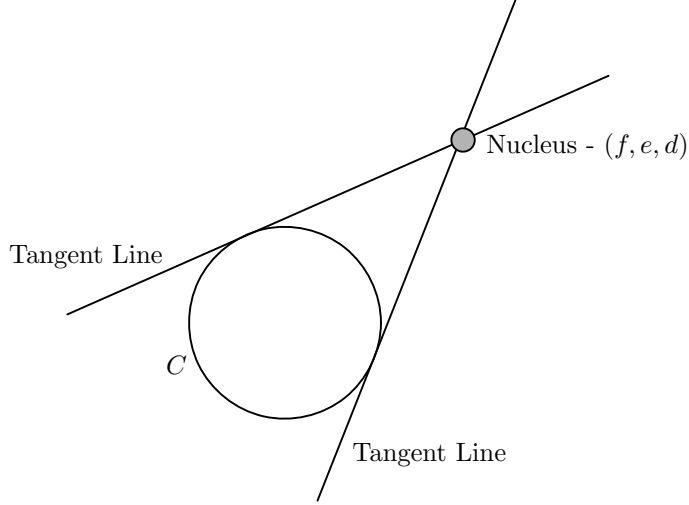


Figure 2: Nucleus of the form (f, e, d)

For our purposes, however, we will focus solely on the case where such a set of points is a result of extending a conic to a hyperoval, known as a *regular hyperoval*. It is a well-known result that the total number of regular hyperovals in a projective plane of order $q > 4$ is $q^5 - q^2$. Note that the number of conics is always $q^5 - q^2$, but in the case where $q = 4$ some collapsing occurs and the extension of a conic to include its nucleus may coincide with the hyperoval resulting from the extension of a different conic.

Some of our arguments will rely on the construction of multiple hyperovals. However, we will constantly refer to the standard hyperoval which arises from the extension of the conic satisfying $y^2 = xz$. Hence, from this point on, we let C be the conic consisting of the set of points satisfying the quadratic form $y^2 = xz$, and we let H be the hyperoval resulting from the extension of this conic to include its nucleus $(0, 1, 0)$.

There is an interesting duality to the structure of finite projective planes. Notice that if we interchange the words “point” and “line” in the axioms, we obtain equivalent statements. Hence, for any finite projective plane π , we naturally obtain a *dual plane* π' where the points and lines of π' are the lines and points, respectively, of π . In fact, every object in π has a natural dual object in π' (and we can still view it as part of π). For instance, a *dual conic* (and, more generally, a *dual arc*) is a set of $q + 1$ lines with the property that no three intersect in a common point. Because no three of the lines intersect the same point in π , the dual set of points has the property that no three are collinear. In other words, the points constitute a typical conic in the dual plane, and hence can be thought of as a dual conic in π . Additionally, the concept of a nucleus extends to this dual conic. By Theorem 2.16, we know that the nucleus of the conic in the dual plane is the point of concurrency of the tangent lines to the conic, the point (f, e, d) . In the context of the

original projective plane π , the *dual nucleus* is the line $[f, e, d]$. This line has the property that it contains all of the “tangent points.” This may seem a strange concept and requires a bit of explanation. The points of a conic have the property that every secant line through them contains a second point of the conic, and every tangent line (of which there is just one) passes through a common point, the nucleus. Translating this concept to the dual conic, we have that every line of a dual conic contains q secant points – points that are incident with another line of the dual conic – and exactly one “tangent point” – a point that is not incident with any other line of the dual conic. Just as the tangent lines to a conic are concurrent, the tangent points to a dual conic are *collinear* on a line which we call the *dual nucleus*. The dual conic together with its dual nucleus can be considered a *dual hyperoval* in π .

Example 2.17. Consider the set of lines $S = \{[0, 1, 1], [0, 1, 0], [1, \omega, \omega^2], [1, 1, 1], [1, \omega, 0]\}$ of $PG(2, 4)$ where ω is the primitive element of $GF(4)$ and necessarily satisfies $1 + \omega = \omega^2$. Notice that no three lines go through a common point, as pictured in Figure 3.

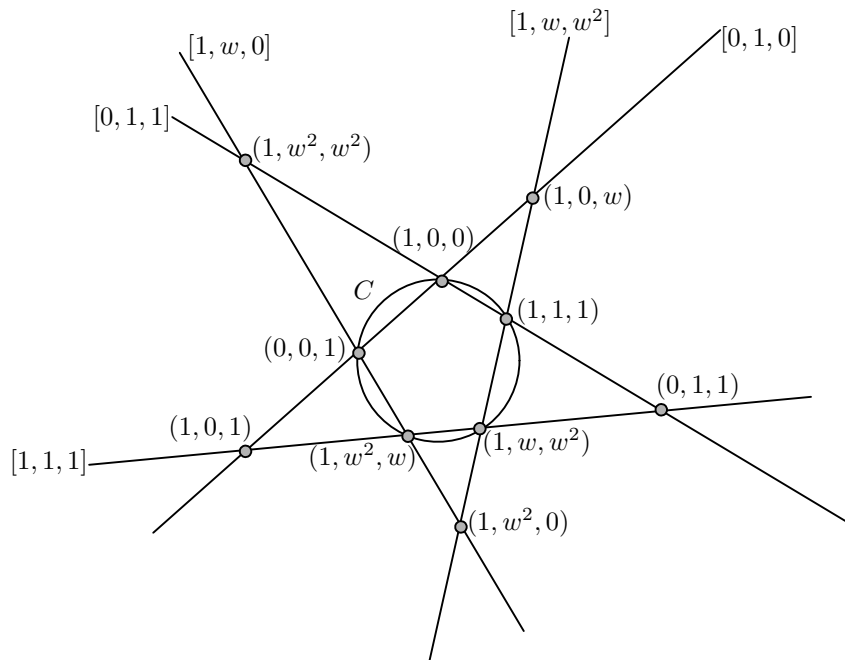


Figure 3: A dual conic when $q = 4$

We can think of this set of lines as a set of points in the dual plane. Since no three of the lines intersect in a common point, the dual set of $q + 1$ points has the property that no three are collinear. In fact, this set of lines has coordinates which satisfy a quadratic form (can you find it?) and hence can be thought of as a dual conic. By Theorem 2.16, we know that the nucleus of this dual conic is $[1, 1, w]$. In the context of the original geometric structure, the nucleus of the dual conic is the line containing the $q + 1 = 5$ points that

each lie on just one line of the dual conic.

2.3 Connections to Coding

The concept of error-correcting codes deals with encoding messages such that if any errors occur when the message is transmitted, then the receiver is able to detect the error and hopefully even correct it. This idea dates back to about 1948 when computer science was just beginning and Claude Shannon wrote his famous paper about the topic.

A binary linear code is a vector space over $GF(2)$ (meaning each code is made up of zeros and ones). We are able to use a matrix consisting of only zeros and ones, or a generator matrix, to represent the codes. To encode a message, we just multiply the message, a vector, by the generator matrix. In return, this will give us the original vector with extra information added on to it. This extra information is the error-correcting information and allows the receiver to fix any errors that may have occurred in the original message. A codeword is defined as the vector space spanned by the rows of the generator matrix (i.e., the row space).

Though this is one way to represent a code, we will be working primarily with parity-check matrices. The rows of a parity-check matrix generate the orthogonal complement of the code. Let $D = (P, L)$ denote the incidence structure of certain points P and lines L taken from a projective plane π . That is, P is a set of points in π and L is a set of lines in π . We will create a parity-check matrix M by utilizing this incidence structure. In order to construct our matrix, we label the columns of the matrix with a subset of the points in π and the rows with a subset of the lines in π . If a point lies on a line, the corresponding entry in the matrix is a one. If a point does not lie on a line, then the corresponding entry is a zero.

The *characteristic vector* v_i of a line l_i is the vector corresponding to the i^{th} row of the incidence matrix (that is, the row labeled with the line l_i). Every coordinate corresponds to a particular point of π , and hence a one in the j^{th} coordinate position indicates that the line intersects the point P_j . Dually, the characteristic vector of a point P_j is the vector corresponding to the j^{th} column of the incidence matrix. In this case, every coordinate corresponds to a specific line of π , and so a one as the i^{th} coordinate indicates that the point lies on the line l_i .

Proposition 2.18. *Let \mathcal{C} be the binary linear code generated by the parity-check matrix M defined by the incidence structure (P, L) . Then a codeword in \mathcal{C} is represented in π by a set of points S such that every line in L intersects S in an even number of points.*

Proof. Let M be a parity check matrix for \mathcal{C} and let \mathbf{c} be a codeword. Then \mathbf{c} must be orthogonal to every row in M . That is, the dot product of any row l and \mathbf{c} equals 0. In order for this to happen, l and \mathbf{c} must have an even number of 1s in common positions. But the row l represents the points lying on a single line. Thus, there must be an even number of points of S with which l is incident. If we vary l for all lines, we see that each line meets S in an even number of points. \square

A code is defined by three parameters and is represented by (n, k, d) where n is the length, k is the dimension, and d is the minimum distance. The length of a code is the number of bits in a transmitted codeword. In our setting, it is also equal to the number of columns in the parity-check matrix.

The dimension of a code is the number of bits that actually contain message information, not error-correcting information. If we take the dimension k of \mathcal{C} , and add it to the rank of the parity-check matrix M , we will get the length, n , of the matrix, or $n = k + \text{rank}(M)$. This is a straightforward result from linear algebra and we will use this property to determine the dimensions of our codes.

The minimum distance of a code shows how “close” the transmitted codewords are to each other. If the codewords are “too close” then it is likely that errors will not be detected. Therefore, we would like the minimum distance to be as large as possible. Under maximum likelihood decoding, if a code \mathcal{C} has a minimum distance of d , then \mathcal{C} can at most decode $t = \lfloor \frac{d-1}{2} \rfloor$ errors. It is important to note that the minimum distance is actually equal to the minimum weight, or the number of ones in a codeword, because of linearity.

In theory, we would like to optimize these three parameters. For instance, we might minimize the length for a fixed dimension and minimum distance, or maximize the minimum distance for a fixed length and dimension. This optimization is a fundamental problem in coding theory.

2.4 Additional Preliminaries for Finite Fields

Some of our arguments for determining the parameters of our codes will rely on the underlying algebra used to supply coordinates to our projective plane π . It is well-known that the non-zero elements of a finite field form a cyclic group under multiplication. A generator for this cyclic group is called a *primitive element* for the field. The choice of primitive element for our chosen finite field will play an important role.

A property of finite fields which is essential for our work is the notion of characteristic. The *characteristic* of a field is the smallest number n such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. For our purposes, we work exclusively with fields of characteristic two, and as a result, two is equivalent to zero. Therefore, when we evaluate $(x + y)^2 = x^2 + 2xy + y^2$, the middle term, $2xy$, simply drops out, leaving us with $(x + y)^2 = x^2 + y^2$. To

further develop the necessary ideas, we must introduce a well-known map on finite fields.

The *absolute trace map*, or simply *trace*, from the finite field with 2^k elements, $GF(2^k)$, to the finite field with only two elements, $GF(2)$ is the map defined by

$$x \mapsto x + x^2 + x^4 + \cdots + x^{2^{k-1}}$$

where $x \in GF(2^k)$. For example, the absolute trace map from $GF(8)$ to $GF(2)$ is $tr(x) = x + x^2 + x^4$. A few more basic statements will come in handy.

Proposition 2.19. *For any $x \in GF(2^k)$, $k \geq 1$, the trace of x^2 is equal to the trace of x .*

Proof. Consider the absolute trace map from $GF(2^k)$ to $GF(2)$.

$$\begin{aligned} tr(x^2) &= x^2 + (x^2)^2 + (x^2)^4 + \cdots + (x^2)^{2^{k-2}} + (x^2)^{2^{k-1}} \\ &= x^2 + x^4 + x^8 + \cdots + x^{2(2^{k-2})} + x^{2(2^{k-1})} \\ &= x^2 + x^4 + x^8 + \cdots + x^{2^{k-1}} + x^{2^k} \\ &= x + x^2 + x^4 + \cdots + x^{2^{k-1}} \\ &= tr(x) . \end{aligned}$$

□

Proposition 2.20. *For any $x \in GF(2^k)$, $k \geq 1$, $tr(x^2 + x) = 0$.*

Proof. Again consider the general trace map from $GF(2^k)$ to $GF(2)$.

$$\begin{aligned} tr(x^2 + x) &= (x^2 + x) + (x^2 + x)^2 + (x^2 + x)^4 + \cdots + (x^2 + x)^{2^{k-2}} + (x^2 + x)^{2^{k-1}} \\ &= x^2 + x + x^4 + x^2 + x^8 + x^4 + \cdots + (x^2)^{2^{k-2}} + x^{2^{k-2}} + (x^2)^{2^{k-1}} + x^{2^{k-1}} \\ &= x^2 + x + x^4 + x^2 + x^8 + x^4 + \cdots + x^{2^{k-1}} + x^{2^{k-2}} + x^{2^k} + x^{2^{k-1}} \\ &= x + x^{2^k} \\ &= x + x \quad (\text{since } x \text{ is a generator for a cyclic group of size } 2^k - 1) \\ &= 0. \end{aligned}$$

□

This final trace proposition adds an interesting twist to solving quadratic equations over $GF(2)$. When presented with an equation of the form $x^2 + x + c = 0$ in characteristic two, if $tr(c) = 1$, then we know that

there are no solutions for x . In fact, it can be shown that the converse is also true. That is, if a quadratic equation of the form above has no solutions, it follows that $\text{tr}(c) = 1$. Trace will come up quite frequently in both our selection of primitive elements and in the solving of quadratic equations.

Just as in \mathbb{R} , we can consider solutions to certain types of equations. In our work, we will be required to solve the quadratic equation $ax^2 + bx + c = 0$ for $x \in GF(2^k)$. Unlike in \mathbb{R} , squaring is a field automorphism, and so every element of a finite field of even characteristic is a square. Because eliminating the squared term results in a linear equation, when considering this quadratic we assume that a is nonzero. Similarly, if $c = 0$, the quadratic reduces to a linear equation. If $b = 0$,

$$\begin{aligned} ax^2 + c &= 0 \\ ax^2 &= -c \\ x^2 &= \frac{-c}{a}. \end{aligned}$$

As previously stated, when the characteristic of the field is even every element is a square. Therefore we can take the square root to obtain a unique solution.

If $a, b, c \neq 0$, we can substitute $\frac{by}{a}$ for x . Then

$$\begin{aligned} ax^2 + bx + c &= 0 \\ a \left(\frac{by}{a} \right)^2 + b \left(\frac{by}{a} \right) + c &= 0 \\ \left(\frac{b^2}{a} \right) y^2 + \left(\frac{b^2}{a} \right) y + c &= 0 \\ \frac{b^2}{a} (y^2 + y) &= -c \\ y^2 + y &= \frac{-ac}{b^2}. \end{aligned}$$

Note that by Proposition 2.20, $\text{tr}(y^2 + y) = 0$. If $\text{tr} \left(\frac{-ac}{b^2} \right) = 1$, then there is no solution. Moreover, there are solutions if and only if $\text{tr} \left(\frac{-ac}{b^2} \right) = 0$ as shown in [9].

As mentioned earlier, the non-zero elements of a finite field form a cyclic group under multiplication and a generator for this group is called a *primitive element*. We will use the variable ω to denote a primitive element. One important aspect of our work relies on the fact that a primitive element can be chosen in a clever way so that the trace of the element is nonzero.

Lemma 2.21. *If ω is a primitive element of $GF(q)$, then $\frac{1}{\omega}$ is also a primitive element.*

Proof. Let ω be a primitive element for $GF(q)$. For contradiction, assume that $\frac{1}{\omega}$ does not span the multiplicative group of $GF(q)$ and so $\frac{1}{\omega^i} = \frac{1}{\omega^j}$ for some distinct integers i and j between 0 and $q-2$. This implies

that $\omega^i = \omega^j$, a contraction. Thus, $\frac{1}{\omega}$ is also a primitive element for $GF(q)$. \square

Theorem 2.22. *For $k \geq 1$, there exists a primitive element ω for $GF(2^k)$ such that $tr(\omega) = 1$.*

Proof. By a result in [8], for any prime power q and any positive integer m , one can always find a primitive normal basis of $GF(q^m)$ as a vector space over $GF(q)$. This is a basis of the form $\{\omega, \omega^q, \omega^{q^2}, \dots, \omega^{q^{m-1}}\}$ where ω is a primitive element for $GF(q)$. Since these elements form a basis, their sum is non-zero (otherwise, there would be a dependency). But notice that when we substitute $q = 2$, this sum is precisely $tr(\omega)$. Hence, it is always possible to find a primitive element whose trace is 1. \square

For some of our results in Section 4, we will need to choose our primitive element ω so that $tr(\frac{1}{\omega}) = 1$. We now know that this is possible. By Theorem 2.22, we can choose a primitive element $\frac{1}{\omega}$ so that its trace is 1. By Lemma 2.21, we know that we can choose ω as a primitive element so that $tr(\frac{1}{\omega}) = 1$.

Corollary 2.23. *If ω is the primitive element for $GF(q)$ chosen as above so that $tr(\frac{1}{\omega}) = 1$, then $x^2 + x + \frac{1}{\omega^2}$ has no solutions for x .*

Proof. Let ω be a primitive element for $GF(q)$ such that $tr(\frac{1}{\omega}) = 1$. By Proposition 2.19 $tr(x) = tr(x^2)$ which implies that $tr(\frac{1}{\omega}) = tr(\frac{1}{\omega^2})$. Now we have

$$\begin{aligned} x^2 + x + \frac{1}{\omega^2} &= 0 \\ x^2 + x &= \frac{1}{\omega^2} . \end{aligned}$$

If there are solutions for x , $tr(x^2 + x) = tr(\frac{1}{\omega^2})$. By Proposition 2.20, $tr(x^2 + x) = 0$. But the primitive element ω was chosen so that $tr(\frac{1}{\omega}) = 1$. This is a contradiction, and hence $x^2 + x + \frac{1}{\omega^2} = 0$ has no solutions for x . \square

We refer to this result as we further examine the applications in Sections 3 and 4.

3 Applications to Cryptography

A useful application of the various properties of conics and hyperovals in finite projective planes lies in secret sharing schemes. Recall that a *secret sharing scheme* is a method of distributing a secret piece of information among a group of individuals. The secret is divided up and dispensed to the participants in such a way that a single individual cannot recover the information by himself. The entire secret can only be

recovered when several individuals reconvene and share their fragments of information. Before expanding upon this application in depth, several geometric properties of conics and hyperovals must be discussed.

3.1 Additional Geometric Properties

Theorem 3.1. *For any five points in a projective plane π , no three of which are collinear, there exists a unique conic containing them.*

Proof. Suppose that five points in π form two conics. We show that the two conics are the same. It is safe to assume that the first conic satisfies the standard form $y^2 = xz$ and the second conic is of the more general form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$. We will count the number of solutions for both equations.

Case 1: Suppose the point $(0, 0, 1)$ satisfies both equations. Notice that this point satisfies the first equation, and when we plug this point into the second equation we get $c = 0$. The remaining points that satisfy the first equation are of the form $(1, t, t^2)$. If we plug these points into the second equation we get $a + bt^2 + ct^4 + dt + et^2 + ft^3 = 0$. Note, however, that $c = 0$. Thus, we are left with the equation $a + bt^2 + dt + et^2 + ft^3 = 0$. This is a cubic equation in t , and hence it has at most three solutions for t . Together with the point $(0, 0, 1)$, this gives us at most four points that lie on both conics. This is a contradiction since we assumed that the conics had five points in common. We conclude that $f = 0$. So the second conic satisfies the quadratic $(b + e)t^2 + dt + a = 0$. Following an argument similar to the previous one, we have that $a = d = 0$ and $b + e = 0$. Hence $b = e$, and so the second conic satisfies the quadratic form $y^2 = xz$. Therefore, these two conics are really the same.

Case 2: Now suppose that the point $(0, 0, 1)$ does not satisfy both equations. Then every point that does satisfy the first equation is of the form $(1, t, t^2)$. If we plug these coordinates into the second equation we obtain $a + bt^2 + ct^4 + dt + et^2 + ft^3 = 0$. Notice, however, that this equation has at most four solutions for t . By repeating the previous argument, we conclude that these two conics are really the same. \square

We have just proved that given five points, no three collinear, we are able to determine a unique conic as shown in Figure 4. Now suppose that we are actually given five points and we must determine the unique conic. In order to figure out the conic we must first plug in each point into the general quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$. Because we have six coefficients, $a, b, c, d, e,$ and f , and only have five points, it seems as though we will not be able to find the exact values for the coefficients. However, we will be able to solve for each coefficient relative to another coefficient. For instance, if we plug in each point into the quadratic form, we obtain five equations which can be represented as a matrix of the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & x_1 \\ 0 & 1 & 0 & 0 & 0 & x_2 \\ 0 & 0 & 1 & 0 & 0 & x_3 \\ 0 & 0 & 0 & 1 & 0 & x_4 \\ 0 & 0 & 0 & 0 & 1 & x_5 \end{bmatrix}$$

where the first five columns represent the coefficients a through e and the last column represents the coefficient f . (Note that other forms for this matrix are possible, but will lead to the same conclusion.) Thus, we have a matrix with solutions for all the coefficients relative to the coefficient f . With this, we are able to work backwards and figure out each variable up to a scalar multiple. This is enough information to figure out the unique conic since scalar multiples of the coefficients are equivalent.

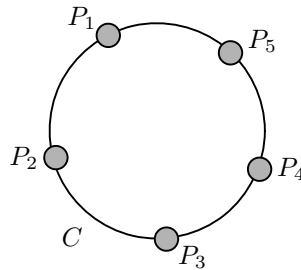


Figure 4: Five points determine a unique conic

We are also able to determine a unique conic given three points and two tangent lines, as pictured in Figure 5. In order to do this, we first take the cross product of the two tangent lines. This cross product gives us the point which lies on both tangent lines. Since all tangent lines intersect at the same point, this point of intersection gives us the nucleus which is of the form (f, e, d) . However, note that we really only know these coefficients up to a scalar multiple. With this information, we are able to plug these values as well as the three points into the general quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$. Then we are left with three nonhomogeneous equations:

$$\begin{aligned} a(x_1)^2 + b(y_1)^2 + c(z_1)^2 &= k_1 \\ a(x_2)^2 + b(y_2)^2 + c(z_2)^2 &= k_2 \\ a(x_3)^2 + b(y_3)^2 + c(z_3)^2 &= k_3, \end{aligned}$$

where (x_i, y_i, z_i) are the three given points. Assuming that the points are not collinear, we are able to solve for the coefficients a , b , and c . However, note that when we solve for the a , b , and c , we will have really found the coefficients $[a, b, c, kd, kf, ke]$. To determine k we can take a point, plug it into the conic equation, and solve for k . This will then give us all of the coefficients.

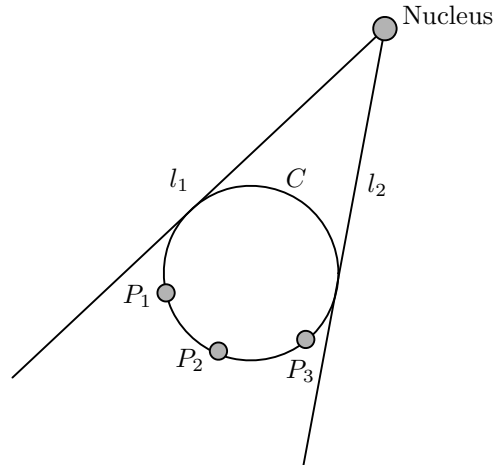


Figure 5: Two tangents and three points determine a conic

Note that if we were given two tangent lines and only two points instead of three, we would not be able to solve for all the coefficients. The reason being is, after solving for d , e , and f and then plugging the two points into the conic equation, we would be left with two equations and three variables. The two resulting equations would not be homogeneous, and hence we would not be able to do the same process of working backwards that we did in the example with five points and six coefficients.

Additionally, one tangent line and four points *do not* necessarily uniquely determine a conic. We provide an example of this.

Example 3.2. Consider the points $(1, 0, 0)$, $(1, \alpha^6, \alpha^5)$, $(1, \alpha^4, \alpha)$, and $(1, \alpha^3, \alpha^6)$ in $PG(2, 8)$, where α is a primitive element satisfying the minimal polynomial $\alpha^3 + \alpha + 1 = 0$. (Note that in $GF(2, 2^s)$, a primitive element has the property that it is a root of an irreducible polynomial of degree s , known as a minimal polynomial). It can be shown that these four points lie on both the standard conic, $y^2 + xz = 0$ and $y^2 + \alpha^3 z^2 + \alpha^2 xy = 0$. Additionally, it can be shown that the line $[1, 0, 0]$ is a tangent line to both conics.

We are now ready to utilize these properties to create some secret sharing schemes.

3.2 Secret Sharing Scenarios

The following secret sharing scenarios make use of the various geometric properties of hyperovals in a finite projective plane π .

Scenario 1: Suppose you are a scientist and you work in a top secret laboratory. There are two types of scientists in this laboratory, the high positioned scientists and the low positioned scientists. To be concise, we will refer to them as the HPS and the LPS. Because the laboratory is top secret, there are certain rooms that require a password and do not allow any one person to enter alone. In order to enter these rooms, either two HPSs or five LPSs have to be together. We will devise such a scheme.

If we pick any particular conic C in the projective plane π and we designate the password for a certain room as the nucleus, then we can give each HPS a tangent line to C and each LPS a point of C . If two HPSs get together, they can find the point where their tangent lines intersect, revealing the nucleus, and hence allowing them to enter the room. Also, if five LPSs get together, they can determine the quadratic form, giving them the coefficients d , e , and f which will then allow them to enter the room.

Scenario 2: Suppose you work in a bank. The bank has two types of employees, the top executive employees who have worked there for decades, and the regular employees who have a few years under their belts. To be concise, we will refer to them as EEs and REs. The “main vault” of the bank is located at the end of a hallway in the bank. The owner of the bank has decided that with time comes trust, and hence the EEs are more trustworthy than the REs. Therefore, the owner of the bank has decided that the only way to get into the “main vault” is by letting three EEs go in together, two EEs and one RE, or five REs. Once again, we can create a scheme such that the only way to get the combination for the “main vault” is if one of these three combinations of people get together.

If we pick a particular conic C in π , we designate the string of coefficients $[a, b, c, d, e, f]$ as the combination for the vault. We can give each EE a tangent line and a point of C , and give each RE a point of C . If two EEs get together, they can find the nucleus, giving them the coefficients d , e , and f . To find a , b , and c , they need a third EE. These three EEs can repeat the same process as in Section 3.1, giving them the needed coefficients, and allowing them to enter the “main vault”. If two EEs get together with one RE, the EEs can determine the nucleus, giving the d , e , and f , and they can use the REs point in conjunction with their points to find a , b , and c . This will allow them to enter the vault. Finally if five REs get together, they can determine the quadratic form, revealing all of the coefficients, and hence allowing them to enter the vault.

Scenario 3: We return to the laboratory setting for our final scenario. Suppose the HPSs and the LPSs

have separate lab rooms. Because of the highly secretive nature of the work done in the HPS lab, an LPS is never allowed to enter. However, because there are very dangerous chemicals located in a locked room within an LPS lab, HPSs are allowed to enter the LPS lab. These chemicals are deemed so dangerous that no one scientist can access the room alone; at least five scientists, three of which must be HPSs, must be present to unlock the door. If two or more LPSs want to use their lab, they are more than welcome to, but they will not be able to get into the room which holds the hazardous chemicals.

We pick a conic C in the projective plane π and designate the password of the LPS lab as the nucleus of C and the combination for the locked room be the coefficients a , b , and c . Then we dole out a tangent line to each LPS and a point of C to each HPS. If two LPS get together, they can determine the nucleus, revealing the coefficients d , e , and f , allowing them to enter the LPS lab. However, if they need to get into the locked room inside the lab, they will need the assistance of at least three HPSs. The three HPSs can solve for the a , b , and c , allowing them to access the locked room. If an HPS needs to access the room without any LPSs, they will need at least four other HPSs. If at least five HPSs get together, they can determine the quadratic form, revealing all of the coefficients $[a, b, c, d, e, f]$, allowing them to enter both the LPS lab and the locked room within.

3.3 Security of our Secret Sharing Schemes

Now that we have our scenarios, let us look at the security of our schemes. For the first scenario, suppose one particular HPS decided that he or she wanted to sneak into a locked top secret room without any other scientist knowing. What is the probability that the HPS would actually guess the password, or in this case, the nucleus? If the HPS is given just a tangent line, the nucleus must be somewhere on that line. Since there are $q + 1$ points on any line, the probability of guessing the nucleus is $\frac{1}{q+1}$.

Now suppose three LPSs got together and tried to enter a locked room. What are the chances that they could guess the password? This requires some counting. We would like to find the number of conics that go through any three non-collinear points. Pick any three such points that are in π , say P_1 , P_2 , and P_3 . We know that the other two points cannot be collinear with any pair of these points. There are $q + 1$ points on the line that contains P_1 and P_2 . Not counting the point P_1 , there are q points on the line that contains P_2 and P_3 . Now if we do not count P_2 and P_3 , there are $q - 1$ points on the line that contains P_2 and P_3 . If we add all these together we get $3q$ points. Take this number and subtract it from the total number of points in π , $q^2 + q + 1$, and we get the total number of points that we can choose as a fourth point, say P_4 , that would not be collinear to any combination of the first three points. This number is $q^2 - 2q + 1$. Now

that we have chosen four points, our last point, say P_5 must be chosen so that no three points are collinear. We do similar counting to find that we have $q^2 - 5q + 6$ choices for the last point. Now, to find the total number of conics that pass through these points we simply multiply $q^2 - 2q + 1$ with $q^2 - 5q + 6$. But note that we have over counted the number of conics. We need to take into account the fact that for a fixed conic there will be multiple choices for P_4 and P_5 . Thus, we need to divide by $(q - 2)$ and $(q - 3)$ which are the total number of choices for P_4 and P_5 on a fixed conic. Thus, we now have $\frac{(q^2 - 2q + 1)(q^2 - 5q + 6)}{(q - 2)(q - 3)}$ which gives us $(q - 1)^2$ conics. We must now show that each of these $(q - 1)^2$ conics has a different nucleus. Suppose we have two conics with the same nucleus. This is a contradiction because three points and a nucleus determine a unique conic. Thus, all of the $(q - 1)^2$ conics have a different nucleus. Therefore, the probability for three LPSs guessing the password, i.e., guessing the conic through a fixed set of three distinct points, is $\frac{1}{(q-1)^2}$.

Note that the probability of one, two, or four LPSs recovering the password can be found in a similar fashion as with three LPSs. The probability of four LPSs figuring out the password is $\frac{1}{q-2}$; two LPSs, $\frac{1}{q^2(q-1)}$; and 1 LPS, $\frac{1}{q^2(q^2-1)}$.

Now suppose that one HPS gets together with four or less LPSs. No matter what the number of LPSs the HPS is with, the probability will always be the same. That is, the probability will always be $\frac{1}{q+1}$ since it is more likely to recover the password with a tangent line than with four or less points.

For scenario two, suppose two EEs get together and try to break into the “main vault.” Because the EEs are given tangent lines and points, and two tangent lines determine the nucleus of a conic, the two EEs will have half of the password, which in this case is the string of coefficients $[a, b, c, d, e, f]$. Because they also have two points, they will be able to solve for two of the other coefficients, say b and c , in terms of the other coefficient, say a . We need to determine the number of conics that pass through two points and a particular nucleus. Because of the projective equivalence of regular hyperovals, through any given nucleus and two points, we have the same number of regular hyperovals. Counting as we did above shows that the probability for two EEs breaking into the “main vault” is $\frac{1}{q-1}$.

What if one EE and two REs decided to try to break into the “main vault”? This is just the probability of one tangent line determining the nucleus, $\frac{1}{q+1}$, multiplied by the probability of two REs figuring out the a , b , and c , $\frac{1}{q-1}$, since these two cases are independent. Thus, this probability is just $\frac{1}{(q+1)(q-1)}$, or $\frac{1}{q^2-1}$. Note that the probability of one EE and one, three, or four REs recovering the password is found using similar counting.

Now if four or less REs got together, it is the same counting problem as in scenario one with the four or less LPSs recovering the password. Hence, the probabilities are all the same as in that section.

With the last scenario, suppose two LPSs have entered their lab, but they want to break into the locked room with the dangerous chemicals. The probability that they would be able to do this is $\frac{1}{q^2(q-1)}$. The reason being is that the total number of conics in π , $q^5 - q^2$, divided by the total number of nuclei in π , $q^2 + q + 1$ (since the nucleus can be any point), will give us the number of conics that pass through a given nucleus, which is $q^2(q-1)$.

Now suppose that two LPSs and one HPS wants to get into the room with the chemicals. Since the LPSs were given tangent lines, these three people will be able to get into the LPS lab without a problem since their lab was designed in this way. So we need to find the number of conics that go through one point and a particular nucleus in order to figure out the coefficients a , b , and c . This is found by taking the number of conics through a particular point in π , $q^2(q^2 - 1)$, and dividing by the number of points in π that are not the nucleus, $q^2 + q$, which gives us $q(q-1)$. Thus, the probability of two LPSs and one HPS getting into the room is $\frac{1}{q(q-1)}$. Finding the probability of two LPSs and two HPS is done in a similar fashion and gives us a probability of $\frac{q^2(q-1)}{q^2}$.

If four or less HPS wanted to try to get into the LPS lab, the same probabilities would apply as in scenario one with the number of points (in that case it was the LPS who were given points) figuring out the nucleus of a conic. It is important to note, however, that if three of four HPSs happened to recover the nucleus and get into the LPS lab, then they would be able to get inside the chemical room. However, if one or two HPSs somehow found the nucleus, they would still not necessarily be able to get into the locked room.

It is also important to remember that we have control over the value of q and thus we have control over the security of our scheme. Since q can be any power of 2, we can choose it to be a very large number. The larger q is, the lower the probability that any person would be able to guess the passwords.

4 Applications to Coding

Recall from Section 2.3 that we can define a code by building a parity-check matrix which is an incidence matrix for subsets of points and lines in a projective plane π . Points are represented by columns of the matrix, and lines are represented by rows of the matrix. Also, recall from Proposition 2.18 that a codeword \mathbf{c} in a binary linear code C corresponds to a set of points S with the property that every line being considered meets S in an even number of points.

For example, consider the parity check matrix

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

where we think of the columns as being labeled with the points P_1 through P_7 and the rows as being labeled with the lines l_1 , l_2 , and l_3 . One codeword for this code is given by the vector $[0, 0, 0, 1, 1, 1, 1]$ which would naturally correspond to the point set $S = \{P_4, P_5, P_6, P_7\}$. Notice that this codeword has 4 ones in common with the first row of the parity check matrix, 2 with the second row, and 2 with the third. In the geometry, this means that l_1 meets S in 4 points, l_2 meets S in 2 points, and l_3 meets S in 2 points. Thus, each line meets S in an even number of points. Shown below in Figure 6 is a visual representation of how sets of points in a projective plane correspond to codewords.

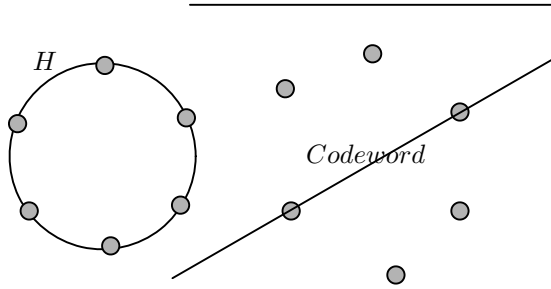


Figure 6: Representing a codeword as a collection of points

We will not consider the case when the full incidence matrix for π is used as a parity check matrix. The resulting code has been studied extensively. We will however make use of the following fundamental result due to K.J.C. Smith [11].

Theorem 4.1. *Let M be the $(0,1)$ -incidence matrix determined by the projective plane $PG(2, 2^s)$, $s \geq 1$, where the entries of M are considered to be over the finite field $GF(2)$. Then the rank of M is $3^s + 1$.*

For example, if $q = 8$, then $q = 2^3$, and hence $s = 3$ and the rank of the matrix is 28.

In this section we will discuss three classes of codes created using parity-check matrices which are determined by various subsets of points and lines in the projective plane π . The codes of \mathcal{C}_{SkNH} are generated by the incidence matrix of skew lines and non-hyperoval points. The codes of \mathcal{C}_{SeA} and \mathcal{C}_{SeNH} are generated by the incidence matrices of secant lines and all points and non-hyperoval points, respectively. For each class of codes, we discuss an arbitrary code \mathcal{C}_q , where q is the order of the finite projective plane used to create it.

4.1 Skew Lines and Non-Hyperoval Points, \mathcal{C}_{SkNH}

Our first class of codes is determined by the set of skew lines and non-hyperoval points. The following is a table of data for \mathcal{C}_{SkNH} collected using the program *Magma*.

q	Length, n	Dimension, k	Minimum Distance, d
2	3	2	2
4	15	10	3
8	63	44	5
16	255	190	
32	1032	812	
64	4095	3430	

Table 3: Code parameters for \mathcal{C}_{SkNH}

We first wish to examine the minimum distance for codes in this class. The table seems to indicate that a possible formula for the minimum distances of these codes could take the form $\frac{q}{2} + 1$. We will soon see that this may not be the case.

Proposition 4.2. *The code $\mathcal{C}_q \in \mathcal{C}_{SkNH}$ has minimum distance $d \geq \frac{q}{2} + 1$.*

Proof. Since minimum distance is the same as minimum weight for linear codes, we bound the minimum weight. Let S be a set of points of π that corresponds to a codeword. Then S is a set of non-hyperoval points with the property that every line skew to H meets S in an even number of points. Pick a point P in S and consider all the skew lines through it. We know then that there is at least one other point of S on each skew line. This gives us $\frac{q}{2}$ more points of S . Now add in the first point P and we get at least $\frac{q}{2} + 1$ points in S . Thus, the minimum distance is greater than or equal to $\frac{q}{2} + 1$. \square

The argument above will be standard for each class of codes we examine. The idea of looking at lines through a point and counting the number of additional points of S that can lie on these lines is very applicable to many code constructions and has appeared in numerous other works (see, for instance, [3, 7, 10]). Our next result is somewhat more general and will raise some interesting questions.

Proposition 4.3. *Let H be the standard hyperoval consisting of the points of the conic $y^2 = xz$ together with its nucleus. Let H' be a second hyperoval in the same plane with $H' \setminus H$ denoting the set of points in H' but not in H . Then $H' \setminus H$ corresponds to a codeword of $\mathcal{C}_q \in \mathcal{C}_{SkNH}$.*

Proof. Let l be a line skew to H . If l does not intersect H' , then it intersects $H' \setminus H$ in 0 points. If l intersects H' in some point P then it necessarily intersects H' in a second point Q . If Q is in $H' \setminus H$, then Q is skew to H and meets $H' \setminus H$ in two points. If Q is not in $H' \setminus H$, then it must lie on H . But if Q is on H , the line l must be a secant line for H , not a skew line as it was defined. Thus, every skew line meets $H' \setminus H$ in zero or two points and, hence, $H' \setminus H$ corresponds to a codeword. \square

Using the fact that the set of points $H' \setminus H$ corresponds to a codeword, we can obtain an upper bound on the minimum distance d . Let H' be a hyperoval that intersects H in the maximum possible number of points. Then, the set $H' \setminus H$ is as small as possible and would therefore give a codeword with small weight. It is certainly possible that codewords could arise via other means and we should not conclude that a hyperoval H' with this property would necessarily determine a *minimum weight* codeword. But this does lead to some interesting questions. In particular, if H is a regular hyperoval and H' is *any* other hyperoval, what is the maximal possible value of $|H \cap H'|$? It is noted in [2] that, in $PG(2, 16)$, the maximal possible such intersection has size 8, thereby giving a codeword of weight 10. This means that a codeword of weight 9 cannot possibly arise from this construction. However, since five points determine a conic, it is certainly possible for two regular hyperovals to intersect in six points. This could occur if the underlying conics share four points and then one additional conic point serves as the nucleus of the other conic. Such a hyperoval H' would necessarily satisfy $|H' \setminus H| = q - 4$ giving us the following.

Corollary 4.4. *In the code $\mathcal{C}_q \in \mathcal{C}_{SkNH}$, there exists a codeword of weight $q - 4$.*

The existence of a hyperoval H' which is completely disjoint from our standard hyperoval H ensures that there is a codeword with weight $q + 2$. While this seems far away from our data above, we provide a proof since the general result will carry over to our remaining classes of codes. We will use a counting argument in order to show that there is in fact a disjoint hyperoval H' .

Lemma 4.5. *In $PG(2, 2^s)$, $s \geq 2$, there exists a hyperoval H' which is completely disjoint from the standard hyperoval H .*

Proof. Let A_i denote the set of conics which contain the point P_i on C , the standard conic $y^2 = xz$. We will use counting techniques to determine the number of conics through each of the $q + 1$ points on the base conic C . In particular, we will use inclusion/exclusion to count $\left| \bigcup_{i=1}^{q+1} A_i \right|$, the number of conics which share at least one point with C . Note that this formula will require us to calculate the intersection of various sets of conics which share points with C . For instance, to count $|A_1 \cap A_2|$ we need to count the number of conics which pass through the two points P_1 and P_2 . Keeping in mind that we must choose our three other points

such that no three are collinear, there are q^2 choices for the third point, $q^2 - 2q + 1$ choices for the fourth point, and $q^2 - 5q + 6$ choices for the fifth point (this sort of counting was done in Section 3.3). But we have overcounted because together with P_1 and P_2 , *any* three points on a given conic C' together with P_1 and P_2 will count C' . Therefore, we divide by the number of ways you can pick these three additional points. So we have counted $\frac{q^2(q^2 - 2q + 1)(q^2 - 5q + 6)}{(q - 1)(q - 2)(q - 3)} = q^2(q - 1)$ conics that share points P_1 and P_2 . Once all of this counting is complete, we determine that there are at most roughly $\frac{5}{8}q^5$ conics which share at least one point with C . Note that this is a little more than half of the roughly q^5 conics in the entire plane π .

The points of the hyperovals resulting from the extension of these conics remain to be considered. Three cases must be studied: the case where a point of C is the nucleus of an otherwise disjoint conic C' , the case where the nucleus of C is a point of C' , and finally the case where the nucleus of C' is the nucleus of C . In the first case, there are $q + 1$ choices for the point on C as the nucleus of C' . Additionally, for a fixed conic C' , the coefficients d , e , and f are given by the coordinates of its nucleus, (f, e, d) . Therefore, there are at most q^3 choices for the coefficients a , b , c , considering that some combinations of coefficients yield degenerate conics. Hence, there are at most q^3 conics which have a particular nucleus. It follows that there are no more than about q^4 hyperovals whose nucleus is a point of C . In the second case, there are $q^2(q^2 - 1)$ conics which go through the particular point $(0, 1, 0)$. Hence, there are no more than q^4 hyperovals which contain the nucleus of C . Finally, there are at most only q^3 hyperovals with nucleus $(0, 1, 0)$.

In conclusion, we know that there are at most $\frac{5}{8}q^5 + 2q^4 + q^3$ hyperovals which share at least one point with our base hyperoval H . Because the difference between the total number of regular hyperovals in the projective plane π , known to be $q^5 - q^2$, and the number of hyperovals which share at least one point with H is roughly $\frac{3}{8}q^5$, a *positive* function of q , there necessarily exists a hyperoval H' which is completely disjoint from H for sufficiently large q . For $q > 8$, our counting ensures the existence of a disjoint hyperoval. For $q = 4$ and $q = 8$, a simple *Magma* computation verifies the existence of a hyperoval disjoint from H . Note that our counting was done in a very conservative way, and so it is certainly possible that we overcounted the number of hyperovals which intersect H . □

Theorem 4.6. *The the code $\mathcal{C}_q \in \mathcal{C}_{SkNH}$ contains a codeword of weight $q + 2$.*

Proof. By Lemma 4.5, we know that there exists a hyperoval disjoint from the standard hyperoval H in the projective plane. Fix one such hyperoval H' and consider $H' \setminus H$, the set of points on H' but not on the standard hyperoval H . Because H' is completely disjoint from H , $H' \setminus H$ is the entire set of points on H' . By Proposition 4.3, $H' \setminus H$ corresponds to a codeword. Therefore, the set of points on H' correspond to a codeword of weight $q + 2$. □

In order to determine the dimension of the code generated by skew lines and non-hyperoval points, we will prove that the rows of the incidence matrix M corresponding to secant lines to the hyperoval H are linear combinations of the rows corresponding to skew lines and tangent lines to the conic C . These linearly dependent rows can be eliminated without changing the rank of the matrix, and hence we can determine an upper and lower bound for the dimension of $\mathcal{C}_q \in \mathcal{C}_{SkNH}$.

Lemma 4.7. *Let C and H be as defined earlier. Let L be the dual conic consisting of the set of lines $[x, y, z]$ satisfying the quadratic form $\frac{1}{\omega^2}y^2 = xz$. Then each of the lines in L meets C in either zero points or one point.*

Proof. First note that it is straightforward to check that the quadratic form determining L is nondegenerate. The coordinates for the lines of L are of the form $[1, 0, 0]$, $[0, 0, 1]$, and $\left[1, y, \frac{1}{\omega^2}y^2\right]$. The line $[1, 0, 0]$ contains only the point $(0, 0, 1)$ on the conic C . The line $[0, 0, 1]$ contains only the point $(1, 0, 0)$ on C . To find how the line $\left[1, y, \frac{1}{\omega^2}y^2\right]$ meets C , we dot this line with $(1, x, x^2)$ and solve for x . We hope to find no solutions for x . To this end,

$$\begin{aligned} \left[1, y, \frac{1}{\omega^2}y^2\right] \cdot (1, x, x^2) &= 0 \\ 1 + x(y) + x^2 \left(\frac{1}{\omega^2}y^2\right) &= 0 \end{aligned}$$

We now refer to the results for when quadratic equations over fields of even characteristic have solutions (Section 2.4). Recall that $ax^2 + bx + c = 0$ has solutions for x if and only if $tr\left(\frac{ac}{b^2}\right) = 0$. Hence, our equation has solutions if and only if $tr\left(\frac{y^2}{\omega^2 y^2}\right) = tr\left(\frac{1}{\omega^2}\right) = 0$. However, if we choose our primitive element ω such that $tr\left(\frac{1}{\omega}\right) = 1$, then $tr\left(\frac{1}{\omega^2}\right) = 1$ as well (Proposition 2.19). Therefore, if $tr\left(\frac{1}{\omega^2}\right) = 1$, then $\left(\frac{1}{\omega^2}y^2\right)x^2 + (y)x + 1 = 0$ has no solutions for x . Hence, excluding the lines $[1, 0, 0]$ and $[0, 0, 1]$ which meet C in one point, L contains only lines which are skew to the hyperoval H . \square

By Theorem 2.16, the nucleus for L is the line given by $[0, 1, 0]$.

Theorem 4.8. *Let l with characteristic vector \mathbf{v} be any line secant to the conic C . Then there exists a set of lines $L = \{l_i\}$, each skew or tangent to C , with corresponding characteristic vectors \mathbf{v}_i , such that $\sum \mathbf{v}_i = \mathbf{v}$.*

Proof. We start by choosing l to be the specific line whose homogeneous coordinates are $[0, 1, 0]$. Now, choose the lines $L = \{l_i\}$ to be precisely the set of lines which constitute the dual conic defined in Lemma 4.7. As these lines form a dual conic in a projective plane over a field of even characteristic, they determine a unique

dual nucleus, a line all of whose points are “tangent” to the lines of the dual conic. In fact, this is exactly the line l as pointed out after the proof of the previous lemma.

Now consider the sum of the characteristic vectors \mathbf{v}_i . Any point P not on the nucleus l is covered by either zero lines of L or exactly two lines of L (since P is not a “tangent point,” and no three lines of L are concurrent). Hence, the coordinate position of $\sum \mathbf{v}_i$ corresponding to the point P will be 0. However, any point Q lying on l will be covered by just one line of L (since Q is a “tangent point”). Therefore, the coordinate position of $\sum \mathbf{v}_i$ corresponding to Q will be 1. In summary, $\sum \mathbf{v}_i$ gives us exactly the characteristic vector for the line l .

We now claim that the choice of l is, in fact, arbitrary. To do this, we appeal to a result from group theory. It is well-known that the group acting on the projective plane $PG(2, q)$ and fixing the conic C is isomorphic to the group $PGL(2, q)$. Moreover, this group acts 2-transitively on the points of C . In other words, the group maps any pair of points of C onto any other pair of points of C . Hence, the group acts transitively on the lines meeting C in two distinct points, the secant lines. Therefore, by applying the appropriate element of $PGL(2, q)$, we can map our secant line l onto any other secant line. The skew lines $\{l_i\}$ will correspondingly move to an alternate set of skew lines whose characteristic vectors will again sum to the characteristic vector for the image of l under this group action. Hence our choice of l was in fact arbitrary, and the characteristic vector for *any* line secant to the conic C can be realized as the sum of characteristic vectors corresponding to a set of skew lines and tangent lines. \square

We should point out that the previous theorem refers only to lines that are secant to C and not to the entire hyperoval H . This means that the rows corresponding to tangent lines to C cannot necessarily be realized as linear combinations of other rows. We now apply this result to our codes.

Corollary 4.9. *For any $s \geq 1$, the code $\mathcal{C}_{2^s} \in \mathcal{C}_{SkNH}$ has dimension k satisfying $4^s - 3^s + 2^s - 1 \leq k \leq 4^s - 3^s - 2$.*

Proof. The rows of the incidence matrix M corresponding to secant lines to the conic C can be eliminated without effecting the rank of the matrix. This follows from the fact the characteristic vector for any such secant line can be realized as a sum of characteristic vectors for a set of skew lines and tangent lines as proven in Theorem 4.8. Therefore, the rank of the matrix obtained after removing the rows corresponding to secant lines to the conic C is exactly $3^s + 1$, where the projective plane has order 2^s . However, the rank of the matrix obtained after subsequently removing the rows corresponding to the tangent lines to the conic C may decrease the rank of the matrix by $q + 1$, the number of such lines. Therefore, the matrix obtained

after removing *all* secant lines to H has rank between $3^s - 2^s$ and $3^s + 1$. Hence it follows that the code $\mathcal{C}_q \in \mathcal{C}_{S_{kNH}}$ has dimension k where $4^s - 3^s + 2^s - 1 \leq k \leq 4^s - 3^s - 2$. \square

Our data from Table 3 seems to indicate that our lower bound is likely the actual dimension, and it would be nice to be able to show this. Proving it would amount to showing that the removal of the rows corresponding to tangent lines would necessarily decrease the rank of the matrix by $q + 1$.

4.2 Secant Lines and All Points, \mathcal{C}_{SeA}

Our next class of codes is generated from the secant lines and all points. The following table presents data collected for \mathcal{C}_{SeA} from *Magma*.

q	Length, n	Dimension, k	Minimum Distance, d
2	7	3	4
4	21	11	6
8	73	45	10
16	273	191	
32	1057	813	
64	4161	3431	

Table 4: Code parameters for \mathcal{C}_{SeA}

We again start by looking at the minimum distance of our codes. From the table, it appears that our minimum distance could be $q + 2$. As in the previous section, we can find a lower bound on d . This argument parallels that of Proposition 4.2.

Proposition 4.10. *The code $\mathcal{C}_q \in \mathcal{C}_{SeA}$ has minimum distance $d \geq \frac{q}{2} + 2$.*

Proof. Let S be a set of points in π which corresponds to a codeword. Then S is a set of non-hyperoval points with the property that every line secant to H meets S in an even number of points. Choose a point P in S and consider the secant lines through P . There is at least one other point of S on each secant line through P . This gives us $\frac{q+2}{2} = \frac{q}{2} + 1$ more points of S . If we add the point P back in, we have at least $\frac{q}{2} + 2$ points. Therefore the minimum distance is at least $\frac{q}{2} + 2$. \square

By Lemma 4.5, we know that there is a hyperoval disjoint from H which would necessarily correspond to a codeword (since *every* line meets a hyperovals in an even number of points). The data from Table 4 seems to

indicate that these codewords are actually the minimum weight codewords. Thus far we have been unable to find either a proof of this fact or a counterexample to the conjecture. On the other hand, we are able to find exact values for the dimensions of these codes. We begin with a lemma similar to that of Lemma 4.7.

Lemma 4.11. *Let C be the conic defined by $y^2 = xz$. Let H be the hyperoval defined by C in addition to its nucleus, $(0, 1, 0)$. Let L be the dual conic consisting of the set of lines $[x, y, z]$ defined by the quadratic form $x^2 + \omega^2 z^2 + \omega xy + \omega^2 xz + \omega^2 yz = 0$. Then each of the lines in L meets C in two points.*

Proof. First note that it is straightforward to check that the quadratic form determining L is nondegenerate. The coordinates for the lines of L are of the form $[0, 1, 0]$, $[0, 1, 1]$, and $\left[1, \frac{\omega^2 z^2 + \omega^2 z + 1}{\omega + \omega^2 z}, z\right]$. The line $[0, 1, 0]$ contains the points $(1, 0, 0)$ and $(0, 0, 1)$, both of which are on the conic C . The line $[0, 1, 1]$ contains the points $(1, 1, 1)$ and $(0, 0, 1)$, both of which are on C . To find how $l = \left[1, \frac{\omega^2 z^2 + \omega^2 z + 1}{\omega + \omega^2 z}, z\right]$ meets C we can dot this line with $(1, x, x^2)$ and solve for x . We hope to find two distinct solutions. To this end,

$$\begin{aligned} \left[1, \frac{\omega^2 z^2 + \omega^2 z + 1}{\omega + \omega^2 z}, z\right] \cdot (1, x, x^2) &= 0 \\ 1 + x \left(\frac{\omega^2 z^2 + \omega^2 z + 1}{\omega + \omega^2 z}\right) + x^2 z &= 0 \\ x^2 (z(\omega + \omega^2 z)) + x(\omega^2 z^2 + \omega^2 z + 1) + (\omega + \omega^2 z) &= 0 \\ (x(1 + \omega z) + \omega)(x(\omega z) + (1 + \omega z)) &= 0 \end{aligned}$$

Here, there are two solutions for x , $x_1 = \frac{\omega}{1 + \omega z}$ and $x_2 = \frac{1 + \omega z}{\omega z}$. If these two solutions are distinct, then l is indeed a secant line to the conic C . However, the case where x_1 and x_2 are the same needs to be addressed. If $x_1 = x_2$,

$$\begin{aligned} \frac{\omega}{1 + \omega z} &= \frac{1 + \omega z}{\omega z} \\ \Rightarrow \omega^2 z &= (1 + \omega z)^2 \\ \Rightarrow \omega^2 z &= 1 + \omega^2 z^2 \\ \Rightarrow \omega^2 z^2 + \omega^2 z + 1 &= 0 \\ \Rightarrow z^2 + z + \frac{1}{\omega^2} &= 0. \end{aligned}$$

We now refer to the results for when quadratic equations over fields of even characteristic have solutions. Recall that $ax^2 + bx + c = 0$ has solutions for x if and only if $\text{tr}\left(\frac{ac}{b^2}\right) = 0$. Hence, our equation has solutions if and only if $\text{tr}\left(\frac{1}{\omega^2}\right) = 0$. However, if we choose our primitive element ω such that $\text{tr}\left(\frac{1}{\omega}\right) = 1$, then $\text{tr}\left(\frac{1}{\omega^2}\right) = 1$ as well (Proposition 2.19). If $\text{tr}\left(\frac{1}{\omega^2}\right) = 1$ then $z^2 + z + \frac{1}{\omega^2} = 0$ has no solutions for z . Hence, L contains only lines which are secant to the hyperoval H . \square

By Theorem 2.16, the nucleus for L is the line given by $[1, 1, \frac{1}{\omega}]$.

Theorem 4.12. *Let l with characteristic vector \mathbf{v} be any line skew to the hyperoval H as defined above. Then there exists a set of lines $L = \{l_i\}$, each secant to H , with corresponding characteristic vectors \mathbf{v}_i , such that $\sum \mathbf{v}_i = \mathbf{v}$.*

Proof. We start by choosing l to be the specific line whose homogeneous coordinates are $[1, 1, \frac{1}{\omega}]$. Now, choose the lines $L = \{l_i\}$ to be precisely the set of lines which constitute the dual conic defined in Lemma 4.11. As these lines form a dual conic in a projective plane over a field of even characteristic, they determine a unique *nucleus*, a line all of whose points are tangent to the dual conic. In fact, this is exactly the line l as pointed out after the proof of the previous lemma.

Now consider the sum of the characteristic vectors \mathbf{v}_i . Any point P not on the nucleus l is covered by either zero lines of L or exactly two lines of L (since P is not a “tangent point,” and no three lines of L are concurrent). Hence, the coordinate position of $\sum \mathbf{v}_i$ corresponding to the point P will be 0. However, any point Q lying on l will be covered by just one line of L (since Q is a “tangent point”). Therefore, the coordinate position of $\sum \mathbf{v}_i$ corresponding to Q will be 1. In summary, $\sum \mathbf{v}_i$ gives us exactly the characteristic vector for the line l .

We now claim that the choice of l is, in fact, arbitrary. This follows from a group theoretic result. It is well-known that the group fixing a conic is isomorphic to $PGL(2, q)$. Now, this group will necessarily send skew lines to other skew lines. The question is whether or not the action of this group on skew lines is transitive. The answer is yes and follows from a more general result by Hamilton and Penttila [4]. They show that the result is true for a much larger class of hyperovals (translation hyperovals) of which the regular hyperovals are a subset. Hence, the choice of l was indeed arbitrary and the characteristic vector for *any* skew line can be realized as a sum of characteristic vectors for a set of secant lines. \square

Corollary 4.13. *For $s \geq 1$, the dimension of $\mathcal{C}_{2^s} \in \mathcal{C}_{SeA}$ is $4^s - 3^s + 2^s$.*

Proof. The rows of the incidence matrix M corresponding to skew lines can be eliminated without affecting the rank of the matrix. This follows from the fact the characteristic vector for any skew line can be realized as a sum of characteristic vectors for a set of secant lines as proven in Theorem 4.12. Since the rank of the matrix obtained after removing the rows corresponding to skew lines is exactly $3^s + 1$, where the projective plane has order $q = 2^s$, it follows that the dimension of the code \mathcal{C}_{SeA} is $(q^2 + q + 1) - (3^s + 1) = 4^s - 3^s + 2^s$. \square

From the known bounds on minimum distances (see <http://www.codetables.de/>) of binary linear codes, the best known code with length 73 and dimension 45 is 10. Similarly the best known code with length 21 and dimension 11 is 6. It may be the case that these codes are in fact optimal, despite that no known bound confirms this for the length 73 case.

4.3 Secant Lines and Non-Hyperoval Points, \mathcal{C}_{SeNH}

Many of the results for the class of codes \mathcal{C}_{SeA} also apply to the class \mathcal{C}_{SeNH} . The following table presents data collected from *Magma* for this final class of codes, \mathcal{C}_{SeNH} .

q	Length, n	Dimension, k	Minimum Distance, d
2	3	0	3
4	15	5	6
8	63	35	10
16	255	173	
32	1032	779	
64	4095	3365	

Table 5: Code parameters for \mathcal{C}_{SeNH}

The bounds on the minimum distance for the code generated by secant lines and non-hyperoval points is the same as that for the minimum distance for the code generated by secant lines and all points, $\frac{q}{2} + 2 \leq d \leq q + 2$. However, the dimension still must be examined. To generate this new class of codes, we could simply take the incidence matrix for secant lines and all points, and remove the columns corresponding to the hyperoval points. Our data in Table 4.3 seems to indicate that this does not affect the rank of the matrix. We show this by constructing certain other conics.

Lemma 4.14. *Let C_1 be the conic determined by the quadratic form $x^2 + y^2 + \omega xy + (\omega + 1)xz = 0$, and let H_1 be its extension to a hyperoval. Then C_1 and the hyperoval H intersect precisely in the point $(0, 0, 1)$. Moreover, the nucleus of C_1 whose homogeneous coordinates are $(0, \omega + 1, \omega)$, does not lie on H .*

Proof. Let $x^2 + y^2 + \omega xy + (\omega + 1)xz = 0$ define the conic C_1 and let H be the hyperoval determined by $y^2 = xz$ with nucleus $(0, 1, 0)$. Note that it is straightforward to show that C_1 is nondegenerate. All the points that lie on H are either $(0, 0, 1)$, the nucleus $(0, 1, 0)$, or are of the form $(1, t, t^2)$. If we plug $(0, 0, 1)$ into the quadratic form for C_1 , we find that the equation is satisfied. However, if we plug a point of the form $(1, t, t^2)$ into C_1 , we get the equation $1 + t^2 + \omega t + (\omega + 1)t^2 = 0$, or $\omega t^2 + \omega t + 1 = 0$. But as stated in

Section 2.4, if $\text{tr}(\frac{ac}{b^2}) = 1$, then the quadratic equation $ax^2 + bx + c = 0$ has no solutions. In our situation, we have $\text{tr}(\frac{\omega}{\omega^2})$ or $\text{tr}(\frac{1}{\omega})$ which we can choose to be equal to 1. Thus, this quadratic has no solutions and all points of the form $(1, t, t^2)$ do not satisfy the quadratic form which determines C_1 . Now, plugging $(0, 1, 0)$ into C_1 we find that this point does not satisfy the equation. Thus, the nucleus $(0, 1, 0)$ of H does not lie on C_1 either. Hence, the only point that lies on both H and H_1 is $(0, 0, 1)$. \square

Lemma 4.15. *Let C_2 be a conic determined by the quadratic form $x^2 + (\omega + 1)y^2 + z^2 + xz = 0$, and let H_2 be its extension to a hyperoval. Then C_2 has no points in common with the hyperoval H . Moreover, the nucleus of C_2 is the point $(0, 1, 0)$, the nucleus for C .*

Proof. Let $x^2 + (\omega + 1)y^2 + z^2 + xz = 0$ be the quadratic form determining the conic C_2 and let H be the hyperoval determined by $y^2 = xz$ with the nucleus $(0, 1, 0)$. Again, it is straightforward to show that C_2 is nondegenerate. All of the conic points that lie on H are either $(0, 0, 1)$ or are of the form $(1, t, t^2)$. If we plug in $(0, 1, 0)$ into C_2 we see that the equation is satisfied. However, if we plug in the point $(0, 0, 1)$ into C_2 we find that the equation is not satisfied. Similarly, if we plug in a point of the form $(1, t, t^2)$, we obtain the equation $1 + (\omega + 1)x^2 + x^4 + x^2 = 0$, which reduces to $x^4 + \omega x^2 + 1 = 0$. We now think of this equation as being a quadratic in x^2 . As stated in Section 2.4, if $\text{tr}(\frac{ac}{b^2}) = 1$, then the quadratic equation has no solutions. In our setting, we have $\text{tr}(\frac{1}{\omega})$, and we have chosen ω in such a way that this trace is 1. Thus, no point of the form $(1, t, t^2)$ satisfies the equation for C_2 . Hence, H_2 and H meet precisely in the point $(0, 1, 0)$. \square

Theorem 4.16. *Let M' be the incidence matrix determined by all points and secant lines. Then the columns corresponding to points of H are linear combinations of the columns corresponding to non-hyperoval points.*

Proof. Let M' be the incidence matrix determined by all points and secant lines. Think of the matrix as being divided vertically into two sections, one side containing the non-hyperoval points and the other side containing the hyperoval points. Let Q be any point of H . We will construct a second hyperoval H' that meets H in precisely the point Q . This will lead to our general result as follows.

Let \mathbf{v}_Q be the characteristic vector for the point Q . Note that this is the column of M' corresponding to Q . Let P_i be points on the hyperoval H' and let \mathbf{v}_{P_i} be the characteristic vector for the non-hyperoval point P_i . Note again that these are just the columns M' corresponding to these points. We will show that $\sum_{i=1}^q \mathbf{v}_{P_i} = \mathbf{v}_Q$. We now construct the hyperoval H' by looking at two distinct cases.

Case 1: Suppose Q is the nucleus $(0, 1, 0)$. By Lemma 4.15, we can choose H' to be the hyperoval H_2

determined by the quadratic form $x^2 + y^2 + \omega xy + (\omega + 1)xz = 0$. This hyperoval possesses all of the desired properties. Now, pick any coordinate position in \mathbf{v}_Q . It will be either a 0 or a 1.

If the chosen coordinate position is a 0, then the line corresponding to that coordinate position, say l , does not pass through Q . So, l is either a secant line for H' (not through Q) or a skew line for H' . If l is a secant line, then l hits H' in two points other than Q . These two points of intersection, say P_i and P_j , are represented with two 1s in the summation $\sum_{i=1}^q \mathbf{v}_{P_i}$, which sum to 0. If l is a skew line, then l hits the conic in 0 points which again produces a sum of 0. In summary, the coordinate position of \mathbf{v}_Q corresponding to the line l is a 0. This is exactly what we want since l is a line not passing through Q .

If, on the other hand, the chosen coordinate position of \mathbf{v}_Q is a 1, then that corresponding line, say m , passes through the point Q , the nucleus of the conic C_2 . Thus, m must be a tangent line of the conic C_2 implying that m is incident with exactly one additional point of H_2 , say the point P_k . Therefore, the coordinate position in $\sum_{i=1}^q \mathbf{v}_{P_i}$ corresponding to the line m is a 1, since all terms in the sum are 0 except for the term corresponding to the point P_k .

Case 2: Now suppose that Q is the particular point $(0, 0, 1)$. By Lemma 4.14, the hyperoval H_1 can be used to find a set of points $\{P_i\}$ such that the characteristic vectors for these points sum to the characteristic vector \mathbf{v}_Q . This is similar to the argument for Case 1. We only need to show that the choice of Q , namely the point $(0, 0, 1)$ is arbitrary. To do this, we note that the group fixing the conic C is isomorphic to the group $PGL(2, q)$. This group acts transitively on the points of C and fixes the nucleus. Hence, by applying the appropriate group element to our plane, we can move the point $(0, 0, 1)$ to any other point of the conic C . This completes the proof. \square

Corollary 4.17. *For $s \geq 1$, the dimension of $\mathcal{C}_{2^s} \in \mathcal{C}_{SeNH}$ is $4^s - 3^s - 2$.*

Proof. By Theorem 4.12, the rows of the incidence matrix M corresponding to skew lines can be removed without effecting the rank. Additionally, the columns of the incidence matrix corresponding to hyperoval points can be removed without changing the rank of the matrix. This follows from the fact that the characteristic vector for any hyperoval point can be realized as a sum of characteristic vectors for a set of non-hyperoval points as proven in Theorem 4.16. Since the rank of the matrix obtained after removing the rows corresponding to skew lines and the columns corresponding to hyperoval points is precisely $3^s + 1$, where the projective plane has order 2^s , it follows that the dimension of the code $\mathcal{C}_q \in \mathcal{C}_{SeNH}$ is $(q^2 - 1) - (3^s + 1) = 4^s - 3^s - 2$. \square

4.4 Summary of Code Properties

We provide the following table to summarize the results shown in the previous sections.

Lines	Points	Length	Dimension	Minimum Distance
Skew	Non-hyperoval	$q^2 - 1$	$4^s - 3^s + 2^s - 1 \leq k \leq 4^s - 3^s - 2$	$\frac{q}{2} + 1 \leq d \leq q + 2$
Secant	All	$q^2 + q + 1$	$4^s - 3^s + 2^s$	$\frac{q}{2} + 2 \leq d \leq q + 2$
Secant	Non-hyperoval	$q^2 - 1$	$4^s - 3^s - 2$	$\frac{q}{2} + 2 \leq d \leq q + 2$

Table 6: Summary of code parameters

5 Conclusion

We have provided a robust method for constructing certain types of secret sharing schemes and binary linear codes based on the geometry of a hyperoval in $PG(2, 2^s)$. One of the areas where questions remain is with the weak bounds on minimum distance. For instance, when creating a code from secant lines and points, our *Magma* computations indicate that the minimum distance for the code generated in $PG(2, q)$ is $q + 2$. It would certainly be nice to provide a proof of this fact. Another possible application of these techniques could be to the construction of authentication codes. Such codes are used to provide reliable communication between parties by allowing users to authenticate a received message. While we did look briefly into this idea, we were unable to find a reasonable construction, and we leave this as a potential future exploration.

References

- [1] A. Beutelspacher and U. Rosenbaum, *Projective Geometry: From Foundations to Applications*. Cambridge University Press, 1998.
- [2] J.M.N. Brown and W.E. Cherowitzo, The Lunelli-Sce Hyperoval in $PG(2, 16)$. *J. Geom.***69**(2000) no. 1-2, 15-36.
- [3] S. Droms, K.E. Mellinger, and C. Meyer, LDPC codes generated by conics in the classical projective plane, *Designs, Codes and Cryptog.*, **40**: 3 (2006) 343-356.
- [4] N. Hamilton and T. Penttila, Groups of Maximal Arcs. *J. Comb Theory, Series A***94** (2001), 63-86.
- [5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford University Press, Second Edition, 1998.
- [6] D. R. Hughes and F. C. Piper, *Projective Planes*. Springer-Verlag, 1973.
- [7] J.-L. Kim, K. E. Mellinger, and L. Storme, Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles, *Designs, Codes and Cryptog.*, **42**: 1 (2007) 73-92.
- [8] H. W. Lenstra, Jr. and R. J. Schoof, Primitive normal bases for finite fields. *Math. Comp.* **48**: 177 (1987), 217–231.
- [9] R. Lidl and H. Niederreiter. *Finite Fields*. Addison-Wesley, 1983.
- [10] K. E. Mellinger, Classes of LDPC codes from quadratic surfaces of $PG(3, q)$, *Contrib. Discrete Math.* **2**: 1 (2007) 35-42.
- [11] K.J.C. Smith. On the p -rank of the incidence matrix of points in hyperplanes in a finite projective geometry. *J. Comb Theory***7**(1969), 122-129.