

THE WEIGHT ENUMERATOR FOR A CLASS OF
LDPC CODES DEFINED BY HYPEROVALS

Katie L. Hunsberger

submitted in partial fulfillment of the requirements for Honors in
Mathematics at the University of Mary Washington

Fredericksburg, Virginia

April 2009

This thesis by **Katie L. Hunsberger** is accepted in its present form as satisfying the thesis requirement for Honors in Mathematics.

DATE

APPROVED

Keith E. Mellinger, Ph.D.
thesis advisor

Randall D. Helmstutler, Ph.D.
committee member

Janusz Konieczny, Ph.D.
committee member

Contents

1	Introduction	1
2	Geometric construction of codes	2
2.1	Geometric preliminaries	2
2.2	Algebraic preliminaries	4
2.3	Coding theory preliminaries	6
2.4	The class from secant lines	7
3	Geometric representations of codewords	7
3.1	The case when $q = 4$	8
3.2	The general case	12
4	Algebraic constructions of small weight codewords	13
4.1	Codewords of weight $2q - 8$	19
4.2	Codewords of weight $2q - 6$	21
5	Conclusion	23

Abstract

In this thesis we look at a class of low-density parity-check codes that are defined by a hyperoval in a finite projective plane. The construction relies on the geometry of hyperovals, and properties of the codes have been explored previously (see [3]). In the present work, we look at the weight enumerator of the codes. Our goal is to determine the number of codewords of various weights and use the geometry of the plane to represent the small weight codewords. Our construction of small weight codewords makes use of intersecting hyperovals, and so we investigate the necessary algebraic conditions for a pair of hyperovals to share a specified number of points. We determine that all codewords in the projective plane $PG(2, 4)$ arise from the geometric configurations we enumerate. For larger values of $q = 2^s$, our investigations show that for $PG(2, 2^s)$, the parity of s affects the maximum number of points in which a pair of hyperovals can intersect, as well as the total number of hyperovals that intersect in a given number of points. As a result, the parity of s affects the number of small weight codewords resulting from these geometric configurations.

1 Introduction

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 [10] "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.

Low-density parity check (LDPC) codes are a specific type of error-correcting code. Developed in the early 1960s, LDPC codes fell out of use until the 1990s when it was discovered by MacKay and Neal [7] that these codes perform incredibly well when used in conjunction with a high-speed decoding algorithm that was adapted from robotics. The structure of an LDPC code is determined by a parity check matrix with a minimal number of nonzero

entries in each row and column. For our purposes we restrict our focus to LDPC codes over $GF(2)$, wherein “1” is the only nonzero element.

We can make use of the natural incidence structure of a finite projective plane π to create such a code. We create a parity-check matrix using an incidence matrix for subsets of points and lines in π . Let $\mathcal{D} = (\mathcal{P}, \mathcal{L})$ denote the incidence structure of a set of points \mathcal{P} and a set of lines \mathcal{L} taken from a projective plane π . To create a parity-check matrix M by utilizing this incidence structure we label the columns of the matrix with the points of \mathcal{P} and the rows with the lines of \mathcal{L} . 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. A more detailed discussion of linear coding can be found in the book by Pless [8].

Our work starts with the geometric background necessary to understand the code constructions. Section 2 gives the ideas needed for this understanding. From there we discuss how the geometry of hyperovals is used to create binary linear codes in Section 2.4. We then investigate the geometric configurations that result in codewords of various weights in Sections 3.1 and 3.2. Finally, in Section 4 we consider the algebraic conditions necessary for such configurations to occur.

2 Geometric construction of codes

In this work, we look at a method for generating LDPC codes using the techniques of finite geometry. Our work will focus on a class of codes that were originally discovered and analyzed during the Jepson Summer Science Institute of 2008 as found in [3]. The work of that project involved three classes of codes, each defined from a geometric technique. We briefly describe the relevant concepts from finite geometry and, in particular, the class of codes that we examine in this work.

2.1 Geometric preliminaries

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. A more advanced discussion can be found in [1].

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

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

Many properties of such a plane can be proven using elementary counting techniques. For more in depth explanation and proofs of the following propositions, see [3].

Let π be an arbitrary finite projective plane. It can be shown that every line in π contains the same number of points, denoted $q + 1$. The integer q is called the *order* of π . It follows that any point in π has $q + 1$ lines running through it. Once the number of points on a line and lines through a point have been established, we can determine the number of points and lines in π . In fact, π contains $q^2 + q + 1$ points and $q^2 + q + 1$ lines.

We now want to look at some arrangements of points of π , specifically objects called *arcs* and *hyperovals*.

Definition 2.2. *In a finite projective plane π , an arc A is a set of points, no three of which are collinear.*

One can use elementary counting techniques to show that if A is an arc in a finite projective plane π of order q , then A contains at most $q + 2$ points. If A contains $q + 2$ points, it can be proven that the order q is even. Therefore, if π has odd order q , the maximum number of points an arc A can contain is $q + 1$. When q is odd we call such a maximal set of $q + 1$ noncollinear points an *oval*. We will focus on the case when q is even.

Definition 2.3. *In a finite projective plane of order q with q even, a set of $q + 2$ points no three of which are collinear is called a hyperoval.*

We will soon see that algebraic methods involving quadratic equations can be used to construct $(q + 1)$ -arcs. For such arcs, it will follow that every point of the arc has exactly one line passing through it that meets the arc in only that point. In other words, through each point of a $(q + 1)$ -arc, there is a unique tangent line. Such a line is called a *tangent*, meeting the arc in exactly one point. Similarly, a *secant* is a line meeting the arc in two points. Interestingly, when q is even, one can always extend a $(q + 1)$ -arc to a $(q + 2)$ -arc. The notion of a *nucleus* must be discussed in order to see that this is true.

Theorem 2.4. *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.

Now, let P be the point where two tangent lines, say l_1 and l_2 , intersect. By the above argument, no other line through P can be secant to the arc. But there are $q + 1$ lines through P , and any point of the arc necessarily determines a line with P . Therefore, the remaining lines through P that intersect the arc must all be tangent lines. There are $q + 1$ lines through P and there are $q + 1$ lines that are tangent to the arc. The only possibility is that all of the tangent lines for the arc are concurrent at the point P . \square

Definition 2.5. *In the finite projective plane of even order q , the point of concurrency of the tangent lines to a $(q + 1)$ -arc A is called the nucleus.*

Consider a $(q + 1)$ -arc that has been extended to a hyperoval H by adding the nucleus. Then all lines are either *skew*, meeting H in zero points, or *secant*, meeting H in two points. 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 straightforward to count the number of secant and skew lines that pass through any point off the hyperoval. For any point not on 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 .

2.2 Algebraic preliminaries

In addition to synthetic properties, we must also introduce the algebraic constructions and properties of finite projective planes. Finite projective planes can be constructed 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.

Using a finite field, we can construct an example of a projective plane. Let V be a three-dimensional vector space over the finite field $GF(q)$. We 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 plane of 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. In order to control this variability, we “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 use orthogonal complements to represent them. The set of vectors orthogonal to the nonzero 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 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 $ax + by + cz = 0$.

Using homogeneous coordinates, we can now discuss an algebraic construction of a hyperoval.

Definition 2.6. *A conic C is a set of points whose coordinates satisfy the quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$, where a, b, c, d, e, f are fixed elements of $GF(q)$, called the coefficients of C .*

Depending on the coefficients, some quadratic forms will yield degenerate conics. For instance, $x^2 = 0$ gives a set of points forming the line $[1, 0, 0]$. 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 particular conic consists of the $q + 1$ points $\{(1, k, k^2) : k \in GF(q)\} \cup \{(0, 0, 1)\}$. We refer to this conic as the *base conic*.

Our work will rely solely on nondegenerate conics and so from this point on, when we refer to a conic C we specifically mean a nondegenerate conic. It can be shown that every conic is an arc (Definition 2.2). For a detailed proof, see [3]. In fact, when q is odd, Segre [9] showed that every collection of $q + 1$ points, no three collinear, is in fact a conic. This result,

although quite remarkable, will have little bearing on our work since we focus on the case when q is even. When q is even, 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) . For a complete proof, see [5].

The $q + 1$ points of a conic together with its nucleus constitute a hyperoval (Definition 2.3). 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. 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*. From this point on, we refer to the hyperoval resulting from the extension base conic to include its nucleus, $(0, 1, 0)$, as the *base hyperoval*.

2.3 Coding theory preliminaries

As our work will ultimately be used to construct some classes of linear codes, we provide a brief background on coding theory. A *binary linear code* is a vector space over $GF(2)$ (meaning each codeword 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 error-correcting information that allows the receiver to fix any errors that may have occurred in the original message. A code 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 work primarily with parity-check matrices. The rows of a parity-check matrix generate the orthogonal complement of the code. Let $\mathcal{D} = (\mathcal{P}, \mathcal{L})$ denote the incidence structure of a set of points \mathcal{P} and lines \mathcal{L} taken from a projective plane π . In order to construct our parity-check matrix M , 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.

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 the code and add it to the rank

of the parity-check matrix M , we will get the length, n , of the matrix, or $n = k + \text{rank}(M)$.

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 \mathbf{C} has a minimum distance of d , then \mathbf{C} can at decode most $t = \lfloor \frac{d-1}{2} \rfloor$ 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.

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 .

2.4 The class from secant lines

Now that we have developed the necessary concepts, we can discuss how the geometry of finite projective planes, and more specifically of hyperovals, is used to create binary linear codes.

As alluded to in Section 2.3, we make use of the incidence structure of points \mathcal{P} and lines \mathcal{L} taken from a projective plane π . We create a parity-check matrix where the columns are labeled with all points of the plane π , and the rows with secant lines to a hyperoval. This matrix generates our class of codes, denoted \mathcal{C} . If a point lies on a secant line, the corresponding entry in the matrix is a 1. If a point does not lie on a line, then the corresponding entry is a 0. As determined in [3], if we use the plane $PG(2, q)$ in our construction, the code in this class has length $q^2 + q + 1$, dimension $4^s - 3^s + 2^s$ where $q = 2^s$, and minimum distance d satisfying $\frac{q}{2} + 2 \leq d \leq q + 2$.

3 Geometric representations of codewords

Our goal is to extend the results of [3] by examining the small weight codewords in \mathcal{C} . Ultimately, we would like to find geometric representations for all of the codewords in the class \mathcal{C} . To do this, we make use of the following fundamental result.

Proposition 3.1. *Let \mathbf{C} be the binary linear code generated by the parity-check matrix M defined by an incidence structure $(\mathcal{P}, \mathcal{L})$. Then a codeword in \mathbf{C} is represented in π by a set of points S such that every line in \mathcal{L} intersects S in an even number of points. Conversely, every set of points with this property necessarily determines a codeword.*

Proof. Let M be the parity check matrix for \mathbf{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} is 0. In order for this to happen, l and \mathbf{c} must have an even number of 1s in shared 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. Since l was a general line in \mathcal{L} , we see that each line in \mathcal{L} meets S in an even number of points.

Conversely, if we start with a set S of points with the desired property, it immediately follows that the characteristic vector for any secant line (i.e., a row of the parity-check matrix) is orthogonal to the characteristic vector for S . This means that the characteristic vector for S is a codeword. \square

We have shown that codewords can be completely characterized by sets of points with the property that every line meets them in an even number of points. This result will prove critical in identifying sets of points which result in codewords. Our goal is to enumerate the different geometric configurations that result in codewords.

3.1 The case when $q = 4$

We first examine the simplest code, where the code is determined by the incidence structure in $PG(2, 2^2)$. We enumerate the geometric configurations that result in codewords of different weights.

Recall from Proposition 3.1 that sets of points S with the property that every line in \mathcal{L} intersects S in an even number of points results in a codeword, and conversely. For the duration of this work, let the code \mathbf{C} be defined by the incidence structure $(\mathcal{P}, \mathcal{L})$, where \mathcal{P} is the set of all points in π and \mathcal{L} is the set of all secant lines to the base hyperoval H . Then any set of points with the property that any *secant line* intersects it in an even number of points will result in a codeword.

In $PG(2, 2^2)$, any hyperoval H' determines a codeword of weight 6. Any such hyperoval has the property that any line of π intersects H' in an even number of points. To see this, consider a line l of π as pictured in Figure 1. Since H' is a hyperoval, *any* line of π is either secant like l_1 , meeting H' in two points, or skew, meeting H' in no points. Then l meets H'

in an even number of points, and such a disjoint hyperoval determines a codeword of weight $|H'| = 6$.

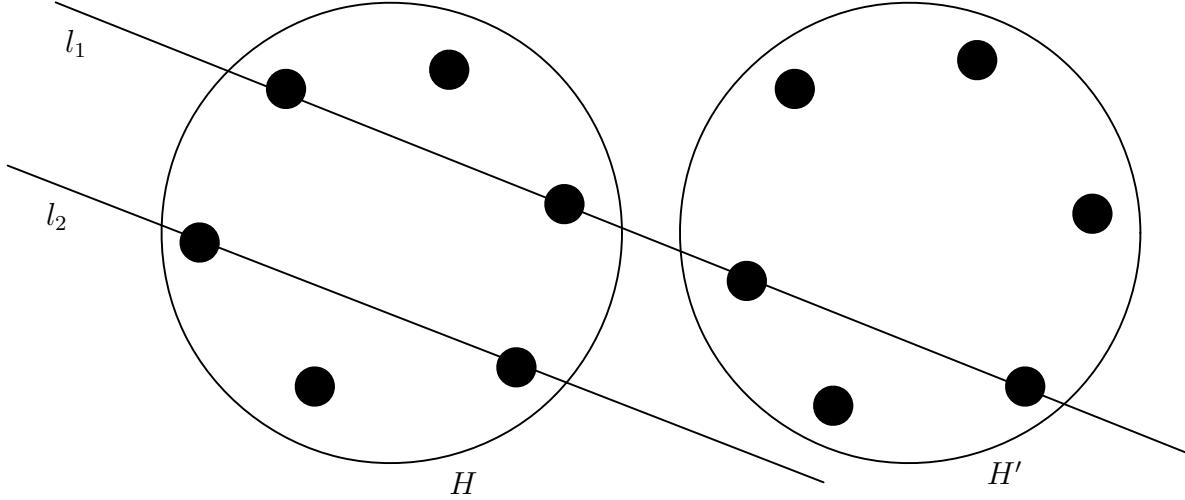


Figure 1: $|H \cap H'| = 0$

A pair of hyperovals H' and H'' such that $|H' \cap H''| = 3$ determines a codeword of weight 6. To see this, consider how a line l meets the set $S = (H' \cup H'') \setminus (H' \cap H'')$. One of several geometric configurations arises. First, l , as l_1 in Figure 2, may be secant to H' and skew to H'' (or vice versa), in which case l meets S in two points. Second, l may be secant to both hyperovals but not contain any point in their intersection, like l_2 in Figure 2. In this case, l meets S in four points. If l meets H' in two points, one of which lies in $H' \cap H''$, like l_3 in the figure below, then l must pass through another point of H'' since no line can be tangent to *any* hyperoval. In this case l intersects S in two points, one on each hyperoval. Next, l may intersect two points of the intersection $H' \cap H''$, like l_4 of Figure 2, in which case l meets S in zero points. Of course, a line could be skew to both H' and H'' , like l_5 in Figure 2 in which case it meets S in zero points. In all of these configurations, l meets S in an even number of points, and hence S determines a codeword of weight $|S| = 6$.

Note that in both of the above two configurations we obtain a set S with exactly six points. It turns out that in the plane $PG(2, 4)$, the set $S = (H' \cup H'') \setminus (H' \cap H'')$, for any pair of hyperovals H' and H'' meeting in three points, is itself a hyperoval. This means that the codewords generated by hyperovals are the same as the codewords generated by a pair of hyperovals meeting in three points. We mention the second example nonetheless since the technique will generalize to larger values of q , and giving different weight codewords in that

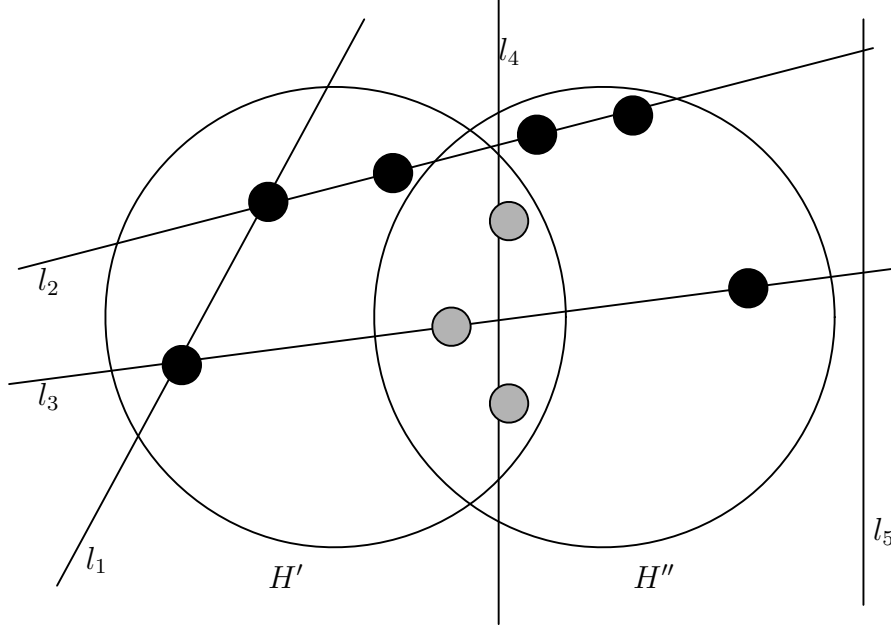


Figure 2: $|H' \cap H''| = 3$

case. We explore this more in the next section.

Hyperovals H' and H'' such that $|H' \cap H''| = 2$ determine codewords of weight 8. The set of points $S = (H' \cup H'') \setminus (H' \cap H'')$ has the property that any line l of π intersects the set in an even number of points. If l is secant to H' and skew to H'' like l_1 in Figure 3, l meets S in 2 points lying entirely on H' . The line l , like l_2 in Figure 3, may intersect H' in 2 points and H'' in 2 points, none of which lie in the intersection $H' \cap H''$, in which case l meets S in four points. The line l may intersect H' in 2 points, one of which lies in $H' \cap H''$, as l_3 does in Figure 3. Since no line can be tangent to the hyperoval H'' , l must pass through another point of H'' , in which case l intersects S in 2 points, one on each hyperoval. Also, l may be secant to H' , intersecting the two points in the intersection $H' \cap H''$ like l_4 in the figure below. In this case, l contains two points of H'' and cannot pass through any additional points of H'' ; otherwise 3 points of H'' would be collinear, violating the definition of a hyperoval. Finally, l may be skew to both hyperovals, like l_5 in Figure 3, meeting S in zero points. In all of these configurations, l contains an even number of points of S , and hence this set of points determines a codeword of weight $|S| = 8$.

Similarly, pairs of hyperovals H' and H'' such that $|H' \cap H''| = 1$ determine codewords of weight 10. The set of points $S = (H' \cup H'') \setminus (H' \cap H'')$ has the property that any line of π intersects the set in an even number of points. To see this, consider a line l of π . Such

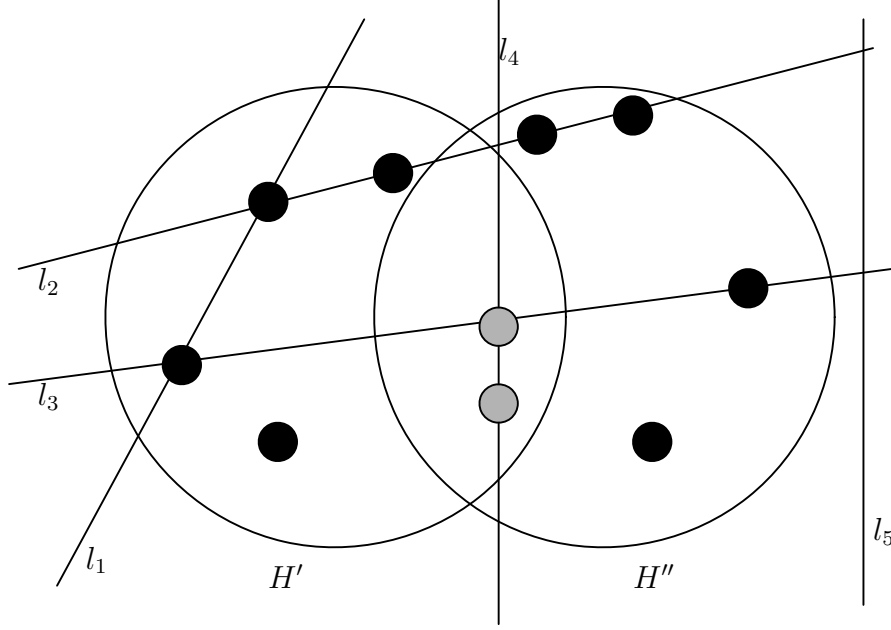


Figure 3: $|H' \cap H''| = 2$

a line l may be secant to H' but skew to H'' (or vice versa), meeting S in two points, such as l_1 in Figure 4. Second, l may be secant to both H' and H'' but not contain their point of intersection, as l_2 in Figure 4, in which case l meets S in four points. Next, l may be secant to H' and contain the point in $H' \cap H''$, like l_3 in the figure below. Then l contains a point of H'' and must pass through another point of this hyperoval. In this case, l intersects S in two points. Of course, l may also be skew to both hyperovals, meeting S in zero points, as l_4 does in Figure 4. In all of these configurations, l intersects S in an even number of points, and thus the set determines a codeword of weight $|S| = 10$.

In much the same way that a single hyperoval determines a codeword, a set of two disjoint hyperovals H' and H'' determine codewords of weight 12. Any line l of π will have to be secant or skew to H' , and similarly to H'' . Then l contains zero points of $S = H' \cup H''$ if l is skew to both hyperovals (see l_1 in Figure 5), two points of S if l is secant to either H' or H'' (see l_2 in Figure 5), or 4 points of S if l is secant to both hyperovals (see l_3 in Figure 5). Since l meets S in an even number of points, such a set S determines a codeword of weight $|S| = 12$.

It is natural to question whether or not all codewords will arise from the configurations outlined above. Using the software package *Magma*, one can easily count the number of codewords of various weights, as well as the number of geometric configurations giving rise to

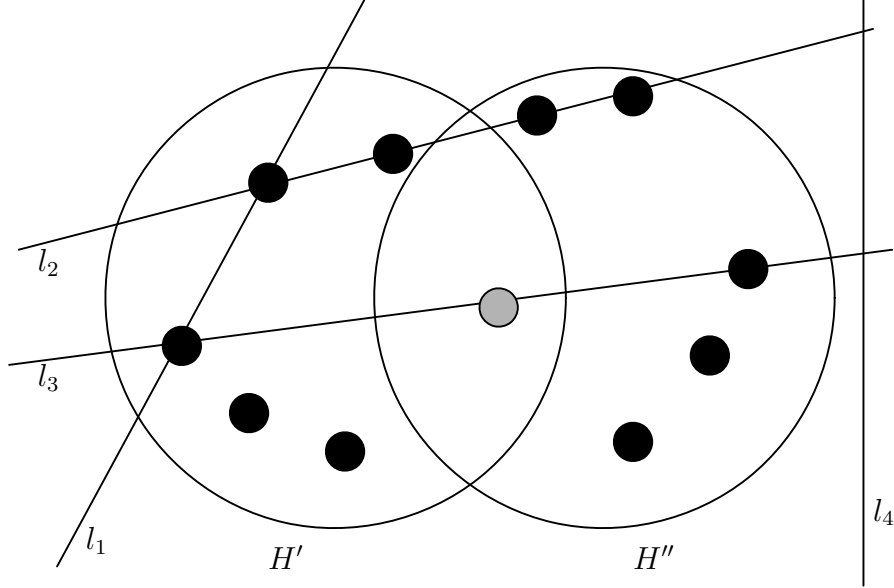


Figure 4: $|H' \cap H''| = 1$

those codewords. Table 3.1 enumerates the different weights and the corresponding number of codewords. We remark that all codewords arising from our construction in $PG(2, 4)$ arise from the geometric configurations described above.

3.2 The general case

The geometric configurations enumerated for the simple case where $q = 4$ can be translated into the more general case where $q = 2^s$.

In this case, a hyperoval H' determines a codeword. Any line l of π meets the hyperoval H' in zero or two number of points, and hence determines a codeword of weight $|H'| = q + 2$.

Just as in the case where $q = 4$, the set of points lying on a pair of hyperovals H' and H'' , but with the intersection points removed, determines a codeword. In addition to those previously enumerated, other geometric intersections arise as q increases.

In general, consider a pair of hyperovals H' and H'' that share exactly k points as in Figure 6. As discussed in Section 3.1, the set $S = (H' \cup H'') \setminus (H' \cap H'')$ has the property that any line of π meets it in an even number of points. This follows by the same argument as in the case when $q = 4$. Hence, S determines a codeword of weight $|S| = 2(q + 2) - 2k = 2q - 2k + 4 = 2(q - k + 2)$.

It is a well-known result that two hyperovals can intersect in as much as half their points (a proof can be found in Chapter 8 of [5]). As a result, larger intersections are possible as q

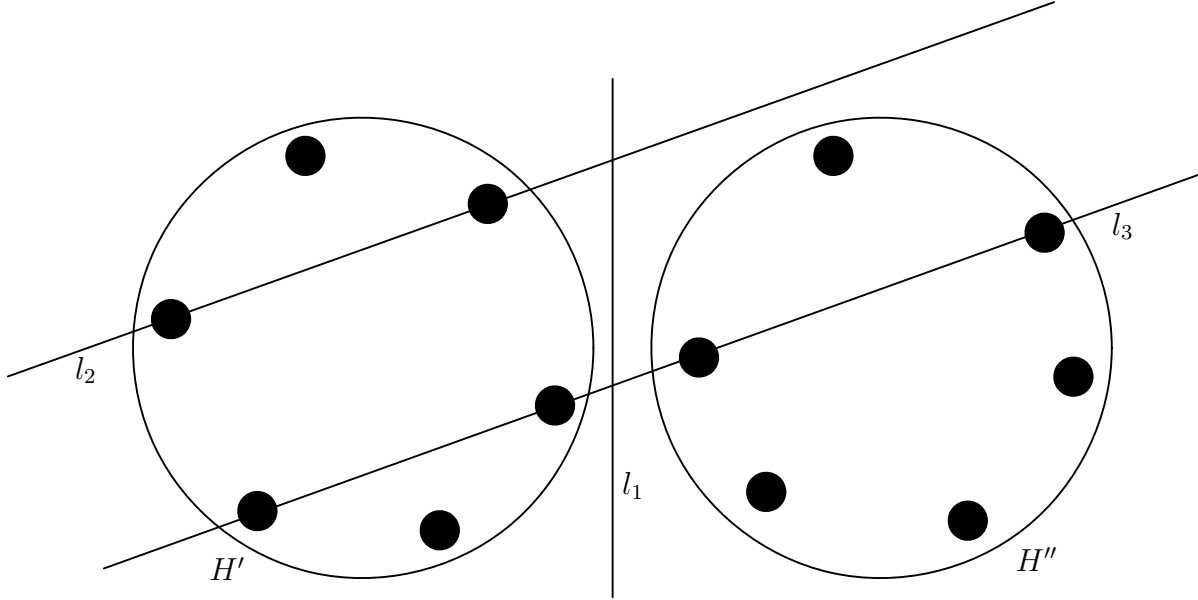


Figure 5: $|H' \cap H''| = 5$

increases, and smaller weight codewords are determined by such configurations. There is a limit, however, to the size of these intersections. Since the hyperovals we are dealing with are *regular* in the sense that they arise from extending a conic, there are algebraic constraints. In particular, it is well-known that five points uniquely determine a conic. Hence, two regular hyperovals can only intersect in at most six points, four common conic points and two additional points that are the nuclei for the two hyperovals. We explore this possible configuration further in Section 4.

While each of the configurations described above will necessarily lead to a codeword, one should question whether or not such configurations actually exist. In the next section we explore the algebraic side, determining conditions under which regular hyperovals can, in fact, intersect in five or six points.

4 Algebraic constructions of small weight codewords

Now that we know what types of geometric configurations result in codewords of various sizes, we would like to establish the algebraic conditions under which such configurations can occur. First we briefly introduce some algebraic concepts including the notion of characteristic and trace.

A property of finite fields which is essential for our work is the notion of characteristic.


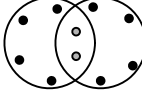
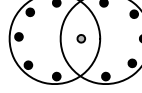
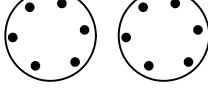

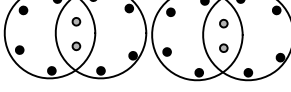
weight	number of codewords	geometric configuration	number of such configurations
6	168		168
8	210		210
10	1008		1008
12	280		280
14	360		360
16	21		21

Table 1: Weights of codewords and number of configurations for $q = 4$

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

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

$$x \mapsto x + x^2 + x^4 + \dots + x^{2^{s-1}}$$

where $x \in GF(2^s)$. For example, the absolute trace map from $GF(8)$ to $GF(2)$ is $tr(x) = x + x^2 + x^4$. Note that letting $y = x + x^2 + x^4 + \dots + x^{2^{s-1}}$ and using the fact that $(a + b)^2 = a^2 + b^2$ in fields of characteristic 2, we have $y^2 = y$ (here, you must observe that $x^{2^s} = x$). Therefore, y is either 0 or 1, and therefore is in $GF(2)$ for every $x \in GF(2^s)$.

Just as in \mathbb{R} , we can consider solutions to quadratic equations. Consider $ax^2 + bx + c = 0$ for $x \in GF(2^s)$. This equation has solutions if and only if $tr\left(\frac{ac}{b^2}\right) = 0$ as shown in [6]. Another result helpful in solving quadratic equations is that for every $x \in GF(2^s)$, $s \geq 1$, $tr(x^2 + x) = 0$. We make frequent use of these trace results in our construction of small weight codewords.

It is well known that the nonzero elements of a finite field form a cyclic group under

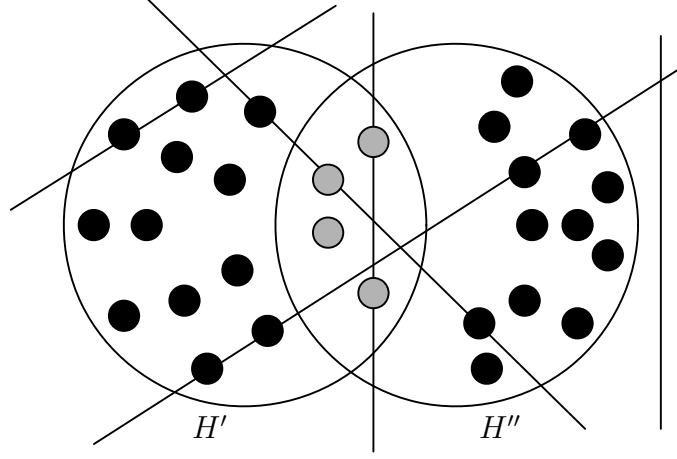


Figure 6: $|H' \cap H''| = k$

multiplication and a generator for this group is called a *primitive element*. We will use the symbol α to denote a primitive element.

Lemma 4.1. *In the finite field $GF(2^s)$, $tr(1) = 0$ if and only if s is even.*

Proof. In the finite field $GF(2^s)$,

$$\begin{aligned} tr(1) = 0 &\Leftrightarrow 1^{2^0} + 1^{2^1} + 1^{2^2} + 1^{2^3} \dots + 1^{2^{s-1}} = 0 \\ &\Leftrightarrow \text{the number of terms is even} \\ &\Leftrightarrow s \text{ is even .} \end{aligned}$$

□

Theorem 4.2. *Let $\pi = PG(2, 2^s)$. Let H be the hyperoval resulting from the extension of the base conic C to include its nucleus $(0, 1, 0)$. Then there exists a regular hyperoval H' such that H shares exactly six points with H' if and only if s is even.*

Proof. First assume that there exists a regular hyperoval H' such that $|H \cap H'| = 6$ and let C and C' be the underlying conics for H and H' , respectively. Then 4 points of $H \cap H'$ are in $C \cap C'$ and the remaining two points are the nucleus of C , which is a conic point for C' , and the nucleus of C' , which is a conic point for C . Without loss of generality, we can assume that the four conic points of C in $C \cap C'$ are $(1, 0, 0)$ $(0, 0, 1)$, $(1, 1, 1)$ and a fourth point $(1, p, p^2)$ for some $p \in GF(q)$. Note that the nuclei of C and C' are also in $H \cap H'$. We briefly explain why we are able to choose these points in this manner.

It is well-known (see [5]) that the group that fixes a conic in $PG(2, q)$ is isomorphic to the group $PGL(3, q)$. Furthermore, this group has a high level of transitivity. More precisely, if you consider *any* three points P_1, P_2 , and P_3 of the conic C , and then any *other* three points of C , say Q_1, Q_2 , and Q_3 , there is an element of $PGL(2, q)$ that fixes C (as a set) and that maps the first three points onto the second three points. Therefore, we can always choose three particular points of C in whatever way best suits our needs.

Let the quadratic form for C' be $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$. The conic C' contains $(1, 0, 0)$, and so all terms containing y or z in the quadratic form drop out when this point is plugged in. In order for the form to be satisfied for the point $(1, 0, 0)$, the coefficient a must be 0. Similarly, since C' contains the points $(0, 1, 0)$ and $(0, 0, 1)$, the coefficients b and c must be 0. Note that in order for C' to be a non-degenerate conic, the coefficients $d, e, f \neq 0$. Since (f, e, d) , the nucleus of C' , is a point of C , it must satisfy $y^2 = xz$, and so $e^2 = fd$. Without loss of generality we can normalize this point and assume that $f = 1$. Then the quadratic form for C' can be simplified as $e^2xy + exy + yz = 0$. Finally $(1, 1, 1)$ is a point of C' , and by plugging this into the quadratic form we obtain $e^2 + e + 1 = 0$. As mentioned earlier, this equation has solutions for e if and only if $tr\left(\frac{ac}{b^2}\right) = tr\left(\frac{1}{1}\right) = tr(1) = 0$. By Lemma 4.1, we know $tr(1) = 0$ if and only if $q = 2^s$ and s is even. Moreover, the equation actually has two solutions. If we call them e_1 and e_2 , this gives us our two additional points $(1, e_1, e_1^2)$ and $(1, e_2, e_2^2)$.

Now assume that s is even. We wish to produce a regular hyperoval H' such that $|H \cap H'| = 6$. Consider a quadratic form $e^2xy + exy + yz = 0$, where $e \in GF(2^s)$, for a conic C' . Clearly the points $(1, 0, 0)$, $(0, 0, 1)$, and $(0, 1, 0)$ all satisfy this quadratic form. When the point $(1, 1, 1)$ is substituted into the form, we obtain $e^2 + e + 1 = 0$. As seen in the forward direction, this equation has solutions for e if and only if $tr\left(\frac{ac}{b^2}\right) = tr\left(\frac{1}{1}\right) = tr(1) = 0$, which occurs if and only if s is even. Hence, there exists an $e \in GF(2^s)$ such that $(1, 1, 1)$ satisfies the quadratic form for C' . Additionally, $(1, e, e^2)$, the nucleus of C' , satisfies the quadratic form for the base conic as $y^2 = (e)^2 = (1)(e^2) = xz$. Hence, $H \cap H'$ contains 6 points. \square

Finding solutions of $e^3 + 1 = 0$ is sufficient for finding solutions of $e^2 + e + 1$ since $e^3 + 1$ factors as $(e + 1)(e^2 + e + 1)$. The nonzero elements of $GF(2^{2k})$ form a cyclic group of order $2^{2k} - 1$. It can be shown that 3 is a factor. Writing $2^{2k} - 1$ modulo 3, we have

$$2^{2k} - 1 \equiv (-1)^{2k} - 1 \equiv 1 - 1 \equiv 0 \pmod{3},$$

and so 3 is indeed a factor.

It follows that the solutions of $e^3 + 1 = 0$ are $e = 1$, $e = \alpha^{\frac{1}{3}(2^s-1)}$, and $e = \alpha^{\frac{2}{3}(2^s-1)}$. We know that $e \neq 1$ since the point $(1, 1, 1)$ is already assumed to be in $H \cap H'$. Hence the only two solutions are $e_1 = \alpha^{\frac{1}{3}(2^s-1)}$ and $e_2 = \alpha^{\frac{2}{3}(2^s-1)}$.

Theorem 4.3. *Let $\pi = PG(2, 2^s)$. Let H be the hyperoval resulting from the extension of the base conic C . Then:*

1. *There exists a hyperoval H' whose nucleus is not in H and $|H \cap H'| = 5$.*
2. *There exists a hyperoval H' whose nucleus is in H and $|H \cap H'| = 5$.*
3. *There does not exist a hyperoval H' such that the nuclei of both H and H' are in $H \cap H'$ and $|H \cap H'| = 5$.*

Proof. Note that if $|H \cap H'| = 5$, at least one shared point is a nucleus, for either C or C' . Let C' be the conic defined by $ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$.

To prove (1), suppose that the nucleus, $(0, 1, 0)$, of the base conic C is a point of $H \cap H'$, but the nucleus for C' is not. Also suppose that $(0, 0, 1)$, $(1, 0, 0)$, and $(1, 1, 1)$ are in H' . Then, since $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1) \in H \cap H'$, the coefficients $a, b, c = 0$, and the quadratic form can be simplified to $dxy + exz + fyz = 0$. Plugging the shared conic point $(1, 1, 1)$ into the quadratic form for C' , we find that $d + e + f = 0$. Note that $d, e, f \neq 0$, otherwise C' is a degenerate conic. Without loss of generality we can assume that $d = 1$, and so $e = f + 1$. Further, assume that H and H' share a point of the form $(1, p, p^2)$ where $p \in GF(q)$ with $p \neq 0, 1$. (Note that any point in $H \cap H'$ different from $(0,0,1)$, $(1, 0, 0)$, and $(1, 1, 1)$ must be of this form since it lies on the base conic C with quadratic form $y^2 = xz$.) Plugging this point into the quadratic form of C' we find:

$$\begin{aligned} p + ep^2 + fp^3 &= 0 \\ 1 + ep + fp^2 &= 0. \end{aligned}$$

But this is a quadratic in p , and has solutions if $\text{tr}\left(\frac{f}{e^2}\right) = 0$. This simplifies to $\text{tr}\left(\frac{e+1}{e^2}\right) = \text{tr}\left(\frac{1}{e} + \frac{1}{e^2}\right) = 0$, which is always true when q is even, as noted earlier. Substituting $f + 1$ for e into (1) we find that $1 + (f + 1)p + fp^2 = 0$. This factors as $(1 + fp)(1 + p) = 0$, with solutions $p = 1$ and $p = \frac{1}{f}$. Since $p \neq 1$, we conclude that $p = \frac{1}{f}$. Then the quadratic form for C' is $xy + (1 + \frac{1}{p})xz + \frac{1}{p}yz = 0$. In order to ensure that the nucleus for C' , $(\frac{1}{p}, 1 + \frac{1}{p}, 1)$

is not a point of C , this point cannot satisfy the quadratic form of C , $y^2 = xz$. Then

$$\begin{aligned} \left(1 + \frac{1}{p}\right)^2 &\neq \frac{1}{p} \\ 1 + \frac{1}{p^2} &\neq \frac{1}{p} \\ p^2 + 1 &\neq p \\ p^2 + p + 1 &\neq 0, \end{aligned}$$

and so p cannot be a solution of $x^2 + x + 1 = 0$. Recall that if p were a solution to this quadratic, we would be forced into the situation described in Theorem 4.2. In summary, if we choose H' to be the hyperoval whose underlying quadratic form is $xy + (1 + \frac{1}{p})xz + \frac{1}{p}yz = 0$ for some p that does not satisfy $p^2 + p + 1 = 0$, then we have the situation described in part (1) of the theorem and $|H \cap H'| = 5$.

To prove (2), suppose the nucleus of C' is in $H \cap H'$, but the nucleus for the base conic C is not. Also suppose that $(0, 0, 1)$, $(1, 0, 0)$, and $(1, 1, 1)$ are in $H \cap H'$. The nucleus for C' is of the form $(1, r, r^2)$ since it lies on C . Then the quadratic form for C' simplifies to $by^2 + r^2xy + rxz + yz = 0$. Since $(1, 1, 1) \in C'$ we have that $b + r^2 + r + 1 = 0$, or $b = r^2 + r + 1$. Note that since $(0, 1, 0) \notin H \cap H'$, $b \neq 0$, and so we restrict the choice of the element r so that it is not a solution of $x^2 + x + 1 = 0$.

Now the quadratic form for C' can be written as $(r^2 + r + 1)y^2 + r^2xy + rxz + yz = 0$. The final point in $H \cap H'$ is of the form $(1, p, p^2)$ where $p \in GF(q)$ with $p \neq 0, 1$, and plugging this point into the quadratic form for C' , we obtain

$$\begin{aligned} (r^2 + r + 1)p^2 + r^2p + rp^2 + p^3 &= 0 \\ (r^2 + r + 1)p + r^2 + rp + p^2 &= 0 \\ p^2 + (r + 1)^2p + r^2 &= 0 \\ (p + 1)(p + r^2) &= 0. \end{aligned}$$

We see that the solutions of this equation are $p = 1$ and $p = r^2$. We know that $p \neq 1$, and so we conclude that $p = r^2$. Then the fifth point in $H \cap H'$ is $(1, r^2, r^4)$. In summary, if we choose H' to be the hyperoval whose underlying quadratic form is $(r^2 + r + 1)y^2 + r^2xy + rxz + yz = 0$, for some r which does not satisfy $x^2 + x + 1 = 0$, then we have the situation of case (2) of the theorem and $|H \cap H'| = 5$.

To prove (3), consider an intersection of size five containing both nuclei. Suppose that $(1, 0, 0)$, $(0, 0, 1)$, and $(1, 1, 1)$ are in $C \cap C'$, as well as $(0, 1, 0)$, the nucleus for C , and (f, e, d) , the nucleus for C' . Without loss of generality we assume that $d = 1$. Since the nucleus for

C' is a conic point for C , (f, e, d) must satisfy $y^2 = xz$, and so $e^2 = f$. Then the nucleus for C' is $(e^2, e, 1)$. Since $(1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$ are in $H \cap H'$, the squared terms of the quadratic form for C' all drop out, leaving us with $xy + exz + e^2yz = 0$. Plugging the shared conic point $(1, 1, 1)$ into the quadratic form, we see that $1 + e + e^2 = 0$. We have already seen that if s is odd, there are no solutions to $x^2 + x + 1 = 0$. Hence, there is no H' in $PG(2, 2^s)$ such that $|H \cap H'| = 5$ and $|C \cap C'| = 3$ when s is odd.

On the other hand, if s is even, there are solutions to $x^2 + x + 1 = 0$. Since $x^3 + 1 = 0$ factors as $(x + 1)(x^2 + x + 1)$, finding the non-identity solutions of $x^3 + 1 = 0$ is equivalent to finding solutions of $x^2 + x + 1 = 0$. Let e be a solution to $x^2 + x + 1 = 0$. Then $f = e^2$ is also a solution to $x^2 + x + 1 = 0$ since $f^3 = e^6 = 1$ (so f is a solution of $x^3 + 1 = 0$) and $f \neq 1$. Note that $f \neq e$. Now plugging $(f^2, f, 1)$ into the quadratic form for C' we have that

$$\begin{aligned} xy + exz + e^2yz &= f^2f + ef^2 + e^2f \\ &= e^6 + e^5 + e^4 \\ &= e^4(e^2 + e + 1) \\ &= e^4(0) \\ &= 0, \end{aligned}$$

and so the point $(f^2, f, 1)$ lies on C' . Notice that $(f^2, f, 1)$ clearly satisfies $y^2 = xz$, and so this point is also a conic point of C . But then H and H' share six points. Hence, there is no H' in $PG(2, 2^s)$ such that $|H \cap H'| = 5$ and $|C \cap C'| = 3$ when s is even. \square

4.1 Codewords of weight $2q - 8$

Now that we have discussed the algebraic conditions necessary for two regular hyperovals to meet in five or six points, we wish to count the number of such configurations, and consequently the number of codewords resulting from such configurations. To do this, we first consider the number of hyperovals which intersect a given fixed hyperoval in a specified number of points, and then use this result to generalize to *any* hyperoval.

We first seek to count pairs of hyperovals H' and H'' that meet in exactly six points, resulting in codewords of weight $2q - 8$. We first determine the number of hyperovals which intersect the fixed hyperoval H .

Lemma 4.4. *Let H be the base hyperoval in $PG(2, 2^s)$ with s even and $s > 2$. Then the number of regular hyperovals H' of $PG(2, q)$ such that $|H \cap H'| = 6$ is $\frac{(q^2 - 1)q}{12}$.*

Proof. Recall from Theorem 4.2 that when $|H \cap H'| = 6$, four of the six points in the intersection are shared conic points and the remaining two points are the nuclei of the hyperovals. First, we choose three conic points of C (note that there is no loss of generality because of the transitivity of the automorphism group for a conic, as discussed in Theorem 4.2), and there are $\binom{q+1}{3}$ ways to do so. Also recall from Theorem 4.2 that once these three points are chosen, the remaining two points of $C \cap H'$ are uniquely determined. Note however that there are two distinct hyperovals which contain these two points (one which has the fourth point as a conic point and the fifth point as its nucleus, the other which has the fourth point as its nucleus and the fifth point as a conic point). Hence, by choosing three distinct points of C in all possible ways to be in the intersection, we have accumulated all of our desired hyperovals.

Note however, that we have overcounted. Of the four non-nucleus points in $H \cap H'$, given a fixed nucleus for C' and $(0,1,0)$ (which is the nucleus of C and a conic point of C'), any three of the four remaining points would determine C' . Since there are four points remaining from which we can choose any three, we have overcounted by a factor of $\binom{4}{3} = 4$. Then the total number of hyperovals H' such that $|H \cap H'| = 6$ is

$$\frac{\binom{q+1}{3} \cdot 2}{4} = \frac{(q+1)(q)(q-1)(2)}{3 \cdot 2 \cdot 1 \cdot 4} = \frac{(q^2-1)q}{12}. \quad \square$$

Theorem 4.5. *Let $q = 2^s$ with s even and $s > 2$. Then the number of pairs of regular hyperovals H' and H'' in $PG(2, q)$ such that $|H' \cap H''| = 6$ is $\frac{q^3(q^2-1)(q^3-1)}{24}$.*

Proof. We must first choose one regular hyperoval of $PG(2, q)$. 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.

We now appeal to a group theoretic result. The full automorphism group of the projective plane $PG(2, q)$ is denoted by $P\Gamma L(3, q)$ and consists of all semi-linear transformations. Under this group, it is well-known (see Section 7.2 of [5]) that all conics lie in a single orbit. In other words, given any two conics C_1 and C_2 , one can always find an automorphism of the plane that maps the points of C_1 onto the points of C_2 (in fact, one can choose the automorphism to be linear, i.e., an element of $PGL(3, q)$). In the language of geometry, we say that conics in the plane $PG(2, q)$ are all *projectively equivalent*.

It then follows by Lemma 4.4 that once we have chosen our first regular hyperoval H' , there are $\frac{(q^2-1)q}{12}$ choices for the second regular hyperoval H'' . Hence, there are $(q^5 - q^2) \left(\frac{(q^2-1)q}{12} \right)$ ways to choose an ordered pair of regular hyperovals H', H'' such that $|H' \cap H''| = 6$. Note, however, that we have overcounted by a factor of two since the a pair of regular hyperovals can be chosen in either order (H' first and H'' second, or H'' first and H' second). Hence, the number of pairs of regular hyperovals H' and H'' that meet in six points is

$$\frac{(q^5 - q^2) \left(\frac{(q^2 - 1)q}{12} \right)}{2} = \frac{q^3(q^2 - 1)(q^3 - 1)}{2} = \frac{q^3(q^2 - 1)(q^3 - 1)}{24}$$

□

4.2 Codewords of weight $2q - 6$

Recall from Theorem 4.3 that it is possible for regular hyperovals to intersect in five points for every order $q = 2^s$, with $s \geq 3$. We shall soon see that the number of such geometric configurations is actually dependent on whether s is even or odd.

Lemma 4.6. *Let H be the base hyperoval in $PG(2, q)$ with $q = 2^s$ and $s \geq 3$. When s is even, the number of regular hyperovals H' of $PG(2, q)$ such that $|H \cap H'| = 5$ is $\frac{q(q^2-1)(q-4)}{24}$. When s is odd, the number of regular hyperovals H' such that $|H \cap H'| = 5$ is $\frac{q(q^2-1)(q-2)}{24}$.*

Proof. Recall from Theorem 4.3 that if $|H \cap H'| = 5$, then either the nucleus of C or the nucleus of C' is in $H \cap H'$, but not both. We break the proof into two cases: first when the nucleus of C is a conic point of C' and second when the nucleus of C' is a conic point of C .

Case One: The nucleus of C is in $H \cap H'$. First, we choose three conic points of C , $(0, 0, 1)$, $(1, 0, 0)$, and $(1, 1, 1)$. Generally, there are $\binom{q+1}{3}$ ways to choose these initial three points. As shown in Theorem 4.3, once these three points are chosen, the fourth conic point is of the form $(1, p, p^2)$, where $p \neq 0, 1$ and p is not a solution to the quadratic $x^2 + x + 1 = 0$. Recall that when s is odd there are no solutions to this quadratic, but when s is even there are two solutions. Hence there are $q - 4$ choices for p when s is even, and $q - 2$ choices for p when s is odd.

Note however, that in both cases, given a fixed nucleus of C' and the nucleus of C , any three of the four remaining non-nucleus points in $H \cap H'$ would determine C' . Since there are four points remaining from which we can choose any three, we have overcounted by a factor of $\binom{4}{3} = 4$.

Then the total number of regular hyperovals H' such that $|H \cap H'| = 5$ is

$$\frac{\binom{q+1}{3}(q-4)}{\binom{4}{3}} = \frac{(q+1)(q)(q-1)(q-4)}{24} \text{ when } s \text{ is even, and}$$

$$\frac{\binom{q+1}{3}(q-2)}{\binom{4}{3}} = \frac{(q+1)(q)(q-1)(q-2)}{24} \text{ when } s \text{ is odd.}$$

Case Two: The nucleus of C' is in $H \cap H'$. Similar to the first case, we choose three conic points of C . In general there are $\binom{q+1}{3}$ ways to choose three points of C . In particular, we select $(0,0,1)$, $(1,0,0)$, and $(1,1,1)$. Recall from Theorem 4.3 that the nucleus of C' is of the form $(1, r, r^2)$, where $r \neq 0, 1$ and r is not a solution of $x^2 + x + 1 = 0$. There are solutions to this quadratic only if s is even. As shown in Theorem 4.3, the fifth point in $H \cap H'$ is $(1, r^2, r^4)$. Hence there are $q - 4$ choices for r when s is even, and $q - 2$ choices when s is odd.

In either case, given the nuclei of both H and H' , any three of the four remaining non-nucleus points in $H \cap H'$ would determine C' , and so we have overcounted by a factor of $\binom{4}{3} = 4$. We are now led to the same conclusions as in Case 1 above. \square

Theorem 4.7. *Let $q = 2^s$ with $s \geq 3$. Then the number of pairs of regular hyperovals H' and H'' in $PG(2, q)$ such that $|H' \cap H''| = 5$ is*

$$\frac{q^3(q^3 - 1)(q^2 - 1)(q - 4)}{48} \text{ when } s \text{ is even,}$$

and

$$\frac{q^3(q^3 - 1)(q^2 - 1)(q - 2)}{48} \text{ when } s \text{ is odd.}$$

Proof. We must first choose one regular hyperoval of the $q^5 - q^2$ in $PG(2, q)$ and, as before, this can be done in $q^5 - q^2$ ways. Once we choose our first regular hyperoval H' , by Lemma 4.6 there are $\frac{\binom{q+1}{3}(q-4)}{\binom{4}{3}} = \frac{(q+1)(q)(q-1)(q-4)}{24}$ choices for the second regular hyperoval H'' when s is even, and $\frac{\binom{q+1}{3}(q-2)}{\binom{4}{3}} = \frac{(q+1)(q)(q-1)(q-2)}{24}$ choices for H'' when s is odd.

As before, we have overcounted by a factor of two since a pair of regular hyperovals can be chosen in either order (H' first and H'' second, or H'' first and H' second). Hence, the number of pairs of regular hyperovals H' and H'' that meet in five points is

$$(q^5 - q^2) \frac{(q+1)(q)(q-1)(q-4)}{48} = \frac{q^3(q^3 - 1)(q^2 - 1)(q - 4)}{48} \text{ when } s \text{ is even, and}$$

$$(q^5 - q^2) \frac{(q+1)(q)(q-1)(q-2)}{48} = \frac{q^3(q^3 - 1)(q^2 - 1)(q - 2)}{48} \text{ when } s \text{ is odd.}$$

\square

5 Conclusion

We have drawn on the work of [3] to investigate the weight enumerator of a class of codes arising from secant lines in $PG(2, 2^s)$. Relying on the intersection of regular hyperovals, our construction of codewords necessitated our investigation of the algebraic conditions under which pairs of regular hyperovals intersect in a given number of points. These conditions in turn affect the number of codewords arising from these intersections. We have shown that the number of small weight codewords actually depends on the parity of s . Further investigation may be done to determine if, as q increases, there are geometric configurations that represent codewords that cannot be described using hyperovals (regular or non-regular). One might also explore whether any of the results set forth here translate to the case where q is odd.

References

- [1] A. Beutelspacher and U. Rosenbaum, *Projective Geometry: From Foundations to Applications*. Cambridge University Press (1998).
- [2] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language. *J. Symbolic Comput.*, **24**: 3-4 (1997) 235–265.
- [3] C. Castleberry and K. Hunsberger, Coding and Cryptography with Hyperovals of $PG(2, 2^s)$, *Department of Mathematics Summer Technical Report*, University of Mary Washington (2008).
- [4] R. G. Gallager, Low density parity-check codes, *IRE Trans. Infom. Theory*, **IT-8** (1962) 21–28.
- [5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford University Press, Second Edition (1998).
- [6] R. Lidl and H. Niederreiter. *Finite Fields*. Addison-Wesley (1983).
- [7] D. J. C. MacKay and R. M. Neal, Near Shannon limit performance of low density parity-check codes, *Electron. Lett.* **32**: 18 (1996) 1645–1646.
- [8] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, third edition, Wiley-Interscience Series in Discrete Mathematics (1998).
- [9] B. Segre, Ovals in a finite projective plane. *Canad. J. Math.* **7** (1955) 414–416.
- [10] C. E. Shannon, A mathematical theory of communication, *Bell System Tech. J.* **27**, (1948) 379–423, 623–656.
- [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.