Finite Projective Geometries and Linear Codes

Tom Edgar

Advisor: Dr. Anton Betten

Department of Mathematics

In partial fulfillment of the requirements

for the degree of Master Science

Fort Collins, Colorado

Spring 2004

Abstract

In this paper, we study the connections between linear codes and projective geometries over finite fields. Often good codes come from interesting structures in projective geometries. For example, MDS codes come from arcs (i.e. sets of points which are extremal in the sense that they admit no other than the obvious dependencies). In addition, we take a closer look at ovals and hyperovals in projective planes and ovoids in projective 3-spaces. In particular, we examine Glynn's condition for the existence of hyperovals.

Contents

1 Introduction

When coding theory was first introduced, the connections to projective geometry were not known and hence not studied. Only recently have there been important advances in the connections between projective geometry and coding theory. In this paper, we introduce some of the basic ideas and connections between finite projective spaces and coding theory. We begin by studying projective geometries in general and extend this to studying certain incidence structures called arcs inside of projective geometries. From this, we introduce some very interesting structures in projective planes which lead to many other interesting areas of finite geometry. Our focus then shifts to coding theory and in particular MDS codes. The main desire in coding theory is to get a great deal of information across a noisy communication channel with only short codewords and a large distance between them. MDS codes turn out to be one possible type of optimal codes and hence are of interest. We attempt to describe some of the results in this area. In addition, we examine the connection between MDS codes and arcs in projective geometries. We intend to introduce at least some of the main open problems and conjectures in this area. We assume a basic graduate level of math is known, and hope to include most of the relevant information in this area. The paper is a compilation of existing results, and we attempt to bring these together. We intend for the paper to read like a textbook so that it may be used as a resource for someone interested in researching and studying projective geometry and coding theory.

2 Projective Geometry

2.1 A Brief Introduction and Basic Definitions

To begin we must first introduce some basic terminology with respect to finite geometry. We consider only finite fields, $\mathbb{F}_q$, where $q = p^d$, p prime. We assume some knowledge of the structure of finite fields and vector spaces is known. Let $\mathbb{F}_q^\times$ be the set of non-zero elements of $\mathbb{F}_q$.

Definition 2.1.1 *A* **finite geometry** *is a pair $G = (\Omega, I)$ where Ω is a finite set and I is a relation on Ω that is symmetric and reflexive. I is called an* **incidence relation** *on Ω.*

Definition 2.1.2 *A* **projective space of dimension n** *over a field* $\mathbb{F}_q$ *is the set of non-zero subspaces of* $\mathbb{F}_q^{n+1}$ *with respect to inclusion. We denote this* $PG_n(\mathbb{F}_q)$*, also called* $PG_n(q)$*.*

Remark 2.1.1 $PG_n(q)$ *is a finite geometry with* Ω *being the set of non-zero subpaces of* $\mathbb{F}_q^{n+1}$ *and* I *is symmetric inclusion. We call the one dimensional subspaces of* $\mathbb{F}_q^{n+1}$ *the* **points***, the two dimensional subspaces of* $\mathbb{F}_q^{n+1}$ *the* **lines***, and the n-dimensional subspaces of* $\mathbb{F}_q^{n+1}$ *the* **hyperplanes** *of the geometry. There are always* $1 + q + ... + q^n$ *points and each line contains* $q + 1$ *points.*

Example 2.1.1 $PG_2(2)$ *is the non-zero subspaces of* $\mathbb{F}_2^3$*. This is the projective plane of order* 2*. There are* $1 + 2 + 2^2 = 7$ *points, each a vector in the vector space. There are* 3 *points on every line. This structure is known as the Fano Plane and is described pictorially in a nice way in Figure 1:*

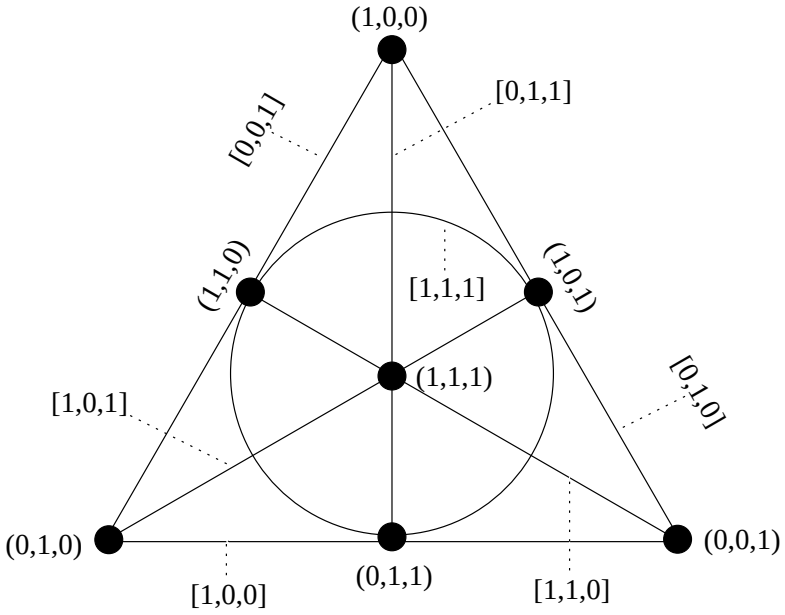

Figure 1: The Fano Plane $PG_2(2)$. This is the 3 dimensional vector space over $\mathbb{F}_2$. We label the points with parentheses and the lines with square brackets. We point out that even though lines look like they cross, they do not actually intersect unless they meet at a point.

Definition 2.1.3 *The points $a_1, a_2, ..., a_m$ in $PG_n(q)$ are* **collinear** *if there exists a line that contains every point a_i.*

We say a point $p = (x_0, ..., x_n)$ is **on** a line $L = [y_0, ..., y_n]$ if and only if $x_0y_0 + x_1y_1 + ... + x_ny_n = 0$.

There is a more general definition of a projective geometry. It turns out that all projective spaces with $n \geq 3$ are of the form $PG_n(q)$ for q a prime power. However, in the special case of $n = 2$, i.e. the **projective planes**, there are certain examples that do not arise from the structure of $\mathbb{F}_q^{n+1}$. In this case, we do include the general definition of a projective plane.

Definition 2.1.4 *A* **projective plane of order** *n is a set (P, B, I), where P is the set of points, B the set of lines, and I the incidence relation between them. The number of points is n^2+n+1 and the number of lines is n^2+n+1. Any line has $n + 1$ points on it and there are $n + 1$ lines on any point. In addition, we require that any two points determine a unique line and that any two lines intersect in a unique point.*

Projective planes in general form an interesting area of study. One of the main conjectures in the area is that projective planes of order n exist if and only if n is a prime power. It has been shown that projective planes of order 6 and order 10 do not exist. The case $n = 12$ is still open. Though there are many fascinating aspects to these general projective planes, from now on, we will only be considering projective spaces of the form $PG_n(q)$ as defined above. Like many disciplines in mathematics, we can learn a great deal about a structures in projective space by studying the automorphisms of a projective geometry.

Definition 2.1.5 *A* **collineation** *of a projective geometry is a permutation of the points such that the lines are mapped onto lines, and thus subpaces are mapped to subspaces.*

Definition 2.1.6 *We consider the set of all invertible semilinear transformations of $PG_n(q)$. This set forms a group under composition called $\Gamma L(n+1, q)$. Now, if H is the pointwise stabiliser of $PG_n(q)$, then H is a subgroup of $\Gamma L(n+1, q)$ and we get that $P\Gamma L(n+1, q) = \Gamma L(n+1, q)/H$ is called the* **projective semilinear group**.

The set of collineations of a projective geometry forms a group called the **automorphism group**, denoted by $\mathrm{Aut}PG_n(q)$.

Theorem 2.1.1 (cf. [1]) *Let $n \geq 2$. Then $AutPG_n(q) = P\Gamma L(n+1, q)$.*

This theorem is known as the **Fundamental Theorem of Projective Geometry**. Baer has a nice proof of this in [1]. A good source of information on the collineations of a projective geometry is [15]. The idea of automorphisms of the projective geometry will allow us to decide if structures are unique up to isomorphism.

Definition 2.1.7 *Two sets of points in $PG_n(q)$ are called* **projectively equivalent** *if there exists an element $\alpha \in P\Gamma L(n+1, q)$ such that α maps one set to the other.*

2.1.1 Quadratic Forms: Classification

Before we can introduce and discuss quadratic forms, we first introduce bilinear forms.

Definition 2.1.8 *A* **bilinear form** *B on $\mathbb{F}_q^n$ is a map from $\mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ defined by $(x, y) \to B(x, y)$ such that:*

1. $B(x + x', y) = B(x, y) + B(x', y)$
2. $B(x, y + y') = B(x, y) + B(x, y')$
3. $B(ax, y) = aB(x, y) = B(x, ay)$

For our purposes, we will only consider **symmetric** bilinear forms. These are the forms which have the special property that $B(x, y) = B(y, x)$ for all x, y. We restrict ourselves to this case since when looking at the second definition of a quadratic form, we find that the bilinear form involved will be a symmetric one. So, from this point on, we only consider that B is symmetric.

Definition 2.1.9 *A* **quadratic form** *is a polynomial function arising from a homogeneous polynomial of degree 2 in n-variables. A homogeneous polynomial of degree 2 has the form*

$$\sum_{1 \leq i \leq j \leq n} c_{i,j} x_i x_j \quad c_{i,j} \in \mathbb{F}$$

It follows from this that if $e_1, ..., e_n$ is a basis for $\mathbb{F}_q^n$, then a quadratic form is a map from ${\mathbb{F}_q}^n \to \mathbb{F}_q$ defined by

$$x = \sum_{i=1}^{n} a_i e_i \to \sum_{i \leq j} c_{i,j} a_i a_j \quad c_{i,j} \in \mathbb{F}$$

In addition to this, there is an alternate definition of a quadratic form using bilinear forms (one can show that these two definitions are equivalent):

Definition 2.1.10 *A* **quadratic form** Q *is a map from* $\mathbb{F}_q^n \to \mathbb{F}_q$ *defined by* $x \to Q(x)$ *such that:*

1. $Q(ax) = a^2 Q(x)$ *for all* $a \in \mathbb{F}_q$ *and for all* $x \in \mathbb{F}_q^n$.
2. $B(x, y) = Q(x + y) - Q(x) - Q(y)$ *is bilinear. We call* B *the* **polarization** *of* Q.

Definition 2.1.11 *The* **radical** *of a bilinear form* B *over a vector space* $\mathbb{F}_q^n$ *is denoted* $rad(B)$ *and given by*

$$rad(B) = \{v \in \mathbb{F}_q^n | B(u, v) = 0 \ \forall u \in \mathbb{F}_q^n\}$$

We are now ready to describe a special condition that can exist for quadratic forms called non-degeneracy. This will eventually lead to nice sets in projective geometries.

Definition 2.1.12 *A quadratic form* Q *on* $\mathbb{F}_q^n$ *with polarization* B *is* **non-degenerate** *if* $v \in rad(B)$ *and* $Q(v) = 0$ *implies that* $v = 0$.

With this basic knowledge of quadratic forms, we now classify the three different types of quadratic forms.

Theorem 2.1.2 (cf. [12]) *Any quadratic form over* $\mathbb{F}_q$ *is of the one of the following forms:*

1. **Parabolic:** $Q_0(x) = x_1 x_2 + x_3 x_4 + ... + x_{n-2} x_{n-1} + c x_n^2$ *where* $c \in \{1, a\}$ *where* $a \in \mathbb{F}_q^{\times 2}$ *if* q *is odd and* $c = 1$ *if* q *is even.*
2. **Hyperbolic:** $Q_1(x) = x_1 x_2 + ... + x_{n-1} x_n$.

3. **Elliptic:** $Q_2(x) = x_1x_2 + ... + x_{n-3}x_{n-2} + p(x_{n-1}, x_n)$, *where* $p(x_{n-1}, x_n)$ *is an irreducible quadratic form in* 2 *variables.*

In general, since quadratic forms are homogeneous polynomials, it makes sense to evaluate them on projective points ($Q(\lambda x) = \lambda^2 Q(x)$ for all $x \in \mathbb{F}_q^{n+1}$). Hence, the zero set of a quadratic form in $PG_n(q)$ is a well-defined set of projective points (i.e. the one-dimensional subspaces of $\mathbb{F}_q^{n+1}$). In $PG_n(q)$, a set of points that make up the zero set of some quadratic form is called a **quadric**. With these basic definitions and ideas in place, we have the tools to help us in studying some interesting structures in projective geometries that will eventually have nice connections to coding theory.

2.2 Arcs, Caps, and Normal Rational Curves

We introduce of points in finite projective spaces with certain properties.

Definition 2.2.1 *A* k**-cap** *in* $PG_n(q)$ *is a set of* k *points such that no* 3 *are collinear.*

Definition 2.2.2 *A* k**-arc** *in* $PG_n(q)$ *is a set* K *of* k *points with* $k \geq n+1$ *such that no* $n+1$ *points lie in a hyperplane.*

Definition 2.2.3 *An arc* K *is* **complete** *if it is not properly contained in a larger arc.*

Definition 2.2.4 *A* **normal rational curve** *of* $PG_n(q)$ *is any set of points in* $PG_n(q)$ *which is projectively equivalent to*

$$\{(1, t, t^2, ..., t^{n-1}, t^n) | t \in \mathbb{F}_q\} \cup \{(0, 0, ..., 0, 1)\}$$

Remark 2.2.1 *A normal rational curve contains* $q+1$ *points. We call the point* $(0, 0, ..., 0, 1)$ *the point at infinity,* P_∞*. For* $q \geq n$*, a normal rational curve forms a* $(q+1)$*-arc.*

Before we look at general k-arcs and k-caps, we look at the special case of $PG_2(q)$. In this space k-arcs and k-caps are the same since hyperplanes in $PG_2(q)$ are just the lines.

2.3 Ovals and Hyperovals in $PG_2(q)$

In this section, we will only be considering $PG_2(q)$, i.e. projective planes. We introduce two special types of k-arcs that are widely studied for their many connections to other geometric structures.

Definition 2.3.1 *A $(q+1)$-arc in $PG_2(q)$ is called an* **oval**.

Definition 2.3.2 *A $(q+2)$-arc in $PG_2(q)$ is called a* **hyperoval**.

Definition 2.3.3 *A line that intersects an oval, or hyperoval, in $\{0,1,2\}$ points is called a* **{external, tangent, secant} line** *respectively.*

Proposition 2.3.1 *For every q, ovals exist in $PG_2(q)$.*

Proof:
We let (x_0, x_1, x_2) with $x_i \in \mathbb{F}_q \ \forall \ i$ be the general form of a point in $PG_2(q)$. Now, we consider the non-degenerate irreducible parabolic quadratic form ${x_1}^2 + x_0x_2$. Then the set of zeros of this quadratic form is

$$\{(1, t, t^2) | t \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$$

Clearly this is a set of $q+1$ points and no 3 are collinear because the form is non-degenerate. Thus this set forms an oval in $PG_2(q)$.

Proposition 2.3.2 *For q even, hyperovals exist in $PG_2(q)$.*

Proof:
We consider the set above which is attained as the zero set of the quadratic form ${x_1}^2 + x_0x_2$. As we have seen this gives us an oval:

$$\theta' = \{(1, t, t^2) | t \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$$

Now for a point $x \in \theta'$, there are q lines through x that hit θ' in at most one more point. However, we know there are $q+1$ lines total through x. First, we note that the point $(0,1,0) \notin \theta'$. Next, we know every point of θ' is collinear with $(0,1,0)$. We claim that the line that connects any point $x \in \theta'$ to $(0,1,0)$ is the unique line through x that hits the oval at no other point. Assume not, then there are two points collinear in θ' such that the line through them contains $(0,1,0)$. A general line through $(0,0,1)$ and another

point of θ' is $[t, 1, 0]$. Now, $(0, 1, 0)$ is not on this line as this would imply that 1=0. Lastly, a general line through two points of $\theta'/\{(0, 0, 1)\}$, $(1, t, t^2)$ and $(1, s, s^2)$ with $s \neq t$, is $[st, s+t, 1]$. If this line contains $(0, 1, 0)$, then this implies $s + t = 0$ which contradicts that $s \neq t$. Thus, we can add the point $(0, 1, 0)$ to our oval θ' to get a hyperoval:

$$\theta = \{(1, t, t^2) | t \in \mathbb{F}_q\} \cup \{(0, 0, 1), (0, 1, 0)\}$$

Note that this does in fact require us to be in characteristic 2 (i.e. we need q to be even).

The construction above is a usual construction of hyperovals which takes an oval and adds a point, called the **nucleus**. In this case $(0, 1, 0)$ was the nucleus. From the previous two propostions we introduce the following theorem:

Theorem 2.3.1 (Bose [3]) *In $PG_2(q)$ we get the following result about arcs:*

1. *For q even, a hyperoval is the largest arc.*
2. *For q odd, an oval is the largest arc.*

The proof of this comes from Bose in 1947.
Proof:
Let K be a k-arc, and suppose $x \in K$. Then, there is at most 1 other point in K on a line through x. Now, there are $q + 1$ lines through x, so we get that $k - 1 \leq q + 1$, so $k \leq q + 2$.

1. Now, first we note that a hyperoval allows no tangent lines. This is true because if K is a hyperoval, then any point x is connected to every other of the $(q + 1)$ points of K. Since x only has $(q + 1)$ lines through it, this requires that every line through x is a secant. Now, let y be a point such that $y \notin K$. If we consider the lines through y, we see that since no tangent lines exist on K, then the lines on y are either external to K or secants of K. Thus, for each line on y that is secant to K, we get 2 points on K. This implies that $q + 2$ is even so we see that q is even.

2. This is just a corollary to the above proof. When q is odd, then if K were a hyperoval (i.e. $q+2$ points, which is odd) then there must be at least one tangent through K, which contradicts that it is a hyperoval. So from this we get that for q odd, we must have $k \leq q+1$. And we know that ovals do exist in $PG_n(q)$.

Not only can we classify that there are no hyperovals in $PG_n(q)$, q odd, but we also have a nice result which classifies the structure of **all** ovals in these spaces.

Theorem 2.3.2 (Segre [19]) *In $PG_2(q)$, q odd, every oval is a conic (the zero set of a non-degenerate quadratic form in 3-variables).*

The proof due to Segre in 1955 is long and involved so it is omitted here. This is however a very important result. This classifies all ovals in odd characteristic, and thus we no longer study this area. So from this point on in this section, we will only be considering $PG_2(q)$, $q = 2^h$ for some h. As we have seen, in this case, there will exist hyperovals. A main area of current study is to classify all different families of infinite hyperovals. To introduce this area of research, we introduce the main form of hyperovals and some known conditions on how to get them in general. There are not many conditions, so the research is often left to an exhaustive computer search to find hyperovals.

As we have seen, we can construct a hyperoval by finding a non-degenerate conic and adding the nucleus. We have a special name for these types of hyperovals:

Definition 2.3.4 *A hyperoval is called* **regular (or hyperconic)** *if it is the union of a non-degenerate conic and its nucleus.*

In general, since Segre classified the structure of all ovals in odd characteristic, a widely studied area of projective planes is to classify the structure of all hyperovals in even characteristic. We introduce a few methods that are used to do this classification, which we point out is still an open problem.

Definition 2.3.5 *If $q = 2^h$, the map $T : \mathbb{F}_q \to \mathbb{F}_2$ defined by*

$$T(x) = x + x^2 + x^4 + ... + x^{2^{h-1}} = \sum_{\alpha \in Aut(\mathbb{F}_q)} \alpha(x)$$

is called the **trace map**.

Basic knowledge in algebraic theory gives us the following theorem about the trace map:

Theorem 2.3.3 *For the trace map T:*

1. *T is well defined.*
2. *T maps $\mathbb{F}_q$ onto $\mathbb{F}_2$.*
3. *T is additive.*
4. *$|ker(T)| = \frac{q}{2}$.*
5. *$T(\alpha(x)) = T(x)\ \forall \alpha \in Aut(\mathbb{F}_q)$*

Proof:

1. Now, we note that $y^2 = y \Leftrightarrow y \in \mathbb{F}_2$. Let $y = T(x)$. Then $T(x)^2 + T(x) = T(x) + T(x) = 0$ since we are in characteristic 2 and we know that $T(x)^2 = T(x)$ because we just rearrange all the automorphisms to get them all back again. (Binomial theorem in characteristic 2).

2. Assume that $Im(T) \neq \mathbb{F}_2$. This implies that $Im(T) = \{0\}$. So we see that from this that

$$x + x^2 + x^4 + ... + x^{2^{h-1}} = 0$$

   for all $x \in \mathbb{F}_q$. However, this polynomial has degree $2^{h-1} = \frac{q}{2}$ and has q roots, which is impossible. So we get a contradction, thus $Im(T) = \mathbb{F}_2$.

3. It suffices to show that $x \to x^2$ is additive. In characteristic 2, $(a+b)^2 = a^2 + b^2$. This then implies that $T(a + b) = T(a) + T(b)$.

4. T is $\mathbb{F}_2$-linear and $dim(Im(T)) = 1$. This means that $dim(ker(T)) = h - 1$. Thus, $|ker(T)| = 2^{h-1} = \frac{q}{2}$.

5. Note that $Aut(\mathbb{F}_q)$ forms a group under composition. With this in mind:

$$T(\alpha(x)) = \sum_{\beta \in Aut(\mathbb{F}_q)} \beta(\alpha(x)) = \sum_{\gamma \in Aut(\mathbb{F}_q)} \gamma(x) = T(x)$$

   since $\beta\alpha$ runs through all the automorphisms.

We can now define a certain type of polynomial that will give rise to hyperovals.

Definition 2.3.6 *A polynomial f such that $D(f) = \{(1, t, f(t)|t \in \mathbb{F}_q\} \cup \{(0, 0, 1), (0, 1, 0)\}$ is a hyperoval is called an* **o-polynomial**.

Lemma 2.3.1 (Slope Condition) *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a $1-1$ and onto function, $q = 2^h$. Then f is an o-polynomial if and only if the following condition holds:*

$$\frac{f(x) + f(y)}{x + y} \neq \frac{f(x) + f(z)}{x + z}$$

for all distinct $x, y, z \in \mathbb{F}_q$.

In addtion to this, Tim Penttila added another condition to require that a function is an o-polynomial.

Theorem 2.3.4 (Penttila [16]) *Let, $f, F, g : \mathbb{F}_q \to \mathbb{F}_q$ be functions, q even. Suppose that $f(0) = 0$, $f(1) = 1$, $F(0) = 0$ and that the following condition holds:*

$$T\Big(F\Big(\frac{f(s) + f(t)}{s + t}\Big)(g(s) + g(t))\Big) = 1$$

for all $s, t \in \mathbb{F}_q$ and $s \neq t$. Then we have that f is an o-polynomial.

Proof:
First, we suppose that f is not injective. Then there would exist two elements $s \neq t$ with $f(s) = f(t)$. This then implies that

$$1 = T\Big(F\Big(\frac{f(s) + f(t)}{s + t}\Big)(g(s) + g(t))\Big) = T(F(0)(g(s) + g(t))) = T(0) = 0$$

This is a contradiction, and thus f is injective.

Now, we show that f satisfies the slope condition (Lemma 2.3.1). Assume that the slope condition is not satisfied. Now we let $r \neq s \neq t \neq r$ all be elements in $\mathbb{F}_q$ with the property that

$$\frac{f(s) + f(t)}{s + t} = \frac{f(s) + f(r)}{s + r} = a$$

This gives us that $f(s)+f(t)=a(s+t)$ and $f(s)+f(r)=a(s+r)$. We add these two equations together to get

$$f(t)+f(r)=a(t+r) \Rightarrow a=\frac{f(t)+f(r)}{t+r} \tag{1}$$

Now because of the assumption in the theorem, $T(F(a)(g(s)+g(t)))=1$ and also $T(F(a)(g(s)+g(r)))=1$. Now we recall that the trace function is additive and so we add these two equations to get

$$T(F(a)(g(t)+g(r)))=1+1=0$$

since we are in characteristic 2. But because of Equation 1, we know that this implies that

$$T\Big(F\Big(\frac{f(t)+f(r)}{t+r}\Big)(g(t)+g(r)\Big)=0$$

which is a contradiction. Thus we see that f satisfies the slope condition. Together, since f is injective and satisfies the slope condition, Lemma 2.3.1 implies that f is indeed an o-polynomial.

This condition helps to test if a function is an o-polynomial. From here we get another nice method that will eliminate possible functions from being o-polynomials.

2.3.1 Glynn's Condition for Existence of Hyperovals

David Glynn has an interesting condition for a function $f(x)$ to give a hyperoval. We introduce some basic theorems, definitions and lemmas that will lead us to Glynn's final result. This area is most interesting as it includes a wide area of combinatorial mathematics, not just projective geometry. As we have seen, when considering a hyperoval, we can assume it has the general form

$$\theta=\{(1,t,f(t))|t\in\mathbb{F}_q\}\cup\{(0,1,0),(0,0,1)\}$$

where $f(t)$ is an o-polynomial with degree less than or equal to $q-2$. Given θ as is, we want to distinguish a condition that will require f to be an o-polynomial. We note that most of the material in the following section is based on [9].

Theorem 2.3.5 (Dickson's Criterion [7]) *Let f be a polynomial over $\mathbb{F}_q$ with degree less than q. Then f induces a permutation of the elements of $\mathbb{F}_q$ if and only if:*

1. *For $gcd(b, q) = 1$ and $1 \leq b \leq q-2$, the degree of $f(x)^b \pmod{x^q - x}$ is at most $q-2$; and*
2. *There is only one solution in $\mathbb{F}_q$ of $f(x) = 0$.*

We now introduce a nice theorem which will allow us to interpolate functions over finite fields by polynomials. This will allow us to find the coefficients in certain polynomials which will be an essential task in Glynn's main proof.

Proposition 2.3.3 (cf. [7]) *If $g(t)$ is a function over $\mathbb{F}_q$, then there exists a function $f(x)$ with degree $\leq q-1$ and $f(x) = g(x)$ for all $x \in \mathbb{F}_q$. Furthermore, $f(x) = \sum_{i=0}^{q-1} a_i x^i$, then the following is true:*

1. $a_0 = g(0)$
2. $a_r = -\sum_{\lambda \in \mathbb{F}_q{}^\times} g(\lambda)\lambda^{-r}$ *for* $1 \leq r \leq q-2$.
3. $a_{q-1} = -\sum_{\lambda \in \mathbb{F}_q} g(\lambda)$

Proof:
We first check the existence of this $f(x)$. We need to make sure that in fact

$$\sum_{i=0}^{q-1} a_i x^i = g(0) - \sum_{i=1}^{q-2} \sum_{\lambda \in \mathbb{F}_q{}^\times} \frac{g(\lambda)}{\lambda^i} x^i - \sum_{\lambda \in \mathbb{F}_q} g(\lambda) x^{q-1}$$

allows for $f(x) = g(x)$ for all $x \in \mathbb{F}_q$.
When $x = 0$, clearly $f(0) = g(0)$.

When $x \neq 0$, we know that $x^{q-1} = 1$.Now we get that

$$\begin{aligned} f(x) &= g(0) - \sum_{i=1}^{q-2} \sum_{\lambda \in \mathbb{F}_q^\times} \frac{g(\lambda)}{\lambda^i} x^i - \sum_{\lambda \in \mathbb{F}_q} g(\lambda) x^{q-1} \\ &= g(0) - \Big(\sum_{\lambda \in \mathbb{F}_q^\times} g(\lambda) + g(0) \Big) - \sum_{\lambda \in \mathbb{F}_q^\times} g(\lambda) \sum_{i=1}^{q-2} \Big(\frac{x}{\lambda} \Big)^i \\ &= - \sum_{\lambda \in \mathbb{F}_q^\times} g(\lambda) \Big(1 + \sum_{i=1}^{q-2} \Big(\frac{x}{\lambda} \Big)^i \Big) \\ &= g(x) \end{aligned}$$

This is because of the fact that when $\lambda = x$ we have that

$$1 + \sum_{i=1}^{q-2} \Big(\frac{x}{\lambda} \Big)^i = -1$$

and when $\lambda \neq 0$ and $\lambda \neq x$

$$1 + \sum_{i=1}^{q-2} \Big(\frac{x}{\lambda} \Big)^i = \frac{(\frac{x}{\lambda})^i - 1}{\frac{x}{\lambda} - 1} = 0$$

Thus we complete this part of the proof.

We now show that this function $f(x)$ is also unique. Assume that there are two functions $f_1(x), f_2(x)$ over $\mathbb{F}_q$ with degree of $f_i(x) \leq q-1$ for $i = 1, 2$ and that $f_1(x) = f_2(x) = g(x)$ for all $x \in \mathbb{F}_q$. Then we see that the polynomial $h(x) = f_1(x) - f_2(x)$ is a polynomial over $\mathbb{F}_q$ with degree $\leq q - 1$. However, since $f_1(x) = f_2(x)$ for all $x \in \mathbb{F}_q$ then $h(x)$ has q zeros. This implies that $h(x) = 0$, and thus $f_1(x) = f_2(x)$. Therefore, the function interpolating $g(x)$ is unique.

Theorem 2.3.6 (Lucas' Theorem cf. [5]) *We consider the binary representation of numbers. Let* $b = \sum_{i=0}^{n} b_i p^i$ *and* $a = \sum_{i=0}^{n} a_i p^i$, *we have*

$$\binom{a}{b} = \prod_{i=0}^{n} \binom{a_i}{b_i} \pmod{p}$$

with $0 \leq b_i < p$ *and* $0 \leq a_i < p$ *for* $i < n$.

Definition 2.3.7 *We say b is* **dominated** *by a if the binary expansion of b is contained in the binary expansion of a, i.e. if $b = \sum_{i=0}^{n} b_i 2^i$ and $a = \sum_{i=0}^{n} a_i 2^i$ then $b_i = 1$ implies $a_i = 1$. We write $b \prec a$.*

From this definition, we get a partial ordering on the integers which can be described by taking Pascal's triangle mod 2.

Example 2.3.1 *We list out Pascal's triangle up the sixth row. Then we mod out by 2. If we want to know if 4 is dominated by 5 for example, then we read across the top to 4 and go down the rows to 5 and see if there is a 1 in the corresponding matrix entry.*

Pascal's Triangle

	0	1	2	3	4	5
0	1	0	0	0	0	0
1	1	1	0	0	0	0
2	1	2	1	0	0	0
3	1	3	3	1	0	0
4	1	4	6	4	1	0
5	1	5	10	10	5	1

Pascal's Triangle (mod 2)

	0	1	2	3	4	5
0	1	0	0	0	0	0
1	1	1	0	0	0	0
2	1	0	1	0	0	0
3	1	1	1	1	0	0
4	1	0	0	0	1	0
5	1	1	0	0	1	1

So clearly 4 is dominated by 5 since there is a 1 in the corresponding spot in the matrix.

We now introduce some lemmas that will help us to prove Glynn's condition.

Lemma 2.3.2 *θ is a hyperoval if and only if the q^2-q lines of $PG_2(2,q)$ not passing through $(0,1,0)$ and $(0,0,1)$ always intersect θ in an even number of points.*

Proof:
First, we verify there are q^2-q lines in $PG_2(q)$ not through (0,0,1) and (0,1,0). Clearly there are $q+1$ lines through (0,0,1) and through (0,1,0), but one of those is the line between (0,0,1) and (0,1,0) so there are a total of $2q+1$ lines in $PG_2(q)$ which go through either (0,0,1) or (0,1,0). Since there are a total of q^2+q+1 lines, there are $q^2+q+1-2q-1=q^2-q$ lines of $PG_2(q)$ not going through (0,0,1) and (0,1,0).
Now, assume that θ is a hyperoval. Then we know that every line in $PG_2(q)$ either does not contain points of θ or is a secant of θ. Therefore, they intersect in 0 or 2 points.
Now, assume that the q^2-q lines in $PG_2(q)$ not through (0,0,1) and (0,1,0) always intersect θ in an even number of points. We have to show that θ is a hyperoval, i.e. that no line of the plane contains more than 2 points of θ. Consider another point of θ, P. There are $q-1$ lines through P that must intersect in at least one other point, not (0,0,1) or (0,1,0). This is because P must have $q+1$ lines on it, with one through (0,0,1) and one through (0,1,0), and the line must intersect θ again by our assumption. Now, there are only $q-1$ points left on $\theta \setminus \{(0,1,0),(0,0,1),P\}$ since θ has $q+2$ points. So there are $q-1$ lines through P and $q-1$ points left on $\theta \setminus \{(0,1,0),(0,0,1)\}$ so each line through P must intersect $\theta \setminus \{(0,1,0),(0,0,1)\}$ at at most one other point. These two statements together say that the lines through P hit $\theta \setminus \{(0,1,0),(0,0,1)\}$ at exactly one more point. So these $q-1$ lines each contain exactly two points of θ. So now we connect each point to (0,0,1) with a line and we have a total of $q+1$ points, no three collinear, since (0,0,1) is not on any of the lines we had before. Note, these lines cannot also go through (010) because there is a unique line between (0,0,1) and (0,1,0) which by assumption cannot hit any points of $\theta \setminus \{(0,1,0),(0,0,1)\}$. So $\theta \setminus \{(0,1,0)\}$ is an oval. Lastly, we show that (0,1,0) is the nucleus of the oval which we have created. This is evident by the fact that each point of $\theta \setminus \{(0,1,0)\}$ has one more line on it which goes through (0,1,0) and these lines were not already in $\theta \setminus \{(0,1,0)\}$ by assumption. Thus, we add (0,0,1) and see that no 3 points are collinear and we have $q+2$ points. So θ is a hyperoval.

This gives a nice combinatorial condition for a hyperoval.

Lemma 2.3.3 *Let $g(t)$ be a polynomial of $\mathbb{F}_q$. Then $g(t) = \mu$ has an even number of solutions $t \in \mathbb{F}_q$ for all $\mu \in \mathbb{F}_q$ if and only if the following holds:*

$$\sum_{\lambda \in \mathbb{F}_q} g(\lambda)^r = 0$$

for all $r = 1, 2, ..., q-1$.

Proof:
First, assume that $g(t) = \mu_i$ has an even number, $2n_i$, of solutions in the field, $\mathbb{F}_q$, for all $\mu_i \in \mathbb{F}_q$. Then clearly, our sum becomes

$$\sum_{i=1}^{\#\text{ solutions of } g(t)} 2n_i(\mu_i)^r$$

where n_i is an integer for all i. However, we are in even characteristic, so all these terms are zero. Thus the condition is fulfilled for all r. Next we assume that the above sum holds. We consider the set:

$$\Omega = \{\mu |\ g(t) = \mu \text{ has an odd number of solutions}\}$$

The proof then depends on Vandermonde's determinant which implies that the vectors $(1, \mu, \mu^2, ..., \mu^{q-1})$ are linearly independent for different $\mu \in \mathbb{F}_q$. So our sum above requires that $\mu_1^r + ... + \mu_n^r = 0$, but this contradicts Vandermonde's determinant, so clearly $\Omega = \varnothing$ and this proves the result.

We can now connect Lemma 2.3.2 and Lemma 2.3.3 to force an algebraic condition on the existence of hyperovals instead of the combinatorial condition from the first lemma.

Lemma 2.3.4 *The $q^2 - q$ lines of $PG_2(q)$ not passing through* (001) *and* (010) *always intersect θ in an even number of points if and only if the following condition holds:*

$$\sum_{\lambda \in \mathbb{F}_q} (f(\lambda) + \lambda x)^r = 0$$

for all $r = 1, 2, ..., q-1$ and for all $x \in \mathbb{F}_q^\times$.

Proof:
Now, let l be a line that does not pass through $(0,0,1)$ or $(0,1,0)$. Then l has the form $[\mu, x, 1], x \neq 0$. If $(0,1,0)$ were on this line, that implies that $0 \cdot \mu + 1 \cdot x + 0 \cdot 1 = 0$ which in turn would imply that $x = 0$, which is a contradiction. If $(0,0,1)$ were on the line, then $0 \cdot \mu + 0 \cdot x + 1 \cdot 1 = 0$, which would imply 1=0, which is a contradiction. Now, for $[\mu, x, 1]$ to contain any other point of θ, $(1, t, f(t))$, then the condition is that $1 \cdot \mu + t \cdot x + f(t) \cdot 1 = 0$, i.e. $f(t) + tx = \mu$.
First, assume that the $q^2 - q$ lines of $PG_2(q)$ not passing through $(0,0,1)$ and $(0,1,0)$ always intersect an even number of points. This implies that $f(t) + tx = \mu$ has an even number of solutions and so for $x \neq 0$, Lemma 2.3.3 implies that the condition above is satisfied.
Assume the condition above is satisfied. Now $f(t) + tx = \mu$ has an even number of solution due to Lemma 2.3.3. So we see there are an even number of points in θ that are on $[\mu, x, 1]$. Thus the $q^2 - q$ lines of $PG_2(q)$ not passing through $(0,0,1)$ and $(0,1,0)$ intersect θ in an even number of points. Note for this, $x = 0$ does not have any affect on the hyperoval since our line requires $x \neq 0$.

Lemma 2.3.5 *If $b \prec a$ then t^b occurs in the expansion of $(1+t)^a$ in characteristic 2.*

Proof:
From Lucas' Theorem (2.3.6), we know that

$$\binom{a}{b} = \prod_{i=0}^{n} \binom{a_i}{b_i} \ (mod\ 2)$$

Now if $b \prec a$ then $\binom{a_i}{b_i} = 1\ \forall i$ since $\binom{1}{0} = 1$ and $\binom{1}{1} = 1$. Conversely if $\binom{a_i}{b_i} = 1\ \forall i$, then we have $b \prec a$. If not, there would exist i such that $a_i = 0$ and $b_i = 1$ and thus $\binom{a_i}{b_i} = 0$ for this i. Together we have $b \prec a \Leftrightarrow \binom{a_i}{b_i} = 1\ \forall i$
So by the binomial theorem, our lemma holds.

Lemma 2.3.6 *$i \prec r \Leftrightarrow r - i \prec q - 1 - i$ for $0 \leq i, r \leq q - 1$.*

Proof:
We note that the binary representation of $q-1-i$ is the bitwise complement of the binary representation of i. (i.e. there is a 1 in the expansion of i if

and only if there is a zero in the expansion of $q-1-i$.)
"$\Leftarrow$" Assume $i \not\prec r$. Consider the first coefficient with i containing a 1 and r containing a 0. $\Rightarrow r-i$ has corresponding coefficent 1.
But i has coefficient 1 $\Leftrightarrow q-1-i$ has coefficient 0.
$\Rightarrow r-i \not\prec q-1-i$. This proves the result by contraposition.

"$\Rightarrow$" Let there be a 1 as coefficient of $r-i$.
Since $i \prec r$, $\Rightarrow r$ has corresponding coefficient 1 and i has corresponding coefficient 0.
i having 0 $\Rightarrow q-1-i$ has corresponding coefficient 1.
$\Rightarrow r-i \prec q-1-i$.
So clearly $r-i \prec q-1-i$.
Now, we can put all of the previous results together to get a nice condition formulated by Glynn which will determine whether or not $f(t)$ is an o-polynomial.

Theorem 2.3.7 (Glynn's Condition [9]) *θ is a hyperoval if and only if the following condition holds: the coefficient of t^a in $[f(t)]^b$ (mod t^q-t) is zero for all pairs (a,b) with $1 \leq b \prec a \leq q-1$ and $b \neq q-1$, where in this particular case the coefficient is not 0.*

Proof:
Now, due to Lemma 2.3.4, we have seen that θ is a hyperoval $\Leftrightarrow$

$$\sum_{\lambda \in \mathbb{F}_q} (f(\lambda)+\lambda x)^r = 0$$

First, we assume that $r < q-1$. Then, evaluating the previous sum using the binomial expansion gives

$$\sum_{\lambda \in \mathbb{F}_q} \Big(\sum_{0 \leq s \prec r} f(\lambda)^{r-s} \lambda^s x^s \Big) = 0$$

for all $r = 1, 2, ..., q-2$. The inner sum is over $s \prec r$ because the other terms have a binomial coefficient of 0 due to the fact that s is not dominated by r. Now this is true for all $x \in \mathbb{F}_q$ since $r < q-1$. Therefore this is a polynomial of degree at most $q-2$ with q roots. Thus since there are more roots than the degree of the polynomial, the polynomial must be the zero polynomial.

Thus the coefficient of each x^i must be zero for $0 \leq i \prec q-2$. So we see that the following is therefore true:

$$\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{r-i} \lambda^i = 0$$

for all $0 \leq i \prec r \leq q-2$.

Now, we consider the case for $r = q-1$.
If $x \neq 0$, then expanding the formula again implies that

$$\sum_{\lambda \in \mathbb{F}_q} \Big(\sum_{0 \leq s \prec r} f(\lambda)^{q-1-s} \lambda^s x^s \Big) = 0$$

Now if $x = 0$, since $f(t)$ is a permutation polynomial, our formula becomes

$$\begin{aligned} \sum_{\lambda \in \mathbb{F}_q} (f(\lambda))^{q-1} &= \sum_{\lambda \in \mathbb{F}_q} (\lambda)^{q-1} \\ &= \sum_{\lambda \in \mathbb{F}_q^\times} 1 \\ &= q-1 \\ &= 1 \end{aligned}$$

This is because $\lambda^{q-1} = 1 \; \forall \; \lambda \in \mathbb{F}_q^\times$ and $q-1 \equiv 1 \pmod 2$.

Now we put the two previous results together and consider the coefficient of x^i.
With $x \neq 0$, we see that our sum

$$\sum_{0 \leq s \prec r} \Big(\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1-s} \lambda^s \Big) x^s = 0$$

is a polynomial of degree at most $q-1$ and by Lemma 2.3.4, it has $q-1$ zeros. Also we note the coefficient of x^{q-1}, i.e. $s = 0$. In this case, we see it is the following sum:

$$\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1} = 1$$

. Similarly, the coefficient of x^0 is

$$\sum_{\lambda \in \mathbb{F}_q} (\lambda)^{q-1} = 1$$

This therefore implies that our formula is $x^{q-1} + ... - 1 = 0$. But $x^{q-1} - 1$ is the unique formula with $q-1$ zeros, so we see that our above double sum in this case is $x^{q-1} - 1$. But this is also true for our case with $x = 0$ since we have seen that for $x = 0$ we get our sum equal to 1. Thus, together we see that when $r = q - 1$

$$\sum_{\lambda \in \mathbb{F}_q} (f(\lambda) + \lambda x)^{q-1} = x^{q-1} - 1$$

$\forall\ x \in \mathbb{F}_q$.
We use this to see that the coefficient of x^{q-1} is clearly 1, and to see that the coefficient of all x^i with $1 \leq i \leq q-2$ is 0 so that:

$$\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1-i} \lambda^i = 0$$

Now, with both cases $r = q - 1$ and $r \leq q - 2$ together, we see that for $r \leq q - 1$, we see that

$$\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{r-i} \lambda^i = 0$$

for all $0 \leq i \prec r \leq q - 1$ as long as $(i, r) \neq (0, q-1)$ or $(q-1, q-1)$. We have seen that in the $(0, q-1)$ case we get the sum is 1. In the $(q-1, q-1)$ case the sum is also 1.

We now use the formula for evaluation of polynomials over a finite field (2.3.3). We first note that $-i = q - 1 - i$ in this case due to reduction by $t^q - t$. This gives us that the coefficient of t^{-i} in $f(t)^{r-i}$ is given by:

$$a_{-i} = \sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{r-i} \lambda^{-(-i)}$$

So this evaluation result along with our conclusion from above implies that the coefficient of t^{-i} in $f(t)^{r-i}$ is 0, i.e. $a_{-i} = 0$. Now, we can mod out by $t^q - t$. By assumption, $i \prec r$ and thus by Lemma 2.3.6 $r - i \prec q - 1 - i$. This implies that $r - i \prec -i$. So, set $r - i = b, -i = a$ and we see that for all pairs of (a, b) with $1 \leq b \prec a \leq q - 1$ with $b \neq q - 1$, we get that the coefficient of t^a in $f(t)^b \pmod{t^q - t}$ is 0. This then proves the result in one direction. So we turn to the other direction.

Now, we assume that all the coefficients are zero. So now, we use this in the expansion of

$$\sum_{\lambda \in \mathbb{F}_q} (f(\lambda) + \lambda x)^r = 0$$

and we see that this is true for all $1 \leq r \leq q-2$. For the case $r = q-1$, and thus $x \neq 0$, we get that

$$\sum_{\lambda \in \mathbb{F}_q} (f(\lambda) + \lambda x)^r$$

reduces to

$$\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1} + \sum_{\lambda \in \mathbb{F}_q} \lambda^{q-1} x^{q-1} = \sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1} + x^{q-1}$$

Now since $x \neq 0$, we see that $x^{q-1} = 1$ and so for the entire expression to be zero, we need

$$\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1} = 1$$

But this is true since we assume that the coefficient $[t^{q-1}]$ in $f(t)^{q-1}$ is not zero, thus it must be 1. From our interpolation formula, this coefficient is given by

$$a_{q-1} = -\sum_{\lambda \in \mathbb{F}_q} f(\lambda)^{q-1}$$

Therefore, we actually get that

$$\sum_{\lambda \in \mathbb{F}_q} (f(\lambda) + \lambda x)^r = 0$$

for all $1 \leq r \leq q-1$ except $(0, q-1)$. Therefore θ is a hyperoval. This completes the result.

Remark 2.3.1 *Glynn's paper does not include the additional assumption that the coefficient of* $[t^{q-1}]$ *in* $f(t)^{q-1}$ *is not* 0*. We have found that the proof requires this assumption and thus we have added it. We make a note that this slight change has been added upon suggestion by Stan Payne.*

Remark 2.3.2 *While this theorem may seem hard to use, we never really raise a polynomial to a power. Instead, just consider the coefficients as defined by Proposition 2.3.3 of a power of a polynomial function.*

Additionally, we get the following result due to Segre and Bartocci as a corollary:

Corollary 2.3.1 ([18]) *An o-polynomial has only even degree terms.*

Proof:
We apply Glynn's condition with $b = 1$. Since if c is odd, then $1 \prec c$ and the coefficient of x^c must be zero.

2.4 k-arcs, k-caps and minihypers in $PG_n(q)$

We now extend the general idea of ovals and hyperoval to any dimension n instead of just the projective planes. Hyperovals and ovals are nice because they are simultaneously k-arcs and k-caps. As we have previously seen, the normal rational curves form $(q+1)$-arcs if $q \geq n$. This of course leads to the question of whether other large size arcs exist in these spaces. We not only want to find other k-arcs, but we especially would like to find k-arcs which are complete and not normal rational curves. To help us study this area, we introduce a few theorems that help us to classify if other k-arcs exist.

2.4.1 k-arcs in general

Theorem 2.4.1 (cf. [13]) *If every $(q+1)$-arc of $PG_n(q)$, $n \geq 3$ and $q \geq n+3$, is a normal rational curve, then $q+1$ is the maximum value of k for which k-arcs exist in $PG_{n+1}(q)$.*

This theorem helps us to search for large size arcs if we can classify that some projective space has only normal rational curves as $(q+1)$-arcs. This naturally leads us to wonder if we can extend a normal rational curve to a $(q+2)$-arc. Due to Storme and Thas, we have the following result:

Theorem 2.4.2 (cf. [13]) *A point $P = (a_0, a_1, ..., a_{q-2})$ extends the normal rational curve $K = \{(1, t, t^2, ..., t^{q-2}) | t \in \mathbb{F}_q\} \cup \{(0, 0, ..., 0, 1)\}$ to a $(q+2)$-arc*

if and only if $F(X) = \sum_{i=0}^{q-2} a_{q-2-i} X^{i+1}$ *defines a hyperoval*

$$\theta = \{1, t, F(t))|\ t \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\}$$

in $PG_2(q)$*. Moreover, we get a* $1-1$ *correspondence if we require* $F(1) = 1$*.*

We also question whether there are maximal complete arcs which are not normal rational curves. David Glynn was able to come up with an example which we will present momentarily. We first provide a lemma about normal rational curves which will help us to prove Glynn's unique result.

Lemma 2.4.1 (cf. [22]) *A normal rational curve in* $PG_4(9)$ *is an intersection of zero sets of non-degenerate irreducible quadratic forms (i.e. an intersection of non-degenerate quadrics).*

Proof:
As we have seen we may assume that our normal rational curve T has the form:

$$T = \{(1, t, t^2, t^3, t^4)|t \in \mathbb{F}_9\} \cup \{(0,0,0,0,1)\}$$

due to projective equivalence. Clearly, we see that $x_1^2 = x_0x_2$, $x_2^2 = x_0x_4$, $x_3^2 = x_2x_4$, and $x_0x_3 = x_1x_2$ are all irreducible quadratic forms (quadrics) containing T. Furthermore, we show that the intersection of these quadrics is T. Now let $(x_0, x_1, x_2, x_3, x_4)$ be in the intersection of the quadrics. Next, fix $x_0 = 1$. Then call $x_1 = s$. So necessarily from the first quadratic form, $x_2 = s^2$. This leads us to see that $x_4 = (s^2)^2 = s^4$ by the second quadratic form. The third quadratic form gives us $x^3 = s^3$. Lastly, if we instead let $x_0 = 0$, then the forms imply that this is necessarily the point $(0,0,0,0,1)$. This proves the result.

We are now ready to introduce an maximal complete arc that is not projectively equivalent to a normal rational curve.

Theorem 2.4.3 (Glynn's 10-arc [8]) *In* $PG_4(9)$*, a normal rational curve is a* 10*-arc. However, there is also another* 10*-arc which is not projectively equivalent to a normal rational curve, but instead it is projectively equivalent to the following set of points:*

$$L = \{(1, x, x^2 + \eta x^6, x^3, x^4)|\ x \in \mathbb{F}_9\} \cup \{(0,0,0,0,1)\}$$

with $\eta \in \mathbb{F}_9$ *and* $\eta^4 = -1$*.*

We give the following nice proof of this statement described in [22].
Proof:
We first show that L is a 10-arc. To do this, we verify that any five points from L span a 5-dimensional vector space over $\mathbb{F}_9$. First consider only points not of the form $(0,0,0,0,1)$. Now we let $\det(1, x_i, x_i^2 + \eta x_i^6, x_i^3, x_i^4)$ denote the determinant of the following matrix:

$$\begin{pmatrix} 1 & x_1 & x_1^2 + \eta x_1^6 & x_1^3 & x_1^4 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_5 & x_5^2 + \eta x_5^6 & x_5^3 & x_5^4 \end{pmatrix}$$

So, we assume that these five points do not span a 5-dimensional vector space. This implies that $\det(1, x_i, x_i^2 + \eta x_i^6, x_i^3, x_i^4) = 0$. Since the determinant is a bilinear form, this also gives us

$$\det(1, x_i, x_i^2 + \eta x_i^6, x_i^3, x_i^4) = \det(1, x_i, x_i^2, x_i^3, x_i^4) + \eta \det(1, x_i, x_i^6, x_i^3, x_i^4).$$

This in turn implies that

$$\det(1, x_i, x_i^2, x_i^3, x_i^4) = -\eta \det(1, x_i, x_i^6, x_i^3, x_i^4). \tag{2}$$

Now, since $\mathbb{F}_9$ has characteristic 3, the map $x \to x^3$ is a field automorphism (Frobenius automorphism). This gives us that

$$[\det(1, x_i, x_i^2, x_i^3, x_i^4)]^3 = -\eta^3 [\det(1, x_i, x_i^6, x_i^3, x_i^4)]^3.$$

This gives us the following relation (due to the fact that in $\mathbb{F}_9$ we have that $x^9 = x \ \forall x$):

$$\det(1, x_i^3, x_i^6, x_i, x_i^4) = -\eta^3 \det(1, x_i^3, x_i^2, x_i, x_i^4).$$

And from linear algebra we know we can rearrange the rows of a matrix without changing the determinant, so suitable rearranging gives us the following relation:

$$\det(1, x_i, x_i^3, x_i^4, x_i^6) = -\eta^3 \det(1, x_i, x_i^2, x_i^3, x_i^4).$$

Additionally by equation 2 along with the previous result we get that

$$\det(1, x_i, x_i^3, x_i^4, x_i^6) = \eta^4 \det(1, x_i, x_i^6, x_i^3, x_i^4) = \eta^4 \det(1, x_i, x_i^3, x_i^4, x_i^6)$$

by rearranging. Now due to Vandermonde's determinant, we know that $\det(1, x_i, x_i^3, x_i^4, x_i^6) \neq 0$, and so this implies that $\eta^4 = 1$. However, we assume

in the theorem that $\eta^4 = -1$, and thus we get a contradiction. We can also make a symmetric argument if we consider one of the five points to be the point $(0, 0, 0, 0, 1)$, and we will get a similar contradiction. Thus we see that any 5 (=4+1) points of L are linearly independent and so L is a 10-arc.

We now must show that L is not a normal rational curve. From Lemma 2.4.1 we know that a normal rational curve in $PG_4(9)$ is an intersection of non-degenerate quadrics. We will prove that L is not the intersection of non-degenerate quadrics. We assume that L is an intersection of quadrics, $\mathcal{Q}_i$, i.e. $L = \cap_{i \in I} \mathcal{Q}_i$. We let

$$\mathcal{Q}_i = \{(x_0, ..., x_4) | x_i \in \mathbb{F}_9, Q_i(x_0, ..., x_4) = 0\}$$

where Q_i is a quadratic form, i.e. $0 \neq Q_i = \sum_{r,s=0}^{4} c_{r,s}^{(i)} x_r x_s$ and $c_{r,s}^{(i)} \in \mathbb{F}_9$. Now, in each quadratic form the coefficient $c_{4,4}^{(i)} = 0$ because $(0, 0, 0, 0, 1) \in L$. Since $(0, 0, 1, 0, 0) \notin L$ then there exists a $Q = Q_i$ such that $c_{2,2} = c_{2,2}^{(i)} \neq 0$. With this Q, we consider the following polynomial:

$$\sum_j a_j x_j = f(x) = Q(1, x, x^2 + \eta x^6, x^3, x^4) \in \mathbb{F}_9[x]$$

Now we know that $(1, x, x^2 + \eta x^6, x^3, x^4) \in L$ for every $x \in \mathbb{F}_9$, and so $\mathbb{F}_9$ vanishes on $f(x)$, i.e. $f(x) = 0$ for all $x \in \mathbb{F}_9$. Because of this, basic field theory tells us that $f(x)$ must be a multiple of $x^9 - x$. Therefore we see that $f(x) = (x^9 - x)h(x)$ where $h(x) \in \mathbb{F}_9$. Since $c_{2,2} \neq 0$ then we know that $(x^2 + \eta x^6)(x^2 + \eta x^6)$ is part of $f(x)$. This implies that $f(x)$ has degree 12, and thus $h(x)$ has degree 3. Now, from this we see that $f(x)$ has no term with degree 8, and thus $a_8 = 0$. However, since $c_{2,2}(x^2 + \eta x^6)(x^2 + \eta x^6)$ is part of $f(x)$ and $c_{4,4}^{(i)} = 0$, we see that $a_8 = 2c_{2,2}\eta$. This is a contradiction as $2c_{2,2}\eta \neq 0$. Therefore, L cannot be an intersection of quadrics. By Lemma 2.4.1 we see that since a normal rational curve is an intersection of quadrics, then L cannot be a normal rational curve.

To my knowledge, this is the only known complete arc which is not attained from a normal rational curve in $PG_n(q)$ with $n > 2$. This is an amazing result, and it is a big challenge to find further examples like this.

2.4.2 A Glimpse into the World of k-caps: Ovoids

We can also study k-caps in general projective spaces. For our purposes, we only consider a special type of k-cap. The special k-cap we are interested in is called an ovoid. There are two separate definitions for an ovoid that turn out to be the same in some cases. In general, ovoids are not only interesting in their connections to codes, but also they have a great deal of relationships with other structures created from projective spaces such as generalized quadrangles, spreads, and translation planes to name a few. We begin with the definition of an ovaloid, which in the special case of $n = 3$ we call an ovoid.

Definition 2.4.1 (due to Segre) *In $PG_3(q)$, a (q^2+1)-cap is called an* **ovoid**. *This can also be stated that an* **ovoid** *is a set of (q^2+1) points in $PG_3(q)$ such that no 3 are collinear.*

Example 2.4.1 *We consider the zero set of the following non-degenerate elliptic quadratic form (i.e. elliptic quadric) in $PG_3(q)$:*

$$x_0^2 + x_0x_1 + ax_1^2 + x_2x_3$$

where $a \in \mathbb{F}_q$ such that $x^2 + x + a$ is irreducible over $\mathbb{F}_q$. We see that the set of points of $PG_n(q)$ which are zero under this form is

$$\{(s, t, s^2 + st + at^2, 1) | s, t \in \mathbb{F}_q\} \cup \{(0, 0, 1, 0)\}$$

and this is a set of $q^2 + 1$ projective points. Since the points come from a non-degenerate elliptic quadratic form, no three are collinear.

From here we can further study ovoids and their properties.

Proposition 2.4.1 (cf. [4]) *In $PG_3(2)$ a maximum k-cap is not an ovoid, but has 8 points.*

Proof:
A hyperplane in $PG_3(2)$ has $(2^3 - 1)/(2 - 1) = 7$ points. Since there are 15 points total, then the complement of a hyperplane has 8 points. Clearly, no three of these are collinear since if they were then there would be a line which is disjoint from a hyperplane, which is a contradiction to the dimension. Since

in this space on any point there are 7 lines, then the maximum possible size for a k-cap is 8.

We proved the previous proposition because it is a special case. For all other q, that is $q > 2$, we get the nice following result:

Theorem 2.4.4 (cf. [2]) *In $PG_3(q)$, $q > 2$, an ovoid is a maximum cap.*

Proof:
For q odd, let P and Q be points of an ovoid O and l the line they span. Now, there are $q + 1$ planes on l, and each of these planes can intersect O in at most $q - 1$ points more (because q is odd and we know that an oval is the largest cap in a plane). So along with P and Q, we get that $|O| \leq (q + 1)(q - 1) + 2 = q^2 + 1$. As mentioned above, the elliptic quadric attains that bound and hence we have equality.
Now assume q is even. First we show that through each point there is at least one tangent to O. To do this, we assume that there are no tangent lines to O. Then, consider two points P and Q in O and the line that connects them, l. There are $q + 1$ planes on l and each of these planes must intersect O in a hyperoval, $q + 2$ points. So we have $q + 1$ planes containing q points other than P and Q. So we see that this implies that $|O| = q(q+1)+2 = q^2+q+2$. Now, we consider a line g which contains no points of O (on any point outside of O we have this or else $|O| = 2(q^2 + q + 2)$ which is not true). Now, let k denote the number of planes through g intersecting O in a hyperoval $(q + 2)$ points. Then we get that

$$k(q + 2) = |O| = q^2 + q + 2$$

Now rewriting we get that $k(q + 2) = (q - 1)(q + 2) + 4$. Then this implies that $(q + 2)$ must divide 4 and so $q = 2$, but we have excluded this case. Thus we get a contradiction, so every point of O must contain at least one tangent line.

We now know that if $q \neq 2$, then there exists a tangent line, m, to O at some point Z. If we consider the $q+1$ planes about m, we see that these can intersect O in at most $q + 1$ points or else would contradict the maximality of a hyperoval. If each plane on m meets O in at most q points we have that $|O| \leq (q + 1)(q - 1) + 1 \leq q^2$ which is a contradiction. So we can assume that there is a plane π on m meeting O in an oval $(q + 1$ points). Then, we

know since q is even that there is a nucleus to this oval, which we can add to form a hyperoval. Because π cannot meet O in a hyperoval, then the nucleus must lie on at least one secant line of O, call this line m'. Then, each plane on m' meets the oval in a tangent. Therefore, any of these planes meets O in at most $q+1$ points. So we consider the $q+1$ planes on m' which can meet O in at most $q-1$ lines other than the two points making m'. This gives $|O| \leq (q+1)(q-1)+2 = q^2+1$. Again, we have the elliptic quadric for equality and so the result is proved.
We now introduce a nice theorem about the structure of ovoids. To prove this theorem, we find the following lemma useful.

Lemma 2.4.2 (cf. [4]) *Let Ω be an ovoid in $PG_3(q)$, $q > 2$. Then for $P \in \Omega$, the union of all the tangent lines on P is a plane.*

Proof:
Case 1: Assume q is odd. Let P, Q be two points of Ω. Now, with q being odd, each plane of $PG_3(q)$ can meet Ω in at most $q+1$ points. Now the planes that are spanned by P and Q intersect Ω in exactly $q+1$ points (an oval), or we would get a contradiction to the maximality of Ω. Therefore, a secant line of Ω can only lie on the planes meeting Ω in an oval. Now we let l_1, l_2 be two tangents to Ω at P and π be the plane they span. Since π contains two tangents to Ω, then it cannot meet Ω in an oval, thus it cannot contain any secants. Therefore we see that $\pi \cap \Omega = \{P\}$ so therefore π must contain all the tangents to P so it is the union of all tangents on P.
Case 2: Assume q is even. Now let $P \in \Omega$ and l be a tangent line to Ω on P. We have seen in Theorem 2.4.4 that there must be a plane π on l with $\pi \cap \Omega$ being an oval with nucleus N on some secant line, m'. Since q is even, we have seen that this each point in this oval is on a tangent line connected to N. So if we consider any plane on m', this plane must contain a tangent line on N by intersection with π. Therefore we see that each plane on m' intersects Ω in an oval. In any of these planes, the nucleus N lies on a unique tangent line ($q+1$ tangent lines and $q+1$ planes on m'). This unique tangent line must be the intersection of the plane with π then. So we see that all of the tangents on the nucleus N must be in π. Now we consider any other plane on our original line l that contains another point of Ω, call the point Q. This plane then contains a secant $< N, Q >$, therefore must meet Ω in an oval. This shows that any plane on our line l intersects Ω in P or in an oval. Therefore, the tangent lines to P must form a plane since they do not

intersect Ω in any further points. This lemma leads to the following theorem which will be relatively easy to prove.

Theorem 2.4.5 (cf. [4]) *Let Ω be an ovoid in $PG_3(q)$. Then exactly q^2+1 planes of $PG_3(q)$ meet Ω in a unique point and the other q^3+q planes meet Ω in an oval.*

Proof:
There are q^3+q^2+q+1 planes in $PG_3(q)$. Now, by Lemma 2.4.2 there are q^2+1 tangent planes to Ω. Thus there must be q^3+q ovoids remaining. If these do not intersect Ω in an oval, then we would contradict the maximality of Ω.

We now turn to an alternate definition of an ovoid. The following definition only relies on axioms to define what is meant by an ovoid.

Definition 2.4.2 (due to Tits) *An* **ovoid** *is a set of points O such that following hold:*

- *No three points of O are collinear.*
- *For each point $P \in O$, the tangents through P cover exactly a hyperplane.*

We see that both definitions of an ovoid coincide for the case of $n = 3$ due to Theorem 2.4.5.

In addition to connecting these two definitions, we see the following theorem defines when an ovoid as defined by Tits can exist:

Theorem 2.4.6 (Dembowski [6]) *If $PG_n(q)$ has an ovoid Ω as defined by Tits, then*

1. $|\Omega| = q^{n-1}+1$
2. $n \leq 3$

Proof:
Let P be a point of Ω

1. Since the tangents on P cover a hyperplane and a hyperplane has $\frac{q^{n-1}-1}{q-1}$ lines, then there are exactly this many tangents on P. This implies there are $q^{n-2}+q^{n-3}+...+q+1$ tangent lines on P and since there are a total of $q^{n-1}+q^{n-2}+q^{n-3}+...+q+1$ total lines on P, then there are q^{n-1} secants on P. So the point P connects to q^{n-1} other points and this is all of the possible points in the ovoid. Thus we have a total of $q^{n-1}+1$ points of O.

2. For $n=2$ we have seen that a non-degenerate parabolic quadratic form (or non-degenerate conic) forms an oval which is $q+1$ points satisfying the above axioms. For $n=3$, we have seen before that the zero set of a non-degenerate elliptic quadratic form is an ovoid.
   Now, assume that $n>3$. We count the number of incident pairs of points of Ω and non-tangent hyperplanes to Ω. We let k be the total number of hyperplanes intersecting Ω in an ovoid in the hyperplane. Then the count gives us
   $$\frac{(q^{n-1}+1)(q^n-q)}{q-1}=k(q^{n-2}+1)$$
   This is true because we know there are $q^{n-1}+...+q+1$ hyperplanes on a point of Ω and one of them must be a tangent giving us a total of $q^{n-1}+...+q=q(q^{n-2}+...+q+1)=\frac{q^n-q}{q-1}$. There are $q^{n-1}+1$ points in Ω. Also, on every hyperplane intersecting Ω in an ovoid, there are $q^{n-2}+1$ points of Ω on each of these hyperplanes.
   Now, we know that for $n>4$, there are always $PG_4(q)$ embedded in $PG_n(q)$. Therefore we will get a contradiction for $n=4$. In the case with $n=4$ we get that if k is again the number of hyperplanes intersecting Ω in an ovoid, then we have
   $$\frac{(q^3+1)(q)(q^3-1)}{q-1}=k(q^2+1)$$
   This yields
   $$(q^3+1)(q)(q^2+q+1)=k(q^2+1)$$
   Therefore we see that q^2+1 must divide $(q^3+1)(q)(q^2+q+1)$. Reducing this modulo q^2+1, we get $(q+1)$ which is not zero. Thus we see that this gives a contradiction as q^2+1 does not divide $(q^3+1)(q)(q^2+q+1)$, and so k would not be a natural number.This proves that any $PG_n(q)$ with $n\geq 4$ cannot have an ovoid since it contains a $PG_4(q)$.

This result is intriguing and has led to many investigations of these ovoids in $PG_3(q)$. As with our study of hyperovals, we can begin to describe the current classifications of ovoids. It turns out that there are not many results about existing ovoids, but we do have the following theorem about existence of ovoids in certain spaces:

Theorem 2.4.7 (cf. [13]) *In $PG_3(q)$ there are two known types of ovoids:*

1. **(Barlotti, Panella)** *For q odd or $q = 4$, an ovoid is an elliptic quadric (i.e. a zero set of a non-degenerate elliptic quadratic form).*

2. **(Tits)** *For $q = 2^{2e+1}$, with $e \geq 1$, there exists an ovoid which is not an elliptic quadric. We call this the* **Tits ovoid**, *and it is projectively equivalent to the set*

$$K = \{(0, 1, 0, 0)\} \cup \{(1, z, y, x) |\ z = xy + x^{\sigma+2} + y^{\sigma}\}$$

where $x, y \in \mathbb{F}_q$ and $\sigma = 2^{e+1}$.

Though we omit the proof of the previous theorem, we note that proof uses the fact that these ovoids are in fact different because they have different stabilizer groups in $P\Gamma L(n+1, q)$. This is a nice way to show that two structures are not projectively equivalent. It is also interesting to note that the only known types of ovoids in any projective spaces are the elliptic quadrics and the Tits ovoids.

2.4.3 Minihypers

On a side note, we take this opportunity to introduce another related structure in projective spaces that will have a nice link to coding theory (though not through MDS codes). Even though it is not related to MDS codes, it is nicely connected to k-arcs that we have been studying.

If we have a k-arc, we can consider the complementing points in the projective space. These points then form a nice structure called a minihyper:

Definition 2.4.3 *A* **{r,k,n,q}-minihyper** *is a set of r points called K in $PG_n(q)$ such that there are at least m points of K on every hyperplane, and one hyperplane contains exactly m points of K.*

Now we know that a k-arc gives a set of k points in $PG_n(q)$ such that no $n+1$ lie in a hyperplane. We define the number $\nu_i = \frac{q^{i+1}-1}{q-1}$ to be the number of points of $PG_i(q)$. Thus, we know that $PG_n(q)$ has $1 + q + ... + q^{n-1} = \nu_n$ points and a hyperplane has $1 + q + ... + q^{n-2} = \nu_{n-1}$ points. The resulting minihyper attained by a complement of a k-arc in $PG_n(q)$ has $r = \nu_n - k$ points with $m = \nu_{n-1} - (n + 1)$.

3 Coding Theory

From projective geometry, we switch to coding theory which will initially appear to have no connection to the ideas above. Before we introduce the main idea of MDS codes, we first discuss some of the basic definitions and ideas in coding theory so that the rest of the article may be fully understood.

3.1 Basic Definitions

Definition 3.1.1 *A* **code** *of length n over an alphabet A of size q, $q \geq 2$, is a set of words constructed from A, i.e. n-tuples with entries in A.*

Definition 3.1.2 *A* **linear** $[n, k, d]$**-code** *C over $\mathbb{F}_q$ is a k-dimensional subspace of the n-dimensional vector space $\mathbb{F}_q^n$ with minimum distance d. From this we see that $|C| = q^k$.*

Definition 3.1.3 *The* **Hamming distance** *between to codewords $x, y \in \mathbb{F}_q^n$, denoted $d(x, y)$ is the number of postions in which $x_i \neq y_i$, for $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$.*

Proposition 3.1.1 *By this definition, the Hamming distance forms a metric and thus turns $\mathbb{F}_q^n$ into a metric vector space.*

Proof:

1. Clearly $d(x, y) \geq 0$ and $d(x, y) = 0 \Leftrightarrow x = y$.
2. Clearly, $d(x, y) = d(y, x)$.
3. For the triangle inequality, we note that $d(x, z) \leq d(x, y) + d(y, z)$ since if $x_i \neq z_i$ then necessarily either $x_i \neq y_i$ or $y_i \neq z_i$.

Definition 3.1.4 *The* **minimum distance** *d of a linear code C is the smallest number of positions in which two different elements of C differ, i.e. $d = min\{d(x,y)|x,y \in C,\ x \neq y\}$.*

Definition 3.1.5 *The* **Hamming weight** *of a vector x in a linear code C is defined as the number of non-zero coordinates of x. We denote this* $\mathbf{wt(x)}$. *From this it can be inferred that the minimum distance and the minimum weight of a linear code are the same.*

It is important to see that the minimum weight is the same as the minimum distance if C is a linear code. This comes from the fact that the zero vector is always in a linear code. From here, we define a few more basic ideas that will be necessary for our discussion of MDS codes.

Definition 3.1.6 *If we have a linear $[n,k,d]$-code, then we also have the* **dual code** *$C^{\perp}$ which is a linear $[n, n-k, d']$-code. We form $C^{\perp}$ by looking at the dual of the vector space which forms C.*

Definition 3.1.7 *For a code, we have two matrices that determine the code:*

1. *A* **generator matrix** *G of a linear $[n,k,d]$-code C is a $k \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis of C.*
2. *A* **parity check matrix** *H of a linear $[n,k,d]$-code C is a $(n-k) \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis of $C^{\perp}$.*

From these two definitions we get some nice relationships between the matrices and codewords.

Proposition 3.1.2 *Let C and $C^{\perp}$ be dual linear codes. The following all hold:*

1. *For any codeword $c \in C$ we have that $cH^T = 0$.*
2. *For any codeword $c' \in C^{\perp}$, we have $c'G^T = 0$.*
3. *$GH^T = 0$*

Proof:
We know that since C and $C^{\perp}$ are dual codes, then G is generator matrix for C and a parity check matrix for $C^{\perp}$, and H is a generator matrix for $C^{\perp}$ and a parity check matrix for C.

1. Since H contains rows that are a basis for $C^{\perp}$, then any codeword, $c \in C$ will have dot product zero with every row.

2. This proof holds for the same reason above because G contains rows that are a basis for $C = (C^{\perp})^{\perp}$.

3. This is just an extension of the above two proofs. We know that any codeword in C has dot product zero with any codeword of $C^{\perp}$ by definition of the dual space.

These rules allow us to use G and H to further understand the linear codes they produce.

Definition 3.1.8 *If C is an $[n, k, d]$-linear code with generator matrix G, then a set of k coordinates (from n) is called an* **information set** *if the corresponding columns of G are linearly independent.*

Theorem 3.1.1 (cf. [14], 1.4.14) *The minimum distance of a $[n, k]$-linear code, C, is d if and only if in any parity check matrix H, any non-empty set of at most $d-1$ columns are linearly independent and there exist d columns which are linearly dependent.*

Proof:
Assume that there are $d-1$ linearly dependent columns. Without loss of generality, we assume they are the first $d-1$ columns in the parity check matrix H. We call these columns $v_1, ..., v_{d-1}$. Then there exist some a_t's such that $a_1v_1 + ... + a_{d-1}v_{d-1} = 0$. However, then we can create a codeword $c = (a_1, a_2, ..., a_{d-1}, 0, ..., 0) \in C$ since $cH^T = 0$ by construction. This is a contradiction though since c has weight $d-1$ and hence distance $d-1$. By a similar argument, if there are not d columns of H linearly independent, then we could not construct a word of weight d hence distance d. This would imply that $d(C) = d+1$ a contradiction.

In addition to these definitions we introduce and prove two important bounds on the minimum distance that will eventually lead to certain types of codes in the situations where we have equalities in the bounds. These codes will connect nicely to some of the projective structures described in section 2.

Theorem 3.1.2 (Singleton Bound [20]) *For any code, C with minimum distance d, we have $|C| \leq q^{n-d+1}$. For a linear $[n, k, d]$-code, this means that $q^k \leq q^{n-d+1}$. This in turn implies that $k \leq n-d+1$ or $d \leq n-k+1$.*

Proof:
If we consider a code with size $|C|$ and distance d, we know that every word differs in at least d positions. If we were to truncate the codewords by ignoring the last $d-1$ positions, all the new codewords must be different. So we still have $|C|$ codewords remaining. But now we are in dimension $n-(d-1)$. We know there are a total of $q^{n-(d-1)}$ codewords of this dimension, therefore we see that $|C| \leq q^{n-d+1}$. We see that this proves the result along with the knowledge that when C is linear, $|C|$ is just the size of the k-dimensional subspace over $\mathbb{F}_q$, which is q^k.

We also introduce another bound which is slightly stronger than the Singleton bound, however first we introduce a few more ideas that will help in the proof.

Definition 3.1.9 *If G is a generator matrix with respect to a linear code C, then we define the* **residual code**, *$Res(C,c)$, of C with respect to $c \in C$ as the code generated by the restriction of G to the columns where c has a zero.*

Lemma 3.1.1 (cf. [11]) *Suppose that C is a linear $[n,k,d]$-code over $\mathbb{F}_q$. Also, let $c \in C$ and $wt(c) = w$ with $w < \frac{dq}{q-1}$. Then $Res(C,c)$ is a linear $[n-w, k-1, d^0]$-code with*

$$d^0 \geq d - w + \left\lceil \frac{w}{q} \right\rceil$$

Proof:
Clearly, $Res(C,c)$ has length $n-w$. Then, without loss of generality we assume that c has the form $c = 00...011...1$. Now, for any other codeword $x \in C$ we write $x = (x^0|x^1)$, where $x^0 \in Res(C,c)$. Now, if $Res(C,c)$ is not a $(k-1)$-dimensional code, then we would have a non-zero codeword x in C with $x^0 = 0$. But then we would have in C that $wt(x - \lambda c) \leq \frac{w(q-1)}{q}$ for some $\lambda \in \mathbb{F}_q$. This contradicts that $w < \frac{dq}{q-1}$.

Now, we let $x \in C$ be such that $wt(x^0) = d^0$. Now for some $\lambda \in \mathbb{F}_q$. at least $\lceil \frac{w}{q} \rceil$ entries of x^1 are equal to λ. Thus this gives

$$d \leq w(x - \lambda c) \leq w - \left\lceil \frac{w}{q} \right\rceil + d^0$$

thus we get that the result holds as $d^0 \geq d - w + \left\lceil \frac{w}{q} \right\rceil$

This lemma leads us easily to the next bound.

Theorem 3.1.3 (Griesmer Bound cf. [11]) *Let C be a linear $[n, k, d]$-code over $\mathbb{F}_q$. Then we must have that $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$.*

Proof:
Now from the previous lemma, the residual code of a linear $[n, k, d]$-code, C, with respect to a word of weight d is a linear $[n-d, k-1, \lceil \frac{d}{q} \rceil]$-code call it C'. This tells us that

$$n - d = |C| - d \geq |C'|$$

Thus, we get that

$$n \geq \left\lceil \frac{d}{q^0} \right\rceil + |C'|$$

From this, we do the same process to $|C'|$. We pick a code word in C' of minimum distance and create the residual code of $|C'|$ with respect to this word and call it C''. So C'' is a linear $[n - d - \lceil \frac{d}{q} \rceil, k - 1 - 1, \lceil \frac{d}{q^2} \rceil]$-code. So using the previous lemma we get

$$|C'| - \left\lceil \frac{d}{q} \right\rceil \geq |C''|$$

This together with the first result gives us that

$$n \geq \left\lceil \frac{d}{q^0} \right\rceil + \left\lceil \frac{d}{q^1} \right\rceil + |C''|$$

Now if we use induction on the size of k (realizing that each time we do this, k decreases by 1) we can continue this process to each successive residual code to get the final desired result. Thus we have proven the Griesmer Bound.

The Singleton bound is a special case of the Griesmer bound. For our specific topic of MDS codes, the Singleton bound will prove to be more useful than the Griesmer bound. However, we do have one nice connection of a structure in projective spaces to the Griesmer bound so we have included it for that reason.

3.2 MDS Codes

We now can finally introduce MDS codes and prove a few things about them. As a reminder, we note that in this section we only discuss linear codes,

as results for non-linear codes are difficult to nicely connect to projective geometry.

Definition 3.2.1 *If C is a $[n, k, n-k+1]$-linear code, i.e. $d = n-k+1$ (Singleton Bound is met), then we call C a* **Maximum Distance Seperable code (or an MDS code)**.

Example 3.2.1 (Trivial Cases) *We demonstrate three trivial examples of MDS codes:*

1. *The vector space $\mathbb{F}_q^n$ itself forms a linear $[n, n, 1]$-MDS code. Note that $1 = n - n + 1$.*

2. *Over $\mathbb{F}_2$, we get a linear $[n, 1, n]$-MDS code. Note that $n = n - 1 + 1$. This is called the repetition code where the only word is the vector $(1, ..., 1)$.*

3. *For $n \geq 2$, we let the even weight code be given by*

$$C = \{c \in \mathbb{F}_2^n \mid wt(c) \equiv 0 \ (mod\ 2)\}.$$

   (Notice that the sum of two even weight words in $\mathbb{F}_2^n$ is again an even weight word). This code forms a linear $[n, n-1, 2]$-MDS code. We see that $2 = n - (n-1) + 1$.

These three examples are all trivial MDS codes. We would like to have a nice way of getting new, non-trivial MDS codes. It turns out that some structures in finite projective spaces actually give us a nice way to construct these non-trivial MDS codes. Before we see learn about this construction, we introduce a nice theorem that helps us work with and gives us more information about MDS codes.

Theorem 3.2.1 (cf. [14]) *If C is any $[n, k, d]$-linear code with corresponding generator matrix G and parity check matrix H, then the following are equivalent:*

1. *C is an MDS code.*

2. *Any $(n-k)$ columns of the parity check matrix H are linearly independent.*

3. *The dual code $C^{\perp}$ is an MDS code.*

4. *Any k columns of the generator matrix G are linearly independent.*

5. *Given any d coordinates, there is a codeword of minimum weight whose non-zero entries are in precisely these coordinates.*

Proof:
$1 \Leftrightarrow 2$, we use Theorem 3.1.1 and note that $d = n - k + 1$ so $d - 1 = n - k$.

$2 \Leftrightarrow 3$, Any $(n-k)$ columns of H are linearly independent. So we assume that $H = [I_{n-k}|A]$ where I is the $(n-k)$ identity matrix and A is a $(n-k) \times k$ matrix. From this, we assume that the codeword of minimum weight, c', occurs in H. Now, this implies that $wt(c') \leq k + 1$ (k entries from A and 1 entry from I). Now if $wt(c') \leq k$ then there is a column in A that will be linearly dependent with $n - k - 1$ columns of I (since it has a zero in some row spot). This contradicts that any $(n-k)$ columns are linearly independent. So $wt(c') = k + 1$. Thus $C^{\perp}$, which is generated by H is a linear $[n, n-k, k+1]$-code, thus $d = k + 1 = n - (n-k) + 1$ and so $C^{\perp}$ is MDS.

$3 \Leftrightarrow 4$, we note that $C^{\perp}$ being a linear MDS $[n, n-k, k+1]$-code implies that in its parity check matrix, any $n-(n-k)$ linearly independent columns. However, we know that the parity check matrix of $C^{\perp}$ is just the generator matrix G of C. Thus any k columns of G are linearly independent.

$2 \Leftrightarrow 5$, since H has any $(n-k)$ columns linearly independent, and the row space is of size $(n-k)$, it follows that any $(n-k+1)$ columns are linearly dependent. So for given any $d = n - k + 1$ coordinates, we take the corresponding columns of H, call them $v_1, ..., v_{n-k+1}$, and construct a word, c of C based on the linear dependence of $v_1, ..., v_{n-k+1}$. This word is in C since $cH^T = 0$. Thus we have a connection between the linear independence of $(n-k)$ columns and the codewords of C with minimum weight d.

With the theory of linear codes, especially MDS codes, in place, we finally get to connect geometry to codes.

4 From Geometry to Linear Codes

We have introduced projective geometries over finite fields and we have seen linear codes come from finite fields. As these two different ideas are linked by their underlying vector spaces, we expect to see some connections between the two. We now explain the relationship between finite geometry and MDS codes. Additionally, we will add some conjectures about further connections.

4.1 Results: Arcs to MDS Codes

Theorem 4.1.1 (cf. [2]) *For n and k positive integers. Then a linear MDS $[n, k, 4]$-code exists if and only if there exists an n-cap in $PG_{n-k-1}(2)$.*

Theorem 4.1.2 *An n-arc in $PG_{n-k-1}(q)$ defines a linear MDS $[n, k, n-k+1]$-code C.*

This theorem comes from [13], however a proof is not included. We include the following basic proof.
Proof:
Let K be an n-arc in $PG_{n-k-1}(q)$. Any point of the arc has the form $(x_0, x_1, ..., x_{n-k-1})$. If we take each point in the arc and make it a column in a matrix, H, then H clearly becomes a $(n-k) \times n$ matrix. This matrix becomes a parity check matrix for a code. Since the columns of H come from an n-arc, then we know that any $n-k-1+1 = n-k$ of them are linearly independent. Due to our theorem about MDS codes, this implies that C, the code defined by H, is an MDS code.

Corollary 4.1.1 *An n-arc in $PG_{k-1}(q)$ corresponds to a linear MDS $[n, n-k, k+1]$-code $C^{\perp}$.*

We see that in fact C and $C^{\perp}$ are dual codes.

We introduce some examples of how to construct an MDS code using the previous construction.

Example 4.1.1 *We consider the projective plane of order 2, i.e. $PG_2(2)$ also known as the Fano plane. This is just the set of non-zero vectors of $\mathbb{F}_2^3$. It is easy to see that the regular hyperoval of this space consists of the 4*

points $\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$. *We take these vectors and create a matrix* H *with columns equal to those vectors.*

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

This is then a parity check matrix for a linear MDS $[4,1,4]$*-code. This is just the repetition code as introduced before; however it still is an MDS code. The code* $C^{\perp}$ *generated by* H *is a linear MDS* $[4,3,2]$*-code which is the trivial even weight code introduced before.*

Example 4.1.2 *We consider the projective plane of order* 4*, i.e.* $PG_2(4)$*. From the definition, we see that this is the set of non-zero vectors of* $\mathbb{F}_4^2$ *where the elements of* $\mathbb{F}_4$ *are* $\{0,1,\omega,\omega^2\}$*. Then if we consider the o-polynomial* $f(t) = t^2$*, as we have seen, we get the regular hyperoval which turns out to be the* 6 *points*

$$\theta = \{(0,0,1),(0,1,0),(1,0,0),(1,1,1),(1,\omega,\omega^2),(1,\omega^2,\omega)\}$$

We again create a matrix H *with column set the same as the hyperoval:*

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 1 & 0 & 0 & 1 & \omega^2 & \omega \end{pmatrix}$$

This is then the parity check matrix for a linear MDS $[6,3,4]$*-code. This is a non-trivial MDS code, the first we have seen. We also see that the dual* $C^{\perp}$ *is a linear MDS* $[6,3,4]$*-code. This code has a special name, the Hexacode.*

We now turn to our last example which will use the Glynn 10-arc. We start with a brief description of the finite field of order 9.

Example 4.1.3 (MDS from Glynn's 10-arc) *We consider the projective space* $PG_4(9)$*. We construct* $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+x+2)$ *since the polynomial* $p(x) = (x^2+x+2)$ *is irreducible over* $\mathbb{F}_3$*. We prove this as there are no linear factors:* $p(0) = 2, p(1) = 1, p(2) = 2$*. The elements of* $\mathbb{F}_9$ *are the set*

$$\{0,1,2,\eta,\eta+1,\eta+2,2\eta,2\eta+1,2\eta+2\}$$

where $\eta^2 + \eta + 2 = 0$ *and* $\eta^4 = -1$. *We now also recall the Glynn* 10*-arc was a set* L *defined to be*

$$L = \{(1, t, t^2 + \eta t^6, t^3, t^4) |\ t \in \mathbb{F}_9\} \cup \{(0, 0, 0, 0, 1)\}$$

Using this we can explicitly construct 10 *points of the Glynn arc. We will show this explicity construction by placing the* 10 *points of* L *in a parity check matrix* H. *First, we note the following relationships hold due to the condtion that* η *satisfies:*

1. $\eta^2 = 2\eta + 1$
2. $\eta^3 = 2\eta + 2$
3. $\eta^4 = 2 = -1$
4. $\eta^6 = \eta + 2$

From here we put each point of L *as a column of* H *where* H *is then the following matrix:*

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 & \eta & \eta+1 & \eta+2 & 2\eta & 2\eta+1 & 2\eta+2 \\ 0 & 0 & \eta+1 & \eta+1 & 2 & 1 & 2\eta+2 & \eta+1 & 2\eta+2 & 1 \\ 0 & 0 & 1 & 2 & 2\eta+2 & 2\eta & 2\eta+1 & \eta+1 & \eta+2 & \eta \\ 1 & 0 & 1 & 1 & 2 & 2 & 1 & 2 & 1 & 2 \end{pmatrix}$$

So we see that this creates a linear MDS $[10, 5, 6]$*-code. This is a non-trivial MDS code. This gives a nice reason as to why new arcs are a desired object in projective spaces. With new arcs, we can attain new MDS codes.*

Before we move on to the basic questions and conjectures that are available for research, we return to our subject of minihypers and the Griesmer bound. While they do not connect to MDS codes, we do have a nice connection between the two and this connection leads to nice codes as well.

4.1.1 Minihypers and the Griesmer Bound

As a short aside, we continue with our brief discussion of minihypers. Though they do not lead to MDS codes, they do give nice codes in general. Since they are related to k-arcs, we introduce this nice connection here. Recall that ν_i is the number of points in a projective space of dimension i over specified q.

Theorem 4.1.3 (Hamada [10]) *For $k \geq 3$ and $1 \leq d < q^{k-1}$, there is a one-to-one correspondence between the set of all non-equivalent $[n, k, d]$-codes C over $\mathbb{F}_q$ meeting the Griesmer bound and the set of all $\{\nu_k - n, \nu_{k-1} - n + d; k - 1, q\}$-minihypers.*

4.2 Conjectures

So we have seen the connection between the study of linear MDS codes and certain structures, arcs and caps, of projective geometries. There are few results in this area, so much is left to conjectures and hypotheses. We introduce a few of the most important questions at this time. All of the following come from an article by Hill ([11]).

Question 1 *Are there any other $(q+1)$-arcs, q-odd, besides the 10-arc of Glynn, in $PG_n(q)$, for $2 < n \leq q - 2$ which is not a normal rational curve?*

The Glynn 10-arc leads us to believe that there must be others, as a single sporadic example does not seem plausible. However, no one has been able to find any other structures of this form.

Conjecture 1 *Suppose $2 \leq k \leq q$ and that $(q, k) \neq (2^h, 3)$ or $(2^h, 2^h - 1)$. Then there exists a linear MDS $[n, k, n - k + 1]$-code over $\mathbb{F}_q$ if and only if $n \leq q + 1$.*

This is basically a similar statement to $(q+1)$-arcs being the largest size of arcs in $PG_{n-k-1}(q)$ with the same restricions on q and k as above. We can formulate this conjecture in a manner that requires no knowledge of geometry and coding theory.

Conjecture 2 *How big can an $r \times s$ matrix over $\mathbb{F}_q$ be $(r, s \geq 2)$ such that any square sub-matrix is non-singular? The guess is:*

$$r + s \leq q + 1$$

unless $q = 2^h$ and $r = 3$ or $s = 3$.

According to Hill, [11] 1989, the smallest case still unresolved in the MDS codes conjecture is the case with $q = 13$ and $k = 6$ or 7.

5 Conclusion

We have been able to introduce and discuss a few of the many interesting structures in projective geometries. With this knowledge, we can continue to study in this area in hopes of finding new structures, larger k-arcs, or even more arcs like the Glynn arc that are not rational curves. The study of finite geometry is ever changing, and with more advances, we see more connections to other areas of combinatorics. Every time we learn more about geometry, we can in turn learn more about, and further advance the world of coding theory.
We have seen a nice connection between k-arcs and and MDS codes as well as shortly introduced the connection between minihypers and codes meeting the Griesmer bound. Many skeptics regard finite incidence geometry to be only a tool of pure mathematics that has no application. However, this nice application provides us with codes that meet the Singleton bound, and in turn have a maximal minimum distance. The study of these codes will then help us advance the world of coding theory and communication theory.
By linking geometry and coding theory, we again just show that there are usually many different ways to attack certain problems. Our main interest lies in finding solutions to problems in hopes of applying them in other areas. We hope that the paper has taught a basic introduction to the theory of finite geometries and coding theory. Additionally, we have added a few interesting open problems at the end in the hope to inspire further thought and advance in the connections between MDS codes and finite projective spaces.

We also note that for further reading in coding theory and finite projective geometries we recommend [17], [14], [21].

References

[1] Reinhold Baer. *Linear algebra and projective geometry*. Academic Press Inc., New York, N. Y., 1952.

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

[3] R. C. Bose. Mathematical theory of the symmetrical factorial design. *Sankhyā*, 8:107–166, 1947.

[4] Matthew Brown. (Hyper)ovals and ovoids in projective spaces, 2000. Socrates Intensive Course, Finite Geometry and its Applications.

[5] Peter J. Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, Cambridge, 1994.

[6] Peter Dembowski. *Finite geometries*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Reprint of the 1968 original.

[7] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[8] David G. Glynn. The nonclassical 10-arc of PG$(4, 9)$. *Discrete Math.*, 59(1-2):43–51, 1986.

[9] David G. Glynn. A condition for the existence of ovals in PG$(2, q), q$ even. *Geom. Dedicata*, 32(2):247–252, 1989.

[10] Noboru Hamada. A characterization of some $[n, k, d; q]$-codes meeting the Griesmer bound using a minihyper in a finite projective geometry. *Discrete Math.*, 116(1-3):229–268, 1993.

[11] R. Hill. Optimal linear codes. In *Cryptography and coding, II (Cirencester, 1989)*, volume 33 of *Inst. Math. Appl. Conf. Ser. New Ser.*, pages 75–104. Oxford Univ. Press, New York, 1992.

[12] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[13] J. W. P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces. *J. Statist. Plann. Inference*, 72(1-2):355–380, 1998. R. C. Bose Memorial Conference (Fort Collins, CO, 1995).

[14] W. Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[15] Maska Law. *Flocks, Generalised Quadrangles, and Translation Planes from BLT-sets*. PhD thesis, University of Western Australia, 2003.

[16] Christine M. O'Keefe and Tim Penttila. Polynomials for hyperovals of Desarguesian planes. *J. Austral. Math. Soc. Ser. A*, 51(3):436–447, 1991.

[17] Tim Pentilla and Maska Law. Flocks, ovals and generalised quadrangles, 2000. Four Lectures in Napoli, June 2000.

[18] B. Segre and U. Bartocci. Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.*, 18:423–449, 1971.

[19] Beniamino Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[20] Richard C. Singleton. Maximum distance q-nary codes. *IEEE Trans. Information Theory*, IT-10:116–118, 1964.

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

[22] Wolfgang Willems. *Codierungstheorie*. Walter de Gruyter, Inc., 1999.