HYPEROVALS AND CYCLOTOMIC SETS IN AG$(2, q)$

by

PHILIP A. DEORSEY

Doctor of Philosophy, University of Colorado Denver, 2015

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Applied Mathematics

2015

This thesis for the Doctor of Philosophy degree by

Philip A. DeOrsey

has been approved for the

Department of Mathematical and Statistical Sciences

by

William Cherowitzo, Advisor

Michael Ferrara, Chair

Stanley Payne

Tim Penttila

Jason Williford

April 22, 2015

DeOrsey, Philip A. (Ph.D., Applied Mathematics)

Hyperovals and Cyclotomic Sets in AG$(2, q)$

Thesis directed by Professor Emeritus William Cherowitzo

ABSTRACT

In this dissertation we introduce a new polynomial representation of hyperovals called a ρ-polynomial. The ρ-polynomial is defined in AG$(2, q)$ and uses a representation of the points of AG$(2, q)$ as elements of GF(q^2). We provide structural results of ρ-polynomials linking properties of their coefficients to specific maps that stabilize the represented hyperoval. Additionally, we provide a connection between ρ-polynomials and o-polynomials, and give nice ρ-polynomial representations for several families of hyperovals.

We also study the orbits of the field automorphisms of GF(q^2) which induce collineations in AG$(2, q)$. We call these orbits cyclotomic sets, and note that cyclotomic sets can be many different structures. We use cyclotomic arcs to build hyperovals, and perform searches for new hyperovals in affine planes of small order. We find no new hyperovals, but these searches classify ρ-polynomials with specific properties in certain affine planes.

In the final chapter we study other structures that appear as cyclotomic sets. We show that configurations can be represented and provide new results on configurations in order to determine when they can appear. We also provide a description of when a cyclotomic set represents each of the other structures they are known to represent.

The form and content of this abstract are approved. I recommend its publication.

Approved: William Cherowitzo

ACKNOWLEDGMENT

First and foremost I would like to thank my wife Tiffany for supporting me throughout this process. Completing my degree took many years of effort and struggle. You are always there to support and encourage me, keeping me level-headed and my eyes on the prize. Thank you Tiffany for your unconditional support and love, I could not have done any of this without you.

I must thank my advisor Bill Cherowitzo for sticking with me through the years. I know I am not the easiest Ph.D. student to advise but you stuck with me through it all. Your calm demeanor was a nice complement to my anxiousness, and helped keep me focused and less worried. You always kept me moving in the right direction with guidance and suggestions for what to do next. You have advised me in more than just my research, you have guided me in teaching, life, and more. Thank you for everything, Bill.

Thanks to the rest of my committee Jason, Mike, Stan, and Tim who gave me many guiding remarks and ideas that helped me finish everything. I have had many discussions with each of you over the years and I truly value each and every minute. Specifically I want to thank Mike Ferrara who had to deal with me more than most. Thanks for guiding me and always being there to discuss anything.

I would like to acknowledge Anton Betten who collaborated with me on much of the computational side of this research. Thank you for taking time out of your busy schedule to work with me.

I would be remiss if I did not mention my undergraduate advisor and friend Mark Miller who introduced me to finite geometry. Thank you Mark for your support and the introduction to such a beautiful side of mathematics.

Finally, thanks to my family, my parents Ken and Ellie, and my siblings Mike, Dave, Michelle, Paul, Maureen, and Lee. You all provided me with motivation without even knowing it. I always strive to make you all proud.

TABLE OF CONTENTS

FIGURES

Figure

TABLES

Table

1. Introduction and Background

1.1 Overview

The main focus of this work is to study a new representation of hyperovals that we call a ρ-polynomial. The ρ-polynomial is an extension of work done by Chris Fisher and Bernhard Schmidt where they use finite Fourier series to represent hyperovals. Hyperovals have traditionally been represented by polynomials called o-polynomials which have become increasingly complicated as new examples have been discovered. It has been over a decade since a new hyperoval has been discovered, which is long, considering hyperovals have only been studied significantly for 50 years. With this motivation we are in need of some new perspective for studying hyperovals, so we suggest the use of ρ-polynomials.

We study the structural properties of ρ-polynomials via their coefficients. Where Fisher and Schmidt looked for representations where many coefficients were 0, we consider hyperovals with coefficients in certain subfields, and with specific coefficients being 0. While studying ρ-polynomials one notices that if the coefficients of the polynomials have certain properties then that implies specific maps stabilize the hyperoval it represents. The orbits of these maps can be used as building blocks of hyperovals which leads to new and interesting searches for hyperovals. This approach has some precedent as it was used by O'Keefe and Penttila in [31], Penttila and Pinneri in [40], and Pentilla and Royle in [42]. We will discuss the results of these searches in affine planes of small order, and give ρ-polynomial representations for all of the known families of hyperovals in these planes. Further, we give ρ-polynomial representations for several families of hyperovals in all planes.

Among the actions that we are particularly interested in are the field automorphisms of $\mathrm{GF}(q^2)$ which induce collineations in $\mathrm{AG}(2,q)$. The orbits of these automorphisms are structures in $\mathrm{AG}(2,q)$ that we call cyclotomic sets. If these sets are arcs then we can use them to build hyperovals. However, as it turns out, they are not

always arcs. We found that these sets can represent other structures, including line segments and grids, but the more interesting configurations can arise. We determine when a cyclotomic set can be each of these different structures. In doing so, we obtain some new results on configurations.

1.2 Background on Finite Fields

A **finite field** is an algebraic structure with two operations called addition and multiplication. The **order** of a finite field is the number of elements in the field. Any finite field has order $q = p^h$ for some prime p and h a positive integer. We will use the notation $\mathrm{GF}(q)$ to denote the finite field of order q. The prime p is called the **characteristic** of the field; it is the least integer p for which $\sum_{j=1}^{p} 1 = 0$. The elements of $\mathrm{GF}(q)$ under addition form an abelian group, and the nonzero elements of $\mathrm{GF}(q)$, denoted $\mathrm{GF}(q)^*$, form a cyclic group under multiplication. A generator of the multiplicative group is called a **primitive** element of $\mathrm{GF}(q)$.

A **subfield** of $\mathrm{GF}(q)$ is a subset of the elements that is a field under the same operations. A subfield of $\mathrm{GF}(p^h)$ of order p^k exists if and only if $k \mid h$. The **prime subfield** of $\mathrm{GF}(p^h)$ is the intersection of all subfields, and is isomorphic to $\mathrm{GF}(p)$. Finite fields of order p^h exist for all primes p and all positive integers h. Furthermore, there is a unique field up to isomorphism of each order.

The group of automorphisms of $\mathrm{GF}(p^h)$ is generated by the map $\sigma : x \to x^p$, which is called the **Frobenius automorphism**. Hence, the group of automorphisms of $\mathrm{GF}(q)$ is $\mathrm{Aut}(\mathrm{GF}(q)) = \{\sigma : x \to x^{p^r} : 1 \leq r \leq h\}$.

A map that is of particular interest to us is the **relative trace map**. Let $F = \mathrm{GF}(q)$, $E = \mathrm{GF}(q^h)$, and $a \in E$. The relative trace map from E to F, $T_{E/F} : E \to F$ is defined as

$$T_{E/F}(a) = a + a^q + a^{q^2} + \cdots + a^{q^{h-1}}.$$

The relative trace map is additive and invariant under automorphisms, that is

- $T_{E/F}(a + b) = T_{E/F}(a) + T_{E/F}(b)$ for all $a, b \in E$, and

- $T_{E/F}(a^\sigma) = T_{E/F}(a)$ for all $a \in E$ and all $\sigma \in \mathrm{Aut}(E)$.

If F is the prime subfield of E then we call this map the **absolute trace map**. The absolute trace map is frequently used, so we reserve the notation tr to denote it. The relative trace map from $\mathrm{GF}(q^2)$ onto $\mathrm{GF}(q)$ will be frequently used, so we will denote this map simply as $T(x)$.

Definition 1.1 *The relative trace map from GF(q^2) to GF(q) is*

$$T(x) = x + x^q.$$

Another map we are interested in is the **relative norm map**. The relative norm map from E to F, $N_{E/F} : E \to F$ is defined as

$$N_{E/F}(a) = a^{1+q+q^2+\cdots+q^{h-1}} = a^{\frac{q^h-1}{q-1}}.$$

The elements whose image under the relative norm map is 1 are called **norm 1 elements**. The form of norm 1 elements is well known and is given in the next theorem.

Theorem 1.2 ([36]) *$N_{E/F}(a) = 1$ if and only if $a = b^{q-1}$ for some $b \in F$.*

We refer to [29] for more information on finite fields.

1.3 Background on PG$(2, q)$

There are finite projective spaces of dimension n for any $n \in \mathbb{Z}^+$, but the focus of this work will be on the 2-dimensional projective space called a projective plane. A **projective plane** is a point-line incidence structure that is defined by the following axioms.

1. Any two distinct points are connected by exactly one line.

2. Any two distinct lines meet at exactly one point.

3. There exists a set of four points no three of which are collinear.

The **order** of a projective plane is defined to be one less than the number of points on a line. In a projective plane of order q there are q^2+q+1 points, q^2+q+1 lines, $q+1$ points on every line, and $q+1$ lines through every point. The only known projective planes have order p^h where p is a prime, and $h \geq 1$ is an integer. It is still an open question as to whether projective planes of non-prime power order exist.

A projective plane of order q can be constructed as a 3-dimensional vector space over GF(q), the finite field with q elements. The points are the 1-dimensional subspaces, and the lines are the 2-dimensional subspaces. Incidence is set-theoretical containment. A projective plane constructed in this manner is denoted PG$(2, q)$. There are projective planes of order q that are not isomorphic to PG$(2, q)$ but we will not discuss them here, see [25] for more information. We often refer to the projective planes constructed in this manner as Desarguesian, since Desargues theorem holds in a projective plane if and only if it is isomorphic to one constructed in this way.

Theorem 1.3 (Desargues) *Two triangles are in perspective from a point if and only if they are in perspective from a line.*

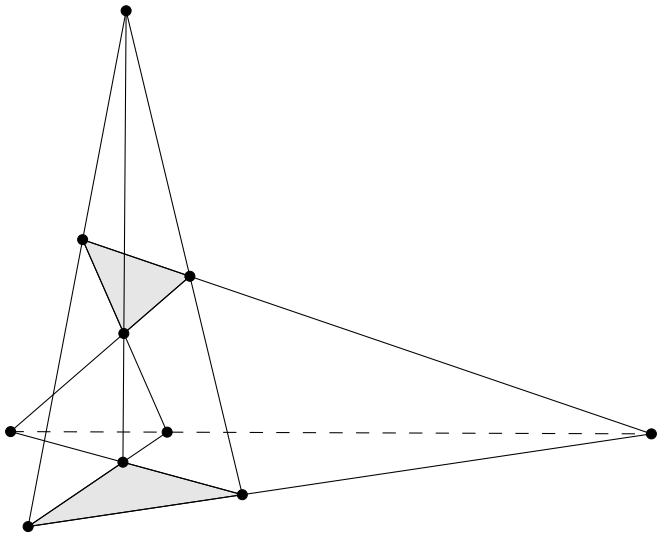


Figure 1.1: Desargues Configuration

This work is focused on a substructure of PG$(2, q)$ called AG$(2, q)$. AG$(2, q)$ is

the affine plane of order q, and can be constructed by removing any one line from $\mathrm{PG}(2,q)$ since all lines are projectively equivalent in $\mathrm{PG}(2,q)$. We denote the line removed as ℓ_∞. The points of $\mathrm{AG}(2,q)$ are the points of $\mathrm{PG}(2,q)$ not on ℓ_∞ and the lines of $\mathrm{AG}(2,q)$ are the lines of $\mathrm{PG}(2,q)$, except ℓ_∞, restricted to the points of $\mathrm{AG}(2,q)$.

A **collineation** is a one-to-one map from a projective plane onto itself that maps collinear points to collinear points. The set of all collineations of a plane is known as the **collineation group** of the plane. The collineation group of $\mathrm{PG}(2,q)$ is denoted $\mathrm{P\Gamma L}(3,q)$. There are two types of collineations in $\mathrm{PG}(2,q)$, homographies and automorphic collineations.

If A is a non-singular 3×3 matrix over $\mathrm{GF}(q)$, then the map $\sigma : \mathrm{PG}(2,q) \rightarrow \mathrm{PG}(2,q)$ defined by

$$(x,y,z) \rightarrow (x,y,z)A$$

is called a **homography**. If α is an automorphism of $\mathrm{GF}(q)$ then the map $\sigma_\alpha : \mathrm{PG}(2,q) \rightarrow \mathrm{PG}(2,q)$ defined by

$$(x,y,z) \rightarrow (x^\alpha, y^\alpha, z^\alpha)$$

is called an **automorphic collineation**. An important subgroup of $\mathrm{P\Gamma L}(3,q)$ is the subgroup consisting of all homographies, denoted $\mathrm{PGL}(3,q)$. The following theorem, known as the fundamental theorem of projective geometry, shows that any collineation is the product of the ones described above.

Theorem 1.4 (Fundamental Theorem of Projective Geometry) *Every collineation of PG(2, q) can be written as the product of a homography and an automorphic collineation.*

One fact that we will use frequently is that $\mathrm{P\Gamma L}(3,q)$ acts transitively on quadrangles, sets of four points, no three of which are collinear. That is, there exists a collineation mapping any quadrangle to any other quadrangle.

Theorem 1.5 ([9]) *Given two ordered quadrangles $A_1A_2A_3A_4$ and $B_1B_2B_3B_4$ of PG(2, q), there exists a unique homography σ with $\sigma(A_i) = B_i$, $1 \leq i \leq 4$.*

We refer to [4], [9], and [24] for more information on PG$(2, q)$.

1.4 Background on Hyperovals

We are interested in studying several structures that exist in projective planes, one of which is an arc. A **k-arc** in a projective plane is a set of k points, no three of which are collinear. It can be shown that $k \leq q + 2$ when q is even, and $k \leq q + 1$ when q is odd. A $(q + 1)$-arc is called a **oval** and a $(q + 2)$-arc is called a **hyperoval**.

Theorem 1.6 ([9]) *The maximum size of an arc in PG(2, q) is $q + 2$.*

Proof: Let A be an arc in PG(2,q) and P be a point on A. Since there are $q+1$ lines containing P, A can have at most one point from each of these lines. With the observation that the lines through P partition the plane we see that $|A| \leq q + 2$. ■

Theorem 1.7 ([9]) *When q is odd the maximum size of an arc in PG(2, q) is $q+1$.*

Proof: Assume to the contrary that A is an arc in PG(2,q), q odd and that $|A| = q + 2$. Let P be a point on A. Since there are $q + 1$ lines through P and there are $q+1$ other points on A each line through P must meet exactly one of these points. Hence, any line of the plane meets A in either 0 or 2 points. Now, let Q be a point not on A. The lines through Q must meet A in either 0 or 2 points, and they must partition A, hence $(q + 2)/2$ is an integer, implying q is even, a contradiction. ■

Theorem 1.8 ([9]) *In PG(2,q), q even, every oval is contained in a unique hyperoval.*

Proof: Let $\mathcal{O}$ be an oval in PG(2,q), q even, and let P be a point on $\mathcal{O}$. Since $\mathcal{O}$ has q points distinct from P, and there is a line joining P to each of these points, and $q + 1$ lines through P, there must be exactly one line tangent to $\mathcal{O}$ at P. Therefore, $\mathcal{O}$ has $q + 1$ tangent lines.

Now, let Q be a point not on $\mathcal{O}$. Since the lines through Q partition $\mathcal{O}$ and $q+1$ is odd, there must be at least one tangent line through Q. Let m be a secant line to $\mathcal{O}$ and say m meets $\mathcal{O}$ at P and R. We know that there is exactly one tangent line through P and R, and given $S \in m$, $S \neq P, R$ there is at least one tangent line through S. Each tangent line to $\mathcal{O}$ meets m in exactly one point, and since there are $q+1$ tangent lines there can be at most one tangent line at each point since each point on m sees at least one. Hence, on any secant line, there is exactly one tangent line through each point.

Let X be the intersection of two tangent lines to $\mathcal{O}$. Since X is on two tangent lines it cannot be on any secant lines. However, the lines through X partition $\mathcal{O}$, so every line through X is a tangent line. Therefore, adding X to A produces a set of $q+2$ points no three of which are collinear, making $A \cup \{X\}$ a hyperoval. ■

In order to discuss our next theorems we need another definition. A **conic** is a set of points satisfying an irreducible homogeneous quadratic equation. It is easily shown that conics are ovals, that is, they are a set of $q+1$ points, no three of which are collinear.

Theorem 1.9 *In PG(2, q), conics are ovals.*

Proof: We can verify that conics are ovals by observing that every conic is projectively equivalent to the set of points $\{(t, t^2, 1) : t \in \mathbb{F}_q\} \cup \{(0, 1, 0)\}$.

If we let $a, b, c \in \mathbb{F}_q$ and consider the matrix

$$\begin{pmatrix} a & a^2 & 1 \\ b & b^2 & 1 \\ c & c^2 & 1 \end{pmatrix}.$$

It is a nonsingular Vandermonde matrix and so has nonzero determinant provided a, b, and c are distinct. Hence we must only check that $(0, 1, 0)$ is not part of any collinear triple. The matrix

$$\begin{pmatrix} a & a^2 & 1 \\ b & b^2 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

has determinant $b - a \neq 0$ provided $a \neq b$. Thus a conic is a set of $q + 1$ points no three of which are collinear. ■

A famous theorem of B. Segre gives the converse of Theorem 1.9 for q odd, that is, in PG$(2, q)$, q odd, all ovals are conics.

Theorem 1.10 (Segre's Theorem [47]) *In PG(2, q), q odd, all ovals are conics.*

Due to Segre's theorem all ovals in PG$(2, q)$, q odd, are classified. Thus, we restrict our attention to the case where q is even, that is, $q = 2^h$.

We may assume that a hyperoval contains the **fundamental quadrangle** $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 1)$, since, by Theorem 1.5, any hyperoval is projectively equivalent to one containing these four points. In [24] it is shown that any hyperoval containing the fundamental quadrangle can be represented by a permutation polynomial.

Theorem 1.11 *Any hyperoval $\mathcal{H}$ in PG(2, q) with $q = 2^h$, $h > 1$, containing the fundamental quadrangle can be represented as*

$$D(f) = \{(t, f(t), 1) : t \in GF(q)\} \cup \{(1, 0, 0), (0, 1, 0)\}$$

where f is a permutation polynomial of degree at most $q - 2$ with $f(0) = 0$ and $f(1) = 1$.

If $D(f)$, as described above, gives a hyperoval we say that f is an **o-polynomial**. The use of o-polynomials gives a compact and usable form for hyperovals, so they have been the traditional way of describing hyperovals. A representative list of o-polynomials for known families of hyperovals is given in Table 1.1.

1.5 A History of Hyperovals

Signficant study of hyperovals dates back to the late 1950's to a paper by Lunelli and Sce [30] in which they use a computer to search for complete arcs in PG(2,16) as suggested by B. Segre. Their search yielded one hyperoval, up to projective equivalence, that was not a conic. This hyperoval is now known as the Lunelli-Sce hyperoval and can be described by the o-polynomial

$$f(t) = t^{12} + t^{10} + \eta^{11}t^8 + t^6 + \eta^2 t^4 + \eta^9 t^2,$$

where η is a primitive element of GF(16) satisfying $\eta^4 = \eta + 1$.

Table 1.1: o-polynomials for known hyperovals

Name	o-polynomial	Field Restriction
Hyperconic [24]	$f(t) = t^2$	None
Translation [46]	$f(t) = t^{2^i}$ $(i,h) = 1$	None
Segre [2]	$f(t) = t^6$	h odd
Glynn 1 [19]	$f(t) = t^{3\sigma+4}$	h odd
Glynn 2 [19]	$f(t) = t^{\sigma+\gamma}$	h odd
Payne [35]	$f(t) = t^{1/6} + t^{1/2} + t^{5/6}$	h odd
Cherowitzo [10]	$f(t) = t^\sigma + t^{\sigma+2} + t^{3\sigma+4}$	h odd
Subiaco [15]	See Below	None
Adelaide [14]	See Below	h even
O'Keefe-Penttila [31]	See Below	PG(2,32)
	$\gamma^4 \equiv \sigma^2 \equiv 2 \pmod{2^h - 1}$	

Subiaco An o-polynomial for some of the Subiaco hyperovals is

$$f(t) = \frac{d^2t^4 + d^2(1+d+d^2)t^3 + d^2(1+d+d^2)t^2 + d^2t}{t^4 + d^2t^2 + 1} + t^{\frac{1}{2}}$$

where tr(1/d) = 1. There is one hyperoval, up to projective equivalence, in the Subiaco family if $h \not\equiv 2 \pmod 4$ and two hyperovals if $h \equiv 2 \pmod 4$. The above

polynomial gives one of the hyperovals when $h \equiv 2 \pmod 4$ and the other can be represented with o-polynomial

$$f(t) = \frac{d^2t^4 + d^5t^3 + d^2t^2 + d^3t}{(t^2 + dt + 1)^2} + \left(\frac{t}{d}\right)^{\frac{1}{2}},$$

where β is an element of multiplicative order $q+1$ in $\mathrm{GF}(q^2)$ and $d = \beta + \beta^q$. We also note that 3 different automorphism groups appear among the Subiaco hyperovals.

Adelaide An o-polynomial for the Adelaide hyperoval is

$$f(t) = \frac{T(b^m)}{T(b)}(t+1) + \frac{T((bt+b^q)^m)}{T(b)}(t + T(b)t^{1/2} + 1)^{1-m} + t^{1/2},$$

where $T(x) = x + x^q$, $b \in \mathrm{GF}(q^2)$, $b \neq 1$, $b^{q+1} = 1$ and $m = \pm\frac{q-1}{3}$.

O'Keefe-Penttila An o-polynomial for the O'Keefe-Penttila hyperoval is

$$f(t) = t^4 + t^{16} + t^{28} + \eta^{11}(t^6 + t^{10} + t^{14} + t^{18} + t^{22} + t^{26}) + \eta^{20}(t^8 + t^{20}) + \eta^6(t^{12} + t^{24}),$$

where η is a primitive element of $\mathrm{GF}(32)$ satisfying $\eta^5 = \eta^2 + 1$.

The Lunelli-Sce hyperoval does not appear in Table 1.1 as it was shown to be in the Subiaco family in [15] and in the Adelaide family in [14]. For more information on the Lunelli-Sce hyperoval see [7].

In 1962, shortly after the work by Lunelli and Sce, B. Segre gave the translation and Segre hyperovals in [46]. These hyperovals remained the only known hyperovals for over 20 years until Glynn gave two new families in [19]. The Glynn hyperovals were yet more examples of what are called **monomial hyperovals**, that is hyperovals that can be represented by monomial o-polynomials. These remain the only known examples of monomial hyperovals.

The 1980's saw a surge in new families of hyperovals with Payne giving a new family in [35] and Cherowitzo providing examples of a new family in [11]. The Cherowitzo hyperovals were proved to be a family in 1998 [10]. The time between the discovery of the first examples of the Cherowitzo hyperovals and the proof of their inclusion in an infinite family was over a decade and new techniques had to be developed to prove the

existence of the family. The specific technique was the use of an algebraic structure called a q-clan which has since been used often in the study of hyperovals. We will not discuss q-clans here, but we refer the reader to [8] for information on q-clans. The use of innovative techniques is not uncommon when studying hyperovals which shows the need for many techniques.

The early 1990's saw yet another surge in the discovery of hyperovals. New examples of hyperovals were found by O'Keefe and Penttila in 1992 [31], as well as Penttila and Pinneri in 1994 [40]. The hyperoval found by O'Keefe and Penttila, known as the O'Keefe-Penttila hyperoval, lives in PG(2,32) and is the only known sporadic hyperoval, that is, a hyperoval not known to be a member of an infinite family. The examples found by Penttila and Pinneri in PG(2,64) were the first distinct examples of Subiaco hyperovals. In 1995 Penntila and Royle [42] found more example of Subiaco hyperovals in PG(2,128) and PG(2,256) as well as the first examples of the Adelaide hyperoval in PG(2,64) and PG(2,256). The Subiaco hyperovals were proved to be an infinite family in 1996 by Cherowitzo, Penttila, Pinneri, and Royle [15]. However, the proof that the Adelaide hyperovals lived in an infinite family took 8 years from their initial discovery, finally being shown in 2003 [14]. Since 2003 no new hyperovals have been discovered. The most notable paper on hyperovals for us since 2003 came from Fisher and Schmidt in 2006. They presented a paper ([17]) that unified the Payne and Adelaide families and provides the basis for this thesis.

However, there has been some work done on the study of monomial hyperovals. We say a monomial hyperoval $\mathcal{H}$ is a **k-bit monomial hyperoval** if an o-polynomial for $\mathcal{H}$ is $f(t) = t^n$ and there are k 1's in the binary representation for n. The 1-bit monomial hyperovals are precisely the translation hyperovals. The 2-bit monomial hyperovals were classified in 1998 [16], and the 3-bit monomial hyperovals were classified in 2010 [51]. The following theorem was also given by Hernando and McGuire in 2012.

Theorem 1.12 ([23]) *For any fixed even positive integer k, if $k \neq 6$ and $k \neq 2^i$ then the set $D(x^k)$ is a hyperoval in PG$(2, q)$ for at most a finite number of values of q.*

The collection of these results suggests that there are no more monomial hyperovals. Combining this information with the o-polynomials of the most recently discovered hyperovals makes us expect that new hyperovals will have increasingly complicated o-polynomials, providing even more motivation for this thesis.

The automorphism groups of hyperovals have played an important role in their study. Historically hyperovals have been identified by their groups. When a new hyperoval was found, it was shown to be distinct from previously known families via its automorphism group, and its existence in different planes. Table 1.2 shows the sizes of the automorphism groups for all known families of hyperovals.

Hyperovals are currently classified in PG$(2, 2^h)$ for $1 \leq h \leq 5$, and hyperovals with nontrivial automorphism group are classified in PG$(2, 64)$. It is well known that all hyperovals in PG$(2, 2^h)$ for $1 \leq h \leq 3$ are hyperconics. See [24] for a proof of this classification. Hyperovals in PG(2,16) were originally classified by Hall in 1975 [22]. All hyperovals in PG(2,16) are projectively equivalent to the hyperoconic, or the Lunelli-Sce hyperoval described above. In order to classify hyperovals in this plane Hall needed the help of a computer, however in 1991 O'Keefe and Penttila [32] classified the hyperovals in PG(2,16) without the aid of a computer.

In 1994 the hyperovals in PG(2,32) were classified by Penttila and Royle by exhaustive computer search [41]. Every hyperoval in PG(2,32) is projectively equivalent to either the hyperconic, translation, Segre, Payne, Cherowitzo, or O'Keefe-Penttila hyperoval. Penttila and Royle are also responsible for the partial classification of hyperovals in PG(2,64). They showed that if a new hyperoval exists in PG(2,64) then it must have a trivial automorphism group in [42]. They use a technique known as "prime at at time" that we discuss in Chapter 3. It is generally believed that there are no other hyperovals in PG(2,64), as a hyperoval with a trivial automorphism group

would have many equivalent copies and should appear in a random search.

Table 1.2: The groups of known hyperovals

Hyperoval $\mathcal{H}$	$\lvert\mathrm{Aut}(\mathcal{H})\rvert$	Field Restriction
Hyperconic [24]	$(q+2)(q+1)q(q-1)h$	$q = 2, 4$
Hyperconic [24]	$(q+1)q(q-1)h$	$q \geq 8$
Translation [24]	$q(q-1)h$	
Segre [33]	$3(q-1)h$	$q = 32$
Segre [33]	$(q-1)h$	$q \geq 128$
Glynn 1 [33]	$(q-1)h$	
Glynn 2 [33]	$3(q-1)h$	$q = 128$
Glynn 2 [33]	$(q-1)h$	$q > 128$
Payne [50]	$2h$	
Cherowitzo [34]	h	
Subiaco [34]	$2h$	$h \not\equiv 2 \pmod 4$
Subiaco [39]	$10h$	$h \equiv 2 \pmod 4$
Subiaco [39]	$\frac{5h}{2}$	$h \equiv 2 \pmod 4$
Adelaide [38]	$2h$	$q \geq 64$
Lunelli-Sce [37]	$(q+2)2h$	$q = 16$
O'Keefe-Penttila [31]	3	$q = 32$

2. The ρ-polynomial Representation

In this chapter we describe an extension of the work of Fisher and Schmidt that we call a ρ-polynomial. First we describe the polar model of $\mathrm{AG}(2,q)$, giving a description of lines and incidence in the plane, followed by a collection of collineations in the polar model. Next, we introduce ρ-polynomials and discuss how to use them to represent hyperovals. Furthermore, we will discuss the structural properties of ρ-polynomials, their relationship to o-polynomials, and give some nice ρ-polynomial representations of several families of hyperovals.

2.1 A Description of the Polar Model

For the remainder of this thesis we will be assuming that $q = 2^h$, with h an integer ≥ 1. We shall represent the points of $\mathrm{AG}(2,q)$ by elements of $\mathrm{GF}(q^2)$. To do this we select an irreducible polynomial of the form $x^2 + x + \delta$, for some $\delta \in \mathrm{GF}(q)$, and let i be a root of this polynomial in $\mathrm{GF}(q^2)$. Irreducible polynomials of this form exist, in fact, δ can be chosen to be any element of absolute trace 1 [24]. We note that $i^q = i + 1$ since the other root of $x^2 + x + \delta$ is $i + 1$. The image of i under the action of the field automorphisms is given in Lemma 2.8. Having chosen i, we associate the point (x, y) of $\mathrm{AG}(2,q)$ with the element $x + iy$ in $\mathrm{GF}(q^2)$. In analogy with complex number representations, we refer to y in $z = x + iy$ as the imaginary part of z, and x as the real part. Observe that both x and y are elements of $\mathrm{GF}(q)$. The following well-known lemma is of considerable use.

Lemma 2.1 *The elements $\alpha, \beta, \gamma \in GF(q^2)$, when thought of as points of $AG(2,q)$, are collinear if and only if $\alpha\beta^q + \beta\gamma^q + \gamma\alpha^q \in GF(q)$.*

Proof: Let $\alpha = A + iB$, $\beta = C + iD$, and $\gamma = E + iF$. Substituting these values shows that the imaginary part of $\alpha\beta^q + \beta\gamma^q + \gamma\alpha^q$ is $BC + AD + DE + CF + FA + EB$. However, these points are collinear if and only if

$$\begin{vmatrix} A & B & 1 \\ C & D & 1 \\ E & F & 1 \end{vmatrix} = 0$$

This determinant is precisely $BC + AD + DE + CF + FA + EB$, forcing $\alpha\beta^q + \beta\gamma^q + \gamma\alpha^q \in GF(q)$. ∎

This lemma gives us a polynomial representation for the line connecting any two points.

Corollary 2.2 *The q points on the line joining α, $\beta \in GF(q^2)$ are solutions to the equation*

$$(\alpha + \beta)x^q + (\alpha + \beta)^q x + \alpha\beta^q + \alpha^q\beta = 0. \tag{2.1}$$

A description of lines in this representation is known and can be seen in [1] and [26]. They provide a description of hyperplanes in $\mathrm{AG}(n, q)$, and so, a description of lines in $\mathrm{AG}(2, q)$. For completeness, we give our own proof of such a description of lines. We will let $\mathcal{N}$ denote the group of $q+1^{st}$ roots of unity in $\mathrm{GF}(q^2)$, the elements of norm 1.

Lemma 2.3 *Any line in $AG(2, q)$, whose points are thought of as elements in $GF(q^2)$, consists of the set,*

$$L(\eta, \lambda) = \{x \in GF(q^2) \mid T_\eta(x) = \lambda\},$$

where $T_\eta(x) = (\eta x)^q + \eta x$ for some $\eta \in \mathcal{N}$ and a fixed $\lambda \in GF(q)$.

Proof: Let α and β be any two distinct elements of $\mathrm{GF}(q^2)$. By Corollary 2.2 the points on the line ℓ joining α and β are solutions to (2.1). Rearranging the terms yields

$$T((\alpha + \beta)^q x) = T(\alpha\beta^q).$$

Thus, the solutions to (2.1) satisfy $T_{(\alpha+\beta)^q}(x) = T(\alpha\beta^q)$. We will now show that given the line ℓ joining α and β we can always find $\gamma, \nu \in \ell$ such that $(\gamma+\nu)^q \in \mathcal{N}$. Observe that $\alpha(s + 1) + \beta s$ is a solution to (2.1) for every $s \in \mathrm{GF}(q)$. As this represents q solutions, every root will have this form. Let

$$\gamma = \alpha(\tau + 1) + \beta\tau,$$

$$\nu = \alpha(s+1) + \beta s$$

be points on ℓ where $s, \tau \in GF(q)$ and $s + \tau = \sqrt{\frac{1}{(\alpha+\beta)^{q+1}}}$. Notice $(\alpha+\beta)^{q+1}$ is in GF(q) since the $q+1^{st}$ power of any element of GF(q^2) is in GF(q), so consequently $\sqrt{\frac{1}{(\alpha+\beta)^{q+1}}} \in$ GF(q). Then,

$$(\gamma+\nu)^{q+1} = ((\alpha+\beta)(s+\tau))^{q+1} = ((\alpha+\beta)^{q+1}(s+\tau)^2) = 1. \tag{2.2}$$

Thus, $\gamma, \nu \in \ell$ and $(\gamma+\nu) \in \mathcal{N}$ which implies $(\gamma+\nu)^q \in \mathcal{N}$, since $\mathcal{N}$ is a multiplicative subgroup of the nonzero elements of GF(q^2).

We will now prove the converse. Assume that $u, v, w \in GF(q^2)$ and $T_\eta(u) = T_\eta(v) = T_\eta(w) = z$, for some $\eta \in GF(q^2)$. Observe that

$$u^q = \eta^{-q}z + \eta^{1-q}u; \quad v^q = \eta^{-q}z + \eta^{1-q}v; \quad w^q = \eta^{-q}z + \eta^{1-q}w$$

and further

$$(u+v)^q = (\eta^{-q}z + \eta^{1-q}u) + (\eta^{-q}z + \eta^{1-q}v) = \eta^{1-q}(u+v).$$

With these observations it is an elementary calculation to show that

$$(u+v)w^q + (u+v)^q w + u^q v + v^q u = 0.$$

Hence u, v, w are collinear by Corollary 2.2. Observe that we have shown this result for general η, so it holds for $\eta \in \mathcal{N}$. ■

Corollary 2.4 *The line $L(\eta, \lambda)$ connecting two points $\alpha, \beta \in GF(q^2)$ is determined uniquely by η and λ, where $\eta = \sqrt{(\alpha+\beta)^{q-1}} \in \mathcal{N}$ and $\lambda = T_\eta(\alpha) = T_\eta(\beta)$.*

Proof: Let ℓ be the line connecting points α and β. From Lemma 2.3 there exists $\eta \in \mathcal{N}$ for which $T_\eta(\alpha) = T_\eta(\beta) = \lambda$. This implies that $(\eta(\alpha+\beta))^q = \eta(\alpha+\beta)$ and so $\eta = \sqrt{(\alpha+\beta)^{q-1}}$. This must be the unique value of η since for any points $\gamma, \nu \in \ell$, such that $\gamma + \nu \in \mathcal{N}$, and $\gamma = \alpha(\tau+1) + \beta\tau$, $\nu = \alpha(s+1) + \beta s$ as in Lemma 2.3, we

have $(\gamma+\nu)^{q+1} = ((\alpha+\beta)(s+\tau))^{q+1} = 1$. Thus

$$s+\tau = \sqrt{\frac{1}{(\alpha+\beta)^{q+1}}}.$$

Hence,

$$\gamma+\nu = (\alpha+\beta)(s+\tau) = \sqrt{\frac{1}{(\alpha+\beta)^{q-1}}},$$

and so $(\gamma+\nu)^q = \sqrt{(\alpha+\beta)^{q-1}}$ as desired. ∎

Following Fisher and Schmidt [17], we want to decompose the elements of GF(q^2) into what we call their *polar coordinates*. Observe that $\mathcal{N}$ is a cyclic group so we may assume that $\mathcal{N}$ is generated by η, and let α generate the cyclic multiplicative group GF(q)* inside GF(q^2).

Lemma 2.5 *Every non-zero element β of GF(q^2) can be decomposed uniquely as the product of a $q+1^{st}$ root of unity times a non-zero element of GF(q), that is $\beta = \eta^k\alpha^j$ for $0 \le k \le q$ and $0 \le j \le q-2$.*

Proof: Let η generate the cyclic group $\mathcal{N}$ and let α generate the cyclic group GF(q)*. There are q^2-1 products of the form $\eta^k\alpha^j$ for $0 \le k \le q$ and $0 \le j \le q-2$, each of which is an element of GF(q^2)*. We will show that each of these products is distinct, proving every element of GF(q^2)* has a unique decomposition. Assume that $\eta^r\alpha^s = \eta^t\alpha^u$ so that $(\eta^r\alpha^s)^{q-1} = (\eta^t\alpha^u)^{q-1}$ which implies $(\eta^t+\eta^r)^2 = 0$ since q is even. Hence $r = t$ and so necessarily $s = u$. Therefore each product is unique, and every non-zero element β of GF(q^2) can be decomposed uniquely as the product of a $q+1^{st}$ root of unity and a non-zero element of GF(q). ∎

In analogy with polar coordinates of $\mathbb{R}^2$, we shall think of η as representing an "angle", and α representing a "radius", with all points centered around 0. This coordinatization is represented in Figure 2.1.

In the sequel we shall refer to elements of GF(q^2) as points in AG$(2,q)$ without explicitly mentioning the equivalence. Using Lemma 2.3 we easily see that the lines

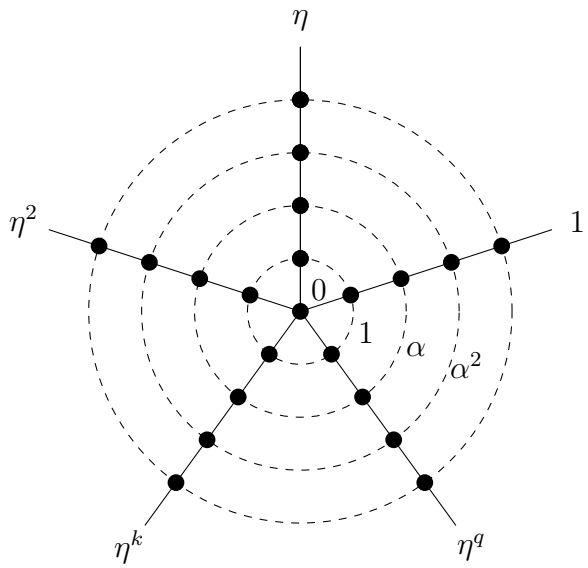


Figure 2.1: The Polar Representation of AG(2,q)

through 0 consist of points in GF(q^2) with the same $q+1^{st}$ root of unity in their polar decomposition. We will refer to sets of points of the form $\{\alpha\eta^j : 0 \leq j \leq q\}$, for fixed $\alpha \in \mathrm{GF}(q)^*$, as a **tier**. Tiers are represented as dashed lines in Figure 2.1, and we will see later that each tier is a conic.

2.2 Collineations in the Polar Model

In this section we will study some collineations in the polar model. The fundamental theorem of projective geometry gives a complete description of collineations in the traditional Cartesian model of the plane, and our goal is to describe some collineations in the polar model that will help with later results.

Lemma 2.6 *Let $\alpha \in GF(q^2)$, $0 \neq \beta \in GF(q^2)$ and consider the points of $AG(2,q)$ as elements of $GF(q^2)$. The action $x \to \beta x + \alpha$ defines a collineation in $AG(2,q)$.*

Proof: Let x, y, z be three collinear points in AG$(2,q)$ represented as elements of GF(q^2). By Lemma 2.1 we have $xy^q + yz^q + zx^q \in \mathrm{GF}(q)$. Consider the points $\beta x+\alpha$, $\beta y + \alpha$, $\beta z + \alpha$ for some $\beta \in \mathrm{GF}(q^2)^*$ and $\alpha \in \mathrm{GF}(q^2)$ and calculate

$$(\beta x + \alpha)(\beta y + \alpha)^q + (\beta y + \alpha)(\beta z + \alpha)^q + (\beta z + \alpha)(\beta x + \alpha)^q$$

$$= \beta^{q+1}(xy^q + yz^q + zx^q) + T(\alpha\beta x) + T(\alpha\beta y) + T(\alpha\beta z) + \alpha^{q+1}.$$

Each of the quantities in the sum is an element of GF(q), so the sum is in GF(q). Hence, the points $\beta x + \alpha$, $\beta y + \alpha$, $\beta z + \alpha$ are collinear by Lemma 2.1. Therefore, the action $x \to \beta x + \alpha$ defines a collineation in AG$(2, q)$ when points are thought of as elements of GF(q^2). ∎

We also know that the field automorphisms of GF(q^2) induce collineations in this model of AG$(2, q)$. However, we wish to note that these are different from the automorphic collineations of AG$(2, q)$ in the Cartesian model, which are the collineations of the form $(x, y) \to (x^\sigma, y^\sigma)$ for some $\sigma \in$ AUT(GF(q)).

Lemma 2.7 *Let $\sigma \in$ Aut(GF(q^2)) and consider the points of AG$(2, q)$ as elements of GF(q^2). The action $x \to x^\sigma$ defines a collineation in AG$(2, q)$.*

Proof: Let x, y, z be three collinear points in AG$(2, q)$ represented as elements of GF(q^2). By Lemma 2.1 we have $xy^q + yz^q + zx^q \in$ GF(q). Consider the points $x^\sigma, y^\sigma, z^\sigma \in$ GF(q^2). Since $\sigma \in$ Aut(GF(q^2)) we have

$$x^\sigma(y^\sigma)^q + y^\sigma(z^\sigma)^q + z^\sigma(x^\sigma)^q = (xy^q + yz^q + zx^q)^\sigma \in \text{GF}(q).$$

Hence, the points $x^\sigma, y^\sigma, z^\sigma$ are collinear by Lemma 2.1. Therefore the action $x \to x^\sigma$ defines a collineation in AG$(2, q)$ where points are elements of GF(q^2). ∎

The traditional form of the collineations defined by the automorphisms of GF(q^2) is easily computed and will give insight into the connection between the polar model and previous methods used to study hyperovals. In order to determine their form we need a preliminary result.

Lemma 2.8 *If i is a root of the irreducible polynomial $x^2 + x + \delta$ where $\delta \in$ GF(q) then*

$$i^{2^k} = i + \sum_{j=0}^{k-1} \delta^{2^j}.$$

Proof: Observe that $i^2 = i + \delta$. We proceed by induction. Assume that

$$i^{2^k} = i + \sum_{j=0}^{k-1} \delta^{2^j}$$

then

$$i^{2^{k+1}} = (i^{2^k})^2 = \left(i + \sum_{j=0}^{k-1} \delta^{2^j} \right)^2 = i + \sum_{j=0}^{k} \delta^{2^j}.$$

Therefore, the result holds by induction. ∎

Lemma 2.9 *The collineation defined by the automorphism $\sigma : x \to x^{2^k}$ of GF(q^2) is equivalent to the collineation defined by*

$$(x, y, z) \to (x^\sigma, y^\sigma, z^\sigma) \begin{pmatrix} 1\,0\,0 \\ s\,1\,0 \\ 0\,0\,1 \end{pmatrix} = (x^\sigma + sy^\sigma, y^\sigma, z^\sigma)$$

where $s = \sum_{j=0}^{k-1} \delta^{2^j}$ when points are thought of as coordinate triples (x, y, z).

Proof: The map σ sends $x + iy \to (x + iy)^\sigma = x^\sigma + \sum_{j=0}^{k-1} \delta^{2^j} y^\sigma + iy^\sigma$. The pre-image of this point under the map $(x, y, 1) \to x + iy$ is $(x^\sigma + \sum_{j=0}^{k-1} \delta^{2^j} y^\sigma, y^\sigma, 1)$, proving the result. ∎

There are also some collineations that preserve the polar model that were given by O'Keefe and Penttila in [33], see Lemma 3.2.

Lemma 2.10 ([33]) *Let J be a cyclic subgroup of order $q + 1$ of PGL(3,q), q even. Suppose that J fixes a point and fixes a line not on the point. Then the orbits of J on the points of PG($2, q$) are the fixed point, the fixed line, and $q - 1$ non-degenerate conics.*

O'Keefe and Penttila also give a specific subgroup that fixes the point $(0, 0, 1)$ and the line $z = 0$ and has $q - 1$ non-degenerate conics as orbits. That is, they give a group that preserves the polar model as visualized in Figure 2.1. Their group is as follows, as quoted from [33].

Consider the following pencil of conics:

$$\lambda(x^2 + ax + y^2) + \mu z^2 = 0$$

for $\lambda, \mu \in \mathrm{GF}(q)$, not both zero, and where $x^2 + ax + 1$ is irreducible over $\mathrm{GF}(q)$. The (degenerate) conic give by $\mu = 0$ is the point $(0, 0, 1)$ and the (degenerate) conic given by $\lambda = 0$ is the line $z = 0$. The other $q - 1$ conics of the pencil are non-degenerate. The $q + 1$ conics of the pencil are pairwise disjoint and cover $\mathrm{PG}(2, q)$.

Let F be the following set of homographies:

$$F = \left\{ \begin{pmatrix} f & g & 0 \\ g & f + ag & 0 \\ 0 & 0 & 1 \end{pmatrix} : f, g \in \mathrm{GF}(q), \text{ not both zero} \right\}.$$

A conic of the pencil is fixed by an element of F provided the matrix has determinant $f^2 + afg + g^2 = 1$.

O'Keefe and Penttila note that F is a cyclic subgroup of order $q^2 - 1$ of $\mathrm{GL}(3, q)$, but when restricted to those matrices with determinant 1, it gives rise to a cyclic subgroup of order $q + 1$ of $\mathrm{PGL}(3, q)$. Hence this group realizes Lemma 2.10. The orbits of this group are the origin, ℓ_∞, and the $q - 1$ tiers from the polar model. Note that the full group stabilizes the model but interchanges the tiers.

2.3 Using ρ-polynomials to Represent Hyperovals

In 2006 Fisher and Schmidt proposed a method of representing hyperovals using finite Fourier series. To use their method one must have a hyperoval in the affine plane containing $(0, 0, 1)$, and represent points as elements of $\mathrm{GF}(q^2)$ as described above. Specifically they use the polar decomposition of points described in Lemma 2.5. Once the hyperoval points are represented as elements of $\mathrm{GF}(q^2)$ they assign an ordering to the nonzero points and represent them using ordered linear combinations

of elements in the set $\mathcal{N} = \{1, \eta, ..., \eta^q\}$. Such an ordered linear combination, as seen in (2.3), is called a **finite Fourier series**. Fischer and Schmidt gave the formula

$$p_j = \sum_{k=0}^{q} \alpha_k \eta^{jk} \tag{2.3}$$

where p_j denotes the j^{th} hyperoval point of a fixed ordering. It is important to note that the ordering of the points plays a crucial role in this representation of hyperovals. Fisher and Schmidt wanted to analyze the coefficients α_k and give necessary and sufficient conditions for a given set of coefficients to produce a hyperoval.

In [17] they search for hyperovals in small planes with a Fourier series representation with at most three nonzero coefficients. They found one that was not a conic, given in the next theorem.

Theorem 2.11 ([17]) *The point set* $\mathcal{O}_0 = \{\eta^j + \eta^{3j} + \eta^{-3j} : 0 \leq j \leq 2^h\}$ *is an oval of* $AG(2, 2^h)$ *whose nucleus is the origin.*

They were also able to identify this hyperoval and in doing so they paired two families of hyperovals that were previously thought to be unrelated.

Theorem 2.12 ([17]) *In* $AG(2, 2^h)$*, the hyperoval* $\mathcal{O}_0 \cup \{0\}$ *is the Payne hyperoval when* h *is odd and the Adelaide hyperoval when* h *is even.*

Their work gives an elegant representation for the Adelaide hyperoval. This representation is much more compact than than the o-polynomial representation. Additionally, this form allowed us to see that the two families could be given with the same construction. Our hope is to study hyperovals in this new perspective to shed some light on their structure. However, choosing the right ordering for the points of the hyperovals is a daunting task.

In the final section of [17] they point out that one could search for hyperovals whose finite Fourier series representation has 4 or 5 nonzero coefficients, and so on, but that task would be arduous and temporary. Instead they suggest a canonical

ordering of the points on the hyperoval: define p_j to be the point of the oval on the line joining the origin to η^j. With this suggestion they give one result and leave further exploration up to the mathematical community.

Theorem 2.13 ([17]) *Let q be a power of 2 and let η be a primitive $(q+1)^{st}$ root of unity in GF(q^2). A set $\{p_0, p_1, \ldots, p_q\}$ of $q+1$ points in GF(q^2)* is labeled so that p_j is on the line joining the origin to η^j if and only if the Fourier coefficients of the point set satisfy $\alpha_k = \alpha_{2-k}^q$ where subscripts are taken modulo $q+1$.*

Theorem 2.13 shows that specific orderings can give very nice representations of hyperovals. In fact, as we will see later, given a specific hyperoval one can use certain orderings to produce nicer representations. Here we follow the suggestion of Fisher and Schmidt and use their canonical ordering to study new representations of hyperovals.

We assume that we are studying hyperovals in the AG$(2, q)$ where the points are represented as elements of GF(q^2). Additionally, we assume that our hyperovals contain the point $0 \in$ GF(q^2). A hyperoval that includes zero must have exactly one additional point from each of the $q+1$ lines through zero. By Lemma 2.3 each of these lines is associated with a $(q+1)^{\text{st}}$ root of unity, that is, each point on that line must have the same root of unity it its polar decomposition. Since $T_\eta(0) = 0$ for all $\eta \in \mathcal{N}$ a line through zero consists of the $q-1$ other roots of $T_\eta(x)$. These roots are points of the form $\eta^q \alpha^k$ for $0 \leq k \leq q-2$. Thus the points on a line through zero consist of points with the same $(q+1)^{\text{st}}$ root of unity it its polar decomposition. Hence, we can define a function $\rho : \mathcal{N} \to$ GF$(q)^*$ which describes any hyperoval containing the origin, by outputting, for each $q+1^{\text{st}}$ root of unity, the GF$(q)^*$ multiplier of the hyperoval point on the line through the origin defined by that $q+1^{\text{st}}$ root of unity. Hence the points of the hyperoval, as elements of GF(q^2), will be $\{x\rho(x) : x \in \mathcal{N}\} \cup \{0\}$.

What can be said about ρ? We return to equation (2.3) of Fisher and Schmidt,

$$p_j = \sum_{k=0}^{q} \alpha_k \eta^{jk}.$$

Using the suggested canonical ordering, let p_j be the hyperoval point on the line adjoining η^j to the origin. Write $p_j = \eta^j \lambda^{t_j}$ and so

$$p_j = \eta^j \lambda^{t_j} = \sum_{k=0}^{q} \alpha_k \eta^{jk},$$

thus

$$\lambda^{t_j} = \sum_{k=0}^{q} \alpha_k (\eta^j)^{k-1}.$$

Hence, if $x = \eta^j$

$$\rho(x) = \sum_{k=0}^{q} \alpha_k (x)^{k-1}.$$

We observe that the coefficients of this polynomial function are exactly the same as those in the Fisher Schmidt representation, we have simply changed the perspective. We give the following formal definition.

Definition 2.14 *A function $\rho : \mathcal{N} \to GF(q)^*$ is called a ρ-polynomial if*

$$\{x\rho(x) : x \in \mathcal{N}\} \cup \{0\}$$

is a hyperoval.

Our goal is to study the structure of ρ-polynomials and give ρ-polynomial representations for the known families of hyperovals.

2.4 Structural Properties of ρ-polynomials

In this section we will discuss the structure of ρ-polynomials. Fisher and Schmidt were concerned with hyperovals that had representations with many zero coefficients. We take a different approach and study when coefficients come from certain subfields, or have specific types of coefficients being zero.

2.4.1 Basic Structural Properties

In [17] Fisher and Schmidt also gave a formula for the coefficients in terms of the points. Using Möbius inversion on (2.3) we obtain the following equation.

$$\alpha_k = \sum_{j=0}^{q} p_j \eta^{-jk}. \tag{2.4}$$

In particular notice that

$$\alpha_0 = \sum_{j=0}^{q} p_j \tag{2.5}$$

and

$$\alpha_1 = \sum_{j=0}^{q} \lambda^{t_j} \tag{2.6}$$

where λ is a generator of the cyclic group $\mathrm{GF}(q)^*$. Based on these equations we can show that $\alpha_0 = 0$ and $\alpha_1 \in \mathrm{GF}(q)$. The fact that $\alpha_1 \in \mathrm{GF}(q)$ is a mere observation, since by (2.6) it is represented as the sum of elements in $\mathrm{GF}(q)$. Showing that $\alpha_0 = 0$ requires a slightly deeper explanation.

Lemma 2.15 *If $\rho(x) = \sum_{k=0}^{q} \alpha_k (x)^{k-1}$ is a ρ-polynomial then $\alpha_0 = 0$.*

Proof: Let $\rho(x) = \sum_{k=0}^{q} \alpha_k (x)^{k-1}$ be a ρ-polynomial describing a hyperoval $\mathcal{H}$ in $\mathrm{AG}(2, q)$ embedded in $\mathrm{PG}(2, q)$. Consider the lines through the points $(1, 0, 0)$ and $(0, 1, 0)$ of the infinite line $z = 0$. The lines through each of these points partition the hyperoval into pairs of points with paired coordinates, since neither point is on the hyperoval. In particular, the points on lines through $(1, 0, 0)$ have the same second coordinate when viewed as coordinate triples in $\mathrm{PG}(2, q)$, and the points on the lines through $(0, 1, 0)$ have the same first coordinate. This means that when we view the points of the hyperoval as $p_j = x_j + iy_j$ the $x_j's$ must be paired, and the $y_j's$ must be paired. Observe that the point $p_{q+1} = 0$ corresponding to $(0, 0)$ is not included in our

sum, so by including p_{q+1} and using (2.5) we obtain

$$\alpha_0 = \sum_{j=0}^{q+1} p_j = \sum_{j=0}^{q+1} (x_j + iy_j) = \sum_{j=0}^{q+1} x_j + i \sum_{j=0}^{q+1} y_j = 0 + i0 = 0.$$

Hence, if $\rho(x)$ is a ρ-polynomial, then $\alpha_0 = 0$. ∎

By Theorem 2.13 we know that the coefficients obey the relationship $\alpha_k = \alpha_{2-k}^q$, where the subscripts are taken mod $q+1$, hence $\alpha_2 = 0$ follows from Lemma 2.15. Therefore we can write

$$\rho(x) = \alpha_1 + \sum_{k=3}^{q} \alpha_k x^{k-1}.$$

Observe that whenever an x^k term has a nonzero coefficient, the term x^{-k} will also have a nonzero coefficient, since exponents are taken modulo $q+1$. Lemma 2.6 shows that multiplying all the points of a hyperoval by a nonzero element produces an equivalent hyperoval. Thus, we can always assume that $\alpha_1 \in \mathrm{GF}(2)$, since $\alpha_1^{-1}\mathcal{H}$ is a hyperoval equivalent to a given hyperoval $\mathcal{H}$.

These observations, along with the fact that our domain is $\mathcal{N}$, shows that we can represent ρ-polynomials in the following way,

$$\rho(x) = \alpha_1 + g(x) + g(x)^q \text{ where } g(x) = \sum_{k=3}^{\frac{q}{2}} \alpha_k x^{k-1}. \tag{2.7}$$

This form can be reduced to $\rho(x) = T(g(x)) + \alpha_1$, which confirms that $\rho(x) \in \mathrm{GF}(q)$, and further gives the following necessary condition since $\rho(x) \in \mathrm{GF}(q)^*$.

Observation 2.16 *If $\rho(x) = \alpha_1 + g(x) + g(x)^q$ is a ρ-polynomial then $T(g(x)) \neq \alpha_1$ for all $x \in \mathcal{N}$.*

2.4.2 Hyperovals Stabilized by Field Automorphisms

As previously mentioned, instead of looking for ρ-polynomials with many nonzero coefficients, we would like to study hyperovals who coefficients have other interesting properties. This section is devoted to hyperovals whose ρ-polynomial coefficients

come from subfields of GF(q^2). As we shall see, a ρ-polynomial having coefficients in a specific subfield is directly related to the hyperoval being stabilized by automorphisms of the corresponding Galois group. Recall that $q = 2^h$.

Theorem 2.17 *Let $k \mid 2h$ so that GF(2^k) is a subfield of GF(q^2), and let ρ be a ρ-polynomial describing a hyperoval $\mathcal{H}$. The polynomial ρ has coefficients in GF(2^k) if and only if $\mathcal{H}$ is stabilized by the map $\sigma : x \to x^{2^k}$.*

Proof: Assume that ρ has coefficients in GF(2^k) with $k \mid 2h$, let $\sigma : x \to x^{2^k}$, and $\eta\rho(\eta) \in \mathcal{H}$ for some $\eta \in \mathcal{N}$. In order to show that $\mathcal{H}$ is stabilized by σ we only need to show that $\rho(\eta)^\sigma = \rho(\eta^\sigma)$. Let

$$\rho(x) = \alpha_1 + \sum_{j=3}^{q} \alpha_j x^{j-1}$$

so that

$$\rho(\eta)^\sigma = \left(\alpha_1 + \sum_{j=3}^{q} \alpha_j \eta^{j-1}\right)^\sigma = \alpha_1 + \sum_{j=3}^{q} \alpha_j (\eta^\sigma)^{j-1} = \rho(\eta^\sigma)$$

since $\alpha_j \in$ GF(2^k) for $3 \le j \le q$. Hence $\mathcal{H}$ is stabilized by σ.

For the converse, assume that $\mathcal{H}$ is stabilized by σ, so that if $\eta\rho(\eta) \in \mathcal{H}$ then $(\eta\rho(\eta))^\sigma = \eta^\sigma \rho(\eta)^\sigma \in \mathcal{H}$, and so, $\rho(\eta)^\sigma = \rho(\eta^\sigma)$. As above let

$$\rho(x) = \alpha_1 + \sum_{j=3}^{q} \alpha_j x^{j-1}$$

so that

$$\left(\alpha_1 + \sum_{j=3}^{q} \alpha_j \eta^{j-1}\right)^\sigma = \alpha_1 + \sum_{j=0}^{q} \alpha_j (\eta^\sigma)^{j-1},$$

and so

$$\sum_{j=3}^{q} (\alpha_j + \alpha_j^\sigma)(\eta^\sigma)^{j-1} = 0. \tag{2.8}$$

The implied polynomial in (2.8) has degree $q-1$ and the $q+1$ elements of $\mathcal{N}$ are roots, so this polynomial must be the zero polynomial. Hence $\alpha_j = \alpha_j^\sigma$ for $3 \le j \le q$, and so, ρ has coefficients in GF(2^k). ■

This theorem allows us to obtain some information about the automorphism group of hyperovals based on the structure of their ρ-polynomials. Additionally, we can say something about the size of the automorphism group. The following corollary is an immediate consequence of Lagrange's Theorem.

Corollary 2.18 *If a hyperoval $\mathcal{H}$ is represented by a ρ-polynomial with coefficients in GF(2^k) with $k \mid 2h$ then $\frac{2h}{k} \mid |Aut(\mathcal{H})|$.*

Proof: By Theorem 2.17 we know that $\mathcal{H}$ is stabilized by the map $\sigma : x \to x^{2^k}$ which has order $\frac{2h}{k}$, hence by Lagrange's Theorem $\frac{2h}{k} \mid |Aut(\mathcal{H})|$. ∎

Further, we can acquire information about specific points that must be on a hyperoval provided the coefficients of its ρ-polynomial come from a small enough subfield.

Theorem 2.19 *Assume $\mathcal{H}$ is a hyperoval in AG($2, q$) with $q = 2^h$, h odd. If $\mathcal{H}$ is represented by a ρ-polynomial ρ with coefficients in GF(4) then $GF(4) \subseteq \mathcal{H}$.*

Proof: Assume that $\rho(x)$ has coefficients in GF(4) and recall that

$$\rho(x) = \alpha_1 + g(x) + g(x)^q$$

with $\alpha_1 \in$ GF(2). Let GF(4) be generated by ω and notice that $1, \omega, \omega^2 \in \mathcal{N}$ since $q + 1 \equiv 0 \pmod 3$. Let s be an arbitrary element of GF(4)*. Since g has coefficients in GF(4), we know $g(s) \in GF(4)$ and so $T(g(s)) \in$ GF(2), with $T(g(s)) \neq \alpha_1$. Hence $\rho(s) = 1$ and $s\rho(s) = s$. Thus GF(4)$^* \subseteq \{x\rho(x) : x \in N\}$ implying GF(4) $\subseteq \mathcal{H}$. ∎

We have seen that a hyperoval $\mathcal{H}$ being stabilized by field automorphisms gives a great deal of structure on the coefficients of the ρ-polynomials of $\mathcal{H}$. The next section shows how being stabilized by a multiplicative map effects the ρ-polynomial.

2.4.3 Hyperovals Stabilized by Multiplicative Maps

The maps we will consider in this section are of the form $x \to \gamma x$ where γ is the generator of the d^{th} roots of unity for some prime $d \mid q + 1$. In order to prove

structural results about the ρ-polynomials representing these hyperovals we first need some lemmas.

Lemma 2.20 *The sum of the d^{th} roots of unity is zero.*

Proof: The coefficient of the x^{d-1} term in the polynomial $x^d - 1$ is zero. Since the roots of this polynomial are the d^{th} roots of unity and the coefficient on x^{d-1} is the negative sum of the roots, the sum is zero. ■

Lemma 2.21 *Let γ be a generator of the multiplicative group of d^{th} roots of unity. If t is an integer with $(d,t) = 1$ then the action $x \to x^t$ permutes the d^{th} roots of unity.*

We are now ready to prove a structural result about hyperovals stabilized by these maps.

Theorem 2.22 *Let d be a prime such that $d \mid q+1$, and let γ generate the d^{th} roots of unity. If a hyperoval $\mathcal{H}$ is stabilized by the action $x \to \gamma x$ then the ρ-polynomial representing $\mathcal{H}$ has the form*

$$\rho(x) = \sum a_{di} x^{di}.$$

Proof: Assume that a hyperoval $\mathcal{H}$ is stabilized by the action $x \to \gamma x$. Let $\eta\rho(\eta)$ be a point on $\mathcal{H}$ for some $\eta \in \mathcal{N}$. Since $\mathcal{H}$ is stabilized by $x \to \gamma x$ we must have that $\gamma\eta\rho(\eta)$ is also on $\mathcal{H}$, and since $\gamma\eta \in \mathcal{N}$ we must have $\gamma\eta\rho(\gamma\eta)$ on $\mathcal{H}$ as well. These points are on the same line through 0, so they must coincide giving $\rho(\eta) = \rho(\gamma\eta)$.

Let

$$\rho(x) = \sum a_i x^i, f(x) = \sum a_{di} x^{di} \text{ and } g(x) = \rho(x) + f(x).$$

Consider the following system of equations

$$\begin{aligned} f(\gamma x) + g(\gamma x) &= \rho(\gamma x) \\ f(\gamma^2 x) + g(\gamma^2 x) &= \rho(\gamma^2 x) \\ &\vdots \\ f(\gamma^{d-1} x) + g(\gamma^{d-1} x) &= \rho(\gamma^{d-1} x). \end{aligned}$$

Observe that there are $d-1$ equations here, and $d-1$ is even since d is a prime, $d \neq 2$. Now, since $f(\gamma x) = f(x)$ and $\rho(\gamma x) = \rho(x)$ we have $f(\gamma^j x) = f(x)$ and $\rho(\gamma^j x) = \rho(x)$ for $1 \leq j \leq d-1$. Thus, by adding the $d-1$ equations together we obtain

$$\sum_{j=1}^{d-1} g(\gamma^j x) = 0.$$

By Lemma 2.20 and Lemma 2.21 we have $\sum_{j=1}^{d-1} \gamma^{jt} = 1$ provided that $t \not\equiv 0 \pmod{d}$, and so,

$$\sum_{j=1}^{d-1} g(\gamma^j x) = \sum_{t \not\equiv 0 \pmod{d}} \left(\sum_{j=1}^{d-1} \gamma^{jt} \right) a_t x^t = g(x) = 0 \text{ for all } x \in \mathcal{N}.$$

Observe that g is a polynomial of degree at most $q-1$ since ρ has degree at most $q-1$. However, the $q+1$ elements of $\mathcal{N}$ are roots of g, so g must be the zero polynomial. Hence

$$\rho(x) = f(x) + g(x) = f(x) \text{ for all } x \in \mathcal{N},$$

showing that ρ has the proposed form. ■

2.5 The Relationship to o-polynomials

We can now give a method for turning known o-polynomials into ρ-polynomials, and vice-versa. We wish to note that this general conversion formula will not always give the most elegant ρ-polynomials, and specific considerations will be given for certain families in the following sections. We begin with a useful formula for converting between cartesian and polar coordinates.

Lemma 2.23 *The point $\eta\alpha$ in polar coordinates corresponds to the point $(\alpha T(\frac{i}{\eta}), \alpha T(\eta), 1)$ in cartesian coordinates.*

Proof: Let $\eta\alpha$ represent a point in polar coordinates. Using the fact that $i^q = i+1$, the following computation shows that the image of $(\alpha T(\frac{i}{\eta}), \alpha T(\eta), 1)$ under the map $(x, y, 1) \to x + iy$ is $\eta\alpha$.

$$\alpha T(\frac{i}{\eta}) + i\alpha T(\eta) = \alpha(\frac{i}{\eta} + (\frac{i}{\eta})^q + i\eta + i\eta^q) = \alpha(\frac{i}{\eta} + i\eta + \eta + i\eta + \frac{i}{\eta}) = \alpha\eta.$$

Hence the element $\eta\alpha$ in GF(q^2) corresponds to the point $(\alpha T(\frac{i}{\eta}), \alpha T(\eta), 1)$ in AG(2,q). ■

This lemma shows that if we consider the hyperoval $\mathcal{H} = \{x\rho(x) : x \in \mathcal{N}\} \cup \{0\}$ in polar coordinates, then the cartesian coordinates of these points are

$$\{(\rho(x)T(\frac{i}{x}), \rho(x)T(x), 1) : x \in \mathcal{N}\} \cup \{(0, 0, 1)\}.$$

By the fundamental theorem of projective geometry we can guarantee that the four points $0, 1, \sqrt{\frac{i+1}{i}}\frac{\sqrt{\delta}}{\beta}, \sqrt{\frac{i}{i+1}}\frac{\sqrt{\delta}}{\beta}$ lie on the hyperoval. Thus $\rho(1) = 1$, $\rho\left(\sqrt{\frac{i}{i+1}}\right) = \frac{\sqrt{\delta}}{\beta}$, and $\rho\left(\sqrt{\frac{i+1}{i}}\right) = \frac{\sqrt{\delta}}{\beta}$, for some β in GF(q) that is specific to each hyperoval and will be determined later.

In order to determine the o-polynomial form of this hyperoval we map these points onto the standard frame. Applying the collineation defined by

$$(x, y, z)\begin{pmatrix} 1 & 1 & 0 \\ 0 & \beta & 1 \\ 0 & 1 & 0 \end{pmatrix} = (x, x + \beta y + z, y)$$

yields the set of points

$$\{(\rho(x)T(\frac{i}{x}), \rho(x)T(\frac{i}{x}) + \beta\rho(x)T(x) + 1, \rho(x)T(x)) : x \in \mathcal{N}\} \cup \{(0, 1, 0)\}.$$

Since $T(1) = 0$, $T(i) = 1$ and $\rho(1) = 1$ we have that the set of points is

$$\{(\rho(x)T(\frac{i}{x}), \rho(x)T(\frac{i}{x}) + \beta\rho(x)T(x) + 1, \rho(x)T(x)) : x \in \mathcal{N} - \{1\}\} \cup \{(0, 1, 0), (1, 0, 0)\}.$$

Now $\rho(x)T(x) \neq 0$ for $x \in \mathcal{N} - \{1\}$ so we can normalize to

$$\{(\frac{T(i/x)}{T(x)}, \frac{T(i/x)}{T(x)} + \beta + \frac{1}{\rho(x)T(x)}, 1) : x \in \mathcal{N} - \{1\}\} \cup \{(0, 1, 0), (1, 0, 0)\}.$$

Observe that $\frac{T(i/x)}{T(x)} = i + \frac{x^2}{(x+1)^2}$, hence the affine points of our hyperoval are

$$\{(i + \frac{x^2}{(x+1)^2}, i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)}, 1) : x \in \mathcal{N} - \{1\}\}. \tag{2.9}$$

We have to guarantee that $(0,0,1), (1,1,1)$ are among these points.

If $i + \frac{x^2}{(x+1)^2} = 0$ then $x = \sqrt{\frac{i}{i+1}} \in \mathcal{N}$. We also want $i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)} = 0$, hence we want,

$$\rho\left(\sqrt{\frac{i}{i+1}}\right) T\left(\sqrt{\frac{i}{i+1}}\right) = \frac{1}{\beta},$$

and so,

$$\rho\left(\sqrt{\frac{i}{i+1}}\right) = \frac{\sqrt{\delta}}{\beta}.$$

If $i + \frac{x^2}{(x+1)^2} = 1$ then $x = \sqrt{\frac{i+1}{i}} \in \mathcal{N}$. We also want $i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)} = 1$, hence we want,

$$\rho\left(\sqrt{\frac{i+1}{i}}\right) T\left(\sqrt{\frac{i+1}{i}}\right) = \frac{1}{\beta},$$

which requires,

$$\rho\left(\sqrt{\frac{i+1}{i}}\right) = \frac{\sqrt{\delta}}{\beta}.$$

We are assuming that $\rho\left(\sqrt{\frac{i}{i+1}}\right) = \frac{\sqrt{\delta}}{\beta}$, and $\rho\left(\sqrt{\frac{i+1}{i}}\right) = \frac{\sqrt{\delta}}{\beta}$ so we have successfully mapped our hyperoval onto the standard frame. If we want these points to satisfy an o-polynomial f(t), we must have

$$i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)} = f\left(i + \frac{x^2}{(x+1)^2}\right),$$

so,

$$\frac{1}{\rho(x)T(x)} = f\left(i + \frac{x^2}{(x+1)^2}\right) + i + \beta + \frac{x^2}{(x+1)^2}. \tag{2.10}$$

Hence, provided the RHS is not zero then we have

$$\rho(x) = \frac{1}{\left(f\left(i + \frac{x^2}{(x+1)^2}\right) + i + \beta + \frac{x^2}{(x+1)^2}\right) T(x)}, \ x \neq 1.$$

Since $x \in \mathcal{N}$ the calculation

$$\left(i + \frac{x^2}{(x+1)^2}\right)^q = i + 1 + \frac{(1/x)^2}{(1/x+1)^2} = i + 1 + \frac{1}{(x+1)^2} = i + \frac{x^2}{(x+1)^2}$$

shows that $i + \frac{x^2}{(x+1)^2} \in GF(q)$. Also, the map $\tau : \mathcal{N} - \{1\} \to \mathrm{GF}(q)$ defined by

$$x \to i + \frac{x^2}{(x+1)^2}$$

is clearly one-to-one and so $\mathrm{GF}(q) = \{i + \frac{x^2}{(x+1)^2} : x \in \mathcal{N} - \{1\}\}$. Letting $t = i + \frac{x^2}{(x+1)^2}$ yields

$$\rho(x) = \frac{1}{(f(t) + t + \beta)T(x)}.$$

Thus if we choose β so that $y = x + \beta$ is an external line to the hyperoval in cartesian form, then our denominator will not be zero on $\mathcal{N} - \{1\}$.

This gives us the following theorem.

Theorem 2.24 *Given an o-polynomial f with line $y = x+\beta$ external to $\{(t, f(t), 1) : t \in GF(q)\}$ the polynomial*

$$\rho(x) = \frac{1}{(f(t) + t + \beta)T(x)},\ t = i + \frac{x^2}{(x+1)^2},\ \rho(1) = 1$$

is a corresponding ρ-polynomial.

2.6 The ρ-polynomials for Known Hyperovals

While Theorem 2.24 gives a general method for finding ρ-polynomials of known families of hyperovals, it does not always produce the most elegant representations. Taking extra information into account for specific hyperovals allows us to obtain better representations. We begin by studying the hyperconic to get a better understanding of the representation and provide some proof techniques.

2.6.1 Hyperconic

Theorem 2.25 *In $AG(2, q)$ the polynomial $\rho(x) = 1$ is a ρ-polynomial that produces a hyperconic.*

Proof: Assume that $\rho(x) = 1$ and let $\mathcal{H} = \{x\rho(x) : x \in \mathcal{N}\} = \mathcal{N}$. The following computation shows that a $\mathrm{GF}(q^2)$ element $x + iy \in \mathcal{N}$ if and only if its corresponding

cartesian point $(x, y, 1)$ is a solution to an irreducible homogenous quadratic equation.

$$\begin{aligned}(x+iy)^{q+1} = 1 &\iff (x+y+iy)(x+iy) = 1 \\ &\iff x^2 + xy + ixy + ixy + iy^2 + i^2y^2 = 1 \\ &\iff x^2 + xy + \delta y^2 + 1 = 0\end{aligned}$$

Hence, $(x, y, 1)$ is a norm 1 element if and only if it is a root of $x^2 + xy + \delta y^2 + z^2$. This shows that the points of $\mathcal{N}$ are the $q+1$ points on a conic. Since each of them lies on a distinct line through 0, we must have that 0 is the nucleus of the conic. Therefore, $\mathcal{N} \cup \{0\}$ is a hyperconic, and $\rho(x) = 1$ is a ρ-polynomial that produces this hyperconic. ■

This, our first example of a ρ-polynomial for a hyperoval, may clearly be called elegant. Additionally, Theorem 2.25 shows that the domain of a ρ-polynomial is this hyperconic. Since any hyperoval has a ρ-polynomial representation this implies that any hyperoval is simply a perturbation of a hyperconic, where the ρ-polynomial describes that perturbation.

Observation 2.26 *Every hyperoval is a perturbation of a hyperconic, where the perturbation is described by its ρ-polynomial.*

We will now look at another nice representation of the hyperconic in the ρ-polynomial form. The polynomial $\rho(x) = 1$ can be viewed as the polynomial from (2.3) with all zero coefficients, except for the constant term. If we take the polynomial where all of these coefficients are 1, we also get a ρ-polynomial for the hyperconic.

Theorem 2.27 *In AG(2, q) the polynomial $\rho(x) = 1 + \sum_{j=2}^{q-1} x^j$ is a ρ-polynomial that describes a hyperconic.*

Proof: Let $\rho(x) = 1 + \sum_{j=2}^{q-1} x^j$. We claim that $\rho(\eta^k) = \eta^k + \eta^{-k}$ for $1 \le k \le q+1$, where η is a generator of $\mathcal{N}$. Assume that $(k, q+1) = d$ so that the elements of the set $\{(\eta^k)^i : 1 \le i \le \frac{q+1}{d}\}$ are precisely the $(\frac{q+1}{d})^{th}$ roots of unity. Additionally, the

multiset $\{(\eta^k)^i : 1 \leq i \leq q+1\}$ contains exactly d copies of the $(\frac{q+1}{d})^{th}$ roots of unity. Hence by Lemma 2.20 we have

$$\sum_{i=1}^{q+1}(\eta^k)^i = 0,$$

so

$$\eta^k + \sum_{i=2}^{q-1}(\eta^k)^i + (\eta^k)^q + (\eta^k)^{q+1} = 0,$$

thus

$$1 + \sum_{i=2}^{q-1}(\eta^k)^i = \eta^k + \eta^{-k},$$

and therefore,

$$\rho(\eta^k) = \eta^k + \eta^{-k}.$$

This alternate form for ρ allows us to write

$$\mathcal{H} = \{x\rho(x) : x \in \mathcal{N}\} \cup \{0\} = \{\eta^{2k} + 1 : 0 \leq k \leq q\} \cup \{1\}.$$

By Lemma 2.21 the map $x \to x^2$ permutes the $q+1^{\text{st}}$ roots of unity so

$$\mathcal{H} = \{\eta^k + 1 : 0 \leq k \leq q\} \cup \{1\}.$$

Theorem 2.25 shows that $\mathcal{N} \cup \{0\}$ is a hyperconic, and adding 1 to all of the points in $\mathcal{N} \cup \{0\}$ yields $\mathcal{H}$ as described above. Therefore, by Lemma 2.6 we find that the polynomial $\rho(x) = 1 + \sum_{j=2}^{q-1} x^j$ is a ρ-polynomial that describes a hyperconic. ■

We get the following as an immediate corollary.

Corollary 2.28 *The polynomial $\rho(x) = x + x^q = T(x),\ \rho(1) = 1$ is a ρ-polynomial that describes a hyperconic.*

The above forms describe hyperconics in $\mathrm{AG}(2, 2^h)$ for all h. There are additional ρ-polynomials for hyperconics that are specific to the case when h is even. We present several different ρ-polynomials including many rational function forms. To begin, we provide an alternative proof of Theorem 2.27 for motivation.

Proof: Let $\rho(x) = 1 + \sum_{j=2}^{q-1} x^j$ and calculate,

$$\begin{aligned}
\rho(x) &= 1 + \sum_{j=2}^{q-1} x^j \\
&= 1 + x^2 \sum_{j=0}^{q-3} x^j \\
&= 1 + x^2 \frac{1 - x^{q-2}}{1 - x}, x \neq 1 \\
&= \frac{x + 1 + x^2(x^{q-2} + 1)}{x + 1} \\
&= \frac{x^q + x^2 + x + 1}{x + 1}
\end{aligned}$$

In order to properly perform these manipulations we have to change the domain to $\mathcal{N} - \{1\}$. So when using this ρ-polynomial the hyperoval points are defined by $\{x\rho(x) : x \in \mathcal{N} - \{1\}\}$. Thus, the formula providing the hyperoval points is

$$\frac{x^{q+1} + x^3 + x^2 + x}{x + 1},$$

where x comes from $\mathcal{N} - \{1\}$, so $x^{q+1} = 1$. Hence

$$x\rho(x) = \frac{x^{q+1} + x^3 + x^2 + x}{x + 1} = \frac{x^3 + x^2 + x + 1}{x + 1} = x^2 + 1.$$

So,

$$\mathcal{H} = \{x^2 + 1 : x \in \mathcal{N} - \{1\}\} \cup \{0, 1\} = \{x + 1 : x \in \mathcal{N} \cup \{0\}\}.$$

Therefore, $\mathcal{H}$ is a hyperconic by Lemma 2.6. ∎

This alternative proof indicates the usefulness of representing ρ-polynomials as rational functions. The following theorems give additional ρ-polynomials for a hyperconic in $\mathrm{AG}(2, 2^h)$ when h is even.

Theorem 2.29 *In AG$(2, 2^h)$, h even, the function*

$$\rho(x) = 1 + (x + 1) \sum_{j=1}^{\frac{q-1}{3}} x^{3j-1} = \frac{x}{x^2 + x + 1}$$

is a ρ-polynomial describing a hyperconic.

Proof: We begin by showing the rational function shown above is equivalent to the polynomial.

$$\begin{aligned}
\rho(x) &= 1 + (x+1)\sum_{i=1}^{\frac{q-1}{3}} x^{3i-1} \\
&= 1 + (x+1)x^2 \sum_{i=0}^{\frac{q-1}{3}-1} (x^3)^i \\
&= 1 + (x+1)x^2 \frac{1-(x^3)^{\frac{q-1}{3}}}{1-x^3}, x \neq 1 \\
&= \frac{x^3+1+(x+1)x^2(x^{q-1}+1)}{x^3+1} \\
&= \frac{(x+1)(x^2+x+1+x^{q+1}+x^2)}{(x+1)(x^2+x+1)} \\
&= \frac{1+x+x^{q+1}}{x^2+x+1}.
\end{aligned}$$

The domain of ρ is $\mathcal{N} - \{1\}$, so $x^{q+1} = 1$. Thus

$$\rho(x) = \frac{x}{x^2+x+1} \tag{2.11}$$

and our hyperoval will be

$$\mathcal{H} = \{\frac{x^2}{x^2+x+1} : x \in \mathcal{N} \cup \{0\}\}.$$

In order to show that this polynomial represents a hyperconic we will show that if $x + iy \in \mathcal{H}$ then $x^2 + xy + (\delta+1)y^2 + 1 = 0$. That is the points of $\mathcal{H}$ satisfy an irreducible homogeneous quadratic equation.

From Theorem 2.25 we know that the points of $\mathcal{N}$ lie on the conic defined by $x^2 + xy + \delta y^2 + 1 = 0$, and the map that sends this conic to the conic defined by $x^2 + xy + (\delta+1)y^2 + 1 = 0$ is $(x, y, 1) \to (\frac{x}{y+1}, \frac{y}{y+1}, 1)$. Hence we want to show that $\mathcal{H}$ is the image of $\mathcal{N}$ under the map $x + iy \to \frac{x+iy}{y+1}$. To do this we will show,

$$\frac{(x+iy)^2}{(x+iy)^2 + (x+iy) + 1} = \frac{x+iy}{y+1}$$

under the assumption that $x^2 + xy + \delta y^2 + 1 = 0$. To start, we must first show that $(x + iy)^2 + (x + iy) + 1 \neq 0$, and $y + 1 \neq 0$. First observe that the roots of $z^2 + z + 1$ are the elements of GF(4)\GF(2) which are not in $\mathcal{N}$ since h is even so $(x + iy)^2 + (x + iy) + 1 \neq 0$. It is left to show that if $y = 1$ then $x + iy \notin \mathcal{N}$. The point $x + iy \in \mathcal{N}$ if and only if $x^2 + xy + \delta y^2 + 1 = 0$. So if $y = 1$ we would need $x^2 + x + \delta + 1$ to have a root in GF(q). However, since h is even $\delta + 1$ has absolute trace 1, showing $x^2 + x + \delta + 1$ has no roots in GF(q), so $y + 1 \neq 0$.

Now, it is clear that

$$x(x^2 + xy + \delta y^2 + 1) + iy(x^2 + xy + \delta y^2 + 1) = 0.$$

Expanding yields

$$x^3 + x^2y + \delta xy^2 + x + ix^2y + ixy^2 + i\delta y^3 + iy = 0,$$

so

$$x^3 + \delta xy^2 + x + ix^2y + ixy^2 + i\delta y^3 + iy = x^2y.$$

Add i^2y^3 to both sides and rearrange the terms to get

$$x^3 + \delta xy^2 + ixy^2 + ix^2y + i\delta y^3 + i^2y^3 + x + iy = x^2y + i^2y^3,$$

and then factor, giving

$$(x + iy)^3 + (x + iy) = (x + iy)^2y.$$

Now, add $(x + iy)^2$ to both sides and factor again to yield

$$(x + iy)[(x + iy)^2 + (x + iy) + 1] = (x + iy)^2(y + 1),$$

and so

$$\frac{(x + iy)^2}{(x + iy)^2 + (x + iy) + 1} = \frac{x + iy}{y + 1}$$

as desired. ■

Theorem 2.30 *In AG(2, 2^h), h even, the function*

$$\rho(x) = 1 + (x+1)\sum_{i=1}^{\frac{q-4}{6}} x^{6i-1} = \frac{x(x+1)^2}{(x^2+x+1)^2}, \quad \rho(1) = 1$$

is a ρ-polynomial describing a hyperconic.

Proof: Similar to the previous proof we will begin by providing a rational function equivalent to the polynomial.

$$\begin{aligned}
\rho(x) &= 1 + (x+1)\sum_{i=1}^{\frac{q-4}{6}} x^{6i-1} \\
&= 1 + (x+1)x^5 \sum_{i=0}^{\frac{q-4}{6}-1} (x^6)^i \\
&= 1 + (x+1)x^5 \frac{1-(x^6)^{\frac{q-4}{6}}}{1-x^6}, x \neq 1 \\
&= \frac{x^6+1+(x+1)x^5(x^{q-4}+1)}{x^6+1} \\
&= \frac{(x+1)(x^5+x^4+x^3+x^2+x+1+x^{q+1}+x^5)}{(x+1)(x^5+x^4+x^3+x^2+x+1)} \\
&= \frac{x^4+x^3+x^2+x+1+x^{q+1}}{x^5+x^4+x^3+x^2+x+1}.
\end{aligned}$$

Again, the domain of ρ is $\mathcal{N} - \{1\}$, so $x^{q+1} = 1$. Thus

$$\begin{aligned}
\rho(x) &= \frac{x^4+x^3+x^2+x}{x^5+x^4+x^3+x^2+x+1} \\
&= \frac{x(x+1)^3}{(x^3+1)(x^2+x+1)} \\
&= \frac{x(x+1)^2}{(x^2+x+1)^2}
\end{aligned}$$

and so our hyperoval is

$$\mathcal{H} = \{\frac{x(x+1)^2}{(x^2+x+1)^2} : x \in \mathcal{N} - \{1\}\} \cup \{0, 1\}.$$

In order to show that $\mathcal{H}$ is a hyperconic we will show that if $x + iy \in \mathcal{H}$ then $x^2 + xy + (\delta+1)y^2 + y = 0$. That is, the point's cartesian coordinates $(x, y, 1)$ give

a solution to $x^2 + xy + (\delta + 1)y^2 + yz = 0$. The collineation that sends this conic to $x^2 + xy + (\delta + 1)y^2 + 1$ is defined by $(x, y, 1) \to (x + 1, y, 1)$ and we know that $x^2 + xy + (\delta + 1)y^2 + 1$ defines the conic associated with the ρ-polynomial given in (2.11) from Theorem 2.29.

Let

$$\rho_1(x) = \frac{x}{x^2 + x + 1}$$

and

$$\rho_2(x) = \frac{x(x+1)^2}{(x^2 + x + 1)^2}.$$

We will show that

$$\eta\rho_1(\eta) + 1 = \eta^{q/2}\rho_2(\eta^{q/2})$$

for arbitrary $\eta \in \mathcal{N}$, which will prove that the map $(x, y, 1) \to (x + 1, y, 1)$ sends the hyperoval associated with ρ_1 to the hyperoval associated with ρ_2.

Let $\eta \in \mathcal{N}$. Clearly,

$$\eta^{2q+2} + \eta^{q+2} + \eta^{2q+1} + \eta^{q+1} + \eta^{2q} + \eta^q = \eta^{2q+1} + \eta^{q+1} + \eta^{2q} + \eta^q + \eta + 1.$$

Factoring both sides yields

$$(\eta^{2q} + \eta^q)(\eta^2 + \eta + 1) = (\eta^{2q} + \eta^q + 1)(\eta + 1)$$

and so

$$\frac{\eta^{2q} + \eta^q}{\eta^{2q} + \eta^q + 1} = \frac{\eta + 1}{\eta^2 + \eta + 1}.$$

Rewriting the terms on both sides gives

$$(\frac{(\eta^{q/2})^2 + \eta^{q/2}}{(\eta^{q/2})^2 + \eta^{q/2} + 1})^2 = \frac{\eta^2}{\eta^2 + \eta + 1} + 1$$

and so

$$\eta\rho_1(\eta) + 1 = \eta^{q/2}\rho_2(\eta^{q/2})$$

as desired. Hence ρ_2 is also a ρ-polynomial describing a hyperconic. ■

Now that we have seen what we can do with hyperconics we turn our attention to the more general translation hyperovals.

2.6.2 Translation Hyperovals

Our goal in this section is to use Theorem 2.24 to determine a general ρ-polynomial form for the translation hyperovals. In order to do this, we must find a line $y = x + \beta$ that is external to the hyperoval.

Lemma 2.31 *The line $y = x + \beta$ is external to the translation hyperoval with o-polynomial $f(t) = t^{2^k}$ if and only if $tr(\beta) = 1$ where tr denotes the absolute trace function.*

Proof: The line $y = x+\beta$ is external to the translation hyperoval with o-polynomial $f(t) = t^{2^k}$ if and only if $x^{2^k} + x + \beta$ has no roots in GF(q).

Now, $x^{2^k} + x + \beta = 0$ if and only if

$$x^{2^k} + \sum_{j=1}^{k-1}(x^{2^j} + x^{2^j}) + x + \beta = (x^{2^k} + x^{2^{k-1}}) + (x^{2^{k-1}} + x^{2^{k-2}}) + \cdots + (x^2 + x) + \beta = 0.$$

Hence β plus a sum of elements of absolute trace 0 is 0, so the equation holds if and only if $tr(\beta) = 0$. Therefore, the equation has no roots if and only if $tr(\beta) = 1$ as desired. ■

Theorem 2.32 *In AG(2,q), with $q = 2^h$, the polynomial*

$$\rho(x) = \frac{x(x+1)^{2\alpha}}{s^2(x^{2\alpha+2}+1) + (s+1)^2(x^{2\alpha} + x^2)},\ \rho(1) = 1$$

is a ρ-polynomial describing the translation hyperoval with o-polynomial $f(t) = t^\alpha, \alpha = 2^k$, where $s = \sum_{j=0}^{k-2} \delta^{2^j}$.

Proof: We begin with (2.10) from Theorem 2.24 and perform the following calculations,

$$\frac{1}{\rho(x)T(x)} = \left(i + \frac{x^2}{(x+1)^2}\right)^\alpha + i + \beta + \frac{x^2}{(x+1)^2}$$

$$\frac{1}{\rho(x)T(x)} = \frac{(i^\alpha + i + \beta)(x+1)^{2\alpha} + x^2(x+1)^{2\alpha-2} + x^{2\alpha}}{(x+1)^{2\alpha}}$$

$$\rho(x) = \frac{(x+1)^{2\alpha}}{[(i^\alpha + i + \beta)(x+1)^{2\alpha} + x^2(x+1)^{2\alpha-2} + x^{2\alpha}]T(x)}$$

$$\rho(x) = \frac{x(x+1)^{2\alpha-2}}{(i^\alpha + i + \beta)(x+1)^{2\alpha} + x^2(x+1)^{2\alpha-2} + x^{2\alpha}}.$$

From Lemma 2.31 we can let $\beta = \delta$ since $tr(\delta) = 1$. So, using Lemma 2.8, and multiplying the numerator and denominator by $(x+1)^2$ yields

$$\rho(x) = \frac{x(x+1)^{2\alpha}}{s^2(x+1)^{2\alpha+2} + x^2(x+1)^{2\alpha} + x^{2\alpha}(x+1)^2}.$$

Finally, by expanding and rearranging the terms we obtain

$$\rho(x) = \frac{x(x+1)^{2\alpha}}{s^2(x^{2\alpha+2}+1) + (s+1)^2(x^{2\alpha} + x^2)}.$$

■

We can see that not only does the ρ-polynomial depend on α but also the choice of δ. We give a simpler form for the ρ-polynomial when h is odd and also give a specific ρ-polynomial for the translation hyperoval with o-polynomial $f(t) = t^4$.

Corollary 2.33 *In AG(2,q), with $q = 2^h$, h odd, the following are ρ-polynomials that produce the translation hyperoval with o-polynomial $f(t) = t^\alpha$, $\alpha = 2^k$.*

- *When k is even*
$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha+2}+1},\ \rho(1) = 1.$$
- *When k is odd*
$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha} + x^2},\ \rho(1) = 1.$$

Proof: Since h is odd we may choose $\delta = 1$ since $tr(1) = 1$. Let $s = \sum_{j=0}^{k-2} \delta^{2^j}$ and observe that $s = 0$ when k is odd and $s = 1$ when k is even. Thus, the result follows immediately from Theorem 2.32 ■

Observation 2.34 *The ρ-polynomial*

$$\rho(x) = \frac{x(x+1)^8}{x^{10}+1}, \rho(1) = 1$$

describes the translation hyperoval with o-polynomial $f(t) = t^4$.

Additionally, we may simplify in the case where $h \equiv 2 \pmod 4$. First we need a lemma about our choice of δ in this case.

Lemma 2.35 *In GF(2^h), $h \equiv 2 \pmod 4$ the polynomial $x^2 + x + \omega$ is irreducible, where ω satisfies $\omega^2 + \omega + 1 = 0$.*

Proof: In order to show $x^2 + x + \omega$ is irreducible we must only show that ω has absolute trace 1. Observe that

$$tr(\omega) = \omega + \omega^2 + \omega^{2^2} + \cdots + \omega^{2^{h-1}}$$

and $\omega^{2^j} = \omega$ if j is even, and $\omega^{2^j} = \omega^2$ if j is odd. Since $\omega^2 + \omega = 1$ we have

$$tr(\omega) = \omega + \omega^2 + \omega^{2^2} + \cdots + \omega^{2^{h-1}} = \sum_{j=1}^{h/2} 1 = 1$$

since $h \equiv 2 \pmod 4$. ∎

Corollary 2.36 *In AG($2, q$), $q = 2^h$, $h \equiv 2 \pmod 4$, the following are ρ-polynomials that produce that translation hyperoval with o-polynomial $f(t) = t^\alpha$, $\alpha = 2^k$.*

- *When $k \equiv 1 \pmod 4$*

$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha} + x^2}, \ \rho(1) = 1.$$

- *When $k \equiv 3 \pmod 4$*

$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha+2} + 1}, \ \rho(1) = 1.$$

Proof: Since $h \equiv 2 \pmod 4$ we may choose $\delta = \omega$ where $\omega^2 + \omega + 1 = 0$ from Lemma 2.35. Let $s = \sum_{j=0}^{k-2} \delta^{2^j}$ and observe that $s = 0$ when $k \equiv 1 \pmod 4$ and $s = 1$ when $k \equiv 3 \pmod 4$, since $\omega^2 + \omega = 1$ and $\omega^{2^j} = \omega$ if j is even, and $\omega^{2^j} = \omega^2$ if j is odd. The result follows immediately from Theorem 2.32. ■

We have given ρ-polynomial forms for all translation hyperovals in the cases when $h \not\equiv 0 \pmod 4$. We will prove a more general result that will encompass this case as well as many others.

Theorem 2.37 *In AG(2, q), $q = 2^h$, the function*

$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha} + x^2},\ \rho(1) = 1$$

is a ρ-polynomial describing a translation hyperoval with o-polynomial $f(t) = t^\alpha$. $\alpha = 2^k$, k odd.

Proof: Let $\alpha = 2^k$ for k odd. We will begin with (2.9) from Section 2.5 so we must choose $\beta \in \mathrm{GF}(q)$ such that $y = x + \beta$ is external to the hyperoval. We can choose any β with $tr(\beta) = 1$ by Lemma 2.31 so let $\beta = \sum_{j=0}^{k-1} \delta^{2^j}$ which has absolute trace 1 since k is odd.

We want to show that

$$\left(i + \frac{x^2}{(x+1)^2}\right)^\alpha = i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)}$$

which reduces to

$$i^\alpha + i + \beta + \frac{x^2}{(x+1)^2} + \frac{x^{2\alpha}}{(x+1)^{2\alpha}} + \frac{x^{2\alpha} + x^2}{(x+1)^{2\alpha+2}} = 0,$$

and so,

$$i^\alpha + i + \beta = 0.$$

However, with our choice of β we know that $i^\alpha + i + \beta = 0$ by Lemma 2.8, which proves the result. ■

This result allows us to give a concise summary of translation hyperovals for all h as we did in Corollary 2.33 for h odd.

Corollary 2.38 *In AG(2,q), with $q = 2^h$ the following are ρ-polynomials that produce the translation hyperoval with o-polynomial $f(t) = t^\alpha$, $\alpha = 2^k$.*

- *When k is even*
$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha+2}+1},\ \rho(1) = 1.$$
- *When k is odd*
$$\rho(x) = \frac{x(x+1)^{2\alpha}}{x^{2\alpha}+x^2},\ \rho(1) = 1.$$

2.6.3 The Segre Hyperoval

Now we turn our attention to the Segre hyperoval. In order to use Theorem 2.24 we must find a line $y = x + \beta$ that is external to the Segre hyperoval.

Lemma 2.39 *The line $y = x + 1$ is external to the Segre hyperoval.*

Proof: In order to show a line $y = x + \beta$ is external to a hyperoval in $\mathrm{AG}(2, q)$ with o-polynomial f we must show that $f(x) + x + \beta$ has no roots in $\mathrm{GF}(q)$. Thus in this case we must show $g(x) = x^6 + x + 1$ has no roots in $\mathrm{GF}(2^h)$ when h is odd.

Assume that $a \in \mathrm{GF}(q)$, and $g(a) = 0$. It is easily checked that g has no roots in $\mathrm{GF}(2^h)$ for $1 \le h \le 5$, thus $q \ge 64$. Since a is a root we must have that a^{2^k} is also a root for $0 \le k \le 5$, and these roots are distinct since $q \ge 64$. We know $x^6 + x + 1$ has at most 6 roots, and these roots lie in an orbit under the map $x \to x^2$, so $a^{64} = a$, implying $a \in GF(64)$ which implies $q = 2^{6k}$. Hence this polynomial has no roots in $\mathrm{GF}(2^h)$ when h is odd and therefore the line $y = x + 1$ is external to the Segre hyperoval. ∎

Theorem 2.40 *In AG(2,q), with $q = 2^h$, h odd, the polynomial*

$$\rho(x) = \frac{x(x+1)^{10}}{i^2x^{12} + x^{10} + x^8 + x^4 + x^2 + i}, \quad \rho(1) = 1$$

produces the Segre hyperoval.

Proof: Again we begin with (2.10) from Theorem 2.24 with $f(x) = x^6$ and $\beta = 1$. Since h is odd we make the additional assumption that $i \in \mathrm{GF}(4)\backslash\mathrm{GF}(2)$. The following calculations prove the result.

$$\frac{1}{\rho(x)T(x)} = \left(i + \frac{x^2}{(x+1)^2}\right)^6 + i + 1 + \frac{x^2}{(x+1)^2}$$

$$\frac{1}{\rho(x)T(x)} = \frac{(x^2 + i(x+1)^2)^6}{(x+1)^{12}} + i + \frac{1}{(x+1)^2}$$

$$\frac{1}{\rho(x)T(x)} = \frac{(x^2 + i(x+1)^2)^6 + i(x+1)^{12} + (x+1)^{10}}{(x+1)^{12}}$$

$$\frac{1}{\rho(x)T(x)} = \frac{x^{12} + ix^4(x+1)^8 + i^2x^8(x+1)^4 + (x+1)^{12} + i(x+1)^{12} + (x+1)^{10}}{(x+1)^{12}}$$

$$\rho(x) = \frac{x(x+1)^{10}}{x^{12} + i^2(x+1)^{12} + (x+1)^{10} + ix^4(x+1)^8 + i^2x^8(x+1)^4}$$

$$\rho(x) = \frac{x(x+1)^{10}}{i^2x^{12} + x^{10} + x^8 + x^4 + x^2 + i}$$

■

As an immediate corollary we see that the Segre hyperoval can always be represented with a ρ-polynomial with coefficients over GF(4), since we can always assume that $i \in \mathrm{GF}(4)/\mathrm{GF}(2)$. Also, we know that the Segre hyperoval is not represented by a ρ-polynomial with coefficients over GF(2) by Corollary 2.18, since the automorphism group of the Segre hyperoval has order $(q-1)h$ or $3(q-1)h$ as seen in Table 1.2.

2.6.4 The Adelaide Hyperoval

We now present a compact ρ-polynomial for the Adelaide hyperoval. We generated ρ-polynomials for the Adelaide hyperoval in some small order planes and made the following observation.

Observation 2.41 *In $AG(2, 2^h)$, $h = 2, 4, 6, 8$, the ρ-polynomial*

$$\rho(x) = 1 + \left((x+1)\sum_{j=1}^{\frac{s}{3}} x^{4j-1}\right) + \left((x+1)\sum_{j=1}^{\frac{s}{3}} x^{4j-1}\right)^q$$

where $s = 2^{h-2} - 1$ is a ρ-polynomial that represents the Adelaide hyperoval.

We turn the polynomial above into a rational function through the following calculations.

$$\begin{aligned}
\rho(x) &= 1 + (x+1)x^3\sum_{j=1}^{\frac{s}{3}} x^{4(j-1)} + \left((x+1)x^3\sum_{j=1}^{\frac{s}{3}} x^{4(j-1)}\right)^q \\
&= 1 + \frac{(x+1)x^3(1-(x^4)^{\frac{s}{3}})}{1-x^4} + \left(\frac{(x+1)x^3(1-(x^4)^{\frac{s}{3}})}{1-x^4}\right)^q, \ x \neq 1 \\
&= 1 + \frac{x^3(x^{\frac{4s}{3}}+1)}{(x+1)^3} + \left(\frac{x^3(x^{\frac{4s}{3}}+1)}{(x+1)^3}\right)^q \\
&= \frac{(x+1)^3 + x^3(x^{\frac{q-4}{3}}+1) + (x^{\frac{q-4}{3}}+1)^q}{(x+1)^3} \\
&= \frac{x^3+x^2+x+1+x^{\frac{q+5}{3}}+x^3+x^{\frac{q(q-4)}{3}}+1}{(x+1)^3} \\
&= \frac{x^{\frac{q(q-4)}{3}}+x^{\frac{q+5}{3}}+x^2+x}{(x+1)^3}.
\end{aligned}$$

For ease of simplification we will temporarily replace x with s^3, which simply reorders

the roots since $q = 2^h$, h even, and proceed with our calculations.

$$\begin{aligned}\rho(s^3) &= \frac{s^{q(q-4)} + s^{q+5} + s^6 + s^3}{(s^3+1)^3} \\ &= \frac{s^{q(q+1)}s^{-5q} + s^{q+1}s^4 + s^6 + s^3}{(s^3+1)^3} \\ &= \frac{s^6 + s^5 + s^4 + s^3}{(s^3+1)^3} \\ &= \frac{s^3(s+1)^3}{(s^3+1)^3}\end{aligned}$$

Now we undo our substitution and obtain

$$\rho(x) = \frac{x(x^{\frac{1}{3}}+1)^3}{(x+1)^3}, \rho(1) = 1.$$

In order to prove that this is a ρ-polynomial for the Adelaide hyperoval we will follow the approach of Fisher and Schmidt (see [17] section 6), and show the points lie on an algebraic plane curve shown to represent the Adelaide hyperoval by Payne and Thas in [38]. First, we show that the points satisfy a sixth degree equation.

Lemma 2.42 *The points* $\{t\rho(t) : t \in \mathcal{N} - \{1\}\} \cup \{1\}$ *where*

$$\rho(t) = \frac{t(t^{\frac{1}{3}}+1)^3}{(t+1)^3}$$

satisfy the equation

$$y^6 + y^4 + xy + x^2 + (\delta+1)y^2 + 1 = 0 \tag{2.12}$$

when thought of as points $(x, y, 1)$ *in cartesian coordinates.*

Proof: Using Lemma 2.23 we know that the cartesian form of the points is

$$\{(\rho(t)T(\frac{i}{t}), \rho(t)T(t), 1) : t \in \mathcal{N} - \{1\}\} \cup \{(1,0,1)\}.$$

Clearly $(1,0,1)$ satisfies this equation so we focus on the other q points. Observe that $T(t) = \frac{(t+1)^2}{t}$ and $T(\frac{i}{t}) = \frac{i(t+1)^2+t^2}{t}$ so that the cartesian form of the points is $(x, y, 1)$ with

$$x = \frac{(t^{1/3}+1)^3(i(t+1)^2+t^2)}{(t+1)^3},\ y = \frac{(t^{1/3}+1)^3}{(t+1)}.$$

Substituting these values of x and y into (2.12), and multiplying the resulting equation by $(t+1)^6$ yields

$$(t^{1/3}+1)^{18} + (t+1)^2(t^{1/3}+1)^{12} + (t^{1/3}+1)^6(i(t+1)^2+t^2)(t+1)^2$$
$$+ (t^{1/3}+1)^6(i(t+1)^2+t^2)^2 + \delta(t^{1/3}+1)^6(t+1)^4 + (t+1)^6.$$

Replacing t with s^3, expanding, and factoring gives

$$(i^2+i+\delta)(s+1)^{10}(s^2+s+1)^4 = 0,$$

since $i^2+i+\delta = 0$. Hence, the result holds. ■

Now, replacing x with x/z and y with y/z in (2.12) and then multiplying by z^6 gives (2.12) in projective coordinates;

$$y^6 + y^4z^2 + z^4(xy + x^2 + (\delta+1)y^2) + z^6 = 0. \tag{2.13}$$

We need one final lemma of Payne and Thas to prove our result; see [38] Lemma 5.1, Theorem 5.2. We change their notation to be consistent with our own.

Lemma 2.43 ([38]) *If $\mathcal{O}$ represents an Adelaide oval as described in section 5 of [38], and $C = \{(t,u,v) \in PG(2,q) : T(\eta)^2v^6 + (v+t)^4(u^2+T(\eta)tu+v^2) = 0\}$, where η is a primitive element of $\mathcal{N}$, then $C = \mathcal{O} \cup (0,1,0)$.*

This lemma shows that the points of the Adelaide oval directly coincide with the points of the algebraic plane curve. We are now ready to prove the main theorem of this section.

Theorem 2.44 *In $AG(2,2^h)$, h even, the polynomial*

$$\rho(x) = \frac{x(x^{\frac{1}{3}}+1)^3}{(x+1)^3}$$

is a ρ-polynomial representing an Adelaide hyperoval.

Proof: Using Lemma 2.43, and substituting $t = y$, $u = T(\eta)x$, $v = y + z$ into $T(\eta)^2v^6 + (v + t)^4(u^2 + T(\eta)tu + v^2) = 0$ gives (2.13) with $\delta = \frac{1}{T(\eta)^2}$. To finish the result we must show that $x^2 + x + \frac{1}{T(\eta)^2}$ is irreducible in GF(2^h), h even. Fisher and Schmidt showed the equation $x^2 + x + 1 + \frac{1}{T(\eta)^2}$ is irreducible, see [17] Theorem 6.2. Hence $tr(1 + \frac{1}{T(\eta)^2}) = 1$ where tr denotes the absolute trace function. Since h is even, and tr is additive we have $tr(1 + \frac{1}{T(\eta)^2}) = tr(1) + tr(\frac{1}{T(\eta)^2}) = tr(\frac{1}{T(\eta)^2}) = 1$. Therefore, $x^2 + x + \frac{1}{T(\eta)^2}$ is irreducible in GF(2^h), h even. ■

2.6.5 The Subiaco Hyperoval

In this section we give a unified form for the hyperovals in the Subiaco family whose automorphism groups have order divisible by $2h$. Computer investigations led us to consider the polynomial

$$\rho(x) = \frac{x^5}{x^{10} + x^6 + x^5 + x^4 + 1}.$$

We will show that ρ is a ρ-polynomial representing a Subiaco hyperoval in AG$(2, q)$, $q = 2^h$ for all $h \geq 1$. Observe that this ρ-polynomial has coefficients over GF(2) so the hyperoval it represents must have an automorphism group with order divisible by $2h$ by Corollary 2.18. As such, this polynomial does not represent every hyperoval in the Subiaco family, up to projective equivalence.

We begin by considering the set of points $\{x\rho(x) : x \in \mathcal{N}\} \cup \{0\}$ and applying the homography defined by

$$(x, y, z) \begin{pmatrix} 1 & 1 & 0 \\ 0 & \beta & 1 \\ 0 & 1 & 0 \end{pmatrix} = (x, x + \beta y + z, y)$$

with $\beta = \sqrt{\delta} + \frac{1}{\delta} + \frac{1}{\delta^2}$ to obtain the set of points

$$\{(i + \frac{x^2}{(x+1)^2}, i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)}, 1) : x \in \mathcal{N} - \{1\}\} \cup \{(0, 1, 0), (1, 0, 0)\},$$

as shown in Section 2.5. We will show that

$$i + \beta + \frac{x^2}{(x+1)^2} + \frac{1}{\rho(x)T(x)} \tag{2.14}$$

represents an o-polynomial for a Subiaco hyperoval in variable $i + \frac{x^2}{(x+1)^2}$. Observe that

$$p(x)T(x) = \frac{x^4(x+1)^2}{x^{10} + x^6 + x^5 + x^4 + 1},$$

so (2.14) reduces to

$$\begin{aligned} & i + \beta + \frac{x^2}{(x+1)^2} + \frac{x^{10} + x^6 + x^5 + x^4 + 1}{x^4(x+1)^2} \\ &= \frac{(i+\beta)x^4(x+1)^2 + x^6 + x^{10} + x^6 + x^5 + x^4 + 1}{x^4(x+1)^2} \\ &= \frac{x^{10} + (i+\beta)x^6 + x^5 + (i+\beta+1)x^4 + 1}{x^4(x+1)^2}. \end{aligned}$$

Now, let $t = i + \frac{x^2}{(x+1)^2}$ so $x = \sqrt{\frac{t+i}{t+i+1}}$. Making this substitution yields

$$h(t) := \frac{(t+i+1)^3}{(t+i)^2}.$$

$$\left[\left(\frac{t+i}{t+i+1}\right)^5 + (i+\beta)\left(\frac{t+i}{t+i+1}\right)^3 + \left(\frac{t+i}{t+i+1}\right)^{5/2} + (i+\beta+1)\left(\frac{t+i}{t+i+1}\right)^2 + 1\right]$$

$$\begin{aligned} &= \frac{(t+i)^5 + (i+\beta)(t+i)^3(t+i+1)^2 + (i+\beta+1)(t+i+1)^3(t+i)^2 + (t+i+1)^5}{(t+i+1)^2(t+i)^2} \\ &\qquad + \sqrt{(t+i+1)(t+i)} \\ &= \frac{t^5 + \beta t^4 + t^3 + (\beta+1)t^2 + (i^2+i+1)^2 t + i^4\beta + i^2\beta + i^2 + i + 1}{(t^2+t+i^2+i)^2} + \sqrt{t^2+t+i^2+i} \\ &= \frac{(\beta + i + \sqrt{i})t^4 + (\beta + i + \sqrt{i} + 1)t^2 + t + (\beta + \sqrt{i})(i^4 + i^2) + i^5 + i^3 + i^2 + i + 1}{(t^2+t+i^2+i)^2} + t^{1/2}. \end{aligned}$$

Recall that $i^2 + i = \delta$, so letting $z = \sqrt{\delta}t$ and reducing h yields

$$h(z) = \frac{\delta^2(\beta+\sqrt{\delta})z^4 + \delta(\beta+\sqrt{\delta}+1)z^2 + \sqrt{\delta}z + (\beta+\sqrt{i})\delta^2 + i^3(i^2+1) + \delta + 1}{\delta^2(z^2 + \frac{1}{\sqrt{\delta}}z + 1)^2} + (\sqrt{\delta}z)^{1/2}.$$

Since $\beta = \sqrt{\delta} + \frac{1}{\delta} + \frac{1}{\delta^2}$ we have

$$h(z) = \frac{(\delta+1)z^4 + (\delta + 1 + \frac{1}{\delta})z^2 + \sqrt{\delta}z}{\delta^2(z^2 + \frac{1}{\sqrt{\delta}}z + 1)^2} + (\sqrt{\delta}t)^{1/2}.$$

Now let $d = \frac{1}{\sqrt{\delta}}$ so that $tr(\frac{1}{d}) = 1$. Simplifying and making the substitution for d yields

$$h(z) = \frac{(\frac{1}{\delta} + \frac{1}{\delta^2})z^4 + (\frac{1}{\delta} + \frac{1}{\delta^2} + \frac{1}{\delta^3})z^2 + \frac{1}{\delta\sqrt{\delta}}z}{(z^2 + \frac{1}{\sqrt{\delta}}z + 1)^2} + (\sqrt{\delta}z)^{1/2}$$

$$= \frac{d^2(d^2+1)z^4 + d^2(1+d^2+d^4)z^2 + d^3z}{(z^2+dz+1)^2} + \left(\frac{z}{d}\right)^{1/2}.$$

Thus, our point set is represented by

$$\{(z, h(z), 1) : z \in GF(q)\} \cup \{(1,0,0), (0,1,0)\}.$$

Next, we normalize h so that $h(1) = 1$ to get the point set

$$\{(x, f(x), 1) : x \in GF(q)\} \cup \{(1,0,0), (0,1,0)\}$$

where

$$f(x) = \frac{1}{d^5 + d^2 + d^{1/2}} \left(\frac{d^3(d^2+1)x^4 + d^3(1+d^2+d^4)x^2 + d^4x}{(x^2+dx+1)^2} + (dx)^{1/2} \right).$$

We claim that this is an o-polynomial for a Subiaco hyperoval.

Lemma 2.45 *Let $d \in GF(q)$ such that $tr(\frac{1}{d}) = 1$. The polynomial*

$$f(x) = \frac{1}{d^5 + d^2 + d^{1/2}} \left(\frac{d^3(d^2+1)x^4 + d^3(1+d^2+d^4)x^2 + d^4x}{(x^2+dx+1)^2} + (dx)^{1/2} \right)$$

is an o-polynomial for a Subiaco hyperoval.

Proof: In Theorem 5 of [15] it is shown that

$$g(x) = \frac{d^4x^4 + d^3(1+d^2+d^4)x^3 + d^3(1+d^2)x}{(d^2+d^5+d^{1/2})(x^2+dx+1)^2} + \frac{d^{1/2}}{d^2+d^5+d^{1/2}}x^{1/2}$$

is an o-polynomial for a Subiaco hyperoval, where d is as described above. Applying the homography defined by

$$(x, y, z) \begin{pmatrix} 0\,0\,1 \\ 0\,1\,0 \\ 1\,0\,0 \end{pmatrix} = (z, y, x)$$

to the hyperoval $\mathcal{H}$ defined by

$$\mathcal{H} := \{(x, g(x), 1) : x \in GF(q)\} \cup \{(1, 0, 0), (0, 1, 0)\}$$

yields the point set

$$\begin{aligned} \mathcal{H}' &= \{(1, g(x), x) : x \in GF(q)\} \cup \{(0, 0, 1), (0, 1, 0)\} \\ &= \{(1, g(x), x) : x \in GF(q)^*\} \cup \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}. \end{aligned}$$

We now normalize the points

$$\{(1, g(x), x) : x \in GF(q)^*\} = \{(\frac{1}{x}, \frac{g(x)}{x}, 1) : x \in GF(q)^*\}.$$

Letting $t = \frac{1}{x}$ gives the points

$$\{(t, tg(\tfrac{1}{t}), 1) : t \in GF(q)^*\}.$$

We now focus our attention on reducing $tg(\frac{1}{t})$.

$$\begin{aligned} tg(\tfrac{1}{t}) &= \frac{t}{d^5+d^2+d^{1/2}} \left(\frac{d^4(1/t)^4 + d^3(1+d^2+d^4)(1/t)^3 + d^3(1+d^2)(1/t)}{(1/t)^2 + d/t + 1)^2} + \left(\frac{d}{t}\right)^{1/2} \right) \\ &= \frac{t}{d^5 + d^2 + d^{1/2}} \left(\frac{d^4 + d^3(1+d^2+d^4)t + d^3(1+d^2)t^3}{(t^2 + dt + 1)^2} + \left(\frac{d}{t}\right)^{1/2} \right) \\ &= f(t). \end{aligned}$$

With the observation that $f(0) = 0$ we see that

$$\mathcal{H}' = \{(t, f(t), 1) : t \in GF(q)\} \cup \{(1, 0, 0), (0, 1, 0)\},$$

so f is an o-polynomial for a Subiaco hyperoval. ■

The above remarks give the following theorem.

Theorem 2.46 *In AG(2, q), $q = 2^h$, the polynomial*

$$\rho(x) = \frac{x^5}{x^{10} + x^6 + x^5 + x^4 + 1}$$

is a ρ-polynomial for a Subiaco hyperoval whose automorphism group has order divisible by $2h$.

This ρ-polynomial describes, up to projective equivalence, all Subiaco hyperovals in AG$(2, 2^h)$ when h is odd, and when $h \equiv 0 \pmod 4$. However, when $h \equiv 2 \pmod 4$ there are Subiaco hyperovals with automorphism group of order $\frac{5h}{2}$, which are not described by this ρ-polynomial. A ρ-polynomial describing a hyperoval with automorphism group of order $\frac{5h}{2}$ cannot have coefficients over GF(2). In fact, GF(16) is the smallest order field in which the coefficients for such a ρ-polynomial could exist. A ρ-polynomial representing the Subiaco hyperoval with automorphism group of order 15 in AG(2,64) is given in Chapter 3.

2.6.6 Other Families

The Glynn, Payne, and Cherowitzo hyperovals have been resilient to showing compact ρ-polynomial representations. The general conversion from their o-polynomial forms as given in Theorem 2.24 are currently the most appealing. The difficulty in conversion stems from the fact that these hyperovals are already quite elegantly represented as o-polynomials. The exponents on the polynomial terms are variable based on the plane they live in, rather than a fixed integer. This in itself presents difficulty in simplification. It may be possible to use case analysis, similar to that in Corollary 2.33, to further simplify the ρ-polynomials for hyperovals in these families, but our work up to this point has not been fruitful.

Through studying the ρ-polynomial representation it has become clear that some hyperovals will be better represented as o-polynomials. Many of the monomials, with exception of the hyperconic, are more elegantly represented as o-polynomials. In fact, as we saw in Theorem 2.40 the Segre hyperoval has its simplest ρ-polynomial

representation over GF(4)! In contrast the Subiaco and Adelaide hyperovals have ρ-polynomial representations over GF(2), where there o-polynomial counterparts do not. Additionally, we will see nice structure represented by the ρ-polynomial of the O'Keefe-Penttila hyperoval that is not represented by its o-polynomial. As such, the intention of the ρ-polynomial method is not to replace o-polynomials, but rather to complement them. Combining the two representations will help us study hyperovals and reveal information about their structure that would likely be overlooked if study was restricted to one representation.

3. A Computational Approach

This chapter is devoted to showing how the ρ-polynomial method can be used to further expand the search for hyperovals by computer. We saw in Sections 2.4.2 and 2.4.3 that the structure of ρ-polynomials directly corresponds to the hyperovals being stabilized by field automorphisms and multiplicative actions. We use these theoretical results to search for hyperovals stabilized by these actions, and in turn search for hyperovals whose ρ-polynomials have the desired properties. This is similar to the approach of Fisher and Schmidt, but we do not restrict ourselves to only the polynomials with many zero coefficients.

3.1 Cyclotomic Sets

While studying the ρ-polynomial representation we noticed a nice property of the hyperovals that have their ρ-polynomials represented over subfields of $\mathrm{GF}(q^2)$. In order to describe the structure of hyperovals whose ρ-polynomials have coefficients in a subfield, we give the following definition.

Definition 3.1 *Given an element $\beta \in GF(q^2)$ and an automorphism $\sigma : x \to x^{2^k}$, of $GF(q^2)$, we can generate the set:*

$$\mathcal{C}_\sigma(\beta) = \{\beta, \beta^\sigma, \beta^{\sigma^2}, \ldots, \beta^{\sigma^{s-1}}\},$$

where $s = \frac{h}{(h,k)}$. $\mathcal{C}_\sigma(\beta)$ is the set of all of the images of β under the automorphism σ. We call this a **cyclotomic set** *and think of it as a geometric structure in $AG(2, q)$.*

A cyclotomic set is the orbit of the point β under the automorphism σ, but we wish to distinguish this set of points as a structure in $\mathrm{AG}(2, q)$, hence the new name. If one wishes to describe these sets in a traditional way, they are sets of points stabilized by the collineations described in Lemma 2.9. Theorem 2.17 shows that if a hyperoval has a ρ-polynomial with coefficients in the subfield $\mathrm{GF}(2^k)$ of $\mathrm{GF}(q^2)$ then the hyperoval can be partioned into cyclotomic sets defined by the automorphism $\sigma : x \to x^{2^k}$. Due to this we use cyclotomic sets as building blocks for hyperovals.

A necessary condition for a cyclotomic set to be part of a hyperoval is that it is an arc. Cyclotomic sets are not always arcs, but we leave that discussion for the next chapter where we determine when a cyclotomic set is an arc (see Corollary 4.7). When a cyclotomic set has a particular structure we often refer to it as a cyclotomic structure, e.g., a cyclotomic arc. We now assume that we know which cyclotomic sets are arcs and describe how we can use them to search for new hyperovals.

3.2 Using ρ-polynomials to Search for Hyperovals

As we have seen in Lemma 2.7, the field automorphisms of GF(q^2) induce collineations. Since each automorphism fixes the origin they permute the lines through the origin defining orbits of these lines. The orbits of the lines through the origin correspond exactly to the orbits of the $q+1^{\text{st}}$ roots of unity, or rather, the cyclotomic sets of $\mathcal{N}$. We refer to each orbit of lines as a **sector** and note that every cyclotomic set lies in exactly one sector as shown in Figure 3.1.

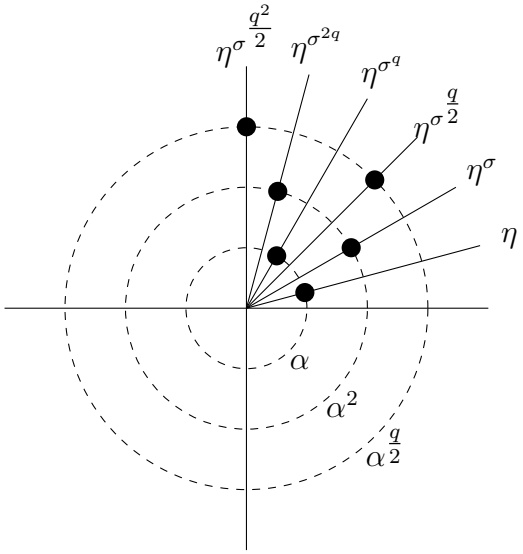


Figure 3.1: A Sector with a Cyclotomic Set

As before, we assume that a hyperoval $\mathcal{H}$ contains 0, and so, must contain exactly one other point on each line through zero. Hence, if $\mathcal{H}$ is stabilized by an automorphism σ, it must contain exactly one cyclotomic set defined by σ from each sector.

Due to this partitioning we are able to do efficient backtrack searches, choosing one element from each sector at a time. We implemented a backtrack search for all hyperovals stabilized by the automorphism $\sigma : x \to x^2$ in AG$(2, 2^h)$ for $4 \leq h \leq 8$ and for hyperovals stabilized by $\tau : x \to x^4$ in AG(2,32). The run times of these searches are given in Table 3.1.

Table 3.1: Run Times for Backtrack Searches

Plane	Action	Time
AG(2,16)	$x \to x^2$	< 1 sec
AG(2,32)	$x \to x^2$	< 1 sec
AG(2,32)	$x \to x^4$	6 sec
AG(2,64)	$x \to x^2$	8.5 sec
AG(2,128)	$x \to x^2$	10 min
AG(2,256)	$x \to x^2$	68 hours

From Corollary 2.18 we know that if we are going to find a hyperoval $\mathcal{H}$ stabilized by $\sigma : x \to x^{2^k}$ then we must have $\frac{2h}{k}$ dividing $\mid \mathrm{Aut}(\mathcal{H}) \mid$. In fact, our results in the following sections show that we find precisely those hyperovals whose automorphism group sizes are divisble by $\frac{2h}{k}$.

As is displayed in Table 3.1 the search time for backtrack searches quickly becomes unmanageable as the size of the field grows. Due to this we looked for alternative search methods. The following method, that we call Clique Finder, is described as follows:

Define a graph $G = (V, E)$ where $V = \{\mathcal{C} : \mathcal{C}$ is a cyclotomic arc$\}$ and $E = \{(x, y) : x \cup y$ is an arc$\}$. Assign colors to the vertices so that two vertices receive the same color if and only if their corresponding cyclotomic arcs lie in the same sector. If a collection of cyclotomic arcs are combined to create a hyperoval then they will appear as a rainbow clique in G, that is, a complete subgraph where all the vertices

are different colors. The graph as described will contain rainbow cliques that are not hyperovals, because there are sets of three cyclotomic arcs whose pairwise unions are arcs, but the union of all three is not. To remedy this, we check for these false triples as the graph is built. This search technique is implemented in the Orbiter package written by Anton Betten, see [3].

We implemented the Clique Finder search for hyperovals stabilized by $\sigma : x \to x^2$ in AG$(2, 2^h)$ for $6 \leq h \leq 9$ and $\tau : x \to x^4$ in AG$(2, 2^h)$ for $5 \leq h \leq 7$, with partial searches done in AG(2,256). Clique finder is significantly faster than the previous backtrack searches as is shown in Table 3.2.

Table 3.2: Run Times for Clique Finder

Plane	Action	Time
AG(2,64)	$x \to x^2$	4 sec
AG(2,128)	$x \to x^2$	7 sec
AG(2,128)	$x \to x^4$	3 min 22 sec
AG(2,256)	$x \to x^2$	2 hours 30 min
AG(2,256)	$x \to x^4$	est. 240 weeks
AG(2,512)	$x \to x^2$	8 hours 45 min

We were unable to complete searches for hyperovals stabilized by $\sigma : x \to x^{2^k}$ for large values of k since the cyclotomic set sizes become small and the graph becomes unwieldy. Also, in order to find certain families of hyperovals in small planes, we have to look for hyperovals stabilized by the action $x \to \eta x$ for $\eta \in \mathcal{N}$. The search for hyperovals stabilized by these actions was implemented using a backtrack search in AG(2,32) and AG(2,64).

Searching for hyperovals stabilized by specific actions has a great precedent in the study of hyperovals. Our approach is closely related to that of O'Keefe and Penttila in [31], Penttila and Pinneri in [40], and Penttila and Royle in [42]. The technique

used in [31] and [40] is called "prime at a time." The technique takes a prime p and constructs all hyperovals $\mathcal{H}$ such that $p \mid |\mathrm{Aut}(\mathcal{H})|$. The technique considers all conjugacy classes of elements of order p in $\mathrm{P\Gamma L}(3,q)$ and finds the hyperovals stabilized by the collineations. Our searches for hyperovals stabilized by the maps $x \to \eta x$ for $\eta \in \mathcal{N}$ are a restricted version of "prime at a time."

In [42] Penttila and Royle use prime at a time, but also search for hyperovals stabilized by the collineation defined by

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \to \begin{pmatrix} 1\,0\,0 \\ a\,1\,0 \\ b\,1\,0 \end{pmatrix} \begin{pmatrix} x^2 \\ y^2 \\ z^2 \end{pmatrix} \tag{3.1}$$

where a and b are elements of absolute trace 1. This collineation is closely related to the collineation induced by automorphisms of $\mathrm{GF}(q^2)$ given in Lemma 2.9.

The prime at a time technique helped discover the O'Keefe-Penttila hyperoval in [31], the first examples of the Subiaco hyperoval in [40], and helped classify hyperovals with non-trivial automorphism group in PG(2,64), which uncovered the first example of the Adelaide hyperoval in [42]. Additionally, the collineation defined in (3.1) was used to discover additional examples of the Adelaide and Subiaco hyperovals in PG(2,256). With this precedent in mind we searched for hyperovals stabilized by our collineations in the polar model in some small planes. We begin our searches in AG(2,16) as it is the smallest order plane with an irregular hyperoval, i.e., a non-hyperconic.

3.2.1 Searches in AG(2,16)

In $\mathrm{AG}(2,16)$ we searched for hyperovals stabilized by the map $x \to x^2$ and the search revealed both the hyperconic and Lunelli-Sce hyperovals. These are the only hyperovals that are contained in this plane so we did not do any further searches. In total eight hyperovals were found, four of each type. The Lunelli-Sce

ρ-polynomials are of particular interest here as they have been shown to be members of the Adelaide and Subiaco families. Since these hyperovals are stabilized by the squaring automorphism they necessarily have ρ-polynomials with coefficients over GF(2) where their o-polynomial counterparts do not. The Lunelli-Sce ρ-polynomial $\rho(x) = x^{14} + x^{13} + x^4 + x^3 + 1$ satisfies the general form for the Adelaide ρ-polynomial given in Theorem 2.44 and the form for the Subiaco hyperoval given in Theorem 2.46. Additionally, all four forms of the hyperconic from Section 2.6.1 are represented. Due to the manageable list and size of each ρ-polynomial we list all of them in their entirety.

Table 3.3: ρ-polynomials for hyperovals in AG$(2, 16)$

Hyperoval	ρ-polynomial
Hyperconic	1
	$x^{12} + x^{11} + x^6 + x^5 + 1$
	$x^{15} + x^{14} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + 1$
	$x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9$ $+x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
Lunelli-Sce	$x^{14} + x^{13} + x^4 + x^3 + 1$
	$x^{14} + x^{11} + x^9 + x^8 + x^6 + x^3 + 1$
	$x^{14} + x^{13} + x^{12} + x^{10} + x^7 + x^5 + x^4 + x^3 + 1$
	$x^{15} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + 1$

3.2.2 Searches in AG(2,32)

In AG$(2, 32)$ we completed three searches, one for hyperovals stabilized by each of the following actions, $x \to x^2$, $x \to x^4$, $x \to \omega x$, where $\omega^3 = 1$. There search using $x \to x^2$ yielded three distinct hyperovals, the hyperconic, translation, and Payne hyperovals. The search using $x \to x^4$ gave the Cherowitzo and Segre hyperovals

in addition to those from the $x \to x^2$ search. Finally, the search using $x \to \omega x$ gave the Segre and O'Keefe-Penttila hyperovals. These are all of the hyperovals in AG(2,32) so this list adds a complete set of ρ-polynomials for hyperovals in this plane. Observe that the hyperovals stabilized by $x \to x^2$ are precisely those hyperovals whose automorphism groups are divisible by $10 = 2h$, and those stabilized by $x \to x^4$ are precisely those hyperovals whose automorphism groups are divisible by $5 = h$. Further, hyperovals stabilized by $x \to \omega x$ are precisely those whose automorphism groups are divisible by 3. As such, the necessary condition given in Corollary 2.18 is also sufficient in this plane.

We chose the most appealing ρ-polynomials to show here. For the O'Keefe-Penttila ρ-polynomial, b is a primitive element of GF(1024) satisfying $b^{10} = b^6 + b^5 + b^3 + b^2 + b + 1$.

Table 3.4: ρ-polynomials for hyperovals in AG$(2, 32)$

Hyperoval	ρ-polynomial
Hyperconic	1
Translation - t^4	$x^{29} + x^{28} + x^{24} + x^{23} + x^{19} + x^{18}$ $+x^{15} + x^{14} + x^{10} + x^9 + x^5 + x^4 + 1$
Segre	$x^{30} + \omega^2 x^{27} + \omega^2 x^{24} + x^{21} + x^{12} + \omega x^9 + \omega x^6 + x^3 + 1$
Payne	$x^{31} + x^{30} + x^{28} + x^{23} + x^{20} + x^{19} + x^{17}$ $+x^{16} + x^{14} + x^{13} + x^{10} + x^5 + x^3 + x^2 + 1$
Cherowitzo	$x^{30} + x^{28} + \omega^2 x^{27} + x^{26} + x^{25} + x^{24} + \omega^2 x^{23} + \omega^2 x^{22}$ $+\omega x^{21} + \omega x^{20} + \omega x^{17} + \omega^2 x^{16} + \omega^2 x^{13} + \omega^2 x^{12} + \omega x^{11}$ $+\omega x^{10} + x^9 + x^8 + x^7 + \omega x^6 + x^5 + x^3 + 1$
O'Keefe-Penttila	$b^{511} x^{30} + b^{924} x^{27} + b^{230} x^{24} + b^{557} x^{21} + b^3 x^{18}$ $+b^{96} x^{15} + b^{433} x^{12} + b^{199} x^9 + b^{924} x^6 + b^{1007} x^3 + 1$

3.2.3 Searches in AG(2,64)

In AG$(2, 64)$ we completed two searches, one for hyperovals stabilized by the actions, $x \to x^2$, and $x \to \gamma x$, where $\gamma^5 = 1$. The search using the action $x \to x^2$ gave the hyperconic and Adelaide hyperovals, as well as the Subiaco hyperoval with automorphism group of order 60. The search using $x \to \gamma x$ gave both Subiaco 15 and Subiaco 60, the Subiaco hyperovals with automorphism groups of order 15 and 60 respectively. Again we choose the most appealing ρ-polynomials to present. For Subiaco 15 we let η be a primitive element of GF(16) satisfying $\eta^4 = \eta + 1$. Since Subiaco 15 has a ρ-polynomial with coefficients over GF(16) we see again that the necessary condition of Corollary 2.18 is also sufficient for the known hyperovals in this plane.

Table 3.5: ρ-polynomials for hyperovals in AG$(2, 64)$

Hyperoval	ρ-polynomial
Hyperconic	1
Adelaide	$x^{63} + x^{62} + x^{60} + x^{59} + x^{58} + x^{57} + x^{49} + x^{35} + x^{33} + x^{32}$ $+x^{30} + x^{16} + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$
Subiaco 15	$\eta x^{60} + \eta^{11} x^{55} + \eta x^{50} + \eta^7 x^{45} + \eta^2 x^{40} + \eta^7 x^{35}$ $+\eta^{13} x^{30} + \eta^8 x^{25} + \eta^{13} x^{20} + \eta^4 x^{15} + \eta^{14} x^{10} + \eta^4 x^5 + \eta^{10}$
Subiaco 60	$x^{60} + x^{50} + x^{45} + x^{35} + x^{30} + x^{20} + x^{15} + x^5 + 1$

3.2.4 Searches in AG(2,128)

In AG(2,128) we performed two searches, one for hyperovals stabilized by $x \to x^2$, and one for hyperovals stabilized by $x \to x^4$. The search using $x \to x^2$ found the hyperconic, translations, Payne, and Subiaco hyperovals, where the search using

$x \to x^4$ found the Segre, Cherowitzo, and Glynn II hyperovals. These are all known hyperovals contained in this plane. We mention yet again that the necessary condition from Corollary 2.18 is also sufficient.

We attempted to do a backtrack search for hyperovals stabilized by the action $x \to \omega x$ where $\omega^3 = 1$, however this search is far to big to complete. We plan to give serious consideration to this search in the future.

3.2.5 Searches in AG(2,256)

In $\mathrm{AG}(2, 256)$ we completed one search for hyperovals stabilized by the map $x \to x^2$. The search yielded all known hyperovals in the plane, which are the hyperconic, translation, Adelaide, and Subiaco hyperovals. Yet again, we point out that the necessary condition of Corollary 2.18 is also sufficient here. The ρ-polynomials of these hyperovals are given in Table 3.8. We represent them in rational function form for space considerations.

Partial searches have been completed with the action $x \to x^4$ and the early results give no new families of hyperovals. We attempted to shorten the estimated full search time of 240 weeks by reducing via the symmetries of the graph that is created in Clique Finder. It appears that these symmetries do not induce collineations and hence group together cliques that should not be associated. Thus our search here is not yet complete. The 240 weeks is realizable with parallel computing, but this has not yet been implemented. We plan to finish the search under this action and hope to continue the search in this plane for hyperovals stabilized by $x \to x^{16}$. However, new techniques may be needed to complete this search.

Table 3.6: ρ-polynomials for hyperovals in AG$(2, 128)$

Hyperconic	1
Translation - t^4	$x^{120} + x^{119} + x^{110} + x^{109} + x^{100} + x^{99} + x^{90} + x^{89} + x^{80} + x^{79}$ $+x^{70} + x^{69} + x^{60} + x^{59} + x^{50} + x^{49} + x^{40} + x^{39} + x^{30} + x^{29}$ $+x^{20} + x^{19} + x^{10} + x^9 + 1$
Segre	$x^{126} + x^{125} + \omega x^{123} + x^{122} + \omega x^{121} + \omega^2 x^{120} + x^{119} + \omega^2 x^{118}$ $+x^{117} + x^{116} + x^{115} + \omega x^{114} + \omega^2 x^{112} + \omega^2 x^{111} + x^{110} + \omega^2 x^{108}$ $+\omega^2 x^{107} + x^{106} + \omega x^{103} + \omega^2 x^{102} + x^{101} + x^{99} + \omega^2 x^{97} + \omega x^{96}$ $+x^{95} + x^{94} + \omega^2 x^{92} + x^{91} + x^{90} + x^{89} + \omega x^{87} + \omega^2 x^{85} + \omega x^{84}$ $+\omega^2 x^{82} + \omega x^{81} + x^{80} + x^{79} + \omega x^{78} + \omega x^{77} + \omega^2 x^{76} + x^{75} + \omega^2 x^{74}$ $+\omega x^{71} + \omega^2 x^{70} + \omega^2 x^{69} + \omega^2 x^{68} + \omega^2 x^{67} + x^{66} + x^{63} + \omega x^{62}$ $+\omega x^{61} + \omega x^{60} + \omega x^{59} + \omega^2 x^{58} + \omega x^{55} + x^{54} + \omega x^{53} + \omega^2 x^{52}$ $+\omega^2 x^{51} + x^{50} + x^{49} + \omega^2 x^{48} + \omega x^{47} + \omega^2 x^{45} + \omega x^{44} + \omega^2 x^{42}$ $+x^{40} + x^{39} + x^{38} + \omega x^{37} + x^{35} + x^{34} + \omega^2 x^{33} + \omega x^{32} + x^{30} + x^{28}$ $+\omega x^{27} + \omega^2 x^{26} + x^{23} + \omega x^{22} + \omega x^{21} + x^{19} + \omega x^{18} + \omega x^{17}$ $+\omega^2 x^{15} + x^{14} + x^{13} + x^{12} + \omega x^{11} + x^{10} + \omega x^9 + \omega^2 x^8 + x^7$ $+\omega^2 x^6 + x^4 + x^3 + 1$
Subiaco	$x^{127} + x^{126} + x^{124} + x^{122} + x^{121} + x^{117} + x^{116} + x^{115} + x^{114}$ $+x^{113} + x^{112} + x^{110} + x^{109} + x^{108} + x^{107} + x^{106} + x^{105} + x^{101}$ $+x^{100} + x^{98} + x^{96} + x^{95} + x^{93} + x^{91} + x^{90} + x^{86} + x^{85} + x^{84}$ $+x^{83} + x^{82} + x^{81} + x^{79} + x^{78} + x^{77} + x^{76} + x^{75} + x^{74} + x^{70}$ $+x^{69} + x^{67} + x^{65} + x^{64} + x^{62} + x^{60} + x^{59} + x^{55} + x^{54} + x^{53}$ $+x^{52} + x^{51} + x^{50} + x^{48} + x^{47} + x^{46} + x^{45} + x^{44} + x^{43} + x^{39}$ $+x^{38} + x^{36} + x^{34} + x^{33} + x^{31} + x^{29} + x^{28} + x^{24} + x^{23} + x^{22}$ $+x^{21} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^8$ $+x^7 + x^5 + x^3 + x^2 + 1$

Table 3.7: ρ-polynomials for hyperovals in AG$(2, 128)$ (2)

Translation - t^8	$x^{123} + x^{122} + x^{116} + x^{115} + x^{109} + x^{108} + x^{102} + x^{101} + x^{96}$ $+x^{95} + x^{89} + x^{88} + x^{82} + x^{81} + x^{75} + x^{74} + x^{68} + x^{67} + x^{62}$ $+x^{61} + x^{55} + x^{54} + x^{48} + x^{47} + x^{41} + x^{40} + x^{34} + x^{33} + x^{28}$ $+x^{27} + x^{21} + x^{20} + x^{14} + x^{13} + x^7 + x^6 + 1$
Payne	$x^{126} + x^{123} + x^{121} + x^{120} + x^{118} + x^{115} + x^{112} + x^{109} + x^{107} + x^{106}$ $+x^{105} + x^{104} + x^{102} + x^{101} + x^{98} + x^{95} + x^{93} + x^{92} + x^{90} + x^{89}$ $+x^{87} + x^{86} + x^{85} + x^{84} + x^{83} + x^{82} + x^{80} + x^{73} + x^{70} + x^{67} + x^{65}$ $+x^{64} + x^{62} + x^{59} + x^{56} + x^{49} + x^{47} + x^{46} + x^{45} + x^{44} + x^{43} + x^{42}$ $+x^{40} + x^{39} + x^{37} + x^{36} + x^{34} + x^{31} + x^{28} + x^{27} + x^{25} + x^{24} + x^{23}$ $+x^{22} + x^{20} + x^{17} + x^{14} + x^{11} + x^9 + x^8 + x^6 + x^3 + 1$
Cherowitzo	$x^{123} + \omega^2 x^{120} + \omega^2 x^{119} + x^{118} + \omega^2 x^{117} + x^{116} + \omega x^{115} + \omega^2 x^{114}$ $+\omega x^{112} + x^{111} + \omega^2 x^{109} + x^{108} + x^{107} + x^{106} + x^{104} + \omega^2 x^{102}$ $+x^{101} + \omega x^{100} + \omega x^{99} + \omega x^{98} + \omega^2 x^{93} + x^{91} + \omega x^{90} + \omega^2 x^{87}$ $+\omega x^{86} + x^{85} + x^{84} + \omega x^{83} + \omega^2 x^{82} + \omega^2 x^{80} + \omega x^{79} + \omega x^{78}$ $+\omega^2 x^{77} + \omega x^{76} + x^{75} + x^{72} + \omega x^{71} + \omega x^{69} + \omega x^{68} + x^{66} + \omega x^{65}$ $+\omega^2 x^{64} + x^{63} + \omega^2 x^{61} + \omega^2 x^{60} + \omega^2 x^{58} + x^{57} + x^{54} + \omega^2 x^{53}$ $+\omega x^{52} + \omega^2 x^{51} + \omega^2 x^{50} + \omega x^{49} + \omega x^{47} + \omega^2 x^{46} + x^{45} + x^{44} +$ $\omega^2 x^{43} + \omega x^{42} + \omega^2 x^{39} + x^{38} + \omega x^{36} + \omega^2 x^{31} + \omega^2 x^{30} + \omega^2 x^{29}$ $+x^{28} + \omega x^{27} + x^{25} + x^{23} + x^{22} + x^{21} + \omega x^{20} + x^{18} + \omega^2 x^{17}$ $+\omega x^{15} + \omega^2 x^{14} + x^{13} + \omega x^{12} + x^{11} + \omega x^{10} + \omega x^9 + x^6 + 1$
Glynn II	$\omega x^{126} + \omega^2 x^{123} + x^{120} + \omega^2 x^{117} + \omega^2 x^{114} + x^{111} + \omega x^{108} + \omega x^{105}$ $+\omega x^{102} + x^{96} + \omega^2 x^{90} + \omega^2 x^{87} + \omega x^{81} + \omega^2 x^{72} + \omega^2 x^{69} + x^{66}$ $+x^{63} + \omega x^{60} + \omega x^{57} + \omega^2 x^{48} + \omega x^{42} + \omega x^{39} + x^{33} + \omega^2 x^{27}$ $+\omega^2 x^{24} + \omega^2 x^{21} + x^{18} + \omega x^{15} + \omega x^{12} + x^9 + \omega x^6 + \omega^2 x^3 + 1$

Table 3.8: ρ-polynomials for hyperovals in AG$(2, 256)$

Hyperoval	ρ-polynomial
Hyperconic	1
Translation - t^8	$\frac{(x+1)^{16}}{x(x^{14}+1)}$
Adelaide	$\frac{x(x^{1/3}+1)^3}{(x+1)^3}$
Subiaco	$\frac{x^5}{x^{10}+x^6+x^5+x^4+1}$

3.2.6 Searches in AG(2,512)

In AG$(2, 512)$ we completed one search for hyperovals stabilized by the action $x \to x^2$. The search yielded 10 hyperovals, 2 each of the hyperconic, translations, Payne, and Subiaco hyperovals. These were precisely the ones we expected to find, that is, those whose automorphism group is divisible by $18 = 2h$. Other searches have not been completed in this plane due to the large search time required. We give the Payne ρ-polynomials as it is the only family above for which we have not yet provided an nice ρ-polynomial representation.

Payne: The polynomial $g(x)$ is given and $\rho(x) = 1 + g(x) + g(x)^q$.

$$g(x) = x^{255} + x^{253} + x^{252} + x^{251} + x^{248} + x^{247} + x^{243} + x^{241} + x^{240} + x^{238} + x^{236} + x^{234} + x^{233} + x^{232} + x^{231} + x^{229} + x^{227} + x^{225} + x^{224} + x^{223} + x^{221} + x^{219} + x^{217} + x^{215} + x^{214} + x^{213} + x^{212} + x^{211} + x^{210} + x^{207} + x^{206} + x^{202} + x^{198} + x^{196} + x^{193} + x^{191} + x^{190} + x^{188} + x^{180} + x^{179} + x^{178} + x^{177} + x^{168} + x^{161} + x^{153} + x^{152} + x^{150} + x^{148} + x^{146} + x^{144} + x^{142} + x^{140} + x^{139} + x^{138} + x^{137} + x^{135} + x^{134} + x^{131} + x^{129} + x^{128} + x^{127} + x^{124} + x^{123} + x^{122} + x^{121} + x^{119} + x^{117} + x^{112} + x^{111} + x^{110} + x^{109} + x^{108} + x^{106} + x^{103} + x^{102} + x^{99} + x^{95} + x^{90} + x^{84} + x^{83} + x^{82} + x^{81} + x^{80} + x^{79} + x^{78} + x^{77} + x^{75} + x^{73} + x^{71} + x^{69} + x^{68} + x^{64} + x^{63} + x^{61} + x^{60} + x^{59} + x^{58} + x^{57} + x^{55} + x^{53} + x^{52} + x^{45} + x^{44} + x^{43} + x^{41} + x^{39} + x^{38} + x^{37} + x^{36} + x^{35} + x^{32} + x^{31} + x^{29} + x^{28} + x^{27} + x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{14} + x^{13} + x^{12} + x^{10} + x^7 + x^5 + x^4 + x^3$$

$$g(x) = x^{256} + x^{255} + x^{254} + x^{252} + x^{249} + x^{247} + x^{246} + x^{244} + x^{239} + x^{237} + x^{236} + x^{234} + x^{233} + x^{231} + x^{230} + x^{229} + x^{228} + x^{227} + x^{226} + x^{224} + x^{221} + x^{219} + x^{218} + x^{217} + x^{216} + x^{214} + x^{213} + x^{210} + x^{207} + x^{204} + x^{203} + x^{201} + x^{200} + x^{199} + x^{198} + x^{196} + x^{193} + x^{191} + x^{190} + x^{188} + x^{183} + x^{180} + x^{179} + x^{177} + x^{176} + x^{174} + x^{173} + x^{170} + x^{165} + x^{163} + x^{162} + x^{160} + x^{153} + x^{150} + x^{147} + x^{145} + x^{144} + x^{143} + x^{142} + x^{140} + x^{137} + x^{135} + x^{134} + x^{132} + x^{127} + x^{125} + x^{124} + x^{122} + x^{121} + x^{119} + x^{118} + x^{117} + x^{116} + x^{115} + x^{114} + x^{112} + x^{105} + x^{102} + x^{99} + x^{97} + x^{96} + x^{94} + x^{93} + x^{90} + x^{85} + x^{83} + x^{82} + x^{80} + x^{79} + x^{77} + x^{76} + x^{74} + x^{71} + x^{69} + x^{68} + x^{66} + x^{65} + x^{63} + x^{62} + x^{61} + x^{60} + x^{59} + x^{58} + x^{56} + x^{55} + x^{53} + x^{52} + x^{50} + x^{45} + x^{43} + x^{42} + x^{40} + x^{37} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{30} + x^{28} + x^{25} + x^{23} + x^{22} + x^{20} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2$$

4. Structures represented by Cyclotomic Sets

This chapter is devoted to structures that appear as cyclotomic sets. While investigating the ρ-polynomial representation of hyperovals we observed that several non-arc structures appeared as cyclotomic sets including lines, sets of lines, and grids, as well as many types of configurations, which we will enumerate later. We begin with the formal definition of a type of configuration.

Definition 1 *An (n_r, v_k) configuration is a point line incidence structure consisting of n points and v lines with the following properties:*

1. *Each point is incidence with r lines.*
2. *Each line is incident with k points.*
3. *Two distinct lines intersect in at most one point and two points are connected by at most one line.*

When $v = n$, and consequently $r = k$, we refer to an (n_r, v_k) configuration as an n_k configuration. We say an n_k configuration is cyclic if there is an automorphism of the configuration that permutes the points in a single cycle. It is natural to identify the points of a cyclic n_k configuration with $\mathbb{Z}_n$ and assume that the automorphism is $x \to x+1$. Classical examples of cyclic configurations are the Desarguesian projective planes, which are examples of cyclic $(q^2 + q + 1)_{q+1}$ configuations. It is clear that they are configurations and a well known theorem of Singer [49] shows that the Desarguesian projective planes are cyclic. Singer's theorem is often used in the study of Desarguesian projective planes, and it is still an open question as to whether or not the theorem characterizes when a given projective plane is Desarguesian.

We focus our attention on cyclic n_3 configurations. In any cyclic n_3 configuration the lines have the form $\{j, j + a, j + b\}$ for $j \in \mathbb{Z}_n$ and $a < b$. Following [20], we use the notation $\mathcal{C}_3[n, a, b]$ for such a configuration. We will call the triple $[0, a, b]$ a *generating block* for $\mathcal{C}_3[n, a, b]$. Cyclic n_3 configurations only exist for $n \geq 7$ and for

each such n a cyclic n_3 configuration exists. In fact, the generating block $[0, 1, 3]$ will generate an n_3 configuration for each $n \geq 7$ [20]. The Desarguesian projective plane of order 2, seen in Figure 4.1, is an example of a cyclic n_3 configuration; it is the unique $C_3[7, 1, 3]$.

A configuration is *polycyclic* if there exists an automorphism of the configuration where all orbits on points and lines are of the same size. This is a generalization of the cyclic configurations described above. See [5] for more information on polycyclic configurations. A polycyclic generalization of cyclic n_k configurations which arises naturally is an $(n_{ks}, (ns)_k)$ configuration. We say an $(n_{ks}, (ns)_k)$ configuration is an *s-n_k configuration* if there exists an automorphism of the configuration of which each orbit is a cyclic n_k configuration. Observe that a 1-n_k configuration is simply a cyclic n_k configuration as previously described.

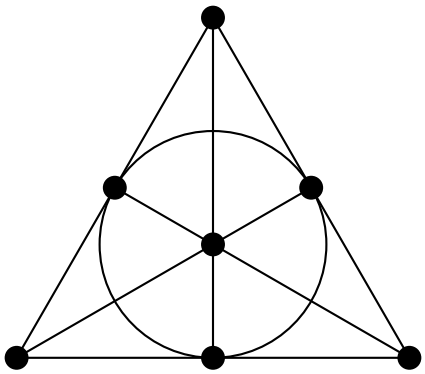


Figure 4.1: PG(2,2): The Fano Plane

In [28] Levi proved that $\mathcal{C}_3[n, 1, b]$ is a configuration for $3 \leq b \leq n - 2$ and $b \notin \{\frac{n+1}{2}, \frac{n}{2}, \frac{n}{2} + 1\}$. More recently, in [27], Koike, Kovács, and Pisanski count the number of non-isomorphic cyclic n_3 configurations, and give conditions for cyclic n_3 configurations to be isomorphic. The question we would like to answer is: For which n, a, b is $\mathcal{C}_3[n, a, b]$ a cyclic n_3 configuration? According to Grünbaum this question is still open and worth solving. [21]

In section 4.1 we characterize the generating blocks for $\mathcal{C}_3[n, a, b]$. This is an

interesting question in its own right, but also can be used to help us give necessary and sufficient conditions for when a cyclotomic set contains an s-n_k configuration. In section 4.2 we describe the structures known to be represented by cyclotomic sets and give some necessary and sufficient conditions for when a cyclotomic set represents each structure.

4.1 Determining Generating Blocks

We study the $C_3[n, a, b]$ via their incidence matrices, 0-1 matrices with columns indexed by the points and rows indexed by the lines, where a 1 indicates incidence. Observe that in the incidence matrix of $C_3[7, 1, 3]$, seen in Figure 4.2, if there are 1's in positions (ℓ, s) and (ℓ, t) then ℓ is the unique row for which this is true. If the incidence matrix of a $C_3[n, a, b]$ has J_2, the 2×2 matrix of all 1's, as a submatrix, then one says that the matrix has an embedded J_2. In [28] Levi observed that the existence of embedded J_2's is enough to determine whether or not a circulant matrix is the incidence matrix of a cyclic n_k configuration. In [27], Koike, Kovács, and Pisanski formalize this observation. We provide a formal proof for convenience.

$$
\begin{array}{c} \\ \ell_0 \\ \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\
\left(\begin{array}{ccccccc}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right)
\end{array}
$$

Figure 4.2: Incidence matrix for $\mathcal{C}_3[7, 1, 3]$

Lemma 4.1 *A circulant (0,1)-matrix generated by k 1's in the first row is the incidence matrix of an n_k configuration if and only if it has no embedded J_2.*

Proof: This condition is clearly necessary since the existence of an embedded J_2 forces there to be two lines through two points. For the converse, assume that we have a circulant matrix C, generated by a row with k 1's, and no embedded J_2. Since the sum of row 0 is k and C is circulant, we must have that every row and column sum is k. Hence there are k lines through every point, and k points on every line. The absence of embedded J_2's forces the third condition, that two distinct lines intersect in at most one point and two distinct points are connected by at most one line. Hence, C is the incidence matrix of an n_k configuration. ■

We specialize this result to the case $k = 3$ in order to answer the question posed by Grünbaum. Throughout we will be assuming $a < b$.

Theorem 4.2 ([27]) *An $n \times n$ circulant matrix C generated by $[0, a, b]$ has no embedded J_2 if and only if the 6 quantities a, $-a$, b, $-b$, $b-a$, $a-b$ are distinct modulo n.*

Proof: Assume that an $n \times n$ matrix C has an embedded J_2. WLOG we may assume that first row of the embedded J_2 is in row 0 of C, and in positions $(0, a)$, $(0, b)$, thus the third 1 in row 0 is in position $(0, 0)$. Assume that the second row of the J_2 is in row ℓ in positions (ℓ, s) and (ℓ, t). Since C is circulant there are only a few possibilities for s and t, they are:

- $s = a + \ell, t = \ell$
- $s = b + \ell, t = \ell$
- $s = \ell, t = a + \ell$
- $s = b + \ell, t = a + \ell$
- $s = \ell, t = b + \ell$

Observe that $t - s$ takes on values in the set $\{-a, a, b, -b, a - b\}$ and necessarily we have $b - a = t - s$, so the quantities mentioned above are not distinct.

For the converse, assume that the quantities are not distinct. Since we are assuming that a and b are distinct, and both are different from 0, the possibilities for equivalent quantities modulo n are:

- $a \equiv -a$
- $a \equiv -b$
- $a \equiv b - a$
- $-a \equiv b$
- $-a \equiv a - b$
- $b \equiv -b$
- $b \equiv a - b$
- $-b \equiv b - a$
- $b - a \equiv a - b$

This reduces to the following four cases:

1. $a = \frac{n}{2}$ or $b = \frac{n}{2}$
2. $a + b \equiv 0$
3. $b \equiv 2a$ or $a \equiv 2b$
4. $b - a \equiv \frac{n}{2}$

We will examine each case.

Case 1: Assume WLOG that $a = \frac{n}{2}$. The generating block is $[0, \frac{n}{2}, b]$ and so the 1's in row 0 in the incidence matrix are located in positions $(0,0), (0, \frac{n}{2}), (0, b)$, and in row $\frac{n}{2}$ the 1's are in positions $(\frac{n}{2}, \frac{n}{2}), (\frac{n}{2}, 0), (\frac{n}{2}, b + \frac{n}{2})$. Thus $(0,0), (0, \frac{n}{2}), (\frac{n}{2}, 0), (\frac{n}{2}, \frac{n}{2})$ is an embedded J_2.

Case 2: Assume that $a + b \equiv 0 \pmod{n}$. This forces the generating block to be $[0, a, n - a]$, and the 1's in row a are located in positions $(a, a), (a, 2a), (a, 0)$. Hence $(0,0), (0, a), (a, 0), (a, a)$ is an embedded J_2.

Case 3: Assume WLOG that $b \equiv 2a \pmod{n}$ so that the generating block is $[0, a, 2a]$. If we shift the block by $-a$ we get $[-a, 0, a]$ as an equivalent generating block, with the sum of the non-zero positions equivalent to $0 \pmod{n}$, and we can reduce to Case 2.

CASE 4: Assume that $b - a \equiv \frac{n}{2} \pmod{n}$. This forces the generating block to be $[0, a, a + \frac{n}{2}]$. In row $\frac{n}{2}$ the 1's are in positions $(\frac{n}{2}, \frac{n}{2}), (\frac{n}{2}, a + \frac{n}{2}), (\frac{n}{2}, a)$ and thus we see $(0, a), (0, a + \frac{n}{2}), (\frac{n}{2}, a), (\frac{n}{2}, a + \frac{n}{2})$ is an embedded J_2.

Hence we have found an embedded J_2 in each case. ■

In order to state this result in a manner similar to Levi, we must only realize that given a, we can always choose b in the range $2a < b < n - a$. Given any generating block $[0, a, b]$ consider the quantity $m = \min\{a, b - a, n - b\}$. If $m = a$ then b is in the appropriate range. If $m = b - a$ shift the block by $-a$ and if $m = n - b$ shift the block by $-b$ to get an equivalent generating block with the desired property. Using this observation and examining the four scenarios in Theorem 4.2 yields the following corollary:

Corollary 4.3 *Given $n \geq 7$, $a \neq \frac{n}{2}$, then $\mathcal{C}_3[n, a, b]$ is a cyclic n_3 configuration if and only if $b \notin \{\frac{n}{2}, \frac{n+a}{2}, a + \frac{n}{2}\}$ when b is chosen in the range $2a < b < n - a$.*

We say two configurations are *multiplier equivalent* if there exists a unit $u \in \mathbb{Z}_n$ for which the map $x \to ux$ is an isomorphism. In [27], it is proved that two cyclic n_3 configurations are isomorphic if and only if they are multiplier equivalent. This leads us to the following question.

Question 1 *Can we use Corollary 4.3 and the results from [27] to give a lexicographically minimal set of generating blocks for each n that produce all non-isomorphic n_3 configurations?*

4.2 Cyclotomic Sets as Geometric Structures

We will describe geometric structures in $\mathrm{AG}(2, q)$, $q = 2^h$, known to be represented by cyclotomic sets. We begin with two observations about the sizes of cyclotomic sets.

Observation 1 *There exists a cyclotomic set of size c in GF(2^{2h}) if and only if $c \mid 2h$. For $\phi : x \to x^2$, $|\mathcal{C}_\phi(\beta)| = c$ if and only if $\beta \in$ GF(2^c) but in no proper subfields of GF(2^c).*

Observation 2 *For $\phi : x \to x^2$, and $\sigma : x \to x^{2^e}$ we have*

$$|\mathcal{C}_\sigma(\beta)| = \frac{|\mathcal{C}_\phi(\beta)|}{(e, |\mathcal{C}_\phi(\beta)|)}.$$

We now describe when a cyclotomic set of size c is a collection of disjoint line segments, which are subsets of points on a line. We use the notation $|\beta|$ to denote the order of β in GF(q^2).

Theorem 4.4 *If $\mathcal{C}_\sigma(\beta)$, with $|\mathcal{C}_\sigma(\beta)| = c$, and $\beta \neq 0$, consists of exactly m disjoint line segments then the line segments are*

$$\ell_j = \{\beta^{\sigma^j}, \beta^{\sigma^{m+j}}, \beta^{\sigma^{2m+j}}, \ldots, \beta^{\sigma^{dm+j}}\}, \text{ where } d = \frac{c}{m} - 1,$$

and $0 \leq j \leq m-1$. We call this a set of m-regular line segments.

Proof: Assume that $\mathcal{C}_\sigma(\beta)$ consists of exactly m disjoint line segments and let $|\mathcal{C}_\sigma(\beta)| = c$ so that the order of $2^e \pmod{|\beta|}$ is c. First observe that if ℓ is a line segment, then ℓ^σ is a line segment with the same length by Corollary 2.7. Since $\mathcal{C}_\sigma(\beta)$ is an orbit we will exhaust all of its elements by repeatedly applying σ, so the disjoint line segments must have the same size. Let the line segments be $\ell_0, \ell_1, \ldots, \ell_{m-1}$. Assume WLOG that $\beta \in \ell_0$. Let $u = \min(\{s : \beta^{\sigma^s} \in \ell_0\} - \{0\})$, $v = \min(\{s : \beta^{\sigma^s} \in \ell_0\} - \{0, u\})$, and call $(\beta, \beta^{\sigma^u}, \beta^{\sigma^v})$ the minimal triple in ℓ_0. We want to show $u = m$ and $v = 2m$. Since the ℓ_j are disjoint we know that β^{σ^u} and β^{σ^v} cannot be on any lines other than ℓ_0. Thus, any collinear triple in $\mathcal{C}_\sigma(\beta)$ containing any of β, β^{σ^u}, or β^{σ^v} must be a triple that lies on ℓ_0. Now, we know that triples of the form $(\beta^{\sigma^s}, \beta^{\sigma^{u+s}}, \beta^{\sigma^{v+s}})$ must be collinear by Corollary 2.7.

Consider the triple $(\beta^{\sigma^u}, \beta^{\sigma^{2u}}, \beta^{\sigma^{u+v}})$ achieved by applying the automorphism σ^u to the minimal triple in ℓ_0. This must be a collinear triple, and so these points must

be on ℓ_0. Hence, $v \leq 2u$ by the definition of v, since $\beta^{\sigma^{2u}}$ lies on ℓ_0. Now, assume that $v < 2u$ and let $z = v - u$ and note $z < u$. Applying the automorphism σ^z to the minimal triple in ℓ_0 gives the collinear triple $(\beta^{\sigma^z}, \beta^{\sigma^{u+z}}, \beta^{\sigma^{v+z}}) = (\beta^{\sigma^z}, \beta^{\sigma^v}, \beta^{\sigma^{v+z}})$, which must be on ℓ_0. However, since $z < u$ this contradicts the minimality of u. Therefore, we must have $v = 2u$.

Continuing in a similar manner we let $w = \min(\{s : \beta^{\sigma^s} \in \ell_0\} - \{0, u, 2u\})$. By an argument similar to that above we must have $w = 3u$, and continuing the argument iteratively yields $\ell_0 = \{\beta^{\sigma^{yu}} : 0 \leq y \leq |\ell_0| - 1\}$. This implies that $2^{eu|\ell_0|} \equiv 1 \pmod{|\beta|}$ and so u is the order of $2^{e|\ell_0|} \pmod{|\beta|}$, hence $u = \frac{c}{(|\ell_0|, c)}$. Since all of the line segments have the same size we know that $|\ell_0| = \frac{c}{m}$, therefore $u = m$.

At this point we have

$$\ell_0 = \{\beta, \beta^{\sigma^m}, \beta^{\sigma^{2m}}, \ldots, \beta^{\sigma^{dm}}\}, \text{ where } d = \frac{c}{m} - 1,$$

so we can apply the automorphisms σ^j, $0 \leq j \leq m-1$ to ℓ_0 to get the lines

$$\ell_j = \{\beta^{\sigma^j}, \beta^{\sigma^{m+j}}, \beta^{\sigma^{2m+j}}, \ldots, \beta^{\sigma^{dm+j}}\}.$$

Since we are assuming the line segments are disjoint we have described them all. ■

Observe that a set of 1-regular line segments is just a single line segment. The structures currently known to be represented by cyclotomic sets are sets of regular line segments, s-n_k configurations, and arcs. Additionally, regular line segments can be superimposed on top of one another, creating grids, and on configurations, creating configurations with a parallelism. The next theorem provides a description of when a cyclotomic set contains a set of m-regular line segments.

Theorem 4.5 *In $AG(2, 2^h)$, $\mathcal{C}_\sigma(\beta)$, with $\sigma : x \to x^{2^e}$, for $0 \leq e \leq h-1$, contains a set of m-regular line segments if and only if $(\beta + \beta^{\sigma^m})^{q-1} \in GF(2^t)$ where $t = (em, 2h)$.*

Proof: Assume that $\mathcal{C}_\sigma(\beta)$ contains a set of m-regular line segments, so neces-

sarily we have that the points $\beta, \beta^{\sigma^m}, \beta^{\sigma^{2m}}$ are collinear. Consequently,

$$\sqrt{(\beta + \beta^{\sigma^m})^{q-1}} = \sqrt{(\beta^{\sigma^m} + \beta^{\sigma^{2m}})^{q-1}}.$$

Thus,

$$(\beta + \beta^{\sigma^m})^{q-1} = [(\beta + \beta^{\sigma^m})^{q-1}]^{\sigma^m}$$

putting $(\beta + \beta^{\sigma^m})^{q-1} \in GF(2^t)$ as desired.

For the converse, assume that $(\beta + \beta^{\sigma^m})^{q-1} \in GF(2^t)$ and let $(\beta + \beta^{\sigma^m})^{q-1} = z^2$, so that $z^{q-1} = \frac{1}{z^2}$ and $z^{\sigma^m} = z$. These observations show that $((z\beta) + (z\beta)^{\sigma^m})^{q-1} = 1$, hence, $T_z(\beta) \in GF(2^t)$. Thus

$$T_z(\beta) = T_z(\beta^{\sigma^{ms}})$$

for $1 \leq s \leq \frac{c}{m} - 1$ and so the points $\beta, \beta^{\sigma^m}, \beta^{\sigma^{2m}}, \ldots, \beta^{\sigma^{(\frac{c}{m}-1)m}}$ are collinear. Applying the automorphisms σ^j for $1 \leq j \leq m-1$ produces the m-regular line segments. ■

When studying cyclotomic sets it is often convenient to talk about the positions of elements by imposing an order on the set. Since each element is the image of the generator β under some power of the automorphism σ, we will refer to the element β^{σ^j} as the element in the j^{th} position. The following lemma is of considerable use in describing when cyclotomic sets can be different structures.

Lemma 4.6 *The $0, a, b$ positions of $\mathcal{C}_\sigma(\beta)$ are collinear if and only if β is a root of the polynomial function $p_{a,b,\sigma} : GF(q^2) \to GF(q^2)$ where*

$$p_{a,b,\sigma}(x) = \prod_{\lambda \in GF(q)} x^{\sigma^a} + \lambda x^{\sigma^b} + (\lambda + 1)x$$

Proof: By Corollary 2.4 we know that the points β, β^{σ^a}, and β^{σ^b} are collinear if and only if

$$\sqrt{(\beta + \beta^{\sigma^a})^{q-1}} = \sqrt{(\beta + \beta^{\sigma^b})^{q-1}},$$

which is true if and only if there exists some $\lambda \in \mathrm{GF}(q)$ for which

$$\beta + \beta^{\sigma^a} = \lambda(\beta + \beta^{\sigma^b}),$$

from which the result follows. ■

We can now describe when a cyclotomic set is an arc. We note that if a cyclotomic set is an arc then it necessarily has no collinear triples. Using Lemma 4.6 we define a polynomial whose roots are all of the elements that generate a cyclotomic set with at least one collinear triple. Let $\mathcal{S} = \{|\mathcal{C}_\sigma(\beta)| : \beta \in GF(q^2)\}$ and $n = \max\{x : x \in S\}$. We define

$$f(x) = \prod_{\substack{1 \le a < \frac{n}{2} \\ a+1 \le b \le n-1}} p_{a,b,\sigma}(x)$$

Observe that if $\mathcal{C}_\sigma(\beta)$ has a collinear triple then we may assume that β is included in a collinear triple, by the cyclic nature of $\mathcal{C}_\sigma(\beta)$. Additionally, we may assume that the middle position of the collinear triple lies between 1 and $\frac{n}{2}$ since otherwise we may use a cyclic shift to produce a collinear triple with this property. This proves the following corollary.

Corollary 4.7 *$\mathcal{C}_\sigma(\beta)$ is an arc if and only if β is a root of the polynomial*

$$A(x) = \frac{x^{q^2} + x}{GCD(f(x), x^{q^2} + x)}.$$

We can now give necessary conditions for when a cyclotomic set could be an s-n_k configuration. Observe that $[0, t_1, t_2, \ldots, t_{k-1}]$ is a generating block for a cyclic n_k configuration if and only if $[t_i, t_j, t_\ell]$ is a generating block for a cyclic n_3 configuration for any choices of i, j, ℓ with $i \neq j \neq \ell$. Recall from Theorem 4.2 that we identified the problem cases for the collinear triple $[0, a, b]$ to generate a cyclic n_3 configuration. We define the following set

$$\mathcal{B}_{a,c} = \{b \in \mathbb{Z}_c : b = \frac{c}{2},\ a + b \equiv 0,\ b \equiv 2a,\ b - a \equiv \frac{c}{2}\}$$

We use this set to describe s-n_k configurations, as we did arcs in Corollary 4.7, so we define the following polynomial,

$$g(x) = \prod_{c \in \mathcal{S}} \prod_{\substack{1 \le a < \frac{c}{2} \\ b \in \mathcal{B}_a}} p_{a,b,\sigma}(x).$$

In order for an s-n_k configuration to exist we have to ensure that only appropriate collinear triples exist. By eliminating the elements that generate cyclotomic arcs, as well as the triples that fail to generate a cyclic n_3 configuration we isolate the $\mathcal{C}_\sigma(\beta)$ that could be s-n_k configurations. The polynomial

$$AC(x) = \frac{x^{q^2} + x}{GCD(g(x), x^{q^2} + x)}$$

has roots that generate a cyclotomic set that is an arc, or a configuration with the appropriate collinearities. Hence, Corollary 4.7 allows us to give necessary conditions for when $\mathcal{C}_\sigma(\beta)$ could be an s-n_k configuration.

Corollary 4.8 *$\mathcal{C}_\sigma(\beta)$ is an s-n_k configuration if and only if β is a root of the polynomial*

$$C(x) = \frac{AC(x)}{GCD(AC(x), A(x))}.$$

4.3 Examples

We conclude with some examples from small planes. The following examples are not exhaustive but rather are chosen to give the reader a feel for what exists. We give the minimal polynomials for GF(q^2) and note that the elements of GF(q) are identified as elements of the form $\beta^{(q+1)j}$ for $0 \leq j \leq q-2$, where β generates the multiplicative group of GF(q^2). In each of the remaining examples the cyclotomic sets are formed under the automorphism $\sigma : x \to x^2$.

4.3.1 AG(2,16)

There are four cyclotomic sets in AG(2,16) that are the Möbius-Kantor configuration. These are the only configurations found as cyclotomic sets in AG(2,16). The configuration polynomial, $N_3(x)$, for these configurations is shown below where we construct GF(256) with minimal polynomial $x^8 + x^4 + x^3 + x^2 + 1$. Each factor in the given factorization below is a polynomial whose roots are the points of a single

Möbius-Kantor configuration.

$$\begin{aligned} N_3(x) &= x^{32} + x^{28} + x^{26} + x^{24} + x^{22} + x^{14} + x^{12} + x^9 + x^4 + x^3 + x^2 + x + 1 \\ &= (x^8 + x^7 + x^6 + x^5 + x^2 + x + 1)(x^8 + x^7 + x^5 + x^3 + 1) \\ &\cdot (x^8 + x^7 + x^6 + x + 1)(x^8 + x^7 + x^4 + x^3 + x^2 + x + 1) \end{aligned}$$

For instance, the roots of $x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$ are elements

$$\beta^{11}, \beta^{22}, \beta^{44}, \beta^{88}, \beta^{176}, \beta^{97}, \beta^{194}, \beta^{133} \in \ GF(q^2).$$

The Möbius-Kantor configuration in Figure 4.3 has points labeled with these roots, showing the appropriate collinearities.

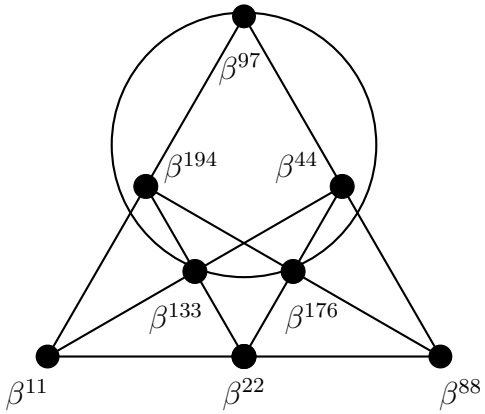


Figure 4.3: $\mathcal{C}_3[8, 1, 3]$: A Möbius-Kantor configuration found in AG(2,16)

4.3.2 AG(2,64)

In AG(2,64) we find instances of cyclotomic sets that are grids, as well as cyclotomic sets that are a configuration with a parallelism. There are 8 instances of the 4×3 grid, 36 cyclic 12_3 configurations, and 12 instances of $(12_4, 16_3)$ configurations that consist of a 12_3 configuration with a 4-regular parallelism. We construct GF(4096) with the minimal polynomial $x^{12} + x^7 + x^6 + x^5 + x^3 + x + 1$. The roots of the polynomial

$$x^{12} + x^8 + x^6 + x^5 + x^3 + x^2 + 1$$

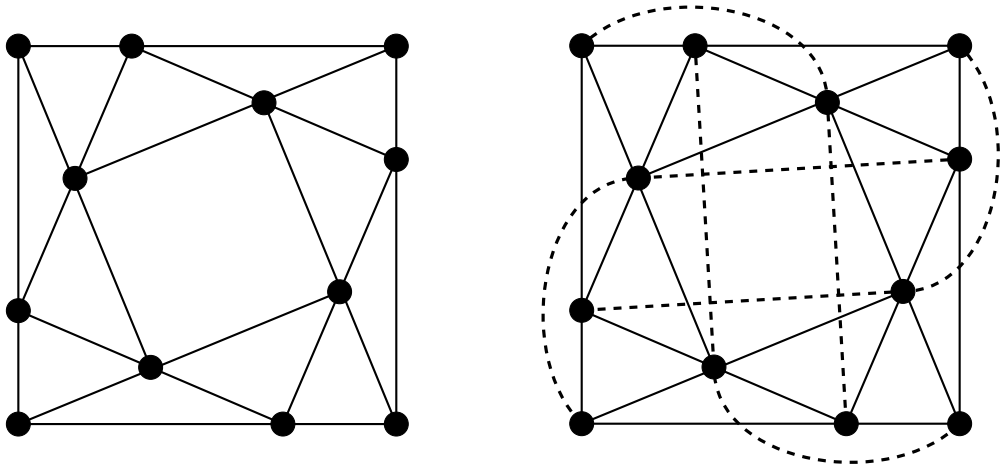
form a cyclotomic set that is the 4×3 grid. The 12_3 configurations appear with many different generating blocks, one of which is $[0, 1, 3]$. The roots of the polynomial

$$x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^3 + x^2 + x + 1$$

form a cyclotomic set that is a $\mathcal{C}_3[12, 1, 3]$, and Figure 4.4a shows a realization of this configuration.

Two of the $(12_4, 16_3)$ configurations that consist of a 12_3 configuration with a 4-regular parallelism, have a $\mathcal{C}_3[12, 1, 3]$ as its underlying cyclic 12_3 configuration. The roots of the following polynomial give a cyclotomic set that is this configuration. A realization is given in Figure 4.4b.

$$x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$$



(a) $\mathcal{C}_3[12, 1, 3]$ (b) $\mathcal{C}_3[12, 1, 3]$ with parallelism (dashed)

Figure 4.4: Configurations found as cyclotomic sets in AG(2,64)

4.3.3 AG(2,256) and Larger Planes

The affine plane AG(2,256) is the smallest plane in which we find an s-n_3 configuration for $s > 1$. There are 16 instances of cyclotomic sets that are a 2-16_3 configuration. We construct GF(2^{16}) with the minimal polynomial $x^{16} + x^5 + x^3 + x^2 + 1$.

The roots of the polynomial

$$x^{16} + x^{10} + x^9 + x^7 + x^6 + x + 1$$

are a 2-16_3 configuration. It decomposes into a $\mathcal{C}_3[16, 1, 5]$ and a $\mathcal{C}_3[16, 3, 10]$. In larger planes we also find s-n_3 configurations, including some with an additional parallelism. In AG(2,512) there are cyclotomic sets that are $(18_7, 42_3)$ configurations. This configuration has a 6-regular parallelism, and removing it produces a 2-18_3 configuration. In AG(2,1024) there are 64 cyclotomic sets that are 2-20_3 configurations, and 4 cyclotomic sets that are 20_4 configurations. In AG(2,2048) there are 12 cyclotomic sets that are 3-22_3 configurations, and in AG(2,4096) there are cyclotomic sets that are n_4 configurations, some with a parallelism.

4.4 Open Questions

In addition to the questions already mentioned, this work leads us to the following open problems about cyclotomic sets.

1. Are there any other structures that can be represented by cyclotomic sets?

2. Is there a better description of cyclotomic arcs that is not by exclusion?

3. Is there an algebraic description, perhaps some conditions on β and σ, that identifies when the union of two cyclotomic arcs is an arc? Such a description would help in the search for new hyperovals as described in Chapter 3.

REFERENCES

[1] Ball, S. *Polynomials in finite geometries.* Surveys in combinatorics, 1999 (Canterbury), 17–35, London Math. Soc. Lecture Note Ser., 267, Cambridge Univ. Press, Cambridge, 1999.

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

[3] Betten, A. *Orbiter - A Program to Classify Discrete Objects.* `http://www.math.colostate.edu/~betten/orbiter/orbiter.html`

[4] Beutelspacher, A., Rosenbaum, U. *Projective geometry: from foundations to applications.* Cambridge University Press, Cambridge, 1998.

[5] Boben, M., Pisanski, T. *Polycyclic configurations.* European J. Combin. **24** (2003), no. 4, 431–457.

[6] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.

[7] Brown, J., Cherowitzo, W. *The Lunelli-Sce hyperoval in PG(2,16).* J. Geom. **69** (2000), no. 1–2, 15–36.

[8] Cardinali, I., Payne, S. E. *q-clan geometries in characteristic 2.* Frontiers in Mathematics. Birkhäuser Verlag, Basel, 2007.

[9] Casse, Rey *Projective geometry: an introduction.* Oxford University Press, Oxford, 2006.

[10] Cherowitzo, W. *α-flocks and hyperovals.* Geom. Dedicata **72**, (1998), (3): 221–246.

[11] Cherowtizo, W. *Hyperovals in Desarguesian planes of even order* Annals Disc. Math. **37** (1986) 87–94.

[12] Cherowitzo, W. *Hyperovals in Desarguesian planes: an update.* Combinatorics (Acireale, 1992). Discrete Math. **155** (1996), no. 1-3, 31–38.

[13] Cherowitzo, W.E., Payne, S.E. *The cyclic q-clans with $q = 2^e$* Advances in Geometry, Special Issue (2003) S158–S185.

[14] Cherowitzo, W.E., O'Keefe C.M., Penttila, T. *A unified construction of finite geometries associated with q-clans in characteristic 2* Adv. Geom. **3** (2003), 1–21.

[15] Cherowitzo, W., Penttila, T., Pinneri, I., Royle, G. F. *Flocks and ovals.* Geom. Dedicata 60 (1996), no. 1, 17–37.

[16] Cherowtizo, W.E., Storme, L. *α-Flocks with Oval Herds and Monomial Hyperovals* Finite Fields and their Applications **4**, (1998) 185–199.

[17] Fisher, J. C., Schmidt, B. *Finite Fourier series and ovals in PG$(2, 2^h)$.* J. Aust. Math. Soc. **81** (2006), no. 1, 21–34.

[18] Glynn, D. *A condition for the existence of ovals in PG$(2, q)$, q even.* Geometria Dedicata **32** (1989), 247–252.

[19] Glynn, D. *Two new sequences of ovals in finite Desarguesian planes of even order.* (Combinatorial mathematics, X) Lecture Notes in Math. 1036, Berlin: Springer,(1983), pp. 217–229.

[20] Grünbaum, B. *Configurations of Points and Lines.* American Mathematical Society, Rhode Island, 2009.

[21] Grünbaum, B. Personal Communication, April 2014.

[22] Hall, M., Jr. *Ovals in the Desarguesian plane of order 16.* Ann. Mat. Pura Appl. (4) **102** (1975), 159–176.

[23] Hernando, F., McGuire, G. *Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes.* Des. Codes Cryptogr. **65** (2012), no. 3, 275–289.

[24] Hirschfeld J.W.P. *Projective Geometries Over Finite Fields.* Oxford Mathematical Monographs. second edition. The Clarendon Press Oxford University Press, New York (1998).

[25] Hughes, D.R. and Piper, F.C. *Projective Planes.* Springer-Verlag New York, 1973.

[26] Jamison, R. *Covering finite fields with cosets of subspaces*, Journal of Combinatorial Theory, Series A, **22** (1977), 253–266.

[27] Koike, H., Kovács, I. Pisanski, T. *The number of cyclic configurations of type (v_3) and the isomorphism problem.* J. Combin. Des. **22** (2014), no. 5, 216 – 229.

[28] Levi, F. *Geometrische Konfigurationen* Hirzel, Leipzig, 1929.

[29] R. Lidl and H. Niederreiter. *Finite Fields (Encyclopedia of Mathematics and its Applications).* Cambridge University Press, 1996.

[30] Lunelli, L., Sce, M. *k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16* Centro di Calcoli Numerici, Politecnico di Milano, 1958.

[31] O'Keefe, C. M., Penttila, T. *A New Hyperoval in PG(2,32)* Journal of Geometry **44** (1992) 117–139.

[32] O'Keefe, C. M., Penttila, T. *Hyperovals in PG(2,16).* European J. Combin. **12** (1991), no. 1, 51–59.

[33] O'Keefe, C. M., Penttila, T. *Symmetries of Arcs.* J. Combin. Th. Ser. A **66**, (1994) 53–67.

[34] O'Keefe, Christine M., Thas, J. A. *Collineations of Subiaco and Cherowitzo hyperovals.* Bull. Belg. Math. Soc. Simon Stevin **3** (1996), no. 2, 177–192.

[35] Payne, S. E. *A new infinite family of generalized quadrangles.* Congressus Numerantium, (1985), **49**: 115–128.

[36] Payne, S.E. *Topics in Finite Geometry: Ovals, Ovoids, and Generalized Quadrangles.* UC Denver Course Notes, 2008.

[37] Payne, S. E.,Conklin, J. E. *An unusual generalized quadrangle of order sixteen.* J. Combinatorial Theory Ser. A **24** (1978), no. 1, 50–74.

[38] Payne, S.E., Thas, J.A. *The Stabilizer of the Adelaide Oval* Discrete Mathematics **294** (2005) 161–173.

[39] Payne, S. E., Penttila, T., Pinneri, I. *Isomorphisms between Subiaco q-clan geometries.* Bull. Belg. Math. Soc. Simon Stevin **2** (1995), no. 2, 197–222.

[40] Penttila, T., Pinneri, I. *Irregular hyperovals in PG(2,64).* J. Geom. **51** (1994), no. 1–2, 89–100.

[41] Penttila, T. Royle, G. *Classification of hyperovals in PG(2,32).* J. Geom. **50** (1994), no. 1–2, 151–158.

[42] Penttila, T., Royle, G. *On Hyperovals in Small Projective Planes* Journal of Geometry **54** (1995) 91–104.

[43] Penttila, T., Storme, L. *Monomial Flocks and Herds Containing a Monomial Oval* Journal of Combinatorial Theory, Series A, **83** (1998), 21–41.

[44] Pisanski, T., Servatius, B. *Configurations from a graphical viewpoint.* Birkhäuser/Springer, New York, 2013.

[45] Robbins, N. *Beginning Number Theory.* Jones and Bartlett, Massachusetts, 2006.

[46] Segre, B. *Ovali e curve o nei piani di Galois di caratteristica due.* Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8) (1962), **32**: 785–790.

[47] Segre, B. *Ovals in a finite projective plane.* Canadian Journal of Mathematics **7** (1955), (0): 414–416.

[48] Segre, B. *Sulle ovali nei piani lineari finite* Rend. Accad. Naz. Lincei 17 (1954), 141 – 142.

[49] Singer, J. *A theorem in finite projective geometry and some applications to number theory.* Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385.

[50] Thas, J. A., Payne, S. E., Gevaert, H. *A family of ovals with few collineations.* European J. Combin. 9 (1988), no. 4, 353–362.

[51] Vis, Timothy L. *Monomial hyperovals in Desarguesian planes.* Thesis (Ph.D.)–University of Colorado at Denver. 2010.