Monomial Hyperovals in Desarguesian Planes

by

Roy G. Hadinata, B.Sc.(Hons)

Thesis submitted to The University of Adelaide
for the degree of Master of Science.

Department of Pure Mathematics,
The University of Adelaide,
South Australia.

November, 1992

Contents

Statement

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference had been made in the text.

I give consent to this copy of my thesis, when deposited in the University Library, being available for photocopying and loan.

SIGNED .. .. **DATE** ....NOVEMBER 27, 1992....

Acknowledgments

I wish to thank Dr. Christine M. O'Keefe for her help, encouragement and supervision without which this thesis would not have been possible.

I also wish to thank my parents for their understanding and support during my years as a student.

I am also grateful to my wife, Irene, for her support.

Summary

It is well known that every oval (set of $q+1$ points, no three collinear) in a Desarguesian plane of odd order is an irreducible conic (and conversely). In the case when the order of the plane is even, this is not true and the classification of ovals is largely unknown. Since every oval in $PG(2,q)$, q even, is contained in a unique hyperoval (set of $q+2$ points no three collinear), we can classify ovals by classifying hyperovals. In this thesis, some progress is made towards the classification of a special class of hyperovals, namely monomial hyperovals, in the Desarguesian planes (of even order).

In Chapter One, a short introduction is given, containing some well known results from the theory of finite fields as well as some relevant results on projective planes. In the next section, the concept of conics in $PG(2,q)$ is given as the motivating concept to hyperovals of $PG(2,q)$. It is quite well known that a hyperoval of $PG(2,q)$, $q > 2$ even, which contains the fundamental quadrangle has a canonical representation as a set of points

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

where $f(t)$ is a permutation polynomial over $GF(q)$ with degree at most $q-2$ satisfying $f(0) = 0$, $f(1) = 1$ and for each $s \in GF(q)$,

$$F_s(x) = \begin{cases} \frac{f(x+s)+f(s)}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

is a permutation polynomial. Conversely, any set $\mathcal{D}(f)$ where f is as above, is a hyperoval. If $\mathcal{D}(f)$ is a hyperoval then f is called an *o-polynomial*. Any hyperoval which is the image under an element of $P\Gamma L(3,q)$ of a hyperoval whose o-polynomial is a monomial x^k, for some positive integer $k \in \{1, \ldots, q-2\}$ is called a *monomial hyperoval*. For ease of notation we write $\mathcal{D}(k)$ for $\mathcal{D}(x^k)$. So far, there are five known classes of monomial hyperovals of $PG(2,q)$ (they are the regular, translation, Segre's $\mathcal{D}(6)$ and the two classes of Glynn's hyperovals) and we are interested in the question whether a given hyperoval must be one of these types. Several authors have

conjectured that this is indeed the case, and the classification has been verified in $PG(2, 2^h)$, $h \leq 28$, by exhaustive computer search [10].

Chapter Two reviews a result by Matthews from the paper entitled "*Permutation properties of the polynomials* $1 + x + \cdots + x^k$ *over a finite field*" [17] which states that $\mathcal{D}(k+1)$ being a hyperoval is equivalent to $1 + x + \cdots + x^k$ being a permutation polynomial over $GF(q)$, q even. For example, $\mathcal{D}(2)$ is a hyperoval corresponding to the permutation polynomial $1 + x$. This result would give an easy proof that the known monomial hyperovals are indeed hyperovals provided we can find the permutation polynomials that give rise to them.

We based our investigation into the classification of monomial hyperovals on a necessary and sufficient numerical condition proved by Glynn in his paper entitled "*Two new sequences of ovals in finite Desarguesian planes of even order*" [9]. This states that a set of points $\mathcal{D}(k)$ is a hyperoval in $PG(2, q)$, q even, if and only if $d \not\preceq kd \bmod q-1$ for all $d \in \{1, \ldots, q-2\}$ (where $\preceq$ is a particular partial ordering of the set of integers $\mathbf{N}_q = \{0, \ldots, q-1\}$). A computer program was developed, using this numerical condition. For each plane $PG(2, 2^h)$, h some positive integer, we considered the list of integers $k = 1, \ldots, q-2$. For each k, we tested whether $\mathcal{D}(k)$ is a hyperoval in $PG(2, 2^h)$ by checking whether there exists any $d \in \{1, \ldots, q-2\}$ such that $d \preceq kd \bmod q-1$. Let $\mathcal{S}(k)$ be the set $\{d : d \preceq kd, d \in \{1, \ldots, q-2\}\}$. If for a particular value of k, $\mathcal{S}(k) = \emptyset$, then $\mathcal{D}(k)$ must be a hyperoval. Otherwise, $\mathcal{D}(k)$ is not a hyperoval and the list $\mathcal{S}(k)$ ($\mathcal{S}(k) \neq \emptyset$) of the value(s) of $d \in \{1, \ldots, q-2\}$ such that $d \preceq kd$ was written alongside this particular value of k.

Inspection of these lists led to conjectures which will be proved in Chapters Three and Four.

Chapter Three contains the main results of the thesis. The first result of the first section states that the list is symmetrical about $k = q/2$ in the sense that $\mathcal{S}(k) = \mathcal{S}(q-k)$. The second section provides the complete determination of the sets $\mathcal{S}(2^n)$ for each positive integer $1 \leq n \leq h-1$. This leads to an alternative proof of the known result that $\mathcal{D}(2^n)$ is a hyperoval of $PG(2, q)$, q even, if and

only if $(n,h) = 1$. The third section of Chapter Three concerns the classification of hyperovals of $PG(2,2^h)$ of the form $\mathcal{D}(k)$ with $k = 2^m + 2^n$ for some positive integers $m > n$. An interesting result is a full classification of hyperovals of the form $\mathcal{D}(2+2^m)$, for $2 \leq m \leq h-1$. Also, a set of points $\mathcal{D}(2^m+2^n)$, $m > n$, is not a hyperoval whenever the index h can be expressed as $h = am + bn$, where a and b are non-negative integers and a is as large as possible (i.e. $0 \leq bn \leq m-1$) which then implies that a set of points $\mathcal{D}(2^2+2^m)$ is not a hyperoval of $PG(2,2^h)$ whenever the index $h \geq m+2$ is even. It is also shown that $\mathcal{D}(2^n+2^m)$ is not a hyperoval of $PG(2,2^h)$ whenever $h = am + bn + 1$ and $h \geq 2m + n + 1$ (where a is as large as possible and $0 \leq bn \leq m-1$) and a special case of this result is a set of points $\mathcal{D}(2^2+2^m)$ for $m \geq 4$ even, is not a hyperoval in $PG(2,2^h)$ whenever the index of the plane $h \geq 2m+3$ is odd.

In Chapter Four a different approach to the problem is undertaken. We choose an integer $d \in \{1,\ldots,q-2\}$ and determine which sets $\mathcal{D}(k)$ have $d \in \mathcal{S}(k)$ and hence are not hyperovals. It turns out that an integer $d \in \{1,\ldots,q-2\}$ with one term in its binomial expansion (that is of the form 2^n for some positive integer n) always belongs to the set $\mathcal{S}(k)$ whenever k is odd. This result can also be obtained by applying the result of Segre-Bartocci [34] which shows that every term in an o-polynomial must have even degree. The next step is to find a result corresponding to a value of d with two terms in its binomial expansion, that is, $d = 2^n + 2^m$ for distinct positive integers m, n. We describe an algorithm to determine, for a given integer $d \in \{1,\ldots,q-2\}$ having two terms in its binomial expansion, the possible integers k such that $d \in \mathcal{S}(k)$, by the use of an example.

A short conclusion and suggestions for further research appear in Chapter Five.

Chapter 1

Introduction and preliminaries

In the first section of this chapter we shall survey some preliminary results on finite fields, projective spaces and projective planes as well as recall the notion of binary representation and binary addition. In the second section we shall introduce the concept of hyperovals of $PG(2,q)$ in general and monomial hyperovals in particular. We then review a necessary and sufficient numerical condition for the existence of monomial hyperovals of $PG(2,q)$, see Glynn [9] Theorem A.

1.1 Some preliminaries

1.1.1 Finite fields

A *finite field* F of *order* q is a set of q elements on which two binary operations, called addition and multiplication, are defined and which contains distinct, distinguished elements 0 and 1, called the zero element and identity element respectively. Furthermore, F is an abelian group with identity 0 with respect to addition and the non-zero elements of F form an abelian group with identity 1 with respect to multiplication. The two operations of addition and multiplication are linked by the left distributive law $a(b+c) = ab + ac$, for all $a, b, c \in F$. The right distributive law $(b+c)a = ba + ca$ follows automatically from the commutativity of multiplication.

It can be shown that, for a finite field to exist, the order q of the field must be a power of a prime p, that is $q = p^h$ for some positive integer h. Conversely, for each prime power $q = p^h$, there exists a unique (up to field isomorphism) finite field of this order denoted by $GF(q)$ for the Galois field of order q, see [7] Chapter 45. The number p is called the *characteristic* of F.

Notation. Let $GF(q)^*$ denote the set $GF(q) \setminus \{0\}$. We use (x, y) to denote the greatest common divisor of two integers x and y.

Lemma 1.1.1 ([16], Lemma 2.3) *If F is a finite field with p^h elements, then every $a \in F$ satisfies $a^{p^h} = a$.*

Proof. If $a = 0$ the lemma is trivially true. On the other hand, the nonzero elements of F form a group under multiplication, of order $p^h - 1$. By Lagrange's theorem, the order of every nonzero element of F divides $p^h - 1$. Thus $a^{p^h-1} = 1$ for all $a \neq 0$ in F. Multiplying this relation by a we obtain that $a^{p^h} = a$. ■

An *automorphism* α of a field F is a one-one function from F to itself such that , for all x and y in F, $\alpha(x+y) = \alpha(x)+\alpha(y)$ and $\alpha(xy) = \alpha(x)+\alpha(y)$. Two properties of an automorphism α of F are $\alpha(0) = 0$ and $\alpha(1) = 1$. The automorphisms of $GF(q)$, $q = p^h$, are the bijections $\alpha : GF(q) \to GF(q)$ where $\alpha : a \longmapsto a^{p^n}$, for all $a \in GF(q)$, where n is an integer, see [16] Theorem 2.21. By lemma 1.1.1, $a^{p^h} = a$ for all $a \in GF(q)$, and hence it may be assumed that $0 \leq n \leq h$.

We now introduce the notions of permutation polynomial, binary representation and binary addition; all of which will be used in later chapters. First, let $GF(q)[x]$ denote the collection of all polynomials in the variable x with coefficients from $GF(q)$.

Definition 1.1.1 Let $GF(q)$ be a finite field of characteristic p, with $q = p^e$, p prime and $e \geq 1$. A polynomial $f \in GF(q)[x]$ is called a *permutation polynomial* of $GF(q)$ if the associated polynomial function $f : c \mapsto f(c)$ from $GF(q)$ into $GF(q)$

is a permutation of $GF(q)$. In other words, the polynomial $f \in GF(q)[x]$ is a permutation polynomial of $GF(q)$ if and only if $f(x) = a$ has a unique solution in $GF(q)$ for each $a \in GF(q)$.

Definition 1.1.2 Let $q = 2^h$, h a positive integer, and let x be a positive integer such that $0 \leq x \leq q-1$. Let x have the binomial expansion $x = \sum_{i=0}^{h-1} x_i 2^i$, where $x_i \in \{0,1\}$. Then we let the *binary representation* of x be $x_0 x_1 \ldots x_{h-1}$. We write $x \overset{\text{bin.rep}^n}{=} x_0 x_1 \ldots x_{h-1}$.

Note that if $x \in \mathbf{N}_q$ is a positive integer as in Definition 1.1.2 then for a given positive integer r, the binary representation of $2^r x \bmod (2^h - 1) \overset{\text{bin.rep}^n}{=} x'_0 x'_1 \ldots x'_{h-1}$ can be obtained by shifting each digit in the binary representation of x by r positions to the right and wrapping in the sense that if x_i, $0 \leq i \leq h-1$, is shifted to the right by r positions and x_{i+r} is such that $i + r \geq h$ then x_{i+r} becomes $x_{i+r \bmod h}$ such that $0 \leq i + r \leq h - 1$. We illustrate this by the use of an example as follows.

Example 1.1.1 *Let $q = 2^5$ and let $x = 11$ so that $x \overset{\text{bin.rep}^n}{=} 11010$. Then the binary representation of $2^1 x$ is 01101 and the binary representation of $2^2 x$ is 10110.*

Let $q = 2^h$, h a positive integer, and let a, b be integers with $0 \leq a, b \leq q-1$. Suppose that a and b have binomial expansions $a = \sum_{i=0}^{h-1} a_i 2^i$ and $b = \sum_{i=0}^{h-1} b_i 2^i$, $a_i, b_i \in \{0,1\}$ for all i, respectively. We illustrate the *binary addition* $a + b \bmod (2^h - 1) \overset{\text{bin.rep}^n}{=} d_0 d_1 \ldots d_{h-1}$, in terms of the binary representations of a and b, as follows:

$$\begin{array}{lcccccc} a \bmod (2^h-1) & \overset{\text{bin.rep}^n}{=} & a_0 & a_1 & \cdots\cdots & a_{h-1} \\ b \bmod (2^h-1) & \overset{\text{bin.rep}^n}{=} & b_0 & b_1 & \cdots\cdots & b_{h-1} \end{array}$$

If $a_0 + b_0 = 0$ or 1 then $d_0 = a_0 + b_0$ else if $a_0 + b_0 = 2$ then $d_0 = 0$ and a carry of $c_0 = 1$ flows over into the next column. Thus at the i^{th} stage, if $a_i + b_i + c_{i-1} = 0$ or 1 then $d_i = a_i + b_i + c_{i-1}$ else if $a_i + b_i + c_{i-1} = 2$ or 3 then $d_i = (a_i + b_i + c_{i-1}) \bmod 2$ and carry $c_i = 1$. If carry $c_{h-1} = 1$ then this must be added to d_0, possibly resulting in further 'carries'. The easiest way to do this is to add $100\ldots0$ to $d_0 d_1 \ldots d_{h-1}$. No carry c_{h-1} will be generated in this addition.

Example 1.1.2 *Let* $q = 2^5$ *and let* $a = 28$, $b = 25$. *Then the binomial expansions of* $28 \bmod 2^5 - 1$ *and* $25 \bmod 2^5 - 1$ *are, respectively,* $2^2 + 2^3 + 2^4$ *and* $2^0 + 2^3 + 2^4$, *which means that the binary representation of* $28 \bmod 2^5 - 1$ *and* $25 \bmod 2^5 - 1$ *are, respectively,* 00111 *and* 10011. *Straight addition of* $28 + 25$ *is* $2^0 + 2^2 + (2^3 + 2^3) + (2^4 + 2^4) = 2^0 + 2^2 + 2^4 + 2^5 \equiv 2^1 + 2^2 + 2^4 \bmod (2^5 - 1)$. *This addition can be illustrated in terms of the binary representations of* a *and* b *as follows:*

$$\begin{array}{lcccccc} 28 \bmod (2^5-1) & \overset{\text{bin.rep}^n}{=} & 0 & 0 & 1 & 1 & 1 \\ 25 \bmod (2^5-1) & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 0 & 1 & 1 \\ & = & 1 & 0 & 1 & 0 & 1 \\ & + & 1 & 0 & 0 & 0 & 0 \\ 53 \bmod (2^5-1) & \overset{\text{bin.rep}^n}{=} & 0 & 1 & 1 & 0 & 1 \end{array}$$

1.1.2 Projective planes

The following material on projective planes can be found in Hirschfeld [13] and Dembowski [5].

Definition 1.1.3 A *projective plane* Π is a set of *points* and a set of *lines* (subsets of points) satisfying the following axioms.

1. Two distinct points are contained in exactly one line.
2. Two distinct lines intersect in one and only one point.
3. Π contains a quadrangle (four distinct points no three of which are incident with the same line).

Let V be an 3-dimensional vector space over the field $GF(q)$ with origin $\underline{0}$. Consider the equivalence relation on the vectors of $V - \{\underline{0}\}$, whose equivalence classes are the one-dimensional subspaces of V with the origin deleted, defined as follows. If $X, Y \in V - \{\underline{0}\}$, and $X = (x_0, x_1, x_2)$, $Y = (y_0, y_1, y_2)$ where $x_i, y_i \in GF(q)$, then X is equivalent to Y if, for some non-zero scalar t, $y_i = tx_i$ for all i. Then

we define the equivalence classes of this equivalence relation to be the points of the 2-*dimensional projective space over* $GF(q)$, and is denoted by $PG(2,q)$. Thus, we can write $PG(2,q)$ to be the set $\{(x_0,x_1,x_2) : x_i \in GF(q),\ x_i \text{ not all zero}\}$ and (x_0,x_1,x_2) is identified with $\rho(x_0,x_1,x_2)$ for $\rho \in GF(q)^*$. The lines of $PG(2,q)$ are the points of a 2-dimensional subspace of V. It is easy to check that $PG(2,q)$ is a projective plane called the classical or Desarguesian projective plane.

We then call $\rho(x_0,x_1,x_2)$ the *homogeneous coordinates* of the point (x_0,x_1,x_2) of $PG(2,q)$. We fix a coordinate system of $PG(2,q)$ by choosing 4 of its points (no 3 collinear) and labelling them $(1,0,0),(0,1,0),(0,0,1)$ and $(1,1,1)$, and calling the *fundamental quadrangle* of $PG(2,q)$. Hence a subspace of V of dimension 1 or 2 is called, respectively, a point or a line of $PG(2,q)$.

The number of points of a projective plane π is $\frac{q^3-1}{q-1} = q^2+q+1$ which is the same as the number of lines of π. Each line has $q+1$ points and each pencil of lines through a point contains $q+1$ lines; these lines exhaust π.

Definition 1.1.4 A *collineation* σ of a projective plane is a one to one mapping of points onto points and lines onto lines which preserves incidence (hence collinearity). We denote the image of X under σ by X^σ. The set of all collineations of $PG(2,q)$ forms a group under composition, which is denoted as $P\Gamma L(3,q)$.

Definition 1.1.5 Let $X(x_0,x_1,x_2)$ and $X'(x_0',x_1',x_2')$ be points of $PG(2,q)$. A *homography* of $PG(2,q)$ is a map $f : PG(2,q) \to PG(n,q)$ where $f : X \mapsto X'$ is defined by:

$$\begin{bmatrix} x_0' \\ x_1' \\ x_2' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix}$$

where $a_{ij} \in GF(q)$, and the matrix $A = [a_{ij}]$ has a nonzero determinant.

Note that a homography f of $PG(2,q)$ is a collineation, see [8] Section 2.4 Theorem 1. The group of homographies of $PG(2,q)$ is denoted by $PGL(3,q)$.

If $\{P_1, P_2, P_3, P_4\}$ and $\{P_1', P_2', P_3', P_4'\}$ are sets of four points, no three collinear in $PG(2,q)$, then there exists a unique homography $f \in PGL(3,q)$ such that $f : P_i \mapsto P_i'$, see [8] Section 3.2 Theorem 6. Thus the group $P\Gamma L(3,q)$ is transitive on the quadrangles of $PG(2,q)$.

We say a line ℓ of a projective plane π is fixed *pointwise* by a collineation $\sigma \in P\Gamma L(3,q)$ if $P^\sigma = P$ for all points P on ℓ. A line ℓ fixed pointwise by a collineation σ is called an *axis* of σ. Dually, a point P of π is fixed *linewise* by a collineation σ if $\ell^\sigma = \ell$ for all lines ℓ through P. A point P fixed linewise by a collineation σ is called a *centre* of σ.

A non-identity collineation has at most one centre and at most one axis, and a collineation σ has a centre P if and only if σ has an axis ℓ (see [2] Chapter II.5 Theorem 4 and 5). If $P \in \ell$ then σ is an *elation* and if $P \notin \ell$ then σ is a *homology.*

Let π be a projective plane. A *translation* of π is an elation of π whose axis is some line L_∞ of π and whose centre is some point $P \in L_\infty$.

1.2 Introduction to hyperovals

In this section we shall introduce the concept of hyperovals of $PG(2,q)$, and give the motivating examples provided by the conics in $PG(2,q)$. In particular we are interested in the known classes of monomial hyperovals in $PG(2,2^h)$ and Glynn's condition for the existence of a monomial hyperoval which is the fundamental result used in chapters 3 and 4.

Definition 1.2.1 A *conic* C in $PG(2,q)$ is the collection of points of $PG(2,q)$ whose coordinates satisfy a homogeneous equation f of degree 2 with coefficients in $GF(q)$.

A *conic* C has equation $f(x) = \sum_{i,j=0}^{2} c_{ij}x_ix_j$, for some $c_{ij} \in GF(q)$. If f is reducible then C comprises a pair of lines, possibly coincident or possibly defined in a quadratic extension of $GF(q)$ with their point of intersection defined in $GF(q)$. If

$\mathcal{C}$ comprises a pair of distinct lines then it is (simply) *degenerate*, and if it comprises a line counted twice then it is *doubly degenerate*. Otherwise $\mathcal{C}$ is *non-degenerate*.

Let $\mathcal{C}$ be a non-degenerate conic of $PG(2,q)$. If $\mathcal{C}$ contains one point P of $PG(2,q)$ (that is, defined in $GF(q)$) then it contains exactly $q+1$ such points, and no three of these are collinear, see [13] Lemma 7.2.2. Furthermore, if $q \geq 4$ there is a unique non-degenerate conic $\mathcal{C}$ of $PG(2,q)$ which contains five distinct given points, no four of which are collinear, see [35] Chapter 5 Theorem 2. Since a line of $PG(2,q)$ always intersects a conic in 0, 1, or 2 points, it is always called an *external*, *tangent* or *secant* line.

Lemma 1.2.1 ([13] Corollary 4 of Lemma 7.2.3) *In $PG(2,q)$ for q even, the $q+1$ tangents to a non-degenerate conic are concurrent. This point of concurrency is called the nucleus.*

Thus, a non-degenerate conic together with its nucleus is a set of $q+2$ points, no three of which are collinear.

Definition 1.2.2 A k-arc $\mathcal{K}$ is a set of k points of $PG(2,q)$ such that no three of them are collinear.

Since no line of $PG(2,q)$ can have more than two points in common with a k-arc $\mathcal{K}$, a line of $PG(2,q)$ is a *chord*, *tangent* or *external line* of $\mathcal{K}$ according as it contains two, one or no points of $\mathcal{K}$. The points of a non-degenerate conic of $PG(2,q)$ form a $(q+1)$-arc, see [13] Lemma 7.2.3, and a conic together with its nucleus is a $(q+2)$-arc when q is even.

Theorem 1.2.2 ([13] Theorem 8.1.3) *Let $\mathcal{K}$ be a k-arc of $PG(2,q)$. Then the maximum attainable value of k is $q+1$ when q is odd and $q+2$ when q is even.*

Definition 1.2.3 An *oval* of $PG(2,q)$ is a $(q+1)$-arc and a *hyperoval* of $PG(2,q)$ is a $(q+2)$-arc.

As an example, the points of a non-degenerate conic in $PG(2,q)$ form an oval and a conic together with its nucleus is a hyperoval. The $q+1$ tangents to an oval of $PG(2,q)$ with q even are concurrent and the point of concurrency is called the *nucleus*, see [13] Lemma 8.1.4. Hence for q even, an oval can be uniquely completed to a hyperoval by adding the nucleus.

Note that in $PG(2,q)$, q even, there exist hyperovals comprising the points of conic and its nucleus; this type of hyperoval is called a *regular* hyperoval.

When q is odd, every oval is an irreducible conic, see [30], thus completing the classification of ovals in $PG(2,q)$ for q odd. However, when q is even this is not the case.

We are interested in the case when q is even, so we let $q = 2^h$ for some positive integer h.

Given a hyperoval, an oval can be obtained by deleting one of the points of the hyperoval. This deleted point is the nucleus of the resulting oval. There are up to $q+2$ ovals which can be obtained from a hyperoval in this way, but we only distinguish those which are distinct under the automorphism group $P\Gamma L(3,q)$ of $PG(2,q)$. Thus to study ovals when q is even, it is useful to first find hyperovals and then to determine the possible ovals contained in it (see [19] Theorem 1.1).

By the transitivity of the collineation group $P\Gamma L(3,q)$ of $PG(2,q)$ on quadrangles, every hyperoval can be mapped by an element of $P\Gamma L(3,q)$ to one containing the *fundamental quadrangle* (1,0,0), (0,1,0), (0,0,1) and (1,1,1). Since we wish to classify hyperovals up to the action of $P\Gamma L(3,q)$, we only need to consider hyperovals which contain the fundamental quadrangle. Any such hyperoval can be described by a *permutation polynomial* according to the next theorem.

Theorem 1.2.3 ([13], Theorem 8.4.2) *A hyperoval of $PG(2,q)$, q even, $q > 2$, which contains the fundamental quadrangle can be written in the form*

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

where $f(t)$ is a permutation polynomial over $GF(q)$ with degree at most $q-2$ satisfying $f(0) = 0$, $f(1) = 1$ and for each $s \in GF(q)$,

$$F_s(x) = \begin{cases} \frac{f(x+s)+f(s)}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

is a permutation polynomial. Conversely, any set $\mathcal{D}(f)$ where f is as above, is a hyperoval containing the fundamental quadrangle.

Such permutation polynomials f are called *o-polynomials*, following Cherowitzo [3].

If f is an o-polynomial then the conditions $f(0) = 0$ and $f(1) = 1$ imply that f has no constant term and that the sum of the coefficients of f is 1. The next theorem also concerns the terms appearing in an o-polynomial.

Theorem 1.2.4 ([34]) *The coefficient of each term of odd power in an o-polynomial is zero. That is, if $\mathcal{D}(f)$ with*

$$f(x) = \sum_{i=1}^{q-2} a_i x^i$$

is a hyperoval of $PG(2,q)$ with $q = 2^h$, $q > 2$, then

$$f(x) = \sum_{j=1}^{\frac{q-2}{2}} a_{2j} x^{2j}.$$

Every known hyperoval in $PG(2,q)$, $q = 2^h$ and $h \geq 2$, is the image under an element of $P\Gamma L(3,q)$ of one of the following hyperovals:

(1) The regular hyperovals $\mathcal{R} = \mathcal{D}(x^2)$, $h \geq 2$;

(2) the translation hyperovals $\mathcal{T} = \mathcal{D}(x^{2^n})$, $(n,h) = 1$, $1 \leq n \leq h-1$ and $h \geq 3$, see Segre 1957 [33];

(3) the Segre(-Bartocci) [34] [31] hyperovals $\mathcal{D}(x^6)$, where $h \geq 5$ is odd;

(4) the Glynn hyperovals [9] $\mathcal{G}_1 = \mathcal{D}(x^{\sigma+\gamma})$, where $h \geq 7$ is odd, with $\sigma \equiv \sqrt{2} \bmod (q-1)$, $\gamma \equiv \sqrt{\sigma} \bmod (q-1)$;

(5) the Glynn hyperovals [9] $\mathcal{G}_2 = \mathcal{D}(x^{3\sigma+4})$, where $h \geq 7$ is odd, $\sigma \equiv \sqrt{2} \bmod (q-1)$;

(6) the Lunelli-Sce [15] hyperovals $\mathcal{L} = \mathcal{D}(f)$, where $f(x) = x^{12} + x^{10} + \eta^{11}x^8 + x^6 + \eta^2 x^4 + \eta^9 x^2$, $q = 16$ and η is a primitive element of $GF(16)$ satisfying $\eta^4 = \eta + 1$. This was the first case of a hyperoval not being equivalent to one described by a monomial o-polynomial;

(7) the Payne hyperovals [26] $\mathcal{P} = \mathcal{D}(x^{\frac{1}{6}} + x^{\frac{3}{6}} + x^{\frac{5}{6}})$, where $h \geq 5$ is odd and the exponents are read modulo $q-1$;

(8) the Cherowitzo hyperovals [3] $\mathcal{C} = \mathcal{D}(x^\sigma + x^{\sigma+2} + x^{3\sigma+4})$, where h=5, 7, 9, 11 or 13 and σ is an automorphism of $GF(q)$ with $\sigma^2 \equiv 2 \bmod (q-1)$;

(9) the O'Keefe-Penttila hyperovals [22] in $PG(2,32)$ $\mathcal{D}(f)$, where $f(x) = x^4 + \omega^{11}x^6 + \omega^{20}x^8 + \omega^{11}x^{10} + \omega^6 x^{12} + \omega^{11}x^{14} + x^{16} + \omega^{11}x^{18} + \omega^{20}x^{20} + \omega^{11}x^{22} + \omega^6 x^{24} + \omega^{11}x^{26} + x^{28}$, with ω being a primitive root of $GF(32)$ satisfying $\omega^5 = \omega^2 + 1$;

(10) Penttila-Pinneri hyperovals [27] in $PG(2,64)$

(I) $\mathcal{D}(f)$ with $f(x) = \omega^{42}x^2 + \omega^{21}x^4 + \omega^{42}x^6 + x^8 + \omega^{21}x^{10} + x^{12} + \omega^{21}x^{14} + \omega^{21}x^{16} + x^{20} + x^{22} + \omega^{42}x^{26} + \omega^{42}x^{28} + \omega^{21}x^{30} + \omega^{42}x^{32} + \omega^{42}x^{36} + \omega^{21}x^{38} + \omega^{42}x^{40} + x^{42} + \omega^{21}x^{44} + \omega^{21}x^{48} + x^{52} + \omega^{21}x^{54} + \omega^{21}x^{56} + \omega^{21}x^{58} + \omega^{21}x^{60} + \omega^{21}x^{62}$, and

(II) $\mathcal{D}(f)$ with $f(x) = \omega^{21}x^4 + \omega 42x^6 + \omega^{21}x^8 + \omega^{21}x^{10} + \omega^{42}x^{12} + \omega^{21}x^{14} + \omega^{21}x^{16} + \omega^{42}x^{18} + \omega^{42}x^{20} + x^{24} + \omega^{42}x^{26} + x^{30} + \omega^{42}x^{32} + \omega^{21}x^{34} + \omega^{42}x^{36} + \omega^{21}x^{38} + \omega^{21}x^{40} + \omega^{42}x^{42} + \omega^{21}x^{44} + \omega^{21}x^{46} + \omega^{42}x^{48} + \omega^{42}x^{50} + \omega^{21}x^{52} + \omega^{21}x^{54} + \omega^{21}x^{58} + \omega^{21}x^{60} + x^{62}$.

where ω is a primitive element of $GF(64)$, satisfying $\omega^4 = \omega + 1$;

(11) Penttila-Royle [28] hyperovals in $PG(2,64)$ $\mathcal{D}(f)$ with $f(x) = x^4 + \omega^{21}x^6 + x^8 + \omega^{42}x^{10} + x^{14} + \omega^{21}x^{16} + \omega^{42}x^{18} + \omega^{42}x^{24} + \omega^{21}x^{26} + \omega^{21}x^{28} + \omega^{21}x^{30} + \omega^{21}x^{32} + x^{34} + \omega^{42}x^{36} + \omega^{21}x^{40} + x^{42} + \omega^{42}x^{44} + x^{48} + \omega^{42}x^{50} + \omega^{42}x^{52} + \omega^{21}x^{58} + \omega^{42}x^{60} + x^{62}$, where ω is a primitive element of $GF(64)$, satisfying $\omega^4 = \omega + 1$;

The first irregular hyperovals to be found were the *translation* hyperovals [33].

If $q = 2, 4$ or 8, every hyperoval of $PG(2, q)$ is regular, see [13], Lemma 8.4.1 and Theorem 9.2.3.

Hall [11] by computer and O'Keefe and Penttila [18] without the use of a computer proved that the only hyperovals in $PG(2, 16)$ are the regular and Lunelli-Sce hyperovals.

Penttila and Royle [28] have classified all hyperovals in $PG(2, 32)$. The hyperovals are the regular, translation, Segre-Bartocci, Payne, Cherowitzo and O'Keefe-Penttila hyperovals.

One class of hyperovals of $PG(2, q)$ that has been completely characterized is the class of *translation hyperovals.* If $\mathcal{D}(f)$ is a hyperoval and $f(x+y) = f(x)+f(y)$ for all $x, y \in GF(q)$, then $\mathcal{D}(f)$ is called a *translation hyperoval.* This is because $\mathcal{D}(f)$ remains fixed under the following elation e_c, $c \in GF(q)$,

$$\begin{aligned} x_0 &\longrightarrow x_0, \\ x_1 &\longrightarrow x_1 + cx_0, \\ x_2 &\longrightarrow x_2 + f(c)x_0 \end{aligned}$$

where (x_0, x_1, x_2),$x_i \in GF(q)$, represents a point of $PG(2, q)$, which is a translation with axis $x_2 = 0$.

The set of points $\mathcal{D}(x^{2^n})$ with $(n, h) = 1$ is a translation hyperoval and conversely, by Segre and Bartocci [31], [34], Payne [25], every translation hyperoval is of the type $\mathcal{D}(x^{2^n})$. An alternative proof can be found in Hirschfeld [12]. For a full account on translation hyperovals, see [13] Section 8.5.

Theorem 1.2.5 ([13] Theorem 8.5.4) *In $PG(2, 2^h)$, $\mathcal{D}(f)$ is a translation hyperoval if and only if $\mathcal{D}(f) = \mathcal{D}(x^{2^n})$ with $(n, h) = 1$.*

In section 3.2 we shall obtain the result that $\mathcal{D}(x^{2^n})$ is a hyperoval if and only if $(n, h) = 1$ using a new method.

Definition 1.2.4 Let $\mathcal{D}(k)$ $(k \not\equiv 0 \bmod (q-1), k \in \mathbf{Z})$ be the set of points of $PG(2,q)$

$$\mathcal{D}(k) = \{(t^k, t, 1) : t \in GF(q)\} \cup \{(1,0,0), (0,1,0)\}.$$

Since $t^{q-1} = 1$ for all $t \in GF(q)^*$; if $x_1 \equiv x_2 \pmod{q-1}$ then $t^{x_1} = t^{x_2}$ for all $t \in GF(q)^*$. Hence we can assume that $1 \leq k \leq q-2$.

We call a hyperoval which is the image under an element of $P\Gamma L(3,q)$ of a hyperoval of type $\mathcal{D}(k)$, $1 \leq k \leq q-2$, a *monomial hyperoval.* Each known monomial hyperoval in $PG(2,q)$ is the image under an element of $P\Gamma L(3,q)$ of one of the following:

1. The regular hyperovals $\mathcal{R} = \mathcal{D}(2)$, $h \geq 2$,
2. the translation hyperovals $\mathcal{T} = \mathcal{D}(2^n)$, $(n,h) = 1$, $1 \leq n \leq h-1$ and $h \geq 3$, see Segre 1957 [33]
3. the Segre hyperovals $\mathcal{D}(6)$, where $h > 5$ is odd, [31]
4. the Glynn hyperovals [9] $\mathcal{G}_1 = \mathcal{D}(\sigma + \gamma)$, where $h \geq 7$ is odd, with $\sigma \equiv \sqrt{2} \bmod (q-1), \gamma \equiv \sqrt{\sigma} \bmod (q-1)$
5. the Glynn hyperovals [9] $\mathcal{G}_2 = \mathcal{D}(3\sigma+4)$, where $h \geq 7$ is odd, $\sigma \equiv \sqrt{2} \bmod (q-1)$.

The following characterization of monomial hyperovals is useful:

Theorem 1.2.6 ([13] Corollary 2 Theorem 8.4.2) *In $PG(2,q)$, with q even and $q > 2$, $\mathcal{D}(k)$ is a hyperoval of $PG(2,q)$ if and only if*

(1) $(k, q-1) = 1$

(2) $(k-1, q-1) = 1$ *and*

(3) $f_k(t) = \frac{(t+1)^k+1}{t}$ *is a permutation polynomial*

(notice that $f_k(t)$ is a polynomial, for q even, implies numerator has no constant term).

Theorem 1.2.7 ([13] Theorem 8.4.3) *If $(k, q-1) = (k-1, q-1) = 1$ then*

$$\mathcal{D}(k) \cong \mathcal{D}(1-k) \cong \mathcal{D}(k^{-1}) \cong \mathcal{D}(1-k^{-1}) \cong \mathcal{D}((1-k)^{-1}) \cong \mathcal{D}(k(k-1)^{-1})$$

where $k, 1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all reduced modulo $q-1$ (0 is reduced to 0 and multiples of $q-1$ reduced to $q-1$) and $\cong$ means that there is a homography which maps one hyperoval to the other.

Our main objective is to investigate whether a monomial hyperoval must be one of the five types above. By the definition of monomial hyperoval, Theorem 1.2.3 and the transitivity of $P\Gamma L(3,q)$ on quadrangles it is enough to determine which integers k are such that $\mathcal{D}(k)$ is a hyperoval in $PG(2,2^h)$. To facilitate our investigation, we shall be using Theorem 1.2.8 below which is a necessary and sufficient numerical condition that determines whether a set $\mathcal{D}(k)$ for a given k is a hyperoval in $PG(2,2^h)$. Before stating the theorem, we need the following partial ordering $\preceq$ on the set of integers n where $0 \leq n \leq q-1$.

Definition 1.2.5 ([9]) The partial ordering $\preceq$ on the set of integers $N_q = \{n : 0 \leq n \leq q-1\}$ is defined as follows : if $a, b \in N_q$, and if

$$a = \sum_{i=0}^{h-1} a_i 2^i, \; b = \sum_{i=0}^{h-1} b_i 2^i$$

where a_i,$b_i \in \{0,1\}$ for all i, then $a \preceq b$ if and only if $a_i \leq b_i$ for all i. In other words, all the terms appearing in the binomial expansion of a must also appear in the binomial expansion of b.

Theorem 1.2.8 ([9] Theorem A) *$\mathcal{D}(k)$ is a hyperoval of $PG(2,q)$ if and only if $d \not\preceq kd$, for all $d \in \{1, 2, \ldots, q-2\}$, where kd is reduced modulo $q-1$ to lie in $N_q = \{1, \ldots, q-2\}$ (with the convention that 0 is reduced to 0 and any multiples of $q-1$ are reduced to $q-1$).*

Since this result is fundamental to our work, we now give the proof, starting with some known result about polynomials.

Theorem 1.2.9 ([6]) *If $f(a) = 0 \iff a = 0$, then $f(t)$ is a permutation polynomial of $GF(q)$ if and only if $[f(t)]^r \bmod (t^q - t)$ has zero coefficient for t^{q-1} for all $1 \leq r \leq q-2$.*

Theorem 1.2.10 ([6]) *Let g be any function from $GF(q)$ to itself. Then there exists a unique polynomial f over $GF(q)$ of degree at most $q-1$ (see Theorem 2.1.1) such that $f(\lambda) = g(\lambda)$ for all $\lambda \in GF(q)$. In fact,*

$$f(t) = \sum_{i=0}^{q-1} a_i t^i, \ a_i \in GF(q),$$

where

$$a_0 = g(0), \ a_r = -\sum_{\lambda \in GF(q)^*} g(\lambda)\lambda^{-r} \ (1 \leq r \leq q-2), \text{ and } a_{q-1} = -\sum_{\lambda \in GF(q)^*} g(\lambda).$$

Theorem 1.2.11 ([9]) *If $k \in \mathbf{Z}$ then the expansion of $(1+t)^k \bmod (t^q - t)$ over $GF(q)$, may be calculated as follows. Firstly, if $k = 0$, then $(1+t)^k = 1$. Secondly, if $k \neq 0$, then reduce $k \bmod (q-1)$ so that $1 \leq k \leq q-1$. Then*

$$(1+t)^k = \sum_{\substack{c \preceq k \\ c \in \overline{N}_q}} t^c \bmod (t^q - t).$$

Proof. Let $k \bmod (q-1) = \sum_{i=0}^{h-1} k_i 2^i$ where $k_i \in \{0,1\}$, be the binomial expansion of k. Then we can write k as a sum of powers of 2 as follows

$$k = 2^a + 2^b + 2^c + \cdots$$

where $a, b, \ldots$ are integers belonging to the set $\{1, 2, \ldots, h-1\}$.

Now, for $k \neq 0$, we have

$$\begin{aligned}
(1+t)^k &= (1+t)^{2^a + 2^b + 2^c + \cdots} \\
&= (1+t)^{2^a}(1+t)^{2^b}(1+t)^{2^c}\cdots \\
&= (1+t^{2^a})(1+t^{2^b})(1+t^{2^c})\cdots
\end{aligned}$$

as all the powers $2^a, 2^b, 2^c, \ldots$ belong to the binomial expansion of k. ■

Proof of Theorem 1.2.8. Suppose that $k \in \{1, \ldots, q-2\}$. Then by Theorem 1.2.6 $\mathcal{D}(k)$ is a hyperoval of $PG(2,q)$ if and only if $f_k(t) = \frac{(t+1)^k+1}{t}$ is a permutation polynomial of $GF(q)$.

Now $f_k(t) = \frac{(t+1)^k+1}{t}$(if $t \neq 0$) $= \frac{(t+1)^k+1}{(t+1)+1} = (t+1)^{k-1}+(t+1)^{k-2}+\cdots+(t+1)+1$. Then,

$$f_k(0) = \underbrace{1+1+\cdots+1}_{k \text{ times}} = \begin{cases} 0 & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd} \end{cases}$$

If $t \neq 0$ then $f_k(t) = 0 \Leftrightarrow (t+1)^k + 1 = 0 \Leftrightarrow (t+1)^k = 1 \Leftrightarrow t+1 = 1^{k^{-1}} \Leftrightarrow t+1 = 1 \Leftrightarrow t = 0$, a contradiction. So $f_k(t)$ is a permutation polynomial if and only if k is even and $[f_k(t)]^r \bmod (t^q - t)$ has zero coefficient for t^{q-1}, for all $r \in \{1, \ldots, q-2\}$.

Now, by Theorem 1.2.10, the coefficient of t^{q-1} in $[f_k(t)]^r \bmod (t^q - t)$ is

$$-\sum_{\lambda \in GF(q)^*} \left(\frac{(\lambda+1)^k+1}{\lambda}\right)^r = 0, \text{ for all } r \in \{1, \ldots, q-2\}.$$

This means the coefficient of t^{q-1} in $[f_k(t)]^r \bmod (t^q - t)$ is zero if and only if

$$\sum_{\lambda \in GF(q)^*} \left(\frac{(\lambda+1)^k+1}{\lambda}\right)^r = 0, \text{ for all } r \in \{1, \ldots, q-2\}.$$

Applying Theorem 1.2.10 again, if we let $g(t) = [(t+1)^k + 1]^r$, $t \in GF(q)$, $1 \leq r \leq q-2$, then g corresponds to a unique polynomial f over $GF(q)$ and $\deg(f) \leq q-1$. Now $f(t) = \sum_{i=0}^{q-1} a_i t^i$, $a_i \in GF(q)$, and for $r = 1, 2, \ldots, q-2$ the coefficient of t^r in $f(t)$ is $a_r = -\sum_{\lambda \in GF(q)^*} \left(\frac{(\lambda+1)^k+1}{\lambda}\right)^r$. Hence,

$$\sum_{\lambda \in GF(q)^*} \left(\frac{(\lambda+1)^k+1}{\lambda}\right)^r = 0, \text{ for all } r \in \{1, \ldots, q-2\} \Longleftrightarrow$$

the coefficient of t^r in $[(t+1)^k + 1]^r$ is zero, for all $r \in \{1, \ldots, q-2\}$.

Now, $[(t+1)^k + 1]^r$ has zero coefficient for t^r if and only if the expansion of $[(t+1)^k + 1]^r \bmod (t^q - t)$, namely (see Theorem 1.2.11)

$$\sum_{\substack{d \preceq r \\ d \in \mathbf{N}_q}} ((t+1)^k)^d,$$

has zero coefficient for t^r for all $r \in \{1, \ldots, q-2\}$. Applying Theorem 1.2.11 again the expansion of $(t+1)^{kd} \bmod (t^q - t)$ can be written as

$$\sum_{\substack{e \preceq kd \\ e \in \mathbf{N}_q}} t^e$$

which means that $\sum_{d \preceq r}((t+1)^k)^d$ has zero coefficient for t^r, for all $r \in \{1, \ldots, q-2\}$, if and only if $\sum_{d \preceq r} \left(\sum_{e \preceq kd} t^e \right)$ has zero coefficient for t^r, for all $r \in \{1, \ldots, q-2\}$.

The terms in $\sum_{d \preceq r} \left(\sum_{e \preceq kd} t^e \right)$ with t^r are exactly $\sum_{d \preceq r} \left(\sum_{r \preceq kd} t^r \right) = a_r t^r$ for some $a_r \in GF(q)$. As the coefficient of t^r is $a_r = 0$, this implies $\sum_{d \preceq r \preceq kd} t^r = 0$. Conversely, $\sum_{d \preceq r \preceq kd} t^r = 0$ implies that $a_r t^r = 0$ and so the coefficient of t^r is 0. Hence $\sum_{d \preceq r} \left(\sum_{e \preceq kd} t^e \right)$ has zero coefficient for t^r, for all $r \in \{1, \ldots, q-2\}$ if and only if $\sum_{d \preceq r \preceq kd} t^r = 0$ for all $r \in \{1, 2, \ldots, q-2\}$.

Now as q is even, $\sum_{d \preceq r \preceq kd} t^r = 0$ if and only if $|\{d : d \preceq r \preceq kd\}| \equiv 0 \bmod 2$, for all $r \in \{1, \ldots, q-2\}$.

Finally we show that $|\{d : d \preceq r \preceq kd\}| \equiv 0 \bmod 2$, for all $r \in \{1, \ldots, q-2\}$, if and only if $d \not\preceq kd$, for all $d \in \{1, \ldots, q-2\}$ as follows. Suppose $|\{d : d \preceq r \preceq kd\}| \equiv 0 \bmod 2$, for all $r \in \{1, \ldots, q-2\}$, and suppose there exists a d' with $d' \preceq kd'$, $d' \in \{1, \ldots, q-2\}$. Suppose further that d' is minimal with respect to $\preceq$. Putting $r = d'$ implies that $\{d : d \preceq d' \preceq kd\} = \{d'\}$. Now $|\{d'\}| = 1 \not\equiv 0 \bmod 2$ which contradicts our initial assumption. Hence there is no such d' and $d \not\preceq kd$, for all $d \in \{1, \ldots, q-2\}$. Conversely, if $d \not\preceq kd$, for all $d \in \{1, \ldots, q-2\}$, then $\{d : d \preceq r \preceq kd\} = \emptyset$ which implies $|\{d : d \preceq r \preceq kd\}| = 0 \equiv 0 \bmod 2$, for all $r \in \{1, \ldots, q-2\}$.

Finally, $d \not\preceq kd$, for all $d \in \{1, \ldots, q-2\}$, implies that $(k, q-1) = (k-1, q-1) = 1$, as follows. If $(k, q-1) = l \neq 1$ say, then $m = \frac{q-1}{l}$ satisfies $m \in \{1, \ldots, q-2\}$ and $mk \equiv q-1 \bmod (q-1)$. Since $mk \bmod (q-1) = 2^0 + 2^1 + \cdots + 2^{h-1}$, we must have $m \preceq mk \bmod (q-1)$ which contradicts our assumption that $d \not\preceq kd$, for all $d \in \{1, \ldots, q-2\}$, and so $(k, q-1) = 1$. Similarly, suppose $(k-1, q-1) = n \neq 1$. Let

$p = \frac{q-1}{n}$. Then p satisfies $p(k-1) \equiv 0 \bmod (q-1)$ which implies $pk \equiv p \bmod (q-1)$. Hence $p \equiv pk \bmod (q-1)$ implies $p \preceq pk \bmod (q-1)$, $p \in \{1, \ldots, q-2\}$, a contradiction. So $(k-1, q-1) = 1$. ■

Chapter 2

Permutation polynomials and hyperovals

In this chapter we provide a review of a result from the paper "*Permutation properties of the polynomials* $1 + x + \cdots + x^k$ *over a finite field*" by Matthews [17], which shows that $\mathcal{D}(k+1)$ is a hyperoval in $PG(2,q)$, q even, if and only if $1+x+x^2+\cdots+x^k$ is a permutation polynomial over $GF(q)$. In other words, the condition that $\mathcal{D}(k+1)$ is a hyperoval in $GF(q)$ is equivalent to $h_k(x)$ being a permutation polynomial over $GF(q)$. This gives an easy proof that some of the known monomial hyperovals are indeed hyperovals, namely the regular, translation and Segre hyperovals. Unfortunately the polynomials corresponding to the Glynn hyperovals are not readily recognizable as permutation polynomials, so this approach does not work.

2.1 Introduction

If $\phi : GF(q) \longrightarrow GF(q)$ is an arbitrary function from $GF(q)$ into $GF(q)$, then there exists a unique polynomial $g \in GF(q)[x]$, of degree less than q, representing ϕ, in the sense that $g(c) = \phi(c)$ for all $c \in GF(q)$. The polynomial g can be found by computing the Lagrange Interpolation polynomial for the given function ϕ according to the following theorem.

Theorem 2.1.1 (Lagrange Interpolation Formula, [16]) *For $n \geq 0$ an integer, let $a_0, \ldots, a_n$ be $n+1$ distinct elements of a finite field F, and let $b_0, \ldots, b_n$ be $n+1$ arbitrary elements of F. Then there exists exactly one polynomial $g \in F[x]$ of degree at most n such that $g(a_i) = b_i$ for $i = 0, \ldots, n$. This polynomial is given by*

$$g(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} (a_i - a_k)^{-1}(x - a_k).$$

Alternatively, we can use the following formula (see [16] Equation (7.1) of Section 7.1) to compute $g(x)$

$$g(x) = \sum_{c \in GF(q)} \phi(c)(1 - (x - c)^{q-1}).$$

In the case when ϕ is already a polynomial function, say $\phi : c \longrightarrow f(c)$, $c \in GF(q)$, with $f \in GF(q)[x]$, g can be obtained from f by reduction modulo $x^q - x$ according to the following result:

Lemma 2.1.2 ([16]) *For $f, g \in GF(q)[x]$, we have $f(c) = g(c)$ for all $c \in GF(q)$ if and only if $f(x) \equiv g(x) \bmod (x^q - x)$.*

Proof. By the division algorithm we can write $f(x) - g(x) = h(x)(x^q - x) + r(x)$ with $h, r \in GF(q)[x]$ and $\deg r < q$. Then $f(c) = g(c)$ for all $c \in GF(q)$ if and only if $r(c) = 0$ for all $c \in GF(q)$ (since if $c \in GF(q)$ then $c^q = c$). This is true if and only if $r = 0$ and hence $f(x) \equiv g(x) \bmod (x^q - x)$. ■

The following is Hermite's Criterion, which is a necessary and sufficient condition for a polynomial to be a permutation polynomial.

Theorem 2.1.3 (Hermite's Criterion, [16]) *Let $GF(q)$ be of characteristic p. Then $f \in GF(q)[x]$ is a permutation polynomial of $GF(q)$ if and only if the following two conditions hold:*

(i) *f has exactly one root in $GF(q)$;*

(ii) *for each integer* t *with* $1 \leq t \leq q-2$ *and* $t \not\equiv 0 \bmod p$, *the reduction of* $f(x)^t \bmod (x^q - x)$ *has degree* $\leq q-2$.

Notation. We let $h_k(x)$ denote the polynomial $1 + x + x^2 + \cdots + x^k$, $k \geq 1$.

We shall also be using the following lemma.

Lemma 2.1.4 ([17]) *Suppose* $h_k(x)$ *is a permutation polynomial over* $GF(q)$.

(i) *If* q *is even then* $(k+1, q-1) = 1$ *and* $k+1 \equiv 0 \bmod p$;

(ii) *If* q *is odd then* $(k+1, q-1) = 2$ *and* $k+1 \not\equiv 0 \bmod p$.

Proof. We note that $h_k(0) = 1$ and as $h_k(x)$ is a permutation polynomial, $h_k(1) \neq 1$. Now $h_k(1) = k+1 \bmod p$; so $k \not\equiv 0 \bmod p$ (otherwise $h_k(1) = 1$). If $x \neq 1$, then $h_k(x) = \frac{x^{k+1}-1}{x-1}$. The solutions of the equation $h_k(x) = 1$ are the solutions of the equation $x^{k+1} = x$ for $x \neq 1$. Hence there are $(k, q-1)$ solutions to the equation $h_k(x) = 1$, as follows.

The solutions of the equation $h_k(x) = 1$ are solutions of the equation $x^{k+1} = x$ if $x \neq 1$, whilst the solutions of the equation $x^{k+1} = x$ are 0 and the solutions of $x^k = 1$. Now, the number of solutions of the equation $x^k = 1$ is $(k, q-1)$ as follows. As $GF(q)^*$ is cyclic, let g be a primitive element, so $GF(q)^* = \{g^0, g^1, \ldots, g^{q-2}\}$. Let $x = g^\mu$ for some $1 \leq \mu \leq q-2$. Then $x^k = g^0 \Leftrightarrow g^{\mu k} = g^0 \Leftrightarrow \mu k \equiv 0 \bmod q-1$. Now let $d = (k, q-1)$. Then $k = k'd$ for $k' = \frac{k}{d}$ and $\left(\frac{q-1}{d}, k'\right) = 1$. Further,

$$\begin{aligned}
\mu k \equiv 0 \bmod q-1 &\iff q-1 \text{ divides } \mu k \\
&\iff \frac{q-1}{d} \text{ divides } \frac{\mu k}{d} \\
&\iff \frac{q-1}{d} \text{ divides } \mu k' \\
&\iff \frac{q-1}{d} \text{ divides } \mu \\
&\iff \mu \equiv 0 \bmod \frac{q-1}{d}.
\end{aligned}$$

Now, the number of $\mu \in \{0, 1, \ldots, q-2\}$ such that $\mu \equiv 0 \bmod \frac{q-1}{d}$ is $(k, q-1)$ because if we let $\mu = \mu' \frac{q-1}{d}$ then $0 \leq \mu' \frac{q-1}{d} \leq q-1 \Leftrightarrow 0 \leq \mu' < d$. Hence there are $(k, q-1)$ solutions to the equation $x^k = 1$.

As $h_k(x)$ is a permutation polynomial, there is only one solution to the equation $h_k(x) = 1$ and so $(k, q-1) = 1$.

Next, assume q is odd and consider the solutions to $h_k(x) = 0$. As $h_k(1) = k + 1 \bmod p$, if $k + 1 \equiv 0 \bmod p$ then $h_k(1) = 0$ and as $h_k(x)$ is a permutation polynomial, there must be no solution to $x^{k+1} = 1$, $x \neq 1$. Thus $(k+1, q-1) = 1$ as 1 is a solution. But, as q is odd, the conditions $(k, q-1) = 1$ and $(k+1, q-1) = 1$ are incompatible (if q is odd, then $q-1$ is even and one of k, $k+1$ must be even). Hence $k + 1 \not\equiv 0 \bmod p$ and $h_k(1) \neq 0$. Now 1 is a solution of $x^{k+1} = 1$ and as $h_k(x)$ is a permutation polynomial, there must exist a unique solution $x_0 \neq 1$ such that $x_0^{k+1} = 1$ and so $h_k(x_0) = 0$. Hence $x^{k+1} = 1$ must have 2 solutions (one being 1) and so $(k+1, q-1) = 2$.

If q is even, then $k \not\equiv 0 \bmod p$ implies $k + 1 \equiv 0 \bmod p$, so $h_k(1) = k + 1 \bmod p = 0$. Hence the equation $x^{k+1} = 1$ must have 1 as its only solution, and so $(k+1, q-1) = 1$. ■

The next theorem gives some examples of permutation polynomials, namely monomials and linear polynomials.

Theorem 2.1.5 ([16]) (i) *Every linear polynomial $f(x) = ax + b$ where $a, b \in GF(q)$ is a permutation polynomial of $GF(q)$.*

(ii) *The monomial x^n is a permutation polynomial of $GF(q)$ if and only if $(n, q-1) = 1$.*

Proof. **(i)** Every linear polynomial permutes the elements of $GF(q)$ as $ax + b = ay + b \Leftrightarrow ax = ay \Leftrightarrow x = y$.

(ii) x^n is a permutation polynomial of $GF(q)$ if and only if the function $\phi : c \longrightarrow c^n$, $c \in GF(q)$, is onto $GF(q)$. Let $\{c_1, c_2, \ldots, c_{q-1}\}$ be all the elements of the

multiplicative group $GF(q)^*$ of nonzero elements of $GF(q)$. Then ϕ is onto $GF(q)$ if and only if $GF(q)^* = \{c_1^n, c_2^n, \ldots, c_{q-1}^n\}$ which is true if and only if $(n, q-1) = 1$ (because the multiplicative group $GF(q)^*$ is cyclic, that is $GF(q)^*$ is generated by c_i^n for some $1 \leq i \leq q-1$). ■

Finally, we state the theorem:

Theorem 2.1.6 ([17]) *$\mathcal{D}(k+1)$ is a hyperoval of $PG(2,q)$, q even, if and only if $h_k(x)$, $k \geq 1$, is a permutation polynomial over $GF(q)$ (and if and only if $h_k(x+1)$ is a permutation polynomial over $GF(q)$, q even).*

Proof. We shall use Theorem 1.2.6 for $\mathcal{D}(k+1)$.

We observe that by Lemma 2.1.4, condition (3) implies conditions (1) and (2) in Theorem 1.2.6, as follows. As q is even,

$$h_k(x) = \begin{cases} \frac{x^{k+1}-1}{x-1} = \frac{x^{k+1}+1}{x+1} & x \neq 1 \\ k+1 \pmod 2 & x = 1 \end{cases}$$

Now $h_k(x+1)$ is a permutation polynomial if and only if $h_k(x)$ is a permutation polynomial. If $h_k(x+1)$ is a permutation polynomial then $h_k(x)$ is a permutation polynomial so by Lemma 2.1.4 we have $(k, q-1) = 1$ and $(k+1, q-1) = 1$.

Hence $\mathcal{D}(k+1)$ is a hyperoval if and only if $h_k(x)$ is a permutation polynomial over $GF(q)$, q even. ■

2.2 Application

We can apply Theorem 2.1.6 to some of the known classes of monomial hyperovals as follows.

Firstly, since $h_1(x) = 1+x$ is a linear polynomial, it is a permutation polynomial over $GF(q)$ (Theorem 2.1.5); so $\mathcal{D}(2)$ is a hyperoval by Theorem 2.1.6.

Consider translation hyperovals $\mathcal{D}(2^n)$, $(n,h)=1$, of $PG(2,2^h)$. Now $h_{2^n-1}(x+1)=\frac{(x+1)^{2^n}-1}{x}=\frac{(x^{2^n}+1)-1}{x}=x^{2^n-1}$, which is a permutation polynomial if and only if $(2^n-1,2^h-1)=1$ (Theorem 2.1.5). Now let $(n,h)=d$. Then $(2^n-1,2^h-1)=1$ if and only if $((2^d)^{\frac{n}{d}}-1,(2^d)^{\frac{h}{d}}-1)=1$. Now 2^d-1 is a common divisor of $(2^d)^{\frac{n}{d}}-1$ and $(2^d)^{\frac{h}{d}}-1$ (because $(2^d)^r-1=(2^d-1)((2^d)^{r-1}+(2^d)^{r-2}+\cdots+1)$) so that 2^d-1 divides $((2^d)^{\frac{n}{d}}-1,(2^d)^{\frac{h}{d}}-1)=1 \iff 2^d-1=1 \iff d=1$. Hence $(2^n-1,2^h-1)=1$ if and only if $d=(n,h)=1$.

Segre's oval $\mathcal{D}(6)$, h odd, turns out to correspond to Dickson's polynomial but we must first present some background material on Dickson's polynomial as follows.

Let R be a commutative ring with identity and let $R[x_1,x_2,\ldots,x_n]$ be the polynomial ring of n indeterminates (see [16]).

Definition 2.2.1 A polynomial $f\in R[x_1,x_2,\ldots,x_n]$ is called *symmetric* if

$$f(x_{i_1},x_{i_2},\ldots,x_{i_n})=f(x_1,x_2,\ldots,x_n)$$

for any permutation $i_1,i_2,\ldots,i_n$ of the integers $1,2,\ldots,n$.

Let z be an indeterminate over $R[x_1,x_2,\ldots,x_n]$ (that is, a symbol not belonging to $R[x_1,x_2,\ldots,x_n]$) and let $g(z)=(z-x_1)(z-x_2)\cdots(z-x_n)$. Then $g(z)=z^n-\sigma_1 z^{n-1}+\sigma_2 z^{n-2}+\cdots+(-1)^n\sigma_n$, where

$$\sigma_k=\sigma_k(x_1,x_2,\ldots,x_n)=\sum_{i\le i_1<\cdots<i_k\le n} x_{i_1}\ldots x_{i_k}$$

and $k=1,2,\ldots,n$. Thus:

$$\begin{aligned}
\sigma_1 &= x_1+x_2+\cdots+x_n\\
\sigma_2 &= (x_1x_2+x_1x_3+\cdots+x_1x_n)+(x_2x_3+\cdots+x_2x_n)+\cdots+x_{n-1}x_n\\
&\vdots\\
\sigma_n &= x_1x_2\ldots x_n.
\end{aligned}$$

As g remains unaltered under any permutation of the x_i, all the σ_k are symmetric polynomials belonging to $R[x_1,x_2,\ldots,x_n]$. The polynomial σ_k =

$\sigma_k(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ is called the k^{th} *elementary symmetric polynomial* in the indeterminates $x_1, x_2, \ldots, x_n$ over R.

Theorem 2.2.1 (Waring's formula, [16] Theorem 1.76) *Let $\sigma_1, \ldots, \sigma_n$ be the elementary symmetric polynomials in the indeterminates $x_1, x_2, \ldots, x_n$ over R, and let*

$$s_k = s_k(x_1, x_2, \ldots, x_n) = \begin{cases} n \in \mathbf{Z} & \text{if } k = 0, \\ x_1^k + \cdots + x_n^k \in R[x_1, \ldots, x_n] & \text{if } k \geq 1. \end{cases}$$

Then for $k \geq 1$,

$$s_k = \sum (-1)^{i_2+i_4+i_6+\cdots} \left(\frac{(i_1 + i_2 + \cdots + i_n - 1)!\ k}{i_1!\ i_2! \cdots i_n!} \right) \left(\sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_n^{i_n} \right)$$

where the summation is extended over all n tuples $(i_1, \ldots, i_n)$ of non-negative integers satisfying $i_1 + 2i_2 + \cdots + ni_n = k$. The coefficient of $\sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_n^{i_n}$ is always an integer.

Now, for any positive integer k, the symmetric polynomial $s_k(x_1, x_2) = x_1^k + x_2^k$ can be expressed in terms of the elementary symmetric polynomials $\sigma_1 = x_1 + x_2$ and $\sigma_2 = x_1 x_2$ by means of Theorem 2.2.1. This yields

$$x_1^k + x_2^k = \sum_{i_1 + 2i_2 = k} (-1)^{i_2} \frac{(i_1 + i_2 - 1)!\ k}{i_1!\ i_2!} (x_1 + x_2)^{i_1} (x_1 x_2)^{i_2}$$

where i_1 and i_2 are non-negative integers.

Putting $i_1 = k - 2j$ and $i_2 = j$, we note that the maximum value of i_2 $(= j)$ occurs when $i_1 = 0$ or 1, that is when $k - 2j = 0$ or 1, that is when $j = \lfloor \frac{k}{2} \rfloor$ (where $\lfloor \frac{k}{2} \rfloor$ denotes the greatest integer less than or equal to $\frac{k}{2}$). Hence

$$\begin{aligned} x_1^k + x_2^k &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^j \frac{(k - 2j + j - 1)!\ k}{(k - 2j)!\ j!} (x_1 + x_2)^{k-2j} (x_1 x_2)^j \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^j \left(\frac{k}{k-j} \right) \frac{(k-j)!}{(k-2j)!\ j!} (x_1 + x_2)^{k-2j} (x_1 x_2)^j \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^j \left(\frac{k}{k-j} \right) \binom{k-j}{j} (x_1 + x_2)^{k-2j} (x_1 x_2)^j. \end{aligned}$$

Hence for any positive integer k,

$$x_1^k + x_2^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-x_1 x_2)^j (x_1 + x_2)^{k-2j}, \tag{2.1}$$

and for $a \in R$ we define the *Dickson polynomial* $g_k(x, a)$ over R by

$$g_k(x,a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}. \tag{2.2}$$

If we work over the complex numbers, then these polynomials are closely related to Chebyshev polynomials of the first kind $T_k(x) = \cos(k \arccos x)$. Substituting $x_1 = e^{i\theta}$ and $x_2 = e^{-i\theta}$ into equation (2.1) we have, by equation (2.2),

$$\begin{aligned}
2\cos k\theta &= \cos k\theta + i \sin k\theta + \cos k\theta - i \sin k\theta \\
&= e^{ik\theta} + e^{-ik\theta} \\
&= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} \left(-e^{i\theta}e^{-i\theta}\right)^j \left(e^{i\theta} + e^{-i\theta}\right)^{k-2j} \\
&= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-1)^j (2\cos\theta)^{k-2j} \\
&= g_k(2\cos\theta, 1),
\end{aligned}$$

which means that

$$\begin{aligned}
2T_k(x) &= \cos(k \arccos x) \\
&= g_k(2\cos(\arccos x), 1) \\
&= g_k(2x, 1).
\end{aligned}$$

Because of this connection, Dickson polynomials are sometimes called *Chebyshev polynomials.*

If we consider a Dickson polynomial $g_k(x, a)$ over a field F, then in the field of rational functions over F in the indeterminate y we have following identity which is obtained by substituting $x_1 = y$ and $x_2 = a/y$ into equation (2.2) and using equation (2.1) as follows

$$\begin{aligned}
g_k\left(y + \frac{a}{y}, a\right) &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j \left(y + \frac{a}{y}\right)^{k-2j} \\
&= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} \left(-\frac{a}{y}y\right)^j \left(y + \frac{a}{y}\right)^{k-2j} \\
g_k\left(y + \frac{a}{y}, a\right) &= y^k + \frac{a^k}{y^k}
\end{aligned} \tag{2.3}$$

In general it is of no interest to consider the case $a = 0$ since $g_k(x, 0) = x^k$.

Theorem 2.2.2 ([16] Theorem 7.16) *The Dickson polynomial $g_k(x, a)$, with $a \in GF(q)^*$, is a permutation polynomial of $GF(q)$ if and only if $(k, q^2 - 1) = 1$.*

Proof. ($\Leftarrow$) Suppose $g_k(b, a) = g_k(c, a)$ for some $b, c \in GF(q)$. Now we can find $\beta, \gamma \in GF(q^2)^*$ such that $b = \beta + a\beta^{-1}$, $c = \gamma + a\gamma^{-1}$ (since there must exist solutions in $GF(q^2)$ to the equations $x^2 - bx + a = 0$ and $x^2 - cx + a = 0$). Then equation (2.3) yields

$$\begin{aligned} g_k(b, a) = g_k(c, a) & \\ \iff & g_k\left(\beta + \frac{a}{\beta}, a\right) = g_k\left(\gamma + \frac{a}{\gamma}, a\right) \\ \iff & \beta^k + \frac{a^k}{\beta^k} = \gamma^k + \frac{a^k}{\gamma^k} \\ \iff & \left(\beta^k - \gamma^k\right)\left(1 - \frac{a^k}{\beta^k\gamma^k}\right) = 0 \\ \iff & \left(\beta^k - \gamma^k\right)\left(\beta^k\gamma^k - a^k\right) = 0, \end{aligned}$$

and so $\beta^k = \gamma^k$ or $\beta^k = \frac{a^k}{\gamma^k}$. Now $(k, q^2 - 1) = 1$ implies, by Theorem 2.1.5, that x^k is a permutation polynomial of $GF(q^2)$, which implies that $\beta = \gamma$ or $\beta = \frac{a}{\gamma}$. In either case, it follows that $b = c$. Hence $g_k(x, a)$ is a permutation polynomial of $GF(q)$.

($\Rightarrow$) Suppose $(k, q^2 - 1) = d > 1$. If d is even, then q must be odd and k even. We must show that $g_k(x, a)$ is not a permutation polynomial of $GF(q)$. Equation (2.2) shows that $g_k(x, a)$ contains only even powers of x, and so $g_k(c, a) = g_k(-c, a)$ for all $c \in GF(q)^*$. But there exists $c \neq -c$ as q is odd, hence $g_k(x, a)$ is not a permutation polynomial of $GF(q)$.

If d is odd, then there exists an odd prime r dividing d. Then r divides k, and either $q - 1$ or $q + 1$ is divisible by r, so that we distinguish these two cases accordingly. In the first case (r divides k and $q - 1$), as the equation $x^r = 1$ has r solutions in $GF(q)$ and as r is an odd prime, there exists $b \in GF(q)$,with $b \neq 1$ or a, such that $b^r = 1$. Then, as r divides k, this implies $b^k = 1$, and so equation (2.3)

yields

$$\begin{aligned} g_k\left(b+\frac{a}{b},a\right) &= b^k+\frac{a^k}{b^k} \\ &= 1+a^k \\ &= g_k(1+a,a). \end{aligned}$$

Since $b+\frac{a}{b}=1+a$ would imply that $b=1$ or $b=a$, we have $b+\frac{a}{b}\neq 1+a$, hence $g_k(x,a)$ is not a permutation polynomial of $GF(q)$.

In the second case (r divides k and $q+1$), let $\gamma\in GF(q^2)$ be a solution of $x^{q+1}=a$. Since $x^r=1$ has r solutions in $GF(q^2)$, there exists $\beta\in GF(q^2)$, with $\beta\neq 1$ or $a\gamma^{-2}$ with $\beta^r=1$. Then also $\beta^{q+1}=1$ and $\beta^k=1$. Hence $\beta^k=1$ implies that $\gamma^k+\frac{a^k}{\gamma^k}=(\beta\gamma)^k+\frac{a^k}{(\beta\gamma)^k}$, which means that

$$g_k(\gamma+a\gamma^{-1},a)=g_k(\beta\gamma+a(\beta\gamma)^{-1},a).$$

Moreover, $\gamma+\frac{a}{\gamma}=\gamma+\frac{\gamma^{q+1}}{\gamma}=\gamma+\gamma^q\in GF(q)$ and $\beta\gamma+\frac{a}{\beta\gamma}=\beta\gamma+\frac{\beta^{q+1}\gamma^{q+1}}{\beta\gamma}=\beta\gamma+(\beta\gamma)^q\in GF(q)$. Now $\gamma+a\gamma^{-1}=\beta\gamma+a(\beta\gamma)^{-1}$ if and only if $\beta=1$ or $\beta=\frac{a}{\gamma^2}$, a contradiction. Hence $\gamma+a\gamma^{-1}\neq\beta\gamma+a(\beta\gamma)^{-1}$ and so $g_k(x,a)$ is also not a permutation polynomial of $GF(q)$. ■

Now we can apply Theorem 2.2.2 as follows. Consider $h_5(x+1)$ which is expressed as follows,

$$\begin{aligned} h_5(x+1) &= 1+(1+x)+(1+x)^2+\cdots+(1+x)^5 \\ &= x^5+6x^4+15x^3+20x^2+15x+6 \\ &= x^5+x^3+x \text{ (due to even characteristic).} \end{aligned}$$

Thus $h_5(x+1)$ is equal to the Dickson polynomial of the first kind $g_5(x,1)$ as

$$\begin{aligned} g_5(x,1) &= x^5+\frac{5}{4}\binom{4}{1}(-1)x^3+\frac{5}{3}\binom{3}{2}x \\ &= x^5-5x^3+5x \\ &= x^5+x^3+x. \end{aligned}$$

By Theorem 2.2.2, $g_5(x,1)$ is a permutation polynomial over $GF(2^h)$ if and only if $(5, 2^{2h}-1) = 1$, and this is true if and only if h is odd, where we can explain the last step as follows. Now $(5, 2^{2h}-1) = 1$ if and only if $2^{2h} \not\equiv 1 \bmod 5$ if and only if $(-1)^h \not\equiv 1 \bmod 5$ if and only if h is odd.

So, by Theorem 2.1.6, $\mathcal{D}(6)$ is a hyperoval of $PG(2,2^h)$ if and only if $h_5(x)$ is a permutation polynomial of $GF(2^h)$, which occurs if and only if h is odd.

2.3 Summary

Thus, in this chapter we have shown, following [17], that $\mathcal{D}(k+1)$ is a hyperoval if and only if a certain polynomial $h_k(x)$ is a permutation polynomial. We then used some known permutation polynomials to give new proofs that 3 classes of known monomial hyperovals are hyperovals.

It would be interesting to identify the permutation polynomials corresponding to the remaining classes of monomial hyperovals; namely the two families of Glynn hyperovals.

Chapter 3

Towards the classification of Monomial Hyperovals

In this chapter we present proofs of the results suggested by our computer searches.

Throughout the chapter we assume that we are working in the Desarguesian projective plane $PG(2,q)$ of even order $q = 2^h$, h a positive integer.

3.1 Which sets $\mathcal{D}(k)$ can be a hyperoval ?

First of all, as a Corollary to Theorems 1.2.4 and 1.2.7, $\mathcal{D}(k)$ is a hyperoval only if the following are true,

- $(k, q-1) = (k-1, q-1) = 1$, and
- $k, 1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all even when reduced modulo $q-1$ to lie in $\{1, \ldots, q-2\}$.

Thus, for a particular plane $PG(2,q)$; $q = 2^h$, we only need to consider the even values of $k \in \{1, \ldots, q-2\}$ which satisfy $(k, q-1) = (k-1, q-1) = 1$ and that $1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all even when reduced modulo $q-1$ (for otherwise, we know that $\mathcal{D}(k)$ is not a hyperoval).

The next result will further reduce the range of values of $k's$ that we need to consider.

Result 3.1.1 *Let $q = 2^h$, h a positive integer. Let $\mathcal{S}(k)$ be the set*

$$\mathcal{S}(k) = \{d : d \in \{1, \ldots, q-2\} \text{ and } d \preceq kd\}.$$

Then $\mathcal{S}(k) = \mathcal{S}(1-k)$. As usual, kd is reduced modulo $q-1$ with the usual convention.

Proof. If $\mathcal{S}(k)$ is empty, then $\mathcal{D}(k)$ is a hyperoval in $PG(2,q)$, which, by Theorem 1.2.7, implies that $\mathcal{D}(1-k)$ is also a hyperoval in $PG(2,q)$ and hence $\mathcal{S}(1-k)$ is empty. Conversely, if $\mathcal{S}(1-k)$ is empty then $\mathcal{S}(k)$ must be empty.

Suppose $\mathcal{S}(k)$ is non-empty and let $d \in \mathcal{S}(k)$ so that $d \preceq kd$. Let $d = \sum_{i=0}^{h-1} d_i 2^i$ be the binomial expansion of d. Now let Ω be the subset of $\{0, \ldots, h-1\}$ such that $d_i = 1$ if and only if $i \in \Omega$. Therefore we have

$$d = \sum_{i \in \Omega} 2^i.$$

Since $d \preceq kd$ then $kd = \sum_{i \in \Omega} 2^i + \sum_{i \in \mathcal{I}} 2^i$, where $\mathcal{I}$ is a subset of $\{0, \ldots, h-1\}$ such that $\Omega \cap \mathcal{I} = \emptyset$. Note that $\mathcal{I}$ can be empty (if $d = kd$). Now

$$\begin{aligned}
(1-k)d &= d - kd \pmod{q-1} \\
&= \sum_{i \in \Omega} 2^i - \left(\sum_{i \in \Omega} 2^i + \sum_{i \in \mathcal{I}} 2^i \right) \pmod{q-1} \\
&= -\sum_{i \in \mathcal{I}} 2^i \pmod{q-1} \\
&\equiv -\sum_{i \in \mathcal{I}} 2^i + (q-1) \pmod{q-1} \\
&= -\sum_{i \in \mathcal{I}} 2^i + \sum_{i=0}^{h-1} 2^i \pmod{q-1} \\
&= \sum_{i \in \mathcal{I}^c} 2^i \pmod{q-1}, \text{ where } \mathcal{I}^c = \{0, \ldots, h-1\} - \mathcal{I}
\end{aligned}$$

Now since $\Omega \cap \mathcal{I} = \phi$, that is $\Omega \subseteq \mathcal{I}^c$. Thus

$$\sum_{i \in \Omega} 2^i \preceq \sum_{i \in \mathcal{I}^c} 2^i$$

and so $d \preceq (1-k)d$.

Conversely, suppose $d \preceq (1-k)d$. Using the forward part of this proof, $d \preceq (1-(1-k))d = kd$. Hence $\mathcal{S}(k) = \mathcal{S}(1-k)$. ■

Theorem 3.1.1 means that for a particular value of k the collection $\mathcal{S}(k)$ of values of d such that $d \preceq kd$ is exactly the same as the collection $\mathcal{S}(1-k)$ of values of d such that $d \preceq (1-k)d$. Hence in our list of the values of k ranging from 1 to $q-1$, we have a "symmetry" about the value $k = \frac{q}{2} = 2^{h-1}$. So when we are looking for hyperovals $\mathcal{D}(k)$ it is only necessary to inspect either the values $k = 1$ to $\frac{q}{2}$ or $k = \frac{q}{2}$ to $q-2$. Without loss of generality we can choose to inspect $k = 1$ to $\frac{q}{2}$. Furthermore, we know that k must be even, $\mathcal{D}(2)$ is a hyperoval and $\mathcal{D}(2^{-1}) = \mathcal{D}(\frac{q}{2})$ is a hyperoval so it is only necessary to inspect values of k ranging from 4 to $\frac{q}{2}-2$ which satisfy the constraints $(k, q-1) = (k-1, q-1) = 1$ and $k, 1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all even when reduced mod $q-1$.

3.2 Sets $\mathcal{D}(k)$ where $k = 2^n$ for some positive integer n

In this section, we consider sets of points of type $\mathcal{D}(2^n)$ in $PG(2,q)$, $q = 2^h$, for some positive integer $1 \leq n \leq h-1$. We shall show that $\mathcal{D}(2^n)$ is a hyperoval if and only if $(n,h) = 1$ using a new method.

This next result gives us a complete determination of the sets $\mathcal{S}(2^n)$, where n is some positive integer. As a corollary, we see which sets $\mathcal{D}(2^n)$ are hyperovals.

Theorem 3.2.1 *Let $q = 2^h$, h a positive integer. For $n = 1, 2, \ldots, h-1$, we have $|\mathcal{S}(k)| = 2^{(n,h)} - 2$. In particular,*

$$\mathcal{S}(2^n) = \left\{ \sum_{i \in \Omega} 2^i : \Omega \in \mathcal{W} \right\}$$

where $\mathcal{W}$ is the set of all nontrivial unions of sets from

$$A_1 = \{0, (n,h), 2(n,h), \ldots, h-(n,h)\}$$

$$\begin{aligned} A_2 &= \{1, (n,h)+1, 2(n,h)+1, \ldots, h-(n,h)+1\} \\ &\vdots \quad \vdots \quad \vdots \\ A_{(n,h)} &= \{(n,h)-1, 2(n,h)-1, \ldots, h-1\} \end{aligned}$$

(so that $\Omega \in \mathcal{W}$ implies that $\Omega \subseteq \{1, \ldots, h-1\}$, $\Omega \neq \emptyset$ and $\Omega \neq \{1, \ldots, h-1\}$).

Proof. We have

$$\begin{aligned} d \in \mathcal{S}(2^n) &\iff d \preceq 2^n d \\ &\iff \sum_{i \in \Omega} 2^i \preceq \sum_{i \in \Omega + n \pmod h} 2^i \\ &\iff \Omega = \Omega + n \pmod h. \end{aligned}$$

Now consider A_1 to $A_{(n,h)}$. Any two elements of A_i, for any $i \in \{1, \ldots, (n,h)\}$, differ by a multiple of (n,h). Since (n,h) divides n, addition by n to an element of A_i taken modulo h will give an element of A_i too. This means $A_i = A_i + n \pmod h$. Hence if $d = \sum_{i \in \Omega} 2^i$ and Ω is the union of some of $A_1, A_2, \ldots, A_{(n,h)}$, then $d \in \mathcal{S}(2^n)$. Now $d \neq 0$ so $\Omega \neq \emptyset$ and $d \neq q-1$ so $\Omega \neq \{1, \ldots, h-1\} = A_1 \cup A_2 \cup \cdots \cup A_{(n,h)}$

Conversely, we have to show that if Ω is any non-trivial subset of $\{0, \ldots, h-1\}$ such that $\Omega = \Omega + n \pmod h$ then Ω must be a non-trivial union of some of $A_1, A_2, \ldots, A_{(n,h)}$.

First, $\Omega = \Omega + n \pmod h$ means that if $x \in \Omega$ then $x + \ell n \pmod h \in \Omega$ for any $\ell \in \mathbf{Z}^+$. Also note that $\mid A_i \mid = \frac{h}{(n,h)}$ for all i.

Since $\Omega \neq \emptyset$, there exists $x \in \Omega$. Since $A_1, \ldots, A_{(n,h)}$ partition the index set $\{0, \ldots, h-1\}$, then $x \in A_i$ for some unique $i \in \{1, \ldots, (n,h)\}$. Then $A_i = \{x + m(n,h) \pmod h : m \in \{0, 1, \ldots, \frac{h}{(n,h)} - 1\}\}$. We thus need to show that $A_i \subseteq \Omega$. In particular we show that the set

$$\{x + m(n,h) \pmod h : m \in \{0, \ldots, \frac{h}{(n,h)} - 1\}\}$$

is the same as the set

$$\{x + \ell n \pmod h : \ell \in \{0, \ldots, \frac{h}{(n,h)} - 1\}\}$$

Now (n,h) divides n and $n = \frac{n}{(n,h)}(n,h)$. Thus the above sets are equal if and only if

$$\{\frac{\ell n}{(n,h)} \pmod{\frac{h}{(n,h)}} : \ell \in \{0,\ldots,\frac{h}{(n,h)}-1\}\} = \{0,\ldots,\frac{h}{(n,h)}-1\}.$$

We show this as follows. Let $\ell' = \frac{n}{(n,h)}$. First suppose $y_1\ell' = y_2\ell' \pmod{\frac{h}{(n,h)}}$ with $y_1, y_2 \in \{0,\ldots,\frac{h}{(n,h)}-1\}$. This is true if and only if $(y_1 - y_2)\ell' \equiv 0 \pmod{\frac{h}{(n,h)}}$. And since

$$\left(\ell', \frac{h}{(n,h)}\right) = \left(\frac{h}{(n,h)}, \frac{n}{(n,h)}\right) = 1$$

we thus conclude $y_1 \equiv y_2 \pmod{\frac{h}{(n,h)}}$. Thus the elements of the set

$$\{\ell\ell' \pmod{\frac{h}{(n,h)}} : \ell \in \{0,\ldots,\frac{h}{(n,h)}-1\}\},$$

are distinct, and lie between 0 and $\frac{h}{(n,h)-1}$; hence the set is $\{0,\ldots,\frac{h}{(n,h)}-1\}$. Thus $A_i \subseteq \Omega$.

Next, pick any element $y \in \Omega$ which is not contained in A_i. Then y must belong to A_j for some unique $j \in \{1,\ldots,(n,h)\}, j \neq i$. By repeating the previous arguments $A_j \subseteq \Omega$ too. Repeating this process will exhaust all the elements of Ω thus showing that Ω must be the union of at least one and at most $(n,h)-1$ of $A_1, A_2, \ldots, A_{(n,h)}$ as required (Ω cannot be the union of all (n,h) of the sets A_i as $\Omega \neq \{1,\ldots,h-1\}$).

Finally, counting we get

$$|\ \mathcal{S}(2^n)\ | = (n,h) + \begin{pmatrix}(n,h)\\2\end{pmatrix} + \cdots + \begin{pmatrix}(n,h)\\(n,h)-1\end{pmatrix} = 2^{(n,h)} - 2. \blacksquare$$

Corollary 3.2.1 *$\mathcal{D}(2^n)$ is a hyperoval in $PG(2,2^h)$ if and only if $(n,h) = 1$.*

Proof. Using Theorem 3.2.1 $\mathcal{D}(2^n)$ is a hyperoval in $PG(2,2^h)$ if and only if $|\ \mathcal{S}(2^n)\ | = 0$. This holds if and only if $2^{(n,h)} = 2$, if and only if $(n,h) = 1$. $\blacksquare$

Note that our Corollary 3.2.1 appears as Corollary 3 of Theorem 8.4.2 in Hirschfeld [13].

We know that the hyperoval $\mathcal{D}(2^n)$, $(n,h)=1$, is equivalent under $P\Gamma L(3,q)$ to $\mathcal{D}(2^{h-n})$ (by Theorem 1.2.7). More generally, it is also true that the set $\mathcal{S}(2^n)$ equals the set $\mathcal{S}(2^{h-n})$ as follows, even when $\mathcal{D}(2^n)$ is not a hyperoval.

Corollary 3.2.2 *$\mathcal{S}(2^n) = \mathcal{S}(2^{h-n})$ for all $n \in \{0,\ldots,h-1\}$.*

Proof.

$$\begin{aligned}
d \in \mathcal{S}(2^n) &\iff d \preceq 2^n d \\
&\iff \sum_{i\in\Omega} 2^i = \sum_{i\in\Omega+n \pmod h} 2^i \\
&\iff \Omega = \Omega + n \pmod h \\
&\iff \Omega = \Omega - n \pmod h \\
&\iff \Omega = \Omega + h - n \pmod h \\
&\iff \sum_{i\in\Omega} 2^i \preceq \sum_{i\in\Omega+h-n} 2^i \\
&\iff d \preceq 2^{h-n} d \\
&\iff d \in \mathcal{S}(2^{h-n}). \ \blacksquare
\end{aligned}$$

To summarize our results so far, we only need to consider values of k which satisfy the following:

- $4 \le k \le \frac{q}{2} - 2$;
- $k, 1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all even when reduced modulo $q-1$;
- $(k, q-1) = (k-1, q-1) = 1$;
- k not a power of 2.

3.3 Sets $\mathcal{D}(k)$ where $k = 2^n + 2^m$ for positive integers n and m

In the last section we considered sets $\mathcal{D}(2^n)$ in $PG(2,q)$, $q = 2^h$. Our next step is to consider sets of points $\mathcal{D}(k)$ with k having 2 terms in its binomial expansion, that is $k = 2^n + 2^m$ for some integers n and m. Without loss of generality we can assume $m > n$. We use the following cases :

A. The order of the plane is 2^h and h is even,

(A1) n even, m odd

(A2) n even, m even

(A3) n odd, m odd

(A4) n odd, m even

B. The order of the plane is 2^h and h is odd,

(B1) n even, m odd

(B2) n even, m even

(B3) n odd, m odd

(B4) n odd, m even

The next result shows that for k in cases **(A1)**, **(A3)** and **(A4)**, $\mathcal{D}(k)$ is never a hyperoval.

Theorem 3.3.1 *In $PG(2,2^h)$, $h \geq 4$ even, the set of points $\mathcal{D}(2^n+2^m)$ where either*

(i) *n is odd and $h-1 \geq m > n \geq 1$, or*

(ii) *n is even and m is odd and $h-1 \geq m > n \geq 0$*

is never a hyperoval.

Proof. **(i)** Suppose that n is odd. We consider first the case when m is odd. Consider

$$d = 2^0 + 2^2 + 2^4 + \cdots + 2^{h-2} = \sum_{i=0}^{\frac{h-2}{2}} 2^{2i}.$$

This d has binary representation $1010\ldots101010$. Now, consider the addition

$$\begin{aligned} 2^n d \pmod{2^h - 1} &\overset{\text{bin.rep}^n}{=} 010101\ldots0101 \\ 2^m d \pmod{2^h - 1} &\overset{\text{bin.rep}^n}{=} 010101\ldots0101 \\ 2^n d + 2^m d \pmod{2^h - 1} &\overset{\text{bin.rep}^n}{=} 101010\ldots1010. \end{aligned}$$

A carry of 2^h occurs in the above addition resulting in a 1 in the 0^{th} binary position in the binary representation of $(2^n + 2^m)d$ when taken modulo $2^h - 1$. The addition thus shows that $d \preceq (2^n + 2^m)d \pmod{2^h - 1}$ (in fact $d = (2^n + 2^m)d$) whenever n and m are both odd. If written as sums of powers of 2, it is also evident that $d \preceq (2^n+2^m)d \pmod{q-1}$ as follows. As n and m are both odd, $2^n d \bmod (2^h-1) = 2^m d \bmod (2^h - 1) = 2^1 + 2^3 + 2^5 + \cdots + 2^{h-1}$ and so

$$\begin{aligned} (2^n + 2^m)d &= 2^n d + 2^m d \\ &= 2(2^1 + 2^3 + \cdots + 2^{h-1}) \\ &= 2^2 + 2^4 + \cdots + 2^h \pmod{2^h - 1} \\ &= 2^0 + 2^2 + \cdots + 2^{h-1}. \end{aligned}$$

The second case is when n is odd and m is even. Consider the same d,

$$d = 2^0 + 2^1 + \cdots + 2^{h-2} = \sum_{i=0}^{\frac{h-2}{2}} 2^{2i}.$$

Consider the addition,

$$\begin{aligned} 2^n d \pmod{2^h - 1} &\overset{\text{bin.rep}^n}{=} 010101\ldots0101 \\ 2^m d \pmod{2^h - 1} &\overset{\text{bin.rep}^n}{=} 101010\ldots1010 \\ 2^n d + 2^m d \pmod{2^h - 1} &\overset{\text{bin.rep}^n}{=} 111111\ldots1111 \end{aligned}$$

Thus from the binary representation of $(2^n+2^m)d$ we have $d \preceq (2^n+2^m)d \pmod{2^h-1}$ whenever n is odd and m is even. When written as sums of powers of 2, we have

the following. As n is odd and m is even, $2^n d \bmod (2^h-1) = 2^1+2^3+\cdots+2^{h-1}$ and $2^m d \bmod (2^h-1) = 2^0+2^2+\cdots+2^{h-2}$; hence $(2^n+2^m)d \bmod (2^h-1) = 2^n d + 2^m d \pmod{2^h-1} = 2^0+2^1+2^3+\cdots+2^{h-2}+2^{h-1}$, showing that $d \preceq (2^n+2^m)d \pmod{2^h-1}$.

Hence, $\sum_{i=0}^{\frac{h-2}{2}} 2^{2i} \in \mathcal{S}(2^n+2^m)$, for $m > n \geq 1$, n odd. So $\mathcal{D}(2^n+2^m)$, n odd, is never a hyperoval.

(ii) When n even and m odd, $m > n \geq 0$, let $d = \sum_{i=1}^{\frac{h-1}{2}} 2^{2i}$ as before. Consider the addition

$$\begin{aligned} 2^n d \pmod{q-1} &\overset{\text{bin.rep}^n}{=} 101010\ldots1010 \\ 2^m d \pmod{q-1} &\overset{\text{bin.rep}^n}{=} 010101\ldots0101 \\ (2^n+2^m)d \pmod{q-1} &\overset{\text{bin.rep}^n}{=} 111111\ldots1111 \end{aligned}$$

which, when expressed as sums of powers of 2, becomes as follows. As n even and m odd, $2^n d \bmod (2^h-1) = 2^0+2^2+\cdots+2^{h-2}$ and $2^m d \bmod (2^h-1) = 2^1+2^3+\cdots+2^{h-1}$; hence $(2^n+2^m)d \bmod (2^h-1) = 2^0+2^1+2^2+\cdots+2^{h-2}+2^{h-1}$. This shows that $\mathcal{D}(2^n+2^m)$, n even m odd, is never a hyperoval. ■

The following result shows that for k belonging to case **(B1)**, $\mathcal{D}(k)$ is never a hyperoval.

Theorem 3.3.2 *In $PG(2,2^h)$ the set of points $\mathcal{D}(2^n+2^m)$, n even, m odd and $h-2 \geq m > n \geq 1$, and the index of the plane $h \geq m+2$ is odd, is never a hyperoval.*

Proof. Let $d = \sum_{i=0}^{\frac{h-(m-n+2)}{2}} 2^{2i}$. So d has binary representation

$$d \overset{\text{bin.rep}^n}{=} \overbrace{10101010\ldots1010101}^{h-m+n-1}\overbrace{0000\ldots000}^{m-n+1}.$$

Consider the binary representations of $2^n d$ and $2^m d$; recalling that multiplying by 2^r shifts the digits in the binary representation by r positions to the right (and wrapping).

$$2^m d \pmod{q-1} \overset{\text{bin.rep}^n}{=} \underbrace{101010\ldots10101}_{n-1}\underbrace{00000\ldots000}_{m-n+1}\underbrace{101010\ldots1010101010}_{h-m}$$

$$2^n d \pmod{q-1} \overset{\text{bin.rep}^n}{=} \underbrace{000000\ldots000000}_{n}\underbrace{1010\ldots10101010101}_{h-m+n-1}\underbrace{0000\ldots0000}_{m-2n+1}$$

where (for the binary representation of $2^n d$) we assume that $m - 2n + 1 > 0$.

When written in terms of sums of powers of 2, we have the following (where the exponents are read modulo h):

$$\begin{aligned} 2^m d \bmod (2^h - 1) &= (2^0 + 2^2 + 2^4 + \cdots + 2^{n-2}) \\ &\quad + (2^m + 2^{m+2} + 2^{m+4} + \cdots + 2^{h-2}) \\ 2^n d \bmod (2^h - 1) &= 2^n + 2^{n+2} + 2^{n+4} + \cdots + 2^{h-m+2n-2} \end{aligned}$$

We must consider all the possible binary representations of $(2^n + 2^m)d \pmod{q-1}$, which takes several different forms according to the following cases:

(i) $m < h - m + 2n - 2 \leq h - 1$

(ii) $n \leq h - m + 2n - 2 \leq m - 1$

(iii) $0 \leq h - m + 2n - 2 \leq n - 3$

We shall show that in each of the three cases we have $d \preceq (2^n + 2^m)d$ (i.e. the binary representation of $(2^n + 2^m)d$ must have 1's occurring at the even numbered binary positions starting from the 0^{th} binary position up to and including binary position number $h - m + n - 2$).

Firstly, in case **(i)**, where $m < h-m+2n-2 \leq h-1$, we consider the following addition of the binary representations of $2^n d$ and $2^m d$ (the addition is being presented over two lines):

$$\begin{array}{rcccccccc|cccccc} & & & & & & & & & \#\ n-2 & & & & & \\ & & & & & & & & & \downarrow & & & & & \\ 2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 2^n d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \cdots \\ (2^n + 2^m)d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots \end{array}$$

$$
\begin{array}{llllllllllllllllllll}
 & & & & & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & & & & & \\
\cdots\cdots & 0 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0 \\
\cdots\cdots & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
\cdots\cdots & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0
\end{array}
$$

As evident, there are 1's occurring at the even numbered binary positions of $(2^n + 2^m)d$ starting from binary position 0 up to $h - m + 2n - 2$. Thus

$$\left(\sum_{i=0}^{\frac{h-m+n-2}{2}} 2^{2i}\right) \preceq (2^n + 2^m)\left(\sum_{i=0}^{\frac{h-m+n-2}{2}} 2^{2i}\right) \pmod{q-1}.$$

Expressing the above binary addition as sums of powers of 2, we have

$$\begin{aligned}(2^n + 2^m)d \bmod (2^h - 1) \;=\; & \left(2^0 + 2^2 + 2^4 + \cdots + 2^{n-2} + 2^n + \cdots + 2^{m-3} + 2^{m-1}\right) \\ & + \left(2^m + 2^{m+1} + 2^{m+2} + \cdots + 2^{h-m+2n-2}\right) \\ & + \left(2^{h-m+2n-1} + 2^{h-m+2n+1} + 2^{h-m+2n+3} + \cdots + 2^{h-2}\right)\end{aligned}$$

For case **(ii)**, where $n \leq h - m + 2n - 2 \leq m - 1$, the addition we should consider is as follows (the addition is being presented over two lines):

$$
\begin{array}{llllllllllllllllll}
 & & & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & & & \\
2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots \\
2^n d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \cdots \\
(2^n + 2^m)d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots
\end{array}
$$

$$
\begin{array}{llllllllllllllllll}
 & & & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & & & \\
\cdots\cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 \\
\cdots\cdots & 1 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
\cdots\cdots & 1 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0
\end{array}
$$

Again, in this case we have 1's occurring at the even numbered binary positions of $(2^n + 2^m)d \pmod{q-1}$ from 0 up to $h - m + 2n - 2$. Expressing in terms of sums of powers of 2, we have

$$\begin{aligned}(2^n + 2^m)d \bmod (2^h - 1) \;=\; & \left(2^0 + 2^2 + 2^4 + \cdots + 2^{n-2} + 2^n + \cdots + 2^{h-m+2n-2}\right) \\ & + \left(2^m + 2^{m+2} + 2^{m+4} + \cdots + 2^{h-2}\right).\end{aligned}$$

Lastly, case **(iii)**, where $0 \leq h-m+2n-2 \leq n-3$, we consider the following addition (the addition is being presented over two lines):

$$\begin{array}{lcccccccccccccccccc}
 & & & & & & & & & & & & \#h-m+2n-2 & & & & & & \\
 & & & & & & & & & & & & \uparrow & & & & & & \\
2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & 1 & 0 & \cdots & & & & \\
2^n d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0 & 0 & \cdots & & & & \\
(2^m+2^n) d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 0 & \cdots & & & & \\
\end{array}$$

$$\begin{array}{lcccccccccccccccccccccc}
\cdots\cdots & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 \\
\cdots\cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & 1 \\
\cdots\cdots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\
 & & & & & \downarrow & & & & & & & & & \downarrow & & & & & & & & \\
 & & & & & \#n-2 & & & & & & & & & \#m & & & & & & & &
\end{array}$$

Now $h-m+n-2 \geq 0$ and since all of the even numbered binary positions of $(2^n+2^m)d$ contain 1's (from 0 up to $h-m+2n-2$), we end up with $d \preceq (2^n+2^m)d \pmod{q-1}$. If expressed as sums of powers of 2, we have

$$\begin{aligned}
(2^n+2^m)d \bmod (2^h-1) = & \left(2^0+2^1+2^2+\cdots+2^{h-m+2n-2}\right) \\
& + \left(2^{h-m+2n-1}+2^{h-m+2n+1}+2^{h-m+2n+3}+\cdots+2^{n-2}+2^n+\cdots+2^{m-1}\right) \\
& + \left(2^m+2^{m+1}+2^{m+2}+\cdots+2^{h-2}+2^{h-1}\right).
\end{aligned}$$

Hence in all of the three cases above we have shown that for n even, m odd, $m > n \geq 0$, $\mathcal{D}(2^n+2^m)$ is never a hyperoval of $PG(2,2^h)$, h odd $(h > m+2)$. ■

In fact, Theorem 3.3.1(ii) can be generalized further into this next result for sets $\mathcal{D}(k)$ where k has more than two binary digits.

Theorem 3.3.3 *Let $PG(2,2^h)$ be the Desarguesian projective plane of even order 2^h for some positive integer $h > 2$. Let $s \geq 2$ be a positive integer such that $h \equiv 0 \pmod{s}$. Then the set of points $\mathcal{D}(2^{r_1}+2^{r_2}+\cdots+2^{r_j})$, with $r_i \equiv 0 \pmod{s}$ for some unique $i \in \{1,\ldots,j\}$ and $\{r_1,\ldots,r_j\}$ a subset of the complete set of residues modulo s, is never a hyperoval of $PG(2,2^h)$.*

Proof. We consider $d = \sum_{i=0}^{\frac{h-s}{s}} 2^{is}$ so that d has binary representation

$$\underbrace{100\ldots00}_{s \text{ terms}}\underbrace{100\ldots00}\ldots\ldots\underbrace{100\ldots00}$$

of s digits $100\ldots0$ repeated $\frac{h}{s}$ times.

Now we consider $kd \pmod{q-1}$, where $k = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_j}$. As there is exactly one $i \in \{1, \ldots, j\}$ such that $r_i \equiv 0 \pmod{s}$, the binary representation of $kd \pmod{q-1}$ must have $1's$ occurring in its $0^{th}, s^{th}, 2s^{th}, 4s^{th}, \ldots, (h-s)^{th}$ binary positions. In other words, the binomial expansion of $kd \pmod{q-1}$ must contain the terms $2^0, 2^s, 2^{2s}, 2^{4s}, \ldots, 2^{h-s}$. This means that

$$d = \sum_{i=0}^{\frac{h-s}{s}} 2^{is} \preceq kd \pmod{q-1}$$

as required. ■

We can apply Theorem 3.3.3 to a set of points $\mathcal{D}(2^m + 2^n)$ of $PG(2, 2^h)$ as follows:

(i) Suppose that n divides m. To apply Theorem 3.3.3 we must assume that $h \equiv 0 \pmod{m}$. Thus $\mathcal{D}(2^n + 2^m)$ is not a hyperoval in $PG(2, 2^h)$.

(ii) If n does not divide m, then we could use Theorem 3.3.3 in three possible ways:

  (a) If $h \equiv 0 \pmod{n}$ and $h \not\equiv 0 \pmod{m}$, then we can use $s = n$ and $\mathcal{D}(2^m + 2^n)$ is not a hyperoval in $PG(2, 2^h)$.

  (b) If $h \equiv 0 \pmod{m}$ and $h \not\equiv 0 \pmod{n}$, then we can use $s = m$ and $\mathcal{D}(2^m + 2^n)$ is not a hyperoval in $PG(2, 2^h)$.

  (c) If $h \equiv 0 \pmod{n}$ and $h \equiv 0 \pmod{m}$, then either $s = m$ or $s = n$ shows that $\mathcal{D}(2^n + 2^m)$ is not a hyperoval in $PG(2, 2^h)$.

(iii) As another example, in the case when n does not divide m and m is even, $m > n$, a set of points $\mathcal{D}(2^m + 2^n)$ is not a hyperoval in $PG(2, 2^h)$ where $h \equiv 0 \pmod{\frac{m}{2}}$. The reason is that n does not divide m implies that n does not divide $\frac{m}{2}$, so if $h \equiv 0 \pmod{\frac{m}{2}}$ then $\mathcal{D}(2^m + 2^n)$ is not a hyperoval by Theorem 3.3.3.

The next result shows that a set of points $\mathcal{D}(2^m + 2^n)$ is not a hyperoval of $PG(2, 2^h)$ whenever the index h can be expressed as a linear combination of m and n as follows.

Theorem 3.3.4 *Let $PG(2, 2^h)$ be the Desarguesian projective plane of order 2^h, and let m, n be positive integers with $m > n$. If the index h can be expressed as:*

$$h = am + bn$$

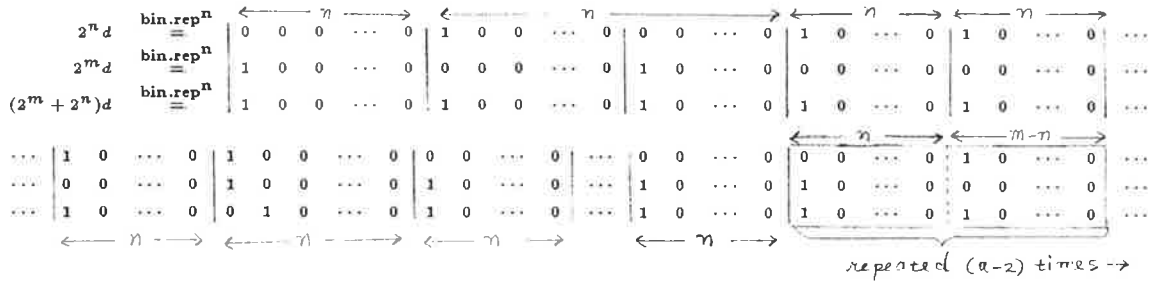
where a and b are non-negative integers and a is as large as possible (i.e. $bn \leq m-1$), then the set of points $\mathcal{D}(2^m + 2^n)$ is not a hyperoval of $PG(2, 2^h)$.

Proof. We use

$$d \overset{\text{bin.rep}^n}{=} \underbrace{1000\cdots0}_{m}(\underbrace{100\cdots0}_{n})^b(\underbrace{1000\cdots0}_{m})^{a-1}$$

as suggested by Cherowitzo [4].

We show that this $d \in \mathcal{S}(2^m + 2^n)$ by illustrating the following binary addition (which is presented over two lines):



Expressing the above addition as sums of powers of two, we have the following:

$$\begin{aligned} d &= 2^0 + (2^m + 2^{m+n} + 2^{m+2n} + \cdots + 2^{m+(b-1)n}) \\ &\quad + (2^{m+bn} + 2^{2m+bn} + 2^{3m+bn} + \cdots + \underbrace{2^{h-m}}_{=2^{(a-1)m+bn}}) \end{aligned}$$

$$\begin{aligned} 2^m d \bmod (2^h - 1) &= 2^0 + 2^m + (2^{2m} + 2^{2m+n} + 2^{2m+2n} + \cdots + 2^{2m+(b-1)n}) \\ &\quad + (2^{2m+bn} + 2^{3m+bn} + \cdots + 2^{h-m}) \end{aligned}$$

$$\begin{aligned} 2^n d \bmod (2^h - 1) = 2^n &+ (2^{m+n} + 2^{m+2n} + \cdots + 2^{m+(b-1)n}) + 2^{m+bn} \\ &+ (2^{m+(b+1)n} + 2^{2m+(b+1)n} + 2^{3m+(b+1)n} + \cdots + 2^{h-2m+n} + 2^{h-m+n}) \end{aligned}$$

$$\begin{aligned} (2^m + 2^n)d \bmod (2^h - 1) &= 2^0 + (2^m + 2^{m+n} + 2^{m+2n} + \cdots + 2^{m+(b-1)n}) \\ &\quad + (2^{m+bn} + 2^{2m+bn} + 2^{3m+bn} + \cdots + 2^{h-m}) \\ &\quad + (2^{2m} + 2^{2m+n} + \cdots + 2^{2m+(b-1)n}) + 2^n \\ &\quad + (2^{m+(b+1)n} + 2^{2m+(b+1)n} + \cdots + 2^{h-m+n}). \end{aligned}$$

Which clearly shows that $d \preceq 2^m d + 2^n d$ as all the terms in the binomial expansion of d occur in the binomial expansion of $2^m d + 2^n d$. ■

Finally, the next result deals with sets of points $\mathcal{D}(2^n + 2^m)$, m and n distinct positive integers, of $PG(2, 2^h)$ whenever $h = am + bn + 1$ (for some non-negative integers a and b) and $h \geq 2m + n + 1$. Note that a special case of this next result which concerns sets of points $\mathcal{D}(2^2 + 2^m)$, $m \geq 4$ even positive integer, of the plane $PG(2, 2^h)$, h odd and $h \geq 2m + 3$, appears in Theorem 3.4.2.

Theorem 3.3.5 *A set of points $\mathcal{D}(2^n + 2^m)$ is not a hyperoval of $PG(2, 2^h)$ whenever*

$$h = am + bn + 1,\ h \geq 2m + n + 1,$$

where a is as large as possible and $0 \leq bn \leq m - 1$.

Proof. We split into three cases, as follows:

1. $m \neq 2n$ and $m \neq n + 1$,
2. $m = 2n$,
3. $m = n + 1$.

Case 1. For the case when $m \neq 2n$ and $m \neq n + 1$ we use

$$d \overset{\text{bin.rep}^n}{=} \left(\overbrace{10\ldots0}^{n}\overbrace{10\ldots0}^{m-n}\overbrace{10\ldots0}^{n}0\right)\overbrace{10\ldots0}^{m}\left(\overbrace{10\ldots0}^{n}\right)^{b-1}\left(\overbrace{10\ldots0}^{m}\right)^{a-2}$$

$$\begin{aligned} d &= 2^0 + 2^n + 2^m + 2^{m+n+1} \\ &\quad + (2^{2m+n+1} + 2^{2m+2n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + (2^{2m+bn+1} + 2^{3m+bn+1} + \cdots + \underbrace{2^{h-m}}_{=2^{(a-3)m+bn+1}}), \end{aligned}$$

to show that $\mathcal{D}(2^m + 2^n)$ is not a hyperoval of $PG(2, 2^h)$ whenever $h = am + bn + 1$ and $h \geq 2m + n + 1$ as follows. (This value of d was suggested by Cherowitzo [4]).

$$\begin{aligned} 2^n d &= 2^n + 2^{2n} + 2^{m+n} + 2^{m+2n+1} + (2^{2m+2n+1} + 2^{2m+3n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + 2^{2m+bn+1} + (2^{2m+(b+1)n+1} + 2^{3m+(b+1)n+1} + \cdots + 2^{h-m+n}) \end{aligned}$$

$$\begin{aligned} 2^m d &= 2^0 + 2^m + 2^{m+n} + 2^{2m} + 2^{2m+n+1} \\ &\quad +(2^{3m+n+1} + 2^{3m+2n+1} + \cdots + 2^{3m+(b-1)n+1} \\ &\quad +(2^{3m+bn+1} + 2^{4m+bn+1} + \cdots + 2^{h-m}) \end{aligned}$$

$$\begin{aligned} (2^n + 2^m)d &= 2^0 + 2^n + 2^m + 2^{m+n+1} \\ &\quad + (2^{2m+n+1} + 2^{2m+2n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + (2^{2m+bn+1} + 2^{3m+bn+1} + 2^{4m+bn+1} + \cdots + 2^{h-m}) \\ &\quad + 2^{m+2n+1} + (2^{2m+(b+1)n+1} + 2^{3m+(b+1)n+1} + \cdots + 2^{h-m+n}) \\ &\quad + 2^{2m} + (2^{3m+n+1} + 2^{3m+2n+1} + \cdots + 2^{3m+(b-1)n+1}). \end{aligned}$$

and it is easy to see that $d \preceq (2^n + 2^m)d$.

Case 2. For $m = 2n$, we use

$$\begin{aligned} d &= 2^0 + 2^n + 2^{m+1} + 2^{m+n+1} \\ &\quad + (2^{2m+n+1} + 2^{2m+2n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + (2^{2m+bn+1} + 2^{3m+bn+1} + \cdots + 2^{h-m}) \end{aligned}$$

to show that $\mathcal{D}(2^{2n}+2^n)$ is not a hyperoval of $PG(2, 2^h)$ whenever $h = a(2n)+bn+1$ as follows,

$$\begin{aligned} 2^n d &= 2^n + 2^{2n} + 2^{m+n+1} + 2^{m+2n+1} \\ &\quad + (2^{2m+2n+1} + 2^{2m+3n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + 2^{2m+bn+1} + (2^{2m+(b+1)n+1} + 2^{3m+(b+1)n+1} + \cdots + 2^{h-m+n}) \end{aligned}$$

$$\begin{aligned} 2^m d &= 2^0 + 2^m + 2^{m+n} + 2^{2m+1} + 2^{2m+n+1} \\ &\quad + (2^{3m+n+1} + 2^{3m+2n+1} + \cdots + 2^{3m+(b-1)n+1}) \\ &\quad + (2^{3m+bn+1} + 2^{4m+bn+1} + \cdots + 2^{h-m}) \end{aligned}$$

$$\begin{aligned} (2^n + 2^m)d &= 2^0 + 2^n + \overbrace{(2^{2n} + 2^m)}^{=2^{m+1}} + 2^{m+n+1} \\ &\quad + (2^{2m+n+1} + 2^{2m+2n+1} + \cdots + 2^{2m+(b-1)n+1}) \end{aligned}$$

$$+ (2^{2m+bn+1} + 2^{3m+bn+1} + \cdots + 2^{h-m})$$
$$+ 2^{m+n} + 2^{2m+1} + (2^{3m+n+1} + 2^{3m+2n+1} + \cdots + 2^{3m+(b-1)n+1})$$
$$+ 2^{m+2n+1} + (2^{2m+(b+1)n+1} + 2^{3m+(b+1)n+1} + \cdots + 2^{h-m+n})$$

and we see that $d \preceq (2^n + 2^{2n})d$.

Case 3. When $m = n + 1$, notice that $2m = 2n + 2 = (m + n) + 1$ implies $(2^{m+n} + 2^{m+n}) + 2^{2m} = 2^{m+n+2}$. Thus we must use the following d,

$$\begin{aligned} d &= 2^0 + 2^n + 2^m + 2^{m+n+2} \\ &\quad + (2^{2m+n+1} + 2^{2m+2n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + (2^{2m+bn+1} + 2^{3m+bn+1} + \cdots + 2^{h-m}) \end{aligned}$$

to show the required result as follows,

$$\begin{aligned} 2^n d &= 2^0 + 2^{2n} + 2^{m+n} + 2^{m+2n+2} \\ &\quad + (2^{2m+2n+1} + 2^{2m+3n+1} + \cdots + 2^{2m+(b-1)n+1}) \\ &\quad + 2^{m+bn+1} + (2^{2m+(b+1)n+1} + 2^{3m+(b+1)n+1} + \cdots + 2^{h-m+n}) \end{aligned}$$

$$\begin{aligned} 2^m d &= 2^0 + 2^m + 2^{2m} + 2^{m+n} + 2^{2m+n+2} \\ &\quad + (2^{3m+n+1} + 2^{3m+2n+1} + \cdots + 2^{3m+(b-1)n+1}) \\ &\quad + (2^{3m+bn+1} + 2^{4m+bn+1} + \cdots + 2^{h-m}) \end{aligned}$$

$$\begin{aligned} 2^n d + 2^m d &= 2^0 + 2^n + 2^m + \overbrace{(2^{m+n} + 2^{m+n} + 2^{2m})}^{=2^{m+n+2}} \\ &\quad + (\underbrace{2^{m+2n+2}}_{2^{2m+n+1}} + 2^{2m+2n+1} + 2^{2m+3n+1} + \cdots 2^{2m+(b-1)n+1}) \\ &\quad + (2^{2m+bn+1} + 2^{3m+bn+1} + 2^{4m+bn+1} + \cdots + 2^{h-m}) \\ &\quad + 2^{2n} + (2^{2m+(b+1)n+1} + 2^{3m+(b+1)n+1} + \cdots + 2^{h-m+n}) \\ &\quad + 2^{2m+n+2} + (2^{3m+n+1} + 2^{3m+2n+1} + \cdots + 2^{3m+(b-1)n+1}). \end{aligned}$$

Finally, the condition that the index of the plane h must be at least $2m+n+1$ is due to the fact that the term 2^{h-m} must occur in the binomial expansion of d as when we multiply d by 2^m (taken modulo $2^h - 1$) the term 2^0 has to be produced in the binomial expansion of $2^m d$. ■

3.4 Sets $\mathcal{D}(2+2^m)$ and $\mathcal{D}(2^2+2^m)$ for positive integers m

We now give a complete determination of which sets of which sets of points of $PG(2,2^h)$ of the form $\mathcal{D}(2+2^m)$, with $m \geq 2$, are hyperovals. Some of the proof was suggested by Cherowitzo [4]. Acknowledgment is given at the appropriate places in the proof.

Theorem 3.4.1 *Let $PG(2,2^h)$ be the Desarguesian projective plane of order 2^h. Then a set of points $\mathcal{D}(2+2^m)$, $2 \leq m \leq h-1$, is not a hyperoval of $PG(2,2^h)$ unless either:*

(i) *$m = 2$ and h is odd, in which case $\mathcal{D}(6)$ is a Segre hyperoval, or*

(ii) *$h = 2m-1$, in which case $\mathcal{D}(2+2^m)$ is a translation hyperoval.*

Proof. Write h as $h = am+b$ where $0 \leq b \leq m-1$. Since $h \geq m+1$ we have $a \geq 1$. We split into four cases, as follows:

(1) $a \geq 1$ and $0 \leq b < m-1$ (if $a = 1$ then $b \geq 1$). Otherwise, we have $a \geq 1$ and $b = m-1$.

(2) $a = 1$ and $b = m-1$. In this case $h = 2m-1$. Otherwise, we have $a \geq 2$ and $b = m-1$.

(3) $a \geq 2$, $b = m-1$ and $m \geq 3$.

(4) $a \geq 2$, $b = m-1$ and $m = 2$, so $m = 2$ and h is odd.

Case (1). We can use $d \overset{\text{bin.rep}^n}{=} 1^b(10^{(m-1)})^a$ (where 1^b means write b $1's$ and likewise $(10^{(m-1)})^a$ means write 1 followed by $m-1$ $0's$ and repeat this block of m symbols a times) as suggested by Cherowitzo [4]:

$$d = \left(2^0 + 2^1 + 2^2 + \cdots + 2^{b-1}\right)$$

$$+\left(2^b+2^{b+m}+2^{b+2m}+\cdots+\underbrace{2^{h-m}}_{=2^{b+(a-1)m}}\right)$$

$$= \sum_{k=0}^{b-1} 2^k + \sum_{\ell=0}^{a-1} 2^{b+\ell i}$$

We shall show that this type of d belongs to the set $\mathcal{S}(k)$ for $k = 2+2^m$. Consider the binary addition $2d + 2^m d \pmod{q-1}$ as follows (the addition is presented over two lines):

$$\begin{array}{rcl}
2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1\ 0\ 0\ 0\ \cdots\ 0 \mid 0\ 0\ 0\ 0\ \cdots\ 0 \mid 1\ 1\ 1\ \cdots \\
2d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 0\ 1\ 1\ 1\ \cdots\ 1 \mid 1\ 0\ 0\ 0\ \cdots\ 0 \mid 0\ 0\ 0\ \cdots \\
2d + 2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1\ 1\ 1\ 1\ \cdots\ 1 \mid 1\ 0\ 0\ 0\ \cdots\ 0 \mid 1\ 1\ 1\ \cdots
\end{array}$$

$$\begin{array}{l}
\cdots\ 1\ 1\ 0\ 0\ \cdots\ 0 \mid 1\ 0\ 0\ \cdots\ 0 \mid 1\ \cdots\ 1\ 0\ 0\ \cdots\ 0 \mid 1\ 0\ 0\ \cdots\ 0 \\
\cdots\ 0\ 0\ 1\ 0\ \cdots\ 0 \mid 0\ 1\ 0\ \cdots\ 0 \mid 0\ \cdots\ 0\ 1\ 0\ \cdots\ 0 \mid 0\ 1\ 0\ \cdots\ 0 \\
\cdots\ 1\ 1\ 1\ 0\ \cdots\ 0 \mid 1\ 1\ 0\ \cdots\ 0 \mid 1\ \cdots\ 1\ 1\ 0\ \cdots\ 0 \mid 1\ 1\ 0\ \cdots\ 0
\end{array}$$

Expressing this binary addition as sums of powers of 2, we get:

$$2^m d \bmod (2^h-1) = 2^0 + (2^m + 2^{m+1} + 2^{m+2} + \cdots + 2^{m+b-1}) + (2^{b+m} + 2^{2m+b} + 2^{3m+b} + \cdots + 2^{h-m})$$

$$2d \bmod (2^h-1) = (2^1 + 2^2 + 2^3 + \cdots + 2^b) + (2^{b+1} + 2^{m+b+1} + 2^{2m+b+1} + \cdots + 2^{h-m+1})$$

$$\begin{aligned}
(2^m+2)d \bmod (2^h-1) \;=\; & (2^0 + 2^1 + 2^2 + \cdots + 2^{b-1}) \\
& + (2^b + 2^{b+m} + 2^{b+2m} + \cdots + 2^{h-m}) \\
& + (2^{b+1} + 2^{b+m+1} + 2^{b+2m+1} + \cdots + 2^{h-m+1}) \\
& + (2^m + 2^{m+1} + 2^{m+2} + \cdots + 2^{m+b-1})
\end{aligned}$$

and it is easy to check that $d \preceq (2+2^m)d$.

Case (3), we use:

$$d \overset{\text{bin.rep}^n}{=} 1^{m-1}0(10^{m-2})(10^{m-1})^{a-1}$$

as suggested by Cherowitzo [4]. When expressed as a sum of powers of 2, this is

$$\begin{aligned} d &= (2^0 + 2^1 + 2^2 + \cdots + 2^{m-2}) \\ &\quad + 2^m + (2^{2m-1} + 2^{3m-1} + 2^{4m-1} + \cdots + \underbrace{2^{h-m}}_{=2^{2m-1+(a-2)m}}). \end{aligned}$$

Consider the following binary addition (presented over two lines):

$$\begin{array}{rcl} 2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & \overset{\longleftarrow m \longrightarrow}{1\ 0\ 0\ 0\ 0\ \cdots\ 0} \mid \overset{\longleftarrow m \longrightarrow}{0\ 1\ 1\ 1\ 1\ \cdots\ 1\ 0} \\ 2d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 0\ 1\ 1\ 1\ 1\ \cdots\ 1 \mid 1\ 0\ 1\ 0\ 0\ \cdots\ 0\ 0 \\ 2d + 2^m d \bmod (q-1) & \overset{\text{bin.rep}^n}{=} & 1\ 1\ 1\ 1\ 1\ \cdots\ 1 \mid 1\ 1\ 0\ 0\ 0\ \cdots\ 0\ 1 \end{array}$$

$$\begin{array}{l} 1\ 0\ 0\ 0\ \cdots\ 0\ 1\ 0\ 0\ \cdots\ 0 \mid \cdots\cdots\ 1\ 0\ 0\ \cdots\ 0 \\ 1\ 0\ 0\ 0\ \cdots\ 0\ 0\ 1\ 0\ \cdots\ 0 \mid \cdots\cdots\ 0\ 1\ 0\ \cdots\ 0 \\ 0\ 1\ 0\ 0\ \cdots\ 0\ 1\ 1\ 0\ \cdots\ 0 \mid \cdots\cdots\ 1\ 1\ 0\ \cdots\ 0 \end{array}$$

Expressing this binary addition as sums of powers of 2, we have the following:

$$\begin{aligned} 2^m d \bmod (2^h - 1) &= 2^0 + (2^m + 2^{m+1} + \cdots + 2^{2m-2}) + 2^{2m} \\ &\quad + (2^{3m-1} + 2^{4m-1} + 2^{5m-1} + \cdots + 2^{h-2m} + 2^{h-m}) \\ 2d \bmod (2^h - 1) &= (2^1 + 2^2 + \cdots + 2^{m-1}) + 2^{m+1} \\ &\quad + (2^{2m} + 2^{3m} + 2^{4m} + \cdots + 2^{h-2m+1} + 2^{h-m+1}) \\ (2 + 2^m) d \bmod (2^h - 1) &= (2^0 + 2^1 + \cdots + 2^{m-2}) + 2^m \\ &\quad + \underbrace{(2^{m+1} + (2^{m+1} + 2^{m+2} + \cdots + 2^{2m-2}))}_{=2^{2m-1}} \\ &\quad + (2^{3m-1} + 2^{4m-1} + \cdots + 2^{h-m}) \\ &\quad + \underbrace{(2^{2m} + 2^{2m})}_{=2^{2m+1}} + (2^{4m} + 2^{5m} + \cdots + 2^{h-m+1}) \end{aligned}$$

and it is easy to check that $d \preceq (2 + 2^m)d$.

Case (4). We have $\mathcal{D}(2 + 2^m) = \mathcal{D}(2 + 2^2) = \mathcal{D}(6)$ in $PG(2, 2^h)$ where h is odd. Now $\mathcal{D}(6)$ is always a hyperoval when h is odd, see Segre [31] or Section 2.2.

Case (2). We show that the set of points $\mathcal{D}(2 + 2^m)$ is a translation hyperoval in $PG(2, 2^{2m-1})$. First,

$$\mathcal{D}(2 + 2^m) \cong \mathcal{D}(2^{m-1}).$$

We show that $(1-2^{m-1})^{-1} \pmod{2^h-1} = 2+2^m$ as follows :

$$\begin{aligned}(1-2^{m-1}).(2+2^m) &= 2^m+2-2^{2m-1}-2^m \\ &\equiv 2-2^{2m-1}+2^{2m-1}-1 \pmod{2^{2m-1}-1} \\ &= 1 \pmod{2^{2m-1}-1}.\end{aligned}$$

This shows that $\mathcal{D}(2+2^m) \cong \mathcal{D}(2^{m-1})$ in $PG(2,2^{2m-1})$. It remains to show that $\mathcal{D}(2^{m-1})$ is a translation oval of $PG(2,2^{2m-1})$ by showing that $(m-1,2m-1)=1$ for any integer $m \geq 2$. Let $(m-1,2m-1) = d$ and let $(2(m-1),2m-1) = (2m-2,2m-1) = d_0$. Now any divisor of $m-1$ and $2m-1$ must divide d_0. However, notice that $d_0 = 1$ as any two consecutive positive integers must be relatively prime (suppose p is a prime number dividing a and $a+1$, $a \in \mathbf{N}$, then $a \equiv 0 \pmod{p}$. Thus $a+1 \equiv 1 \pmod{p} \implies p$ does not divide $a+1$. The fact that any integer can be expressed as a product of primes completes the argument). Thus d divides d_0 implies that $d=1$ and so $\mathcal{D}(2^{m-1})$ is a translation oval of $PG(2,2^{2m-1})$.

Alternatively, it is also true that $\mathcal{D}(2+2^m) \cong \mathcal{D}(2^m)$ since

$$2^m(2^m-1)^{-1} \pmod{2^{2m-1}-1} \equiv 2+2^m.$$

Then $\mathcal{D}(2^m)$ is a translation oval of $PG(2,2^{2m-1})$ as $(m,2m-1)=1$, which can be proved using a similar method as above. ■

Example 3.4.1 *As an illustration to case (1) in Theorem 3.4.1, we consider $k=6$. When h is even ($h \geq 4$), $\mathcal{D}(6)$ is not a hyperoval and we can use $d \overset{\text{bin.rep}^n}{=} 1^b(10^{(m-1)})^a$ from case (1) to show that $\mathcal{D}(6)$ is never a hyperoval for h even. For instance when $h=12$ we have $a=6$ and $b=0$ and the following binary addition shows that $d \preceq kd$:*

$$\begin{array}{rcccccccccccc} d & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 2d & \overset{\text{bin.rep}^n}{=} & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 2^2d & \overset{\text{bin.rep}^n}{=} & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 6d & \overset{\text{bin.rep}^n}{=} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

which, when expressed as sums of powers of 2, becomes:

$$\begin{aligned} d &= 2^0 + 2^2 + \cdots + 2^{10} \\ 2d &= 2^1 + 2^3 + \cdots + 2^{11} \\ 2^2 d &= 2^0 + 2^2 + \cdots + 2^{10} \\ 6d &= 2^0 + 2^1 + 2^2 + \cdots + 2^{11}. \end{aligned}$$

The next result concerns sets of points of the form $\mathcal{D}(2^2 + 2^m)$, and is a special case of Theorems 3.3.4 and 3.3.5.

Theorem 3.4.2 *A set of points $\mathcal{D}(2^2+2^m)$, where $m \geq 4$ is even, is not a hyperoval of $PG(2, 2^h)$, $h \geq \begin{cases} 2m+3 & h \text{ odd} \\ m+2 & h \text{ even} \end{cases}$.*

Proof. Theorem 3.3.4 implies that a set of points $\mathcal{D}(2^m + 2^2)$ with $m \geq 4$ even is not a hyperoval of $PG(2, 2^h)$ when the index h is even. This is simply because any even integer $h \geq m + 2$ can be expressed in the form $h = am + 2b$ for some integers a and b where a is as large as possible (which means $2b \leq m - 2$ as m is even).

When $h \geq 2m + 3$ is odd, we express the index h of the plane in the form $h = am + 2b + 1$, where a and b are non-negative integers and a is as large as possible and $0 \leq 2b \leq m - 1$. We can divide into the two cases $m = 4$ and $m \geq 6$ even and using Theorem 3.3.5 the result follows. ■

3.5 Summary

In this chapter we have first of all identified that there is a symmetry $\mathcal{S}(k) = \mathcal{S}(q-k)$, $k \in \{1, \ldots, q-2\}$. In other words, when classifying hyperovals $\mathcal{D}(k)$ we only need to consider values of k belonging to either the set $\{1, 2, \ldots, \frac{q}{2}\}$ or $\{\frac{q}{2}, \ldots, q-2\}$. We finally concluded in section one that it is only necessary to consider values of k which satisfy:

- $k, 1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all even when reduced modulo $q-1$;
- $4 \leq k \leq \frac{q}{2} - 2$;
- $(k, q-1) = (k-1, q-1) = 1$.

Theorem 3.2.1 is a complete determination of the sets $\mathcal{S}(2^n)$ for each positive integer n with $1 \leq n \leq h-1$. This led to an alternative proof of the known result that $\mathcal{D}(2^n)$ is a hyperoval of $PG(2,q)$, q even, if and only if $(n,h) = 1$.

Our next objective, in section 3.3, was to consider sets of points of type $\mathcal{D}(2^n + 2^m)$ for some positive integer n and m (without loss of generality we assume $m > n$). We divided into the following cases:

A. The order of the plane is 2^h and h is even,

(A1) n even, m odd

(A2) n even, m even

(A3) n odd, m odd

(A4) n odd, m even

B. The order of the plane is 2^h and h is odd,

(B1) n even, m odd

(B2) n even, m even

(B3) n odd, m odd

(B4) n odd, m even

We summarize the results on our attempt to classify hyperovals of type $\mathcal{D}(2^n + 2^m)$ in section 3.3 as follows.

We first showed that for k belonging to cases **(A1)**, **(A3)**, **(A4)** and **(B1)**, the set of points $\mathcal{D}(k)$ is not a hyperoval of $PG(2, 2^h)$.

A consequence of Theorem 3.3.3 is that a set of points $\mathcal{D}(2^m+2^n)$, with $m > n$, can be shown to be not a hyperoval of $PG(2,2^h)$ according to the following cases:

(i) When n divides m, then $\mathcal{D}(2^m + 2^n)$ is not a hyperoval of $PG(2,2^h)$ whenever $h \equiv 0 \bmod m$;

(ii) When n does not divide m, then $\mathcal{D}(2^m + 2^n)$ is not a hyperoval of $PG(2,2^h)$ if the following cases hold:

(a) $h \equiv 0 \bmod n$ (but $h \not\equiv 0 \bmod m$);

(b) $h \equiv 0 \bmod m$ (but $h \not\equiv 0 \bmod n$);

(c) $h \equiv 0 \bmod m$ and $h \equiv 0 \bmod n$);

(d) $h \equiv 0 \bmod \frac{m}{2}$.

Furthermore, a set of points $\mathcal{D}(2^m + 2^n)$, $m > n$, is not a hyperoval whenever the index h can be expressed as $h = am+bn$, where a and b are non-negative integers and a is as large as possible (i.e. $0 \leq bn \leq m-1$).

It was also showed that $\mathcal{D}(2^n + 2^m)$ is not a hyperoval of $PG(2,2^h)$ whenever $h = am + bn + 1$ and $h \geq 2m + n + 1$ (where a is as large as possible and $0 \leq bn \leq m-1$).

Two special cases dealing with sets of points of $PG(2,2^h)$ of the form:

1. $\mathcal{D}(2 + 2^m)$, $2 \leq m \leq h-1$;

2. $\mathcal{D}(2^2 + 2^m)$, $m \geq 4$ even;

are provided in section 3.4, which is summarized as follows.

First is a full classification of sets of points of the form $\mathcal{D}(2+2^m)$, for $2 \leq m \leq h-1$, in the sense that a set of points $\mathcal{D}(2 + 2^m)$ is not a hyperoval of $PG(2,2^h)$ unless either:

(i) $m = 2$, h odd, in which case $\mathcal{D}(6)$ is a Segre hyperoval, or

(ii) $h = 2m - 1$, in which case $\mathcal{D}(2 + 2^m)$ is a translation hyperoval.

Finally it was showed that a set of points $\mathcal{D}(2^2 + 2^m)$, where $m \geq 4$ is even, is not a hyperoval of $PG(2, 2^h)$ whenever the index of the plane $h \geq 2m + 3$ is odd and also whenever the index of the plane $h \geq m + 2$ is even.

In conclusion, in order to fully classify hyperovals of type $\mathcal{D}(k)$ where the integer k has two terms in its binomial expansion, we still need to investigate the remaining cases in **(A2)**, **(B2)**, **(B3)** and **(B4)**.

In particular, we must note that the following hyperovals of $PG(2, 2^h)$ occur in cases **(B2)**, **(B3)** and **(B4)**:

1. In **(B2)**, there exist hyperovals of type $\mathcal{D}(\sigma + \gamma)$, whenever $h \equiv 7 \bmod 8$ with $\sigma = 2^{\frac{h+1}{2}}$ and $\gamma = 2^{\frac{h+1}{4}}$;

2. in **(B3)**, there exist hyperovals of type $\mathcal{D}(\sigma + \gamma)$ whenever $h \equiv 1 \bmod 8$ with $\sigma = 2^{\frac{h+1}{2}}$, $\gamma = 2^{\frac{3h+1}{4}}$;

3. in **(B4)**, there exist the following two types of hyperovals:

   - $\mathcal{D}(\sigma + \gamma)$, with $\sigma = 2^{\frac{h+1}{2}}$, where:

     (i) if $h \equiv 3 \bmod 8$ then $\gamma = 2^{\frac{h+1}{4}}$;

     (ii) if $h \equiv 5 \bmod 8$ then $\gamma = 2^{\frac{3h+1}{4}}$;

   - $\mathcal{D}(2^{h-1} + 2^{h-2})$, which is a translation hyperoval equivalent to $\mathcal{D}(2)$ and $\mathcal{D}(2^{h-2})$.

It can also be observed that there are no known hyperovals of type $\mathcal{D}(k)$ of $PG(2, 2^h)$ for integer k belonging to case **(A2)**.

Also, since it has been shown that a set of points $\mathcal{D}(2^2 + 2^m)$ for some even integer $m \geq 4$ is not a hyperoval of $PG(2, 2^h)$ whenever the index h is even and that a set of points $\mathcal{D}(k)$ with k belonging to cases **(A1)** and **(B1)** are non-hyperovals, what remains to be done in order to complete the classification of sets of points of $PG(2, 2^h)$ of the form $\mathcal{D}(2^2 + 2^m)$, for any integer $2 < m < h - 1$, is to classify the

case when the index of the plane h is odd and $m+1 \leq h \leq 2m+1$. Note that this belongs to case **(B2)** and that Glynn's hyperovals $\mathcal{D}(\sigma+\gamma)$ occur in the planes $PG(2,2^h)$ whenever the index $h \equiv 7 \bmod 8$ and $\sigma = 2^{\frac{h+1}{2}}$, $\gamma = 2^{\frac{h+1}{4}}$ (for example, $\mathcal{D}(2^2+2^4)$ is a hyperoval of $PG(2,2^7)$).

Chapter 4

Further results on classification of Monomial Hyperovals

In the last chapter, we have been considering the values of $k \in \{1, \ldots, q-2\}$ and showing that certain sets $\mathcal{D}(k)$ in $PG(2, 2^h)$ are not hyperovals by producing a value of $d \in \{1, \ldots, q-2\}$ such that $d \preceq kd$, then using Theorem 1.2.8. In this chapter we shall take a different approach by considering an integer $d \in \{1, \ldots, q-2\}$ and investigating which type(s) of k are "ruled out" by this type of d. In other words, given d, which k satisfy $d \preceq kd$ so that $\mathcal{D}(k)$ is not a hyperoval. Thus, for a given type of d, we try to determine the possible binary representations of k such that $d \in \mathcal{S}(k)$.

4.1 Which $\mathcal{D}(k)$ does a particular value of d rule out?

First we note that if $d \in \mathcal{S}(k)$ then so is every element of the orbit (in $GF(q)^*$) of d under $Aut(GF(q)^*)$.

Theorem 4.1.1 *Let $PG(2, 2^h)$ be the Desarguesian projective plane of even order $q = 2^h$ and let $k \in \{1, \ldots, q-2\}$. Then $d \in \mathcal{S}(k)$ if and only if $d^\alpha \in \mathcal{S}(k)$, for all*

$\alpha \in Aut(GF(2^h))$.

Proof. Now $Aut(GF(2^h))$ is the automorphism group of the field $GF(2^h)$, so that

$$Aut(GF(2^h)) = \{2^n : n \in \{0, \ldots, h-1\}\}$$

see Hirschfeld [13]. First, we let

$$d = \sum_{i \in \Omega} 2^i \text{ and } kd = \sum_{i \in \mathcal{I}} 2^i \text{ for subsets } \Omega \text{ and } \mathcal{I} \text{ of } \{0, \ldots, h-1\}.$$

Then

$$\begin{aligned}
d \preceq kd \pmod{q-1} &\iff \sum_{i \in \Omega} 2^i \preceq \sum_{i \in \mathcal{I}} 2^i \\
&\iff \Omega \subseteq \mathcal{I} \\
&\iff \Omega + n \subseteq \mathcal{I} + n \pmod{h} \\
&\iff \sum_{i \in \Omega + n} 2^i \preceq \sum_{i \in \mathcal{I} + n} 2^i \\
&\iff \left(2^n \sum_{i \in \Omega} 2^i\right) \preceq \left(2^n \sum_{i \in \mathcal{I}} 2^i\right) \\
&\iff 2^n d \preceq 2^n kd \\
&\iff 2^n d \preceq k(2^n d) \\
&\iff 2^n d \in \mathcal{S}(k). \ \blacksquare
\end{aligned}$$

An orbit of a particular value of $d \in \mathcal{S}(k)$ is the set

$$\left\{2^0 d, 2^1 d, 2^2 d, 2^3 d, \ldots, 2^{h-1} d\right\},$$

(where, as usual, all multiplications are taken modulo $2^h - 1$) and Theorem 4.1.1 shows that a non-empty set $\mathcal{S}(k)$ is a union of the orbits of some $d \in \mathcal{S}(k)$ under the action of the automorphism group $Aut(GF(2^h))$. So for a particular value of k, we only need to find one representative from each orbit of $d \in \mathcal{S}(k)$.

Back to our objective, we first of all consider d with only one term in its binomial expansion, that is d being a power of 2. An orbit of d of this type is a set congruent to $\{2^0, 2^1, 2^2, \ldots, 2^{h-1}\}$ and by Theorem 4.1.1 we need consider only one

representative from the orbit of d of type 2^n and without loss of generality, we let $d = 1$ be the representative.

Let $k \in \{1, \ldots, q-2\}$ and let $k_0 k_1 \ldots k_{h-1}$ be the binary representation of k. Now

$$\begin{aligned} 1 \in \mathcal{S}(k) &\iff 1 \preceq k \\ &\iff k_0 = 1 \\ &\iff k \text{ is odd} \end{aligned}$$

shows that d of type 2^n always belongs to $\mathcal{S}(k)$ with k odd, and consequently $\mathcal{D}(k)$ with k odd is never a hyperoval (note that this result is known; it follows from Theorem 1.2.4).

The next step is to consider d with two terms in its binomial expansion, that is d is of the form $2^m + 2^n$, for $0 \leq m, n \leq h-1$. An orbit of d of this type is a set $\{2^m + 2^n, 2^{m+1} + 2^{n+1}, \ldots, 2^0 + 2^n, \ldots, 2^{h-1}(2^m + 2^n)\}$ which is congruent to $\{1 + 2^n, 2 + 2^{n+1}, \ldots, 2^{h-1} + 2^{h+n-1}\}$. Thus, without loss of generality, by Theorem 4.1.1, we can let $d = 1 + 2^n$ for some positive integer n be the representative of d having 2 terms in its binomial expansion. Furthermore, by Theorem 4.1.1 we can assume that :

$$1 \leq n \leq \frac{h-2}{2}, \text{ if } h \text{ is even, and} \tag{4.1}$$

$$1 \leq n \leq \frac{h-1}{2}, \text{ if } h \text{ is odd} \tag{4.2}$$

(for if $1 + 2^n \in \mathcal{S}(k)$ then $2^{h-n}(1 + 2^n) \pmod{2^h - 1} = 1 + 2^{h-n} \in \mathcal{S}(k)$ also).

If $k = \sum_{i=0}^{h-1} k_i 2^i$ and $(1 + 2^n)k = \sum_{i=0}^{h-1} c_i 2^i$, where $c_i, k_i \in \{0, 1\}$ then, by Definition 1.1.2, $k_0 k_1 \ldots k_{h-1}$ and $c_0 c_1 \ldots c_{h-1}$ are the binary representations of k and $(1 + 2^n)k$ respectively.

For a given integer n which satisfies either condition (4.1) or (4.2) accordingly, it is possible to determine all the possible binary representations of $k \in \{1, \ldots, q-2\}$ such that $1 + 2^n \in \mathcal{S}(k)$. We shall illustrate the method involved by the use of an example below.

We also assume that k satisfies the following properties :

(i) $4 \leq k \leq \frac{q}{2} - 2$

(ii) $k, 1-k, k^{-1}, 1-k^{-1}, (1-k)^{-1}, k(k-1)^{-1}$ are all even when read $\bmod(q-1)$

(iii) $(k, q-1) = (k-1, q-1) = 1$

(iv) k is not a power of 2

Example 4.1.1 Let $PG(2, 2^h)$ be the Desarguesian projective plane with the index of the plane $h \geq 6$. We consider the case when $\mathbf{d = 33}$, that is $n = 5$. Now $k < \frac{q}{2}$ implies that $k_{h-1} = 0$ whilst k being even implies that $k_0 = 0$.

We are considering $(1 + 2^5)k$ and the addition between k and $2^5 k$ (in terms of binary representations) is illustrated as follows:

$$\begin{array}{rcccccccccccc}
k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & k_2 & k_3 & k_4 & k_5 & \cdots\cdots & k_{h-6} & k_{h-5} & \cdots & 0 \\
2^5 k & \overset{\text{bin.rep}^n}{=} & k_{h-5} & k_{h-4} & k_{h-3} & k_{h-2} & 0 & 0 & \cdots\cdots & \cdots & \cdots & \cdots & k_{h-6} \\
(1+2^5)k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & c_2 & c_3 & c_4 & 1 & \cdots\cdots & \cdots & \cdots & \cdots & c_{h-1}
\end{array}$$

Suppose $(1+2^5) \in \mathcal{S}(k)$ so that $c_0 = c_5 = 1$. We can separate this problem into two different cases, the first is when a carry of 2^h occurs in the addition process and the second is when there is no carry of 2^h produced. A carry of 2^h when taken modulo $q-1$ results in a 1 being added to the 0^{th} binary position. No carry results from addition in the 0^{th} binary position. Also, further restrictions on h may follow from the calculations. That is, we assume h large enough to accommodate all the binary positions shown. For smaller values of h, the algorithm is easier, see Example 4.1.2.

If there is a **carry of $\mathbf{2^h}$** produced in the above addition then $h \geq 7$; this is because if $h = 6$ then

$$\begin{array}{rcccccc}
k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & k_2 & k_3 & k_4 & 0 \\
2^5 k & \overset{\text{bin.rep}^n}{=} & k_1 & k_2 & k_3 & k_4 & 0 & 0
\end{array}$$

and the carry of 2^h does not occur as $k_5 = k_0 = 0$. Furthermore,

$$c_0 = 1 \text{ and } k_0 = 0 \implies k_{h-5} = 0 \text{ (since } k_0 + k_{h-5} + 1 = c_0), \text{ and}$$

$$k_{h-1} = 0 \implies k_{h-6} = 1.$$

Note that if a carry of 2^h occurs then $c_0 = 1$ gives $k_{h-5} = 0$.

Note that in order for a carry of 2^h to occur, we need a $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ at some position in the above addition to produce the carry, and all subsequent positions (up to the position $h-1$) must be of the form $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ or $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to "propagate" the carry. So far we have shown that the binary representation of k is :

$$0\ k_1\ k_2\ k_3\ k_4\ k_5\ \cdots\cdots\ 1\ 0\ k_{h-4}\ k_{h-3}\ k_{h-2}\ 0$$

We now consider all the possibilities for $k_{h-4}\ k_{h-3}\ k_{h-2}$, namely 100, 010, 001, 000, 111, 110, 101, 011. We take the value 100 to illustrate the method. The addition of k to 2^5k is then as follows :

k	$\overset{\text{bin.rep}^n}{=}$	0	k_1	k_2	k_3	k_4	k_5	$\cdots$	$-$	$-$	$-$	1	$-$	1	1	1	0	1	0	0	0
2^5k	$\overset{\text{bin.rep}^n}{=}$	0	1	0	0	0	0	$\cdots$	.	.	.	.	.	$-$	$-$	$-$	1	$-$	1	1	1

Now $k_{h-2} = k_{h-3} = 0$ implies that $k_{h-7} = k_{h-8} = 1$. As $k_{h-4} = 1$, we can thus have k_{h-9} equal to 0 or 1, of course if $k_{h-9} = 1$ then we are done and a carry of 2^h is produced. We have placed a '$-$' on k_{h-9} to indicate that it could be a 0 or a 1. The same reason applies for $k_{h-11}, k_{h-12}, k_{h-13}$ where we have placed a '$-$' on these positions. Note that in all these cases, the value of h must be large enough such that for example, when $k_{h-13} = 1$, this means h must be at least 14 so that $k_{h-13} \neq k_0$. This applies to the rest of this example.

A carry of 2^h will be produced in the above addition if either of the following cases hold:

(i) $k_{h-9} = 1$ ($k_{h-11}, k_{h-12}, k_{h-13}$ can take any value)

(ii) $k_{h-9} = 0$ and $k_{h-11} = 1$ (k_{h-12}, k_{h-13} can take any value)

(iii) $k_{h-9} = k_{h-11} = 0$ and $k_{h-12} = 1$ (k_{h-13} can take any value)

(iv) $k_{h-9} = k_{h-11} = k_{h-12} = 0$ and $k_{h-13} = 1$.

Now suppose that k_{h-9}, k_{h-11}, k_{h-12}, k_{h-13} are all 0. Then we have the following:

k	$\overset{\text{bin.rep}^n}{=}$	0	k_1	$\cdots$	k_5	$\cdots$	1	1	1	$-$	1	0	0	0	1	0	1	1	1	0	1	0	0	0
2^5k	$\overset{\text{bin.rep}^n}{=}$	0	1	$\cdots$	0	$\cdots$	.	.	.	.	.	1	1	1	$-$	1	0	0	0	1	0	1	1	1

Where again we want ' $-$ ' to mean that it can either be 0 or 1. A carry of 2^h is produced if $k_{h-15} = 1$. If $k_{h-15} = 0$ then we need to construct the suitable binary pattern for k in the addition $k + 2^5 k$ which is similar to what has been done above. Repeating the same process will show us that the possible binary patterns of k (excluding k_1 up to k_5) should look like the following :

$$0\ k_1\ k_2\ k_3\ k_4\ k_5\ \cdots\ -\ -\ -\ 1\ -\ \underbrace{1\,1\,1\,0\,1}\ \underbrace{0\,0\,0\,1\,0}\ \cdots\cdots\ \underbrace{1\,1\,1\,0\,1}\ 0\,0\,0$$

OR

$$0\ k_1\ k_2\ k_3\ k_4\ k_5\ \cdots\ -\ 1\ \underbrace{0\,0\,0\,1\,0}\ \underbrace{1\,1\,1\,0\,1}\ \cdots\cdots\ \underbrace{1\,1\,1\,0\,1}\ 0\,0\,0$$

As before, we want the positions where ' $-$ ' occur to mean that it can be a '0' or a '1'. If a '1' occurs in that particular position then a carry of 2^h is produced. Given a particular k_{h-i} with ' $-$ ' is equal to 1, it is not necessary for any other k_{h-j}, $j > i$, containing ' $-$ ' to be equal to 1 for a carry of 2^h to result in the addition.

The final stage is to determine all the possible values of k_1 up to k_5 by using the constraint $c_5 = 1$. As we chose $k_{h-4}k_{h-3}k_{h-2}$ to be '100', the addition we should consider is as follows:

$$\begin{array}{ccccc} k_1 & k_2 & k_3 & k_4 & k_5 \\ 1 & 0 & 0 & 0 & 0 \\ c_1 & c_2 & c_3 & c_4 & 1 \end{array}$$

This enables us determine all the possible values of $k_1k_2k_3k_4k_5$ each of which will result in $c_5 = 1$ when added to '10000'. For instance, in this particular case, they are {11110, 01111, 11101, 01101, 11011, 01011, 10111, 00111, 10011, 00011, 10101, 00101, 11001, 01001, 10001, 00001}.

The same process could be done for each of the other values of $k_{h-4}k_{h-3}k_{h-2}$ to produce other possible binary patterns of k still in the case when we assume that there is a carry of 2^h.

Now suppose there is **no carry of 2^h** in the addition $k + 2^5k$. Then $c_0 = 1$ implies that $k_{h-5} = 1$ (which in turn implies that $k_{h-10} = 0$). Contrary to the case when there is a carry of 2^h we need a $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ at some binary position $(h - i)$ in the addition $k + 2^5k$ as well as no $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ occurring in any binary position $(h - j)$, with $j > i$. To determine the appropriate binary patterns of k, we use the same method as what was described in the case when there is a carry of 2^h. The addition $k + 2^5k$ is now as follows (we still use $k_{h-4}k_{h-3}k_{h-2} = 100$):

$$\begin{array}{rcccccccccccccccccc}
k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & k_2 & k_3 & k_4 & k_5 & \cdots\cdots & 0 & 0 & - & - & - & 1 & 1 & 0 & 0 & 0 \\
2^5k & \overset{\text{bin.rep}^n}{=} & 1 & 1 & 0 & 0 & 0 & 0 & \cdots\cdots & . & . & . & . & . & 0 & 0 & - & - & - \\
k + 2^5k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & c_2 & c_3 & c_4 & 1 & \cdots\cdots & . & . & . & . & . & . & . & . & . & .
\end{array}$$

Now $k_{h-1} = k_{h-2} = k_{h-3} = 0$ implies that k_{h-6}, k_{h-7} and k_{h-8} can be a '0' or a '1'. Evidently, the cases for which no carry of 2^h is produced are:

(i) $k_{h-6} = 0$

(ii) $k_{h-6} = 1$ and $k_{h-7} = 0$

(iii) $k_{h-6} = k_{h-7} = 1$ and $k_{h-8} = 0$

Supposing that $k_{h-6} = k_{h-7} = k_{h-8} = 1$ and repeating the process shall give us the following addition:

$$\begin{array}{rcccccccccccccccccc}
k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & \cdots & k_5 & \cdots & - & - & - & - & - & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
2^5k & \overset{\text{bin.rep}^n}{=} & 1 & 1 & \cdots & 0 & \cdots & . & . & . & . & . & - & - & - & - & - & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
k + 2^5k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & \cdots & 1 & \cdots & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & .
\end{array}$$

By observation the only possible binary representation of k in the case where there is no carry of 2^h produced in the addition $k + 2^5k$ (with the assumption that $k_{h-4}k_{h-3}k_{h-2}$ takes the value 100) is:

alternating 00000 and 11111

$$0\ k_1\ \cdots\ k_5\ \cdots\ - - - - - \underbrace{0\,0\,0\,0\,0}\underbrace{1\,1\,1\,1\,1}\ \cdots\ \underbrace{1\,1\,1\,1\,1}\ 0\,0\,0.$$

Whereby the '$-$' means the same as before, except (contrary to the case where there is a carry of 2^h) we would like to have a '0' at some position $(h - i)$ where a

'$-$' occurs instead of a '1'. Finally, note that the range of values of $k_1 \cdots k_5$ is the same as the one in the case where there is a carry of 2^h. ■

Example 4.1.2 For a clearer illustration of the method used in Example 4.1.1, we consider the particular case when $h = 8$ and determine the possible binary representations of k such that $33 \preceq 33k \bmod (2^8 - 1)$ as follows.

Let k have binary representation as in Example 4.1.1, that is

$$k \overset{\text{bin.rep}^n}{=} 0k_1k_2 \ldots k_{h-2}0$$

We consider the addition between k and 2^5k assuming that $(1 + 2^5) \in \mathcal{S}(k)$ (so that $c_0 = c_5 = 1$) as follows:

$$\begin{array}{rcccccccccc} k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & 0 \\ 2^5k & \overset{\text{bin.rep}^n}{=} & k_3 & k_4 & k_5 & k_6 & 0 & 0 & k_1 & k_2 \\ 33k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & c_2 & c_3 & c_4 & 1 & c_6 & c_7 \end{array}$$

Firstly, we assume that there is a **carry of** 2^h occurring in the above binary addition. This implies that $k_3 = 0$ (as $0 + k_3 +$ carry must be equal to $c_0 = 1$) and $k_2 = 1$ (as $k_7 = 0$).

Hence

$$\begin{array}{rcccccccccc} k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & 1 & 0 & k_4 & k_5 & k_6 & 0 \\ 2^5k & \overset{\text{bin.rep}^n}{=} & 0 & k_4 & k_5 & k_6 & 0 & 0 & k_1 & 1 \\ 33k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & c_2 & c_3 & c_4 & 1 & c_6 & c_7 \end{array}$$

Now, we inspect the possible values of $k_4k_5k_6$ with regards to our assumption that a carry of 2^h occurs and also $c_5 = 1$.

It is **not** possible for $k_4k_5k_6$ to adopt one of the following values:

1. 100 (as we have a $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ on the 3^{rd} position which will result in $c_5 = 0$);
2. 000 (for the same reason as for 100);

3. 001 (as we have a $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ on the 4^{th} position);

4. 010 (as a carry of 2^h cannot be produced by having $k_6 = 0$);

5. 110 (as we have a $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ on the 3^{rd} position and either a $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ or a $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ in the subsequent positions which will result in no carry of 2^h);

6. 111 (as we then have a $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ on the 2^{nd} position producing a carry which is then "propagated" resulting in $c_5 = 0$).

Hence the only possible values of $k_4k_5k_6$ are 011 and 101 and so when there is a carry of 2^h, the only possible binary representations of k such that $33 \preceq 33k$ in $PG(2, 2^8)$ are

1. $\{01100110\}$ (when $k_4k_5k_6 = 011$) and

2. $\{01101010\}$ (when $k_4k_5k_6 = 101$).

We have shown that $\mathcal{D}(102)$ and $\mathcal{D}(86)$ are not hyperovals in $PG(2, 2^8)$ since $33 \in \mathcal{S}(102)$ and $\mathcal{S}(86)$.

Now, let's assume that there is **no carry** of 2^h occurring in the addition $k+2^5k$,

$$\begin{array}{rcccccccc} k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & 0 \\ 2^5k & \overset{\text{bin.rep}^n}{=} & k_3 & k_4 & k_5 & k_6 & 0 & 0 & k_1 & k_2 \\ 33k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & c_2 & c_3 & c_4 & 1 & c_6 & c_7 \end{array}$$

Then $c_0 = 1$ implies that $k_3 = 1$ (as $0 + k_3 = 1$). Now, as $k_7 = 0$, the value of k_2 can be 0 or 1. We now consider the case when $k_2 = 0$ as follows.

$$\begin{array}{rcccccccc} k & \overset{\text{bin.rep}^n}{=} & 0 & k_1 & 0 & 1 & k_4 & k_5 & k_6 & 0 \\ 2^5k & \overset{\text{bin.rep}^n}{=} & 1 & k_4 & k_5 & k_6 & 0 & 0 & k_1 & 0 \\ 33k & \overset{\text{bin.rep}^n}{=} & 1 & c_1 & c_2 & c_3 & c_4 & 1 & c_6 & c_7 \end{array}$$

Similarly, it is not possible for $k_4k_5k_6$ to adopt the following values:

1. 100 (as $k_2 = 0$ will not result in $c_5 = 1$);

2. 001 (for the same reason as for 100);

3. 000 (for the same reason as for 100);

4. 111 (as we have a $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ on the 3^{rd} position and a $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ on the 4^{th} and 5^{th} positions resulting in $c_5 = 0$).

Hence the possible binary representations of k such that $33 \preceq 33k$ (for the case when $k_2 = 0$ and assuming there is no carry resulting in the addition $k + 2^5k$) are

1. $\{00011100\}$ (corresponding to $k_4k_5k_6 = 110$);

2. $\{00011010\}$ and $\{01011010\}$ (corresponding to $k_4k_5k_6 = 101$);

3. $\{00010100\}$ and $\{01010100\}$ (corresponding to $k_4k_5k_6 = 010$);

4. $\{00010110\}$ and $\{01010110\}$ (corresponding to $k_4k_5k_6 = 011$).

Similarly, we have shown that $\mathcal{D}(56)$, $\mathcal{D}(88)$, $\mathcal{D}(90)$, $\mathcal{D}(40)$, $\mathcal{D}(42)$, $\mathcal{D}(104)$ and $\mathcal{D}(106)$ are not hyperovals in $PG(2, 2^8)$.

Finally, for the case when $k_2 = 1$ and assuming that a carry of 2^h occurs in the addition $k + 2^5k$, we can apply the same method to obtain the possible binary representations of k such that $33 \preceq 33k$. ■

It is possible to apply and generalize the same method in Example 4.1.1 for any value of n so that we could determine, assuming $(1 + 2^n) \in \mathcal{S}(k)$, all the possible binary representations of k.

By using the above method, we could determine some general patterns of k such that $\mathcal{D}(k)$ is not a hyperoval due to some d having 2 terms in its binomial expansion. Two such patterns are described in the following result.

Theorem 4.1.2 *Let $4 \leq k \leq \frac{q}{2} - 2$ be even and let $k = \sum_{i=0}^{h-1} k_i 2^i$, $k_i \in \{0,1\}$, so that $k_0 k_1 \ldots k_{h-1}$ is the binary representation of k. Also, if $kd = \sum_{i=0}^{h-1} c_i 2^i$ then $c_0 c_1 \ldots c_{h-1}$ is the binary representation of kd.*

Any set $\mathcal{D}(k)$ with k having one of the following binary representations is not a hyperoval of $PG(2, 2^h)$:

(A) $1 \leq n \leq \begin{cases} \frac{h-1}{2} & \text{if } h \text{ is odd} \\ \frac{h-2}{2} & \text{if } h \text{ is even} \end{cases}$

- $k_n = 1, k_0 = k_{h-1} = 0$
- $k_{h-i} = \begin{cases} 1 & \text{if } i = (n+1) + 2jn, (n+2) + 2jn, \ldots, 2n + 2jn \\ 0 & \text{if } i = 1 + 2jn, 2 + 2jn, \ldots, n + 2jn \end{cases}$

  Where the variable j ranges from 0 up to some integer m satisfying

$$0 \leq m \leq \begin{cases} \frac{h-2-2n}{2n} & \text{if } h \text{ is even} \\ \frac{h-3-2n}{2n} & \text{if } h \text{ is odd} \end{cases}$$

- *There exists at least one l such that $k_l = 1$ where $l \in \{h - (2n + 2mn) - n, h-(2n+2mn)-(n-1), \ldots, h-(2n+2mn)-1\}$ if $h-(2n+2mn)-n \geq 1$ and $l \in \{1, 2, \ldots, h - (2n + 2mn) - 1\}$ otherwise.*

Thus

$$k \overset{\text{bin.rep}^n}{=} 0\ k_1\ k_2\ \cdots\ k_{n-1}\ 1\ \cdots\cdots\ \underbrace{- - \cdots -}_{n}\ \underbrace{11\cdots1}_{n}\ \underbrace{00\cdots0}\ \underbrace{11\cdots1}\ \cdots\cdots\ \underbrace{11\cdots1}\ \underbrace{00\cdots0};$$

where the collection of n dashes ($-$ - ^{1}) means that at least one of the n entries is equal to 1. Then $\mathcal{D}(k)$ is not a hyperoval of $PG(2, 2^h)$ where $h \geq 2mn + 2n - 2$. If $h = 2mn + 2n - 2$ then

$$k \overset{\text{bin.rep}^n}{=} 0\ k_1\ \underbrace{1\,1\,\cdots\,1}\ \underbrace{0\,0\,\cdots\,0}\ \cdots\cdots\ \underbrace{1\,1\,\cdots\,1}\ \underbrace{0\,0\,\cdots\,0}$$

where we must have $k_1 = 1$.

(B) *n is odd and* $1 \leq n \leq \begin{cases} \frac{h-1}{2} & \text{if } h \text{ is odd} \\ \frac{h-2}{2} & \text{if } h \text{ is even} \end{cases}$

- $k_{h-i} = \begin{cases} 1 & \text{if } i = 2+2j \\ 0 & \text{if } i = 1+2j \end{cases}$, *where* $j = 0, 1, 2, \ldots, m$ *for some integer* $m \in \{n+1, \ldots, h-2\}$.
- $k_{h-(2+2m)-1} = 1$, $k_0 = k_{h-1} = 0$
- *Together with* $k_1 k_2 \ldots k_n$ *taking all the possible (appropriate) forms such that when added to* $1010\cdots10100$ *will result in* $c_n = 1$. *In other words,* $k_1 k_2 \ldots k_n$ *satisfies the following addition:*

k_1	k_2	k_3	k_4	$\cdots\cdots$	k_{n-4}	k_{n-3}	k_{n-2}	k_{n-1}	k_n
1	0	1	0	$\cdots\cdots$	1	0	1	0	0
c_1	c_2	c_3	c_4	$\cdots\cdots$	c_{n-4}	c_{n-3}	c_{n-2}	c_{n-1}	1

Thus

$$k \overset{\text{bin.rep}^n}{=} 0\ k_1\ k_2\ \cdots\ k_n\ \cdots\cdots\ \underbrace{1}_{h-(2+2mn)-1} 10101010101\cdots0101010$$

where the values of $k_1 \ldots k_n$ *are appropriate in the sense described above. In this case,* $\mathcal{D}(k)$ *is not a hyperoval of* $PG(2, 2^h)$ *with*

$$h \geq \begin{cases} 2m+4 & \text{if } h \text{ is even} \\ 2m+5 & \text{if } h \text{ is odd} \end{cases}$$

Proof. Suppose k has a binary pattern as described in case **(A)**. We must show that $c_0 = c_n = 1$, or in other words show $d = 1 + 2^n \in \mathcal{S}(k)$. Consider the addition $kd = k + 2^n k$ in terms of their binary representations:

									carry				
k	$\overset{\text{bin.rep}^n}{=}$	0	k_1	$\cdots$	k_{n-1}	1	$\cdots\cdots$	$---\cdots-$	$11\cdots1$	$00\cdots0$	$\cdots$	$11\cdots1$	$00\cdots0$
$2^n k$	$\overset{\text{bin.rep}^n}{=}$	0	0	$\cdots$	0	0	$\cdots\cdots$	$\cdots$	$---\cdots-$	$11\cdots0$	$\cdots$	$00\cdots0$	$11\cdots1$
kd	$\overset{\text{bin.rep}^n}{=}$	1	c_1	$\cdots$	c_{n-1}	1	$\cdots\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

As one of the dashes is equal to 1, a carry is produced somewhere between the binary positions number $(h-2mn-(n+1))$ and $(h-2mn-2n)$ in the above addition (marked by *'carry'*). Furthermore, as the binary positions $h-(n+2mn)$ up to $h-1$ consist of alternating $\begin{pmatrix} 00\cdots0 \\ 11\cdots1 \end{pmatrix}$ and $\begin{pmatrix} 11\cdots1 \\ 00\cdots0 \end{pmatrix}$, this carry is propagated through to produce a carry of 2^h which translates into c_0 being equal to 1. Also, as $k_n = 1$

is added to $k_0 = 0$, this produces $c_n = 1$. Hence if k has a binary representation as described in **(A)** then $\mathcal{D}(k)$ is never a hyperoval because $(1+2^n) \in \mathcal{S}(k)$ for some n.

Now let k satisfy the binary pattern described in case **(B)**. We show that $c_0 = c_n = 1$, that is $d = (1+2^n) \in \mathcal{S}(k)$ for some n odd and $1 \leq n \leq \begin{cases} \frac{h-1}{2} & \text{if } h \text{ is odd} \\ \frac{h-2}{2} & \text{if } h \text{ is even} \end{cases}$.
As above, consider the addition $k + 2^n k$ in terms of their binary representations:

										@			*			
k	$\overset{\text{bin.rep}^n}{=}$	0	k_1	k_2	k_3	$\cdots$	k_{n-1}	k_n	$\cdots\cdots$	1	10101	$\cdots$	1	0	1	$\cdots$ 101010
$2^n k$	$\overset{\text{bin.rep}^n}{=}$	0	1	0	1	$\cdots$	0	0	$\cdots\cdots$	.....		$\cdots$	1	1	0	$\cdots$ 010101
dk	$\overset{\text{bin.rep}^n}{=}$	1	.	.	.	$\cdots$	.	1	$\cdots\cdots$	.....		$\cdots$	.	.	.	$\cdots$ .....

As $k_{h-(2+2m)-1} = 1$ (marked by '@') and because n is odd, a carry is produced at the binary position $(h-(2+2m)-1+n)$ (marked by '$*$') and then propagated to the end position $(h-1)$ resulting in a carry of 2^h (this is because the subsequent binary positions from $(h-(2+2m)+n-1)$ up to $(h-1)$ consist of alternating $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$). This carry of 2^h when taken modulo $q-1$ results in c_0 being equal to 1. Finally, we assume that $k_1 \cdots k_n$ takes the correct value such that when addition to $1010\cdots10100$ is performed, we shall have the result $c_n = 1$.

Hence if k is of the form as in case **(B)**, $\mathcal{D}(k)$ is never a hyperoval. ■

4.2 Summary

In this chapter we have first of all established that, for a particular value of k, a set $\mathcal{S}(k) = \{d : 1 \leq d \leq q-2, d \preceq kd\}$ is the union of orbits of $d \in \mathcal{S}(k)$ under the action of the automorphism group $Aut(GF(2^h))$. We then deduced that an integer $d \in \{1, \ldots, q-2\}$ having one term in its binomial expansion (that is of the form 2^n for some positive integer n) always belongs to the set $\mathcal{S}(k)$ whenever k is odd. This gives an alternative proof to the known result that a set of points $\mathcal{D}(k)$ of $PG(2, 2^h)$ is not a hyperoval whenever k is odd, a result which follows from Theorem 1.2.4.

Having considered d having one term in its binomial expansion, we then focused

our attention to an integer $d \in \{1, \ldots, q-2\}$ having two terms in its binomial expansion, that is d of the form $2^m + 2^n$ for two distinct positive integers m and n. By our initial observation, that a set $\mathcal{S}(k)$ is the union of orbits of $d \in \mathcal{S}(k)$ under the action of $Aut(GF(2^h))$, we let $d = 1 + 2^n$, for some positive integer $n \geq 2$, be the representative from an orbit of d of this type. Finally, we illustrated, by the use of an example, an algorithm that determines, for a given $d = 1 + 2^n$, the possible binary representations of integers k such that $d \in \mathcal{S}(k)$. Hence, for a given value of $d \in \{1, \ldots, q-2\}$ having two terms in its binomial expansion, we can work out what types of k satisfy $d \in \mathcal{S}(k)$.

Finally, using this algorithm we formulated two general types of k (in terms of their binary representations) such that $\mathcal{D}(k)$ is not a hyperoval if the integer k has a binary representation which fits any of these two types.

Chapter 5

Conclusion and further research

In order to fully classify monomial hyperovals of the form $\mathcal{D}(2^m + 2^n)$, for some positive integers $m > n$, it is necessary to work on the cases not dealt with in Section 3.3. Among those is the classification of sets of points of $PG(2, 2^h)$, h odd and $m+1 \leq h \leq 2m+1$, having the form $\mathcal{D}(2^2 + 2^m)$, for some even integer $m \geq 4$. Doing so will provide a full description of sets of points of $PG(2, 2^h)$ of the form $\mathcal{D}(2^2 + 2^m)$, for any integer $2 < m < h - 1$.

A useful result in the problem of classification of hyperovals of the form $\mathcal{D}(2^m + 2^n)$ is conjectured as follows.

Conjecture 5.0.1 *Let $\mathcal{D}(k)$ be a set of points of $PG(2, 2^h)$ with k having two terms in its binomial expansion such that it is not a translation hyperoval. Then all the equivalents of $\mathcal{D}(k)$ (being $\mathcal{D}(k^{-1})$, $\mathcal{D}(1-k)$, $\mathcal{D}(1-k^{-1})$, $\mathcal{D}((1-k)^{-1})$ and $\mathcal{D}(k(k-1)^{-1})$) have the form $\mathcal{D}(k')$ where the integer k' has at least three terms in its binomial expansion.*

If true, the conjecture above implies that the only hyperovals of $PG(2, 2^h)$ having the form $\mathcal{D}(2^m + 2^n)$, for some distinct positive integers m and n, are Glynn's hyperovals $\mathcal{D}(\sigma + \gamma)$, Segre's hyperovals $\mathcal{D}(6)$ and the two translation hyperovals $\mathcal{D}(2^{h-1} + 2^{h-2})$ and $\mathcal{D}(2 + 2^m)$ (when $h = 2m - 1$). This would be useful as it shows

exactly which numbers k equal the sum of two powers of 2 appear as hyperovals $\mathcal{D}(k)$.

A similar approach in order to show that there are no other hyperovals of the form $\mathcal{D}(2^m + 2^n)$ apart from the ones mentioned above in $PG(2, 2^h)$ would be to show that the only translation hyperovals of $PG(2, 2^h)$ having the form $\mathcal{D}(2^n + 2^m)$ are $\mathcal{D}(2^{h-1} + 2^{h-2})$ and $\mathcal{D}(2 + 2^m)$ (when $h = 2m - 1$). If this could be shown then it implies that any other sets of points of the form $\mathcal{D}(k)$ with k having two terms in its binomial expansion would not be a translation hyperoval (i.e. all its equivalents would be of the form $\mathcal{D}(k')$ where the integer k' has at least two terms its binomial expansion). Furthermore, we conjecture that if, in addition, $\mathcal{D}(k)$ is not one of:

1. Glynn's $\mathcal{D}(\sigma + \gamma) = \mathcal{D}(2^2 + 2^4)$ in $PG(2, 2^7)$; or
2. Segre's $\mathcal{D}(6)$ in $PG(2, 2^5)$

then all the equivalents of $\mathcal{D}(k)$ must be of the form $\mathcal{D}(k'')$ where the integer k'' must have at least three terms in its binomial expansion; thus showing that the only hyperovals of the form $\mathcal{D}(2^n + 2^m)$ for distinct positive integers m, n are Glynn's $\mathcal{D}(\sigma + \gamma)$, Segre's $\mathcal{D}(6)$ and the two translation hyperovals $\mathcal{D}(2^{h-1} + 2^{h-2})$ and $\mathcal{D}(2 + 2^m)$ (when $h = 2m - 1$).

Finally, as it does not appear that there are hyperovals of the form $\mathcal{D}(2^m + 2^n)$ (m and n are both even) of $PG(2, 2^h)$, h even, it may be worthwhile to pursue the idea of classifying sets of points of $PG(2, 2^h)$, h even, of the form $\mathcal{D}(2^m + 2^n)$ with m and n both even. The approach would probably be to firstly express the index of the plane h as $h = am + bn + r$ where a, b and r are non-negative integers and a is as large as possible and $0 \leq bn \leq m - 1$. Note that the case when $r = 0$ occurs in Result 3.3.4. Also note that as h, m and n are all even, this implies that $r \in \{0, 2, 4, \ldots, m - 2\}$ (that is r takes an even value between 0 and $m - 2$). Afterwards, it would then seem reasonable to deal with the case when $h = am + bn + 2$ by trying to find what type of $d \in \{1, \ldots, q - 2\}$ would satisfy $d \in \mathcal{S}(k)$ for k having the form $2^m + 2^n$, m and n being distinct even integers.

Bibliography

[1] Bose, R. C., "Mathematical theory of the symmetrical factorial design", *Sankhya*, **8** (1947), 107-166.

[2] Bumcrot, R. J., *Modern Projective Geometry*, Holt, Rinehart and Winston Inc. (1969).

[3] Cherowitzo, W., "Hyperovals in Desarguesian planes of even order", *Annals Disc. Math* **37** (1988), 87–94.

[4] Cherowitzo, W., personal communication.

[5] Dembowski, P., *Finite Geometries*, Springer Verlag (1968).

[6] Dickson, L. E., *Linear Groups, with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.

[7] Fraleigh, J. B., *A First Course in Abstract Algebra*, Addison Wesley (1982).

[8] Garner, L. E., *An Outline of Projective Geometry*, Elsevier North Holland (1981).

[9] Glynn, D. G., "Two new sequences of ovals in finite Desarguesian planes of even order", *Combinatorial Mathematics X, Lecture Notes in Mathematics* **1036**, Springer Verlag (1983), 217–229.

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

[11] Hall, M. Jr., "Ovals in Desarguesian plane of order 16", *Ann. Mat. Pura Appl.* **102** (1975), 79–89.

[12] Hirschfeld, J. W. P., "Ovals in Desarguesian planes of even order", *Ann. Mat. Pura Appl. (4)* **102** (1975), 79–89.

[13] Hirschfeld, J. W. P., *Projective Geometries over Finite Fields*, Oxford University Press, New York (1979).

[14] Hungerford, T. W., *Algebra*, Graduate Texts in Mathematics 73, Springer Verlag (1989).

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

[16] Lidl, R. and Niederreiter, H., *Finite Fields*, Encyclopedia Math. Appl., Vol. **20**, Cambridge University Press, Cambridge, 1986.

[17] Matthews, R., "Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field", submitted to *Proc. Amer. Math. Society.*

[18] O'Keefe, C. M. and Penttila, T., "Hyperovals in $PG(2, 16)$", *Europ. J. Combinatorics* **12** (1991), 51–59.

[19] O'Keefe, C. M., "Ovals in Desarguesian Planes", *Australas. J. Combin.* **1** (1990), 149–159.

[20] O'Keefe, C. M., "Quadrics and K-Caps in finite linear spaces of dimension two and three", Honours Pure Mathematics Project, University of Adelaide, 1981.

[21] O'Keefe, C. M., Penttila, T. and Praeger, C. E., "Stabilisers of hyperovals in $PG(2, 32)$", in *Advances in finite geometries and designs*, Eds. Hirschfeld J. W. P., Hughes D. R. and Thas J. A., pp. 337–351, Oxford University Press (1991).

[22] O'Keefe, C. M. and Penttila, T., "A new hyperoval in $PG(2, 32)$", *J. Geometry* **44** (1992), 117–139.

[23] O'Keefe, C. M. and Penttila, T., "Polynomials for Hyperovals of Desarguesian planes", *J. Austral. Math. Soc. (Series A)* **51** (1991), 436–447.

[24] O'Keefe, C. M. and Penttila, T., "Symmetries of Arcs", *J. Combin. Theory (A)*, to appear.

[25] Payne, S. E., "A complete determination of translation ovoids in finite Desarguesian planes", *Atti. Accad. Naz. Lincei, Rend.* (8) 51 (1971), 328–331.

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

[27] Penttila, T. and Pinneri, I., "Irregular hyperovals in $PG(2,64)$", submitted to *J. Geometry.*

[28] Penttila, T. and Royle, G. F., "Classification of hyperovals in $PG(2,32)$", *J. Geometry*, to appear.

[29] Sce, M., "Preliminari ad una teoria aritmetico-gruppale dei k-archi", *Rend. Mat. e Appl* **19** (1960), 241–291.

[30] Segre, B., "Lectures on modern geometry", *Casa Editrice Cremonese (Roma)*, 1960.

[31] Segre, B., "Ovali e curve σ nei piani di Galois di caratteristica due", *Atti Accad. Naz. Lincei. Rend.* (8) **32** (1962), 785–790.

[32] Segre, B., "Ovals in a finite projective plane", *Can. J. Math.* **7** (1955), 414–416.

[33] Segre, B., "Sui k-archi nei piani finiti di caratteristica 2", *Revue de Math. Pures Appl.* **2** (1957), 289–300.

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

[35] Semple, J. G. and Kneebone, G. T., *Algebraic Projective Geometry*, Oxford at the Clarendon Press (1952).

[36] Thas, J. A., Payne, S. E. and Gevaert, H., "A family of ovals with few collineations", *European J. Combin* **9** (1988), 353–362.

ERRATA

Page 2, line 15

The expression $\alpha(xy) = \alpha(x) + \alpha(y)$ should be changed to $\alpha(xy) = \alpha(x)\alpha(y)$

Page 5, line 9

`... and calling the ...' should be changed to `... and calling them the ...'

Page 5, line 20

$f: PG(2,q) \to PG(n,q)$ should be changed to $f: PG(2,q) \to PG(2,q)$

Page 7, line 8

Delete `always' in the statement `... it is always called an *external, tangent ...*'

Page 9, line 11

`... each term of odd power ...' should be `... each term of odd degree ...'

Page 9, line 23

The statement `where x^σ and x^γ are automorphisms of $GF(q)$' must be appended to the end of the line

Page 10, line 2

The statement `where x^σ is an automorphism of $GF(q)$' must be added to the end of the line

Page 10, line 10

`... $\sigma$ is an automorphism ...' should be `... x^σ is an automorphism ...'

Page 12, line 15

The statement `where x^σ and x^γ are automorphisms of $GF(q)$' must be appended to the end of the line

Page 12, line 17

The statement `where x^σ is an automorphism of $GF(q)$' must be added to the end of the line

Page 13, line 24

$N_q = \{1,\ldots,q-2\}$ should be $N_q = \{1,\ldots,q-1\}$

Page 14, line 2

`... known result ...' should be changed to `... known results ...'

Page 18, line 4

Delete the sentence `In other words, the condition that $D(k+1)$ is a hyperoval in $GF(q)$ is equivalent to $h_k(x)$ being a permutation polynomial over $GF(q)$'

Page 18, lines 7-9

The sentence `Unfortunately the polynomials corresponding to the Glynn hyperovals are not readily recognizable as permutation polynomials, so this approach does not work' should be changed to `Unfortunately this approach is difficult to use in general, as indicated by the fact that the polynomials corresponding to the Glynn hyperovals are not readily recognizable as permutation polynomials'

Page 20, line 5

The statement `with q being a power of a prime p' should be appended to the end of the sentence

Page 20, line 17

$1 \le \mu \le q-2$ should be changed to $0 \le \mu \le q-2$

Page 21, line 2

$0 \le \mu' \dfrac{q-1}{d} \le q-1$ should be changed to $0 \le \mu' \dfrac{q-1}{d} < q-1$

Page 21, line 15

`If $q$ is even, then ...'should be changed to `If q is even, so that $p=2$, then ...'

Page 30, line 21

Delete `since' in `Now since ...'

Page 31, line 22

$|S(k)| = 2^{(n,h)} - 2$ should be changed to $|S(2^n)| = 2^{(n,h)} - 2$

Page 38, line 13

$0 \le h - m + 2n - 2 \le n - 3$ should be changed to $m - 2n + 1 \le 0$

Page 40, line 1

$0 \le h - m + 2n - 2 \le n - 3$ should be changed to $m - 2n + 1 \le 0$

Page 40, line 16

$(h > m+2)$ should be changed to $(h \ge m+2)$

Page 59, line 19

`... if either of ...' should be changed to `... if any of ...'