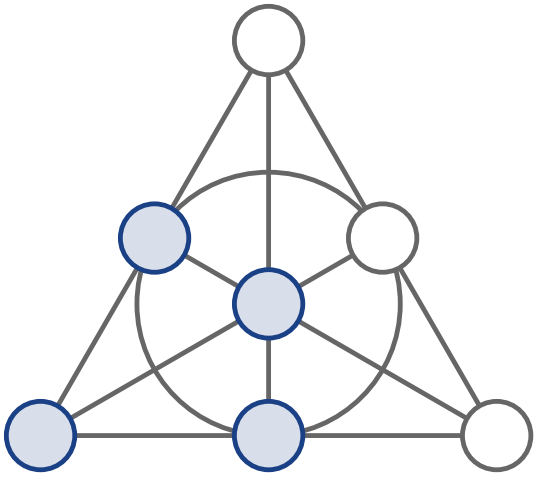
Universität Rostock

Traditio et Innovatio

o-Polynomials and Explicit Formula for o-Monomials



Name: Alexander Oertel

Matrikelnummer: 219 202814

Abgabedatum: 19.08.2024

Betreuer und Gutachter: Prof. Dr. rer. nat. Gohar Kuyreghyan
Universität Rostock
Institut für Mathematik

Gutachter: Lucas Krompholz M.Sc.
Universität Rostock
Institut für Mathematik

https://doi.org/10.18453/rosdok_id00004695

Masterarbeit am Institut für Mathematik
Mathematisch-Naturwissenschaftliche Fakultät

Contents

Introduction **1**

1 Preliminaries **3**

2 o-Polynomials **6**
2.1 Ovals and Hyperovals 6
2.1.1 Basic Objects 6
2.1.2 Describing Ovals and Hyperovals by o-Polynomials 9
2.2 Equivalence of o-Polynomials 13
2.2.1 o-Equivalence 13
2.2.2 Ovals and the Magic Action 16
2.2.3 Application to Hyperovals 27

3 Known Families and Formulas for o-Monomials **37**
3.1 Monomial Families 38
3.1.1 Regular, Translation and Segre Hyperovals 38
3.1.2 Glynn Hyperovals 40
3.1.3 Stabilizers of Monomial Hyperovals 50
3.2 Non-Monomial Families 52
3.2.1 q-Clans 52
3.2.2 Subiaco and Adelaide Hyperovals 53
3.2.3 Payne and Cherowitzo Hyperovals 55
3.3 Explicit Formulas for the Known Monomial Hyperovals 56
3.3.1 Segre Exponents 56
3.3.2 Glynn Exponents 58
3.3.3 Translation Exponents 65

4 Application: 2-to-1 Binomials **68**
4.1 Even Characteristic 68
4.1.1 The 2-to-1 Characterization 68
4.1.2 Equivalence of 2-to-1 Binomials and o-Monomials 71
4.1.3 2-to-1 Binomials from o-Monomials 72
4.2 Odd Characteristic 75
4.2.1 Ovals in Odd Characteristic 75
4.2.2 Families of 2-to-1 Binomials 78
4.2.3 Segre's Theorem and Application to 2-to-1 Binomials 81

Bibliography **83**

Introduction

Hyperovals are fascinating combinatorial objects in finite Desarguesian planes of even order q. They are maximum size arcs, that is, sets of $q+2$ points with no three points being on a single line. Their study was pioneered by Beniamino Segre in the 1950s, and much research since then has given rise to many characterizations, connections to other areas, and a multitude of examples which have been almost completely sorted in a number of infinite families and whose properties have been diligently investigated. However, despite all this work, hyperovals continue to fiercely resist a complete classification, indicating that this is a very hard problem.

One particularly fruitful connection is that hyperovals may be represented by a specific class of permutation polynomials over binary finite fields called o-polynomials. This association allows for a reduction to an algebraic problem, so that a major part of the study of hyperovals is actually the study of specific polynomials over finite fields. One goal of this thesis is to survey what is known about o-polynomials.

There are relations between hyperovals and various other geometric and combinatorial objects, see for example [13]. Other applications include the cryptographically relevant bent functions [15] and designs [16, 29]. They also play a role in the MDS conjecture in coding theory, see for example [2].

The application we focus on is the connection of o-polynomials to the 2-to-1 polynomials. An interesting class of 2-to-1 polynomials are the 2-to-1 binomials, which are relevant in the study of finite fields, see for example [30]. Recently, Kölsch and Kyureghyan [25] proved that so-called o-monomials induce 2-to-1 binomials and vice versa. This allows for a convenient construction of 2-to-1 binomials. There is also an equivalence relation called o-equivalence on the set of o-polynomials. Considering its equivalence classes, one can find some transformations mapping o-monomials to different o-monomials. These different o-monomials then give rise to different 2-to-1 binomials. Given an o-monomial from the known families, finding explicit formulas for the o-equivalent o-monomials and then giving the ensuing list of 2-to-1 binomials is the other goal of this thesis.

After beginning with a brief introduction in Chapter 1 to projective planes and their collineations, we turn to the mostly combinatorial elementary properties of hyperovals and how to represent them using o-polynomials in the beginning of Chapter 2. Then we focus on the fascinating question of exactly when o-polynomials are o-equivalent. Various possible transformations have been identified in the past, which are surveyed in [5]. A systematic study of all the possible transformations was started by Penttila and O'Keefe through the introduction of the magic action [35]. Using this powerful machinery they found several transformations, which together fully explain a more restricted equivalence relation we call os-equivalence. As a second step, in [15] these results were lifted to explain o-equivalence as well by Davidova, Budaghyan, Carlet, Helleseth,

Ihringer, and Penttila by considering one further transformation. We replicate this development in greater detail and correct some technical issues as well. Further, we apply this theory to the case of o-monomials and obtain a new proof that each equivalence class contains at most six different o-monomials. The arguments required here are mostly of algebraic nature.

Next we turn our attention to the known families of hyperovals and the known o-polynomials in Chapter 3. As we intend to continue using the o-monomials for our application, we treat them more carefully by reproducing proofs that show that they are indeed o-monomials. We survey the non-monomial o-polynomials and elucidate only briefly how they were found. Following this, for an o-monomial from the list of the known families we calculate explicit formulas for all the o-equivalent o-monomials.

As the last step in preparation for our application, we illuminate the known link between the o-polynomials and the 2-to-1 polynomials in detail using a mixture of combinatorial and algebraic arguments in the first half of Chapter 4. By combining this with our list of o-monomials, we obtain a list of 2-to-1 binomials.

Finally, in the second half of Chapter 4, we generalize some of the applications to the case of odd characteristic, where so far this connection has not been explored. Many arguments and results can be transferred from the even case and as a conclusion to this thesis we achieve a complete classification of a specific class of 2-to-1 binomials.

For this work we assume some familiarity with finite fields, specifically with the subgroups of cyclic groups and the trace map, in addition to the basic notions. Other concepts will be introduced as required. We follow the usual convention of identifying polynomials with the maps they induce, although we sometimes mention this more explicitly when a map is given in non-polynomial form.

1 Preliminaries

In this chapter we briefly introduce the necessary definitions and the background information needed. Our references for this are [1] and [24]. Let q denote a prime power.

1.0.1 Definition. The *projective plane* $\mathrm{PG}(2,q)$ is defined as the set of all subspaces of the vector space $\mathbb{F}_q^3$. The *points* of the plane are the one dimensional subspaces denoted by

$$(x_1,x_2,x_3) := \left\langle \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \right\rangle$$

and its *lines* are the two dimensional subspaces. Incidence is defined via inclusion in $\mathbb{F}_q^3$: A point $x \leq \mathbb{F}_q^3$ is *incident* with a line $l \leq \mathbb{F}_q^3$ if x is a subspace of l. In this case we write $x \in l$ and generally use terms common to geometry. Further, we call points *collinear* if there is a line containing them.

As a point is a vector space, one can always assume one of its coordinates is 1 and we will consistently use the first nonzero coordinate for this normalization, except when describing lines.

The projective plane $\mathrm{PG}(2,q)$ is called the Desarguesian plane of order q. Its lines, the two dimensional subspaces, are uniquely determined by their one dimensional orthogonal complement, so by a point.

1.0.2 Notation (Lines of $\mathrm{PG}(2,q)$)**.** The lines of $\mathrm{PG}(2,q)$ are

- $l_{a,b} := \left\langle \left(\begin{smallmatrix} a \\ b \\ 1 \end{smallmatrix}\right) \right\rangle^{\perp}$ for $a,b \in \mathbb{F}_q$,
- $l_a := \left\langle \left(\begin{smallmatrix} a \\ 1 \\ 0 \end{smallmatrix}\right) \right\rangle^{\perp}$ for $a \in \mathbb{F}_q$, and
- $l_\infty := \left\langle \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right) \right\rangle^{\perp}$.

Next, we give some of the most important properties that we use later.

1.0.3 Lemma (Properties of $\mathrm{PG}(2,q)$)**.** *The projective plane* $\mathrm{PG}(2,q)$ *has the following properties.*

1. *There are exactly* q^2+q+1 *points and also exactly* q^2+q+1 *lines.*
2. *For two distinct points there is a unique line containing them both and two distinct lines meet in a unique point.*

3. A point is contained in exactly $q+1$ lines and a line contains exactly $q+1$ points.

We write the unique line containing the points A and B as $A \vee B$. Similarly, the unique point contained in the lines l and g is written as $l \wedge g$.

An important part of the study of projective planes are its collineations, which are incidence preserving bijective maps from the plane to itself. To cover them, we need the notion of group actions, for which we follow [26].

1.0.4 Definition (Group Action)**.** Let G be a group with identity e and let X be a set. A *group action* of G on X is a map $G \times X \to X$, written $(g, x) \mapsto gx$, with the properties

(i) $ex = x$ for all $x \in X$ and

(ii) $(g_1 g_2)x = g_1(g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$.

We say the group G *acts* on X. The sets

$$x^G := \{gx : g \in G\}$$

for $x \in X$ are called the *orbits* and the action is called *transitive* if X itself is an orbit. Further, for a subset $A \subseteq X$ the set

$$\{g \in G : gA = A\}$$

is called the *stabilizer* of A.

Now we can introduce the group of collineations and the group of projectivities. They are bijective maps $\mathrm{PG}(2,q) \to \mathrm{PG}(2,q)$, induced by (semi-) linear maps $\mathbb{F}_q^3 \to \mathbb{F}_q^3$.

1.0.5 Definition. Define

$$\mathrm{P\Gamma L}(3,q) := \{\psi : \mathrm{PG}(2,q) \to \mathrm{PG}(2,q),\ x \mapsto Ax^\gamma : A \in \mathrm{GL}(3,q), \gamma \in \mathrm{Aut}(\mathbb{F}_q)\},$$

the *group of collineations* of $\mathrm{PG}(2,q)$, where by x^γ we mean the automorphism γ applied to (a representative of) x component-wise. Define further

$$\mathrm{PGL}(3,q) := \{\varphi : \mathrm{PG}(2,q) \to \mathrm{PG}(2,q),\ x \mapsto Ax : A \in \mathrm{GL}(3,q)\},$$

the *group of projectivities* of $\mathrm{PG}(2,q)$.

These groups act on $\mathrm{PG}(2,q)$ by mapping an element of $\mathrm{PG}(2,q)$ just as the element of $\mathrm{P\Gamma L}(3,q)$, respectively $\mathrm{PGL}(3,q)$, would. Collineations are precisely those bijective maps, which preserve incidence. Therefore, a mapping rule for the points of $\mathrm{PG}(2,q)$ suffices to describe a collineation.

Equivalence of two point sets of $\mathrm{PG}(2,q)$ is to be understood as equivalence under $\mathrm{P\Gamma L}(3,q)$.

1.0.6 Definition. Two sets of points $\mathcal{S}_1, \mathcal{S}_2$ of $\mathrm{PG}(2,q)$ are *equivalent* if there is a collineation $\varphi \in \mathrm{P\Gamma L}(3,q)$ with $\varphi\mathcal{S}_1 = \mathcal{S}_2$.

A set of four points of $\mathrm{PG}(2,q)$, no three of them collinear, is called a frame of $\mathrm{PG}(2,q)$. One simple example is the fundamental quadrangle

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

An element of $\mathrm{PGL}(3,q)$ is uniquely determined by its values on a frame of $\mathrm{PG}(2,q)$ and the group acts transitively on the set of frames of $\mathrm{PG}(2,q)$ (by mapping each point of the frame individually).

Finally, we would like to mention that there is a more abstract notion of a projective plane with properties as in Lemma 1.0.3, of which $\mathrm{PG}(2,q)$ is only one example, but not the only one.

2 o-Polynomials

In this chapter we introduce hyperovals and the functions describing them, the o-polynomials.

2.1 Ovals and Hyperovals

2.1.1 Basic Objects

In this subsection we start by describing ovals and hyperovals and their basic properties. For the first few (mostly counting) arguments we follow [22]. Although we state the results for the projective plane $\mathrm{PG}(2,q)$, these basic properties remain valid for arbitrary projective planes.

2.1.1 Definition (k-Arc)**.** A *k-arc* in the projective plane $\mathrm{PG}(2,q)$ is a set of k points of $\mathrm{PG}(2,q)$, for which no three of them are collinear.

2.1.2 Definition. Let $\mathcal{A}$ be a k-arc of $\mathrm{PG}(2,q)$. An *external line* of $\mathcal{A}$ is a line of $\mathrm{PG}(2,q)$, which does not meet $\mathcal{A}$, a *tangent* of $\mathcal{A}$ is a line of $\mathrm{PG}(2,q)$ meeting $\mathcal{A}$ in exactly one point and a *bisecant* of $\mathcal{A}$ is a line of $\mathrm{PG}(2,q)$ meeting $\mathcal{A}$ in exactly two points.

Note that there cannot be a line meeting the k-arc $\mathcal{A}$ in more than two points, because these points would be collinear. Next, we count the external lines, tangents and bisecants, with the goal of understanding maximum size arcs.

2.1.3 Lemma. *Let $\mathcal{A}$ be a k-arc of $\mathrm{PG}(2,q)$ and P be a point of $\mathcal{A}$. Then*

(i) the number of tangents through P is $t := t(P) := q + 2 - k$,

(ii) the number of external lines is $\tau_0 := \frac{(q-1)q}{2} + \frac{t(t-1)}{2}$,

(iii) the number of tangents is $\tau_1 := kt$, and

(iv) the number of bisecants is $\tau_2 := \frac{k(k-1)}{2}$.

Proof. There are $q+1$ lines through P, as $\mathrm{PG}(2,q)$ has order q. Furthermore, there are no external lines through P and we can find all bisecants meeting $\mathcal{A}$ in P by constructing the unique lines from P to each of the remaining $k-1$ points of $\mathcal{A}$. Thus we conclude that there are

$$q + 1 - (k-1) = q + 2 - k = t$$

tangents through P. Because two points of $\mathcal{A}$ do not share tangents, there are $kt = \tau_1$ tangents overall. We can find all bisecants of $\mathcal{A}$ by choosing two points of $\mathcal{A}$ and constructing the unique line incident with both points. Thus we have $\tau_2 = \binom{k}{2} = \frac{k(k-1)}{2}$ bisecants. Finally, there are $q^2 + q + 1$ lines in $\mathrm{PG}(2, q)$ overall, so we calculate

$$\begin{aligned}\tau_0 &= q^2 + q + 1 - kt - \frac{k(k-1)}{2} = q^2 + q + 1 - \frac{2kt + k(k-1)}{2} \\ &= \frac{2q^2 + 2q + 2 - k(k + 2t - 1)}{2} = \frac{2q^2 + 2q + 2 - (q + 2 - t)(q + t + 1)}{2} \\ &= \frac{2q^2 + 2q + 2 - q^2 - qt - q - 2q - 2t - 2 + qt + t^2 + t}{2} \\ &= \frac{q^2 - q + t^2 - t}{2} = \frac{q(q-1)}{2} + \frac{t(t-1)}{2},\end{aligned}$$

where we substituted $k = q + 2 - t$. □

2.1.4 Definition. Let $\mathcal{A}$ be a k-arc of $\mathrm{PG}(2, q)$ and let Q be a point not on $\mathcal{A}$. Then let $\sigma_i(Q)$ denote the number of lines through Q meeting $\mathcal{A}$ in exactly i points for $i = 0, 1, 2$.

2.1.5 Lemma. *Let $\mathcal{A}$ be a k-arc of $\mathrm{PG}(2, q)$ and let Q be a point not on $\mathcal{A}$. Then we have $\sigma_1(Q) + 2\sigma_2(Q) = k$.*

Proof. Consider the lines l_P from Q to a point P of $\mathcal{A}$. If l_P is tangent, it will appear only once when going through all the points P. If l_P is a bisecant, it will appear twice when going through the points P. So we have $\sigma_1(Q) + 2\sigma_2(Q) = k$. □

2.1.6 Theorem. *Let $\mathcal{A}$ be a k-arc in $\mathrm{PG}(2, q)$. Then*

$$k \leq \begin{cases} q + 2 & : q \text{ even}, \\ q + 1 & : q \text{ odd}. \end{cases}$$

Proof. By Lemma 2.1.3 we have $0 \leq t = q + 2 - k$ tangents, so $k \leq q + 2$. Let q be odd now and assume there is a $(q + 2)$-arc $\mathcal{A}$. Then by Lemma 2.1.3 there are no tangents to $\mathcal{A}$. Picking a point $Q \in \mathrm{PG}(2, q) \setminus \mathcal{A}$ and applying Lemma 2.1.5 we get $2\sigma_2(Q) = k = q + 2$. As $q + 2$ is odd, we have a contradiction. □

2.1.7 Definition (Oval)**.** An *oval* $\mathcal{O}$ of $\mathrm{PG}(2, q)$ is a set of $q + 1$ points, for which no three of them are collinear. Equivalently, an oval is a $(q + 1)$-arc of $\mathrm{PG}(2, q)$.

2.1.8 Definition (Hyperoval)**.** A *hyperoval* $\mathcal{H}$ of $\mathrm{PG}(2, q)$ is a set of $q + 2$ points, for which no three of them are collinear. Equivalently, a hyperoval is a $(q + 2)$-arc of $\mathrm{PG}(2, q)$.

Theorem 2.1.6 implies that ovals are the largest arcs for q odd and that hyperovals may only exist when q is even, i.e. when the characteristic of the underlying field $\mathbb{F}_q$ is two. These bounds are sharp, see Example 2.1.16 for a hyperoval and Example 4.2.4 for an oval. Note that ovals in odd characteristic are very well understood via Segre's Theorem, which we state and use in Subsection 4.2.3. Also note that in earlier literature

the term oval was used to denote arcs of maximum size and that the distinction between ovals and hyperovals came only later (see for example the definitions given in the book [22, Chapter 8] and the survey [42]).

Next, we illustrate the connection between ovals and hyperovals in characteristic two.

2.1.9 Lemma. *Let q be even and $\mathcal{O}$ be an oval of* $\mathrm{PG}(2,q)$*. Then two distinct tangents of $\mathcal{O}$ do not intersect on a bisecant of $\mathcal{O}$.*

Proof. Consider $Q \in \mathrm{PG}(2,q) \setminus \mathcal{O}$. By Lemma 2.1.5 we have $\sigma_1(Q) + 2\sigma_2(Q) = q+1$. Because $q+1$ is odd, $\sigma_1(Q)$ must be odd as well, so $\sigma_1(Q) \geq 1$.

Let l be an arbitrary bisecant of $\mathcal{O}$. Then for every point $P \in l$, there is at least one tangent of $\mathcal{O}$ meeting P: For points P outside of $\mathcal{O}$, the preceding argument holds and for points P inside $\mathcal{O}$ Lemma 2.1.3 implies that there are exactly $q+2-(q+1) = 1$ tangents meeting P.

Again by Lemma 2.1.3 there are $q+1$ tangents to $\mathcal{O}$ overall. On an arbitrary bisecant l of $\mathcal{O}$ there are $q+1$ points and every one of these points has a tangent meeting it, by the preceding argument. Furthermore, two distinct points on l cannot share a single tangent, as the tangent would be uniquely identified as l by the two points. So we have a unique tangent for each point of l. In particular, no two tangents meet in the same point of l. □

2.1.10 Theorem. *Let q be even and $\mathcal{O}$ be an oval of* $\mathrm{PG}(2,q)$*. Then the $q+1$ tangents of $\mathcal{O}$ are concurrent, i.e. they meet in a common point. Furthermore, given a hyperoval $\mathcal{H}$ of* $\mathrm{PG}(2,q)$*, we can obtain an oval by deleting any point of $\mathcal{H}$.*

Proof. Let Q be the meet of two distinct tangents of $\mathcal{O}$. Then by Lemma 2.1.9 Q does not lie on a bisecant, so $\sigma_2(Q) = 0$. An application of Lemma 2.1.5 yields $\sigma_1(Q) = q+1$, so all $q+1$ tangents meet in Q.

For the second statement, we note that deleting points from an arc preserves the property of no three points being collinear. Thus deleting an arbitrary point from $\mathcal{H}$ gives a $(q+1)$-arc, so an oval. □

The preceding basic property of ovals in even characteristic is very important and implies a unique extension of ovals to hyperovals. Note that Theorem 2.1.6 implies that this is not possible if the characteristic is odd. The common point is called the nucleus.

2.1.11 Definition (Nucleus)**.** Let $\mathcal{O}$ be an oval in $\mathrm{PG}(2,q)$ for q even. The common point of the tangents of $\mathcal{O}$ described in Theorem 2.1.10 is called the *nucleus* of $\mathcal{O}$.

2.1.12 Lemma (Extension of Ovals to Hyperovals)**.** *An oval $\mathcal{O}$ in* $\mathrm{PG}(2,q)$*, with q even, may be uniquely extended to a hyperoval by appending its nucleus.*

Proof. Lemma 2.1.9 implies that appending the nucleus of $\mathcal{O}$ does not add a point to a previous bisecant, so there are no three collinear points and we have a hyperoval.

Suppose we added another point $Q \in \mathrm{PG}(2,q) \setminus \mathcal{O}$ to $\mathcal{O}$. The point Q can be only on one tangent, because otherwise Q would be the intersection of two, and hence of all, tangents. So by Lemma 2.1.5 we have $1 + 2\sigma_2(Q) = q+1$, thus Q is on at least one bisecant. Appending Q to $\mathcal{O}$ would then produce three collinear points. Hence the extension is unique. □

2.1.2 Describing Ovals and Hyperovals by o-Polynomials

In this subsection we define and use o-polynomials to characterize ovals and hyperovals, following [28, Section 3]. Let $q = 2^n$ with $n \in \mathbb{N}$ throughout this subsection.

The first important observation is that collineations take hyperovals to hyperovals, as they preserve incidence relations between the points of the hyperoval. Because for ovals and hyperovals no three points are collinear, any four points of the oval or hyperoval make up a frame of $\mathrm{PG}(2,q)$. Since $\mathrm{P\Gamma L}(3,q)$ acts transitively on the frames of $\mathrm{PG}(2,q)$, for any hyperoval there is an equivalent hyperoval containing the fundamental quadrangle

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

Under this assumption hyperovals can be described with o-polynomials.

2.1.13 Definition (o-Polynomial)**.** The polynomial $f \in \mathbb{F}_q[x]$ is called an *o-polynomial* if the set

$$\mathcal{H}(f) := \{(1,s,f(s)) : s \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\}$$

is a hyperoval containing the fundamental quadrangle.

2.1.14 Definition. A monomial $x^e \in \mathbb{F}_q[x]$ is called an *o-monomial*, if it is an o-polynomial and the exponent e is called an *o-exponent* if the monomial x^e is an o-monomial.

2.1.15 Theorem. *Let $f \in \mathbb{F}_q[x]$ be a polynomial. The set $\mathcal{H}(f)$ is a hyperoval if and only if*

(i) f is a permutation polynomial with $f(0) = 0$ and $f(1) = 1$ and

(ii) the polynomial $g_a(x) = (f(x+a) + f(a))x^{q-2}$ is a permutation polynomial for all $a \in \mathbb{F}_q$.

Furthermore, every hyperoval $\mathcal{H}$ containing the fundamental quadrangle may be expressed as $\mathcal{H}(f)$ with an o-polynomial f.

Proof. Let $\mathcal{H}$ be a hyperoval containing the fundamental quadrangle and set

$$P_1 = (1,0,0),\ A = (0,1,0),\ B = (0,0,1),\ P_2 = (1,1,1)$$

and let $P_3, \ldots, P_q$ denote the remaining points of $\mathcal{H}$. We first focus on condition (i), yielding a polynomial f describing $\mathcal{H}$ as $\mathcal{H}(f)$.

Consider the line at infinity, that is,

$$l_\infty = A \vee B = \left\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle = \left\langle \begin{pmatrix}1\\0\\0\end{pmatrix} \right\rangle^{\perp}.$$

No other point of $\mathcal{H}$ is on l_∞, because no three points are collinear. Thus every other point of $\mathcal{H}$ is of the form $(1, c, d)$ with $c, d \in \mathbb{F}_q$. So, let $c_i, d_i \in \mathbb{F}_q$ such that $P_i = (1, c_i, d_i)$ for $i = 1, \ldots, q$. Now assume $c_i = c_j$ for a pair (i, j) with $1 \leq i \neq j \leq q$. Consider the line

$$h := l_{c_i} = B \vee P_i = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ c_i \\ d_i \end{pmatrix} \right\rangle.$$

We have

$$\begin{pmatrix} 1 \\ c_j \\ d_j \end{pmatrix} = \begin{pmatrix} 1 \\ c_i \\ d_i \end{pmatrix} + (d_i + d_j) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

so $P_j \in h$. But then there would be three distinct points of $\mathcal{H}$ on the same line h, so we conclude $c_i \neq c_j$.

Analogously assume $d_i = d_j$ for a pair (i, j) with $1 \leq i \neq j \leq q$. This time we consider the line

$$h := l_{d_i,0} = A \vee P_i = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ c_i \\ d_i \end{pmatrix} \right\rangle.$$

We have

$$\begin{pmatrix} 1 \\ c_j \\ d_j \end{pmatrix} = \begin{pmatrix} 1 \\ c_i \\ d_i \end{pmatrix} + (c_i + c_j) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

and thus $P_j \in h$. This, again, is a contradiction to $\mathcal{H}$ being a hyperoval, so we get $d_i \neq d_j$.

All in all, we obtain that the map $f : c_i \mapsto d_i$ for $i = 1, \ldots, q$ is a permutation satisfying $f(0) = 0$ and $f(1) = 1$, since $P_1 = (1, 0, 0)$ and $P_2 = (1, 1, 1)$.

On the other hand, if a polynomial $f \in \mathbb{F}_q[x]$ satisfies condition (i), $\mathcal{H}(f)$ is a set of $q + 2$ distinct points containing the fundamental quadrangle and there are only two points on the line at infinity. Thus only the equivalence of condition (ii) to no three points of $P_1, \ldots, P_q$ being collinear has yet to be shown.

Let $a, b, c \in \mathbb{F}_q$ be distinct elements. Then the distinct points

$$\left\langle \begin{pmatrix} 1 \\ a \\ f(a) \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 \\ b \\ f(b) \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 1 \\ c \\ f(c) \end{pmatrix} \right\rangle$$

are not collinear if and only if

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ f(a) & f(b) & f(c) \end{pmatrix} \neq 0.$$

A computation of the determinant yields

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ f(a) & f(b) & f(c) \end{pmatrix} = bf(c) + cf(a) + af(b) + bf(a) + cf(b) + af(c) \neq 0$$

and thus

$$b\,(f(a) + f(c)) + af(c) \neq c\,(f(a) + f(b)) + af(b) \tag{2.1}$$

for all distinct $a, b, c \in \mathbb{F}_q$. By adding $af(a)$ to both sides, Formula (2.1) is equivalent to

$$(a + b)\,(f(a) + f(c)) \neq (a + c)\,(f(a) + f(b))$$

and thus to

$$(f(a) + f(c))\,(a + c)^{q-2} \neq (f(a) + f(b))\,(a + b)^{q-2} \tag{2.2}$$

for all distinct $a, b, c \in \mathbb{F}_q$. By counting the image size of

$$\mathbb{F}_q \setminus \{a\} \to \mathbb{F}_q^*,\ t \mapsto (f(t) + f(a))(t + a)^{q-2}$$

Formula (2.2) is seen to be equivalent to

$$\left\{(f(t) + f(a))(t + a)^{q-2} : t \in \mathbb{F}_q \setminus \{a\}\right\} = \mathbb{F}_q^* \tag{2.3}$$

for all $a \in \mathbb{F}_q$. Finally, through substituting $x = t + a$, Formula (2.3) is equivalent to the polynomial $g_a(x) = (f(x + a) + f(a))\,x^{q-2}$ being a permutation polynomial for all $a \in \mathbb{F}_q$. □

We can now give a simple example for an o-polynomial and a hyperoval.

2.1.16 Example. The polynomial $f(x) = x^2$ is an o-polynomial for q even. Indeed, since q is even, the map $x \mapsto x^2$ is a bijection. We have $f(1) = 1$ and $f(0) = 0$, thus condition (i) is met. For condition (ii), we have

$$g_a(x) = \left((x + a)^2 + a^2\right) x^{q-2} = x^q = x,$$

so $g_a(x)$ is a permutation polynomial for all $a \in \mathbb{F}_q$. The resulting hyperoval $\mathcal{H}(f)$ is called the regular hyperoval. See Figure 2.1 for this example in $\mathrm{PG}(2, 2)$.

There are some restrictions on the form of o-polynomials.

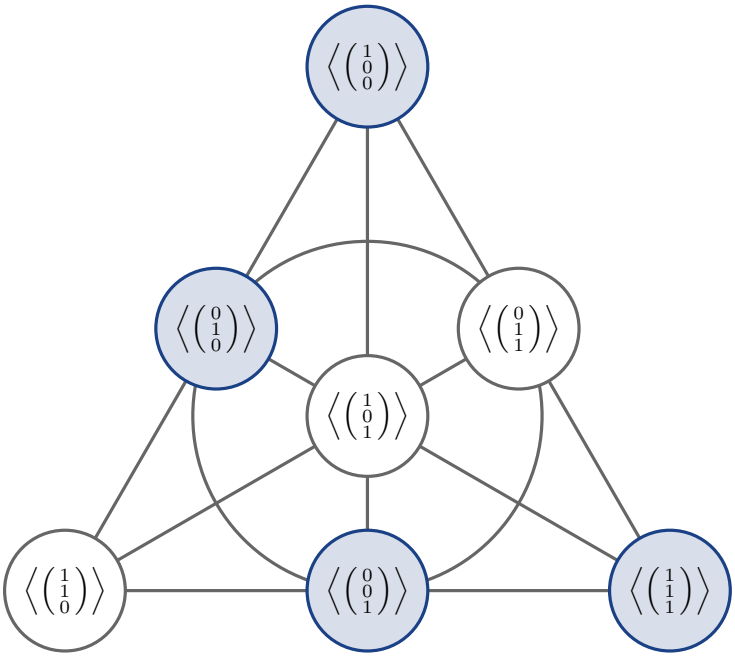


Figure 2.1: The hyperoval $\mathcal{H}(x^2)$ with its points shaded in $\mathrm{PG}(2,2)$.

2.1.17 Corollary. *Let $f \in \mathbb{F}_q[x]$ be an o-polynomial. Then f is of the form*

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

with $b_{2j} \in \mathbb{F}_q$ for $j = 1, \ldots, \frac{q-2}{2}$.

Proof. Let $f(x) = \sum_{j=0}^{q-1} b_j x^j$. Firstly, because $f(0) = 0$, we have $b_0 = 0$. For $a \in \mathbb{F}_q$ we have

$$\begin{aligned} g_a(x) = (f(x+a) + f(a))x^{q-2} &= x^{q-2} \left(\sum_{j=1}^{q-1} b_j \sum_{i=0}^{j} \binom{j}{i} a^{j-i} x^i + \sum_{j=1}^{q-1} b_j a^j \right) \\ &= x^{q-2} \left(\sum_{j=1}^{q-1} \sum_{i=1}^{j} \binom{j}{i} b_j a^{j-i} x^i \right) \\ &= \sum_{j=1}^{q-1} \sum_{i=1}^{j} \binom{j}{i} b_j a^{j-i} x^{i-1}. \end{aligned}$$

We therefore obtain

$$g_a(0) = \sum_{j=1}^{q-1} \binom{j}{1} b_j a^{j-1} = b_1 + a^2 b_3 + \ldots + a^{q-2} b_{q-1} = 0$$

for all $a \in \mathbb{F}_q$ by condition (ii). Equivalently, $A \begin{pmatrix} b_1 \\ \vdots \\ b_{q-1} \end{pmatrix} = 0$, where $A = (a^{2i})_{0 \le i \le \frac{q-2}{2}, a \in \mathbb{F}_q}$.

Because A contains a Vandermonde matrix, it has full rank, so $b_1 = b_3 = \ldots = b_{q-1} = 0$ follows. □

Note that the preceding corollary is a special case ($b = 1$) of a more general condition due to Glynn [19], which we only state for the sake of brevity.

2.1.18 Definition. Let $a, b \in \mathbb{N}$. The number a *covers* b if for every 1 in the binary expansion of b there is a 1 in the binary expansion of a at the same position as well.

2.1.19 Theorem. *A polynomial $f \in \mathbb{F}_q[x]$ with $f(0) = 0$ and $f(1) = 1$ is an o-polynomial if and only if the coefficient of x^a in $f(x)^b \mod x^q + x$ is zero for all pairs (a, b) with $1 \leq b \leq a \leq q-1$ and $b \neq q-1$ such that a covers b.*

2.2 Equivalence of o-Polynomials

The goal of this section is to understand the notion of o-equivalence, that is, when two o-polynomials describe hyperovals which are equivalent under $\mathrm{P\Gamma L}(3, q)$. A natural question to ask would be: Given an o-polynomial, how can one find all other o-polynomials o-equivalent to that o-polynomial? After this question has been settled, we specialize this question to o-monomials, where we find exactly 5 transformations, so six o-equivalent o-monomials all in all.

For this entire section we assume q to be a power of 2.

2.2.1 o-Equivalence

In this subsection we define o-equivalence and give a few examples of equivalent o-polynomials and how to find them. For the notion of o-equivalence we follow [34]. The examples build upon results taken from [5, Section 3.1].

2.2.1 Definition (o-Equivalence)**.** Two o-polynomials $f, g \in \mathbb{F}_q[x]$ are *o-equivalent* if their corresponding hyperovals $\mathcal{H}(f), \mathcal{H}(g)$ are equivalent.

Given an o-polynomial $f \in \mathbb{F}_q[x]$, a natural method for finding an equivalent o-polynomial $g \in \mathbb{F}_q[x]$ is taking a collineation ψ mapping $\mathcal{H}(f)$ to a hyperoval $\psi\mathcal{H}(f)$ containing the fundamental quadrangle and then recovering g from the points of $\psi\mathcal{H}(f)$. The important idea here is that we do not have check the assumptions of Theorem 2.1.15 because we already know that the polynomial describing $\psi\mathcal{H}(f)$ is an o-polynomial.

2.2.2 Example (Permutation of the Coordinates)**.** Let $f \in \mathbb{F}_q[x]$ be an o-polynomial and let f^{-1} denote the compositional inverse of f. Consider the map $\psi : \mathrm{PG}(2, q) \to \mathrm{PG}(2, q), (a, b, c) \mapsto (a, c, b)$. This map is a projectivity given by the matrix

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

stabilizing the fundamental quadrangle. To find the o-polynomial g o-equivalent to f we calculate

$$\begin{aligned}\psi\mathcal{H}(f) &= \psi\{(1,s,f(s)) : s \in \mathbb{F}_q\} \cup \psi\{(0,1,0),(0,0,1)\} \\ &= \{(1,f(s),s) : s \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\} \\ &= \{(1,\hat{s},f^{-1}(\hat{s})) : \hat{s} \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\} \\ &= \mathcal{H}(f^{-1}),\end{aligned}$$

where we have substituted $\hat{s} = f(s)$. Thus we conclude $g = f^{-1}$ and that the compositional inverse map $\mathrm{inv} : f \mapsto f^{-1}$ maps o-polynomials to o-equivalent o-polynomials.

2.2.3 Example (Permutations of the Coordinates II)**.** Let $f \in \mathbb{F}_q[x]$ be an o-polynomial and let $\bar{f}$ denote the reciprocal polynomial $\bar{f}(x) = xf(x^{q-2})$. Consider the map $\psi : \mathrm{PG}(2,q) \to \mathrm{PG}(2,q), (a,b,c) \mapsto (b,a,c)$. This map is a projectivity given by the matrix

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

stabilizing the fundamental quadrangle. We may calculate again

$$\begin{aligned}\psi\mathcal{H}(f) &= \psi\{(1,s,f(s)) : s \in \mathbb{F}_q\} \cup \psi\{(0,1,0),(0,0,1)\} \\ &= \{(s,1,f(s)) : s \in \mathbb{F}_q\} \cup \{(1,0,0),(0,0,1)\} \\ &= \{(1,s^{q-2},s^{q-2}f(s)) : s \in \mathbb{F}_q^*\} \cup \{(0,1,0),(1,0,0),(0,0,1)\} \\ &= \{(1,\hat{s},\hat{s}f(\hat{s}^{q-2})) : s \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\} \\ &= \mathcal{H}(\bar{f}),\end{aligned}$$

where in the third step we swapped out the point $(0,1,0)$ and scaled the coordinates by s^{q-2} to yield a 1 as the first coordinate. In the fourth step we substituted $\hat{s} = s^{q-2}$ and swapped the point $(1,0,0)$ back in. So in conclusion, the map $\phi : f \mapsto \bar{f}$ maps o-polynomials to o-equivalent o-polynomials.

Note that the permutations from the two preceding Examples 2.2.2 and 2.2.3 generate the group of permutations S_3, so that we might define a group action of S_3 on the set of o-polynomials. The orbits of the action would then be the equivalence classes. This has been done first by Cherowitzo in [9], where he has also started the investigation of this topic.

A natural question would be, whether the transformations induced by the permutations of the coordinates are all possible transformations of o-polynomials. The answer in general is no, but for o-monomials it is yes. The next two subsections are devoted to finding all transformations.

To close this section, we count how many polynomials are o-equivalent to a given o-polynomial $f \in \mathbb{F}_q[x]$, given originally in [34]. Recall that we identify polynomials with their maps.

2.2.4 Theorem. *Let $q = 2^n$ and $f \in \mathbb{F}_q[x]$ be an o-polynomial and let G denote the stabilizer of $\mathcal{H}(f)$ under $\mathrm{P\Gamma L}(3,q)$. Then there are*

$$\frac{n(q+2)(q+1)q(q-1)}{|G|}$$

different o-polynomials o-equivalent to f.

Proof. By Theorem 2.1.15 we need to count the number of different hyperovals containing the fundamental quadrangle equivalent to $\mathcal{H}(f)$ under $\mathrm{P\Gamma L}(3,q)$. Let $S(Q)$ be the set of hyperovals that are equivalent to $\mathcal{H}(f)$ and that contain a fixed frame Q of $\mathrm{PG}(2,q)$. Further, let $N(Q) = |S(Q)|$ denote the number of such hyperovals. Note that $N(Q)$ does not actually depend on Q, because a collineation taking Q to a different frame Q' maps the set $S(Q)$ bijectively to $S(Q')$, so $N(Q) = N(Q')$. Our goal is now to determine $N := N(Q)$.

So, let A denote the number of pairs $(\mathcal{H}', Q)$, where $\mathcal{H}'$ is a hyperoval equivalent to $\mathcal{H}(f)$ and Q is a frame contained in $\mathcal{H}'$. On the one hand, we can determine A by first choosing a frame Q. For the first point P_1 we have q^2+q+1 possibilities and for the second point P_2 we have q^2+q remaining points to choose from. The third point must not lie on the line $P_1 \vee P_2$, so there are q^2 remaining possible choices. For the last point we need to exclude the lines $P_1 \vee P_2$, $P_1 \vee P_3$ and $P_2 \vee P_3$. Since each of the points P_1, P_2 and P_3 is excluded twice, there are

$$q^2+q+1-3q-3+3 = q^2-2q+1 = (q-1)^2$$

remaining choices for P_4. Because the order of the points is irrelevant, we obtain

$$A = \frac{(q^2+q+1)\,(q^2+q)\,q^2(q-1)^2}{4!}N. \tag{2.4}$$

On the other hand, we can count the number of hyperovals $\mathcal{H}'$ equivalent to $\mathcal{H}(f)$ and then choose a frame in $\mathcal{H}'$. The set of all hyperovals equivalent to $\mathcal{H}(f)$ is

$$\{\varphi\mathcal{H}(f) : \varphi \in \mathrm{P\Gamma L}(3,q)\}.$$

To obtain its size, we need to factor out all the collineations stabilizing $\mathcal{H}(f)$. We have

$$|\mathrm{P\Gamma L}(3,q)| = n\left(q^2+q+1\right)\left(q^2+q\right)q^2(q-1)^2$$

by choosing an automorphism γ of $\mathbb{F}_q$ and then choosing the values on a frame of $\mathrm{PG}(2,q)$ (which themselves make up a frame). All in all, we obtain

$$A = [\mathrm{P\Gamma L}(3,q) : G]\binom{q+2}{4} = \frac{n\,(q^2+q+1)\,(q^2+q)\,q^2(q-1)^2}{|G|}\binom{q+2}{4}. \tag{2.5}$$

Combining Equations (2.4) and (2.5) now yields

$$N = \frac{n(q+2)(q+1)q(q-1)}{|G|}.$$ □

2.2.2 Ovals and the Magic Action

In order to obtain strong results, we restrict our attention in this subsection to ovals induced by o-permutations. We follow mainly [35]. For o-permutations, we drop the condition that $f(1) = 1$. Equivalently, we drop the assumption that the resulting hyperoval contains the point $(1, 1, 1)$.

2.2.5 Definition (o-Permutation)**.** Let $f \in \mathbb{F}_q[x]$. Then f is called an *o-permutation* if

(i) f is a permutation polynomial with $f(0) = 0$,

(ii) the polynomial $g_a(x) = (f(x+a) + f(a))x^{q-2}$ is a permutation polynomial for all $a \in \mathbb{F}_q$.

2.2.6 Definition (Oval Induced by o-Permutation)**.** Let $f \in \mathbb{F}_q[x]$ be an o-permutation. The corresponding oval is defined as

$$\mathcal{O}(f) = \{(1, s, f(s)) : s \in \mathbb{F}_q\} \cup \{(0, 1, 0)\}.$$

2.2.7 Definition (os-Equivalence)**.** Two o-permutations $f, g \in \mathbb{F}_q[x]$ are *os-equivalent* if their corresponding ovals $\mathcal{O}(f)$ and $\mathcal{O}(g)$ are equivalent.

Note that an o-permutation f may also induce a hyperoval

$$\mathcal{H}(f) = \{(1, s, f(s)) : s \in \mathbb{F}_q\} \cup \{(0, 1, 0), (0, 0, 1)\},$$

which does not contain the point $(1, 1, 1)$ because condition (ii) together with f being a permutation polynomial guarantees that no three points are collinear (cf. Theorem 2.1.15). Then dropping the point $(0, 0, 1)$ gives rise to an oval with nucleus $(0, 0, 1)$. The advantage of o-permutations is the added flexibility of having scalar multiples.

Next, we show that the nucleus has a special role when considering os-equivalent o-permutations. This forces helpful restrictions on the collineations one has to consider when investigating os-equivalent o-permutations.

2.2.8 Lemma. *Let $f, g \in \mathbb{F}_q[x]$ be os-equivalent o-permutations. If $\psi : \mathrm{PG}(2, q) \to \mathrm{PG}(2, q)$ is a collineation mapping $\mathcal{O}(f)$ to $\mathcal{O}(g)$, then $\psi((0, 0, 1)) = (0, 0, 1)$.*

Proof. Consider the tangents $l_1, \ldots, l_{q+1}$ of $\mathcal{O}(f)$. They are concurrent and meet in the nucleus of $\mathcal{O}(f)$, which is $(0, 0, 1)$. The lines $\psi l_1, \ldots, \psi l_{q+1}$ are the tangents of $\psi\mathcal{O}(f) = \mathcal{O}(g)$ because ψ preserves incidence. The tangents of $\mathcal{O}(g)$ also meet in the nucleus $(0, 0, 1)$ of $\mathcal{O}(g)$, so ψ must take $(0, 0, 1)$ to $(0, 0, 1)$. □

2.2.9 Corollary. *Let $f, g \in \mathbb{F}_q[x]$ be os-equivalent o-polynomials. Then they are o-equivalent.*

Proof. Let $\varphi \in \mathrm{P\Gamma L}(3,q)$ denote a collineation taking $\mathcal{O}(f)$ to $\mathcal{O}(g)$. Because we have $\varphi(0,0,1) = (0,0,1)$, we can extend $\varphi\mathcal{O}(f) = \mathcal{O}(g)$ to $\varphi\mathcal{H}(f) = \mathcal{H}(g)$, so f and g are o-equivalent. □

Now we introduce our primary tool for the os-equivalence of o-permutations, the magic action by O'Keefe and Penttila [35]. It is a group action of the group of the collineations of the projective line on the set of o-permutations. We need some notations and definitions first.

2.2.10 Notation. Let γ be an automorphism of $\mathbb{F}_q$. We write $\gamma(x) =: x^\gamma$ for $x \in \mathbb{F}_q$. Furthermore, we write $x^{\frac{1}{\gamma}} := \gamma^{-1}(x)$ for $x \in \mathbb{F}_q$. For a vector $x \in \mathbb{F}_q^k$ (with $k = 2,3$) by x^γ we mean γ applied component-wise and for projective points $\langle x\rangle^\gamma$ is meant to be understood as $\langle x^\gamma\rangle$. Further, for a polynomial $f(x) = \sum_{i=0}^{q-1} a_i x^i$ we define

$$f^\gamma(x) := \left(f\left(x^{\frac{1}{\gamma}}\right)\right)^\gamma = \sum_{i=0}^{q-1} a_i^\gamma x^i.$$

Given a matrix $A = (a_{ij})_{i,j=1,\dots,k}$ we write A^γ for the matrix $(a_{ij}^\gamma)_{i,j=1,\dots,k}$.

2.2.11 Definition. Let

$$\Gamma\mathrm{L}(2,q) := \{\psi : \mathbb{F}_q^2 \to \mathbb{F}_q^2,\ x \mapsto Ax^\gamma : A \in \mathrm{GL}(2,q), \gamma \in \mathrm{Aut}(\mathbb{F}_q)\}$$

be the *group of semilinear maps* of $\mathbb{F}_q^2$ and let

$$\mathrm{P\Gamma L}(2,q) = \{\psi : \mathrm{PG}(2,q) \to \mathrm{PG}(2,q),\ x \mapsto Ax^\gamma : A \in \mathrm{GL}(2,q), \gamma \in \mathrm{Aut}(\mathbb{F}_q)\}$$

be the *group of collineations* of the projective line over $\mathbb{F}_q$. Further, we define

$$\mathcal{F} := \{f : \mathbb{F}_q \to \mathbb{F}_q \mid f(0) = 0\}.$$

2.2.12 Theorem (Magic Action on $\mathcal{F}$)**.** *The group* $\mathrm{P\Gamma L}(2,q)$ *acts on* $\mathcal{F}$ *through* $\psi f : \mathbb{F}_q \to \mathbb{F}_q$ *defined by*

$$x \mapsto |A|^{-\frac{1}{2}} \left((bx+d)f^\gamma\left(\frac{ax+c}{bx+d}\right) + bxf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right), \tag{2.6}$$

where $\psi = x \mapsto Ax^\gamma$ *with* $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$ *and* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$*. This action is called the magic action. The denominators, say* t*, are meant to be read as multiplying by* t^{q-2}*. So, if a denominator is zero, then the corresponding term is zero as well.*

Proof. We begin by showing that the group $\Gamma\mathrm{L}(2,q)$ acts on $\mathcal{F}$ via Formula (2.6) and then that the group $\mathrm{P\Gamma L}(2,q)$ inherits this action.

So let $\psi \in \Gamma\mathrm{L}(2,q)$ with automorphism γ and matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and let $f \in \mathcal{F}$. Then we have

$$(\psi f)(0) = |A|^{-\frac{1}{2}} \left(df^\gamma\left(\frac{c}{d}\right) + df^\gamma\left(\frac{c}{d}\right)\right) = 0,$$

so $\psi f \in \mathcal{F}$. Let $\mathrm{id} \in \Gamma\mathrm{L}(2,q)$, that is, $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x$. Then we have

$$(\mathrm{id}f)(x) = 1\left[(0x+1)f\left(\frac{1x+0}{0x+1}\right) + 0xf\left(\frac{1}{0}\right) + 1f\left(\frac{0}{1}\right)\right] = f(x),$$

thus $\mathrm{id}f = f$.

Let $\psi_1, \psi_2 \in \Gamma\mathrm{L}(2,q)$ with $\psi_1 : x \mapsto A_1 x^{\gamma_1}, \psi_2 : x \mapsto A_2 x^{\gamma_2}$, and

$$A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

We have $\psi_2\psi_1(x) = \psi_2\left(A_1 x^{\gamma_1}\right) = A_2\left(A_1 x^{\gamma_1}\right)^{\gamma_2} = A_2 A_1^{\gamma_2} x^{\gamma_1\gamma_2}$ and

$$A_2 A_1^{\gamma_2} = \begin{pmatrix} a_1^{\gamma_2}a_2 + c_1^{\gamma_2}b_2 & b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2 \\ a_1^{\gamma_2}c_2 + c_1^{\gamma_2}d_2 & b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2 \end{pmatrix}.$$

All in all, we obtain

$$\begin{aligned}\left((\psi_2\psi_1)f\right)(x) = |A_2 A_1^{\gamma_2}|^{-\frac{1}{2}}\Bigg[\\ \left(\left(b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2\right)x + b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2\right) f^{\gamma_1\gamma_2}\left(\frac{\left(a_1^{\gamma_2}a_2 + c_1^{\gamma_2}b_2\right)x + a_1^{\gamma_2}c_2 + c_1^{\gamma_2}d_2}{\left(b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2\right)x + b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2}\right) \\ + \left(b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2\right)xf^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}a_2 + c_1^{\gamma_2}b_2}{b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2}\right) + \left(b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2\right) f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}c_2 + c_1^{\gamma_2}d_2}{b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2}\right)\Bigg].\end{aligned} \tag{2.7}$$

Next, we calculate $\left(\psi_2\left(\psi_1 f\right)\right)(x)$. For the sake of readability we write $g(x) := \left(\psi_1 f\right)(x)$, that is,

$$g(x) = |A_1|^{-\frac{1}{2}}\left((b_1x + d_1)f^{\gamma_1}\left(\frac{a_1x + c_1}{b_1x + d_1}\right)b_1xf^{\gamma_1}\left(\frac{a_1}{b_1}\right) + d_1f^{\gamma_1}\left(\frac{c_1}{d_1}\right)\right).$$

We need an expression for $g^{\gamma_2}(x)$. So we calculate

$$\begin{aligned} g^{\gamma_2}(x) &= \left(g\left(x^{\frac{1}{\gamma_2}}\right)\right)^{\gamma_2} \\ &= \underbrace{\left(|A_1|^{-\frac{1}{2}}\right)^{\gamma_2}}_{=:h_1}\Bigg[\left(b_1^{\gamma_2}x + d_1^{\gamma_2}\right)\underbrace{\left(f^{\gamma_1}\left(\frac{a_1x^{\frac{1}{\gamma_2}} + c_1}{b_1x^{\frac{1}{\gamma_2}} + d_1}\right)\right)^{\gamma_2}}_{=:h_2} \\ &\qquad + b_1^{\gamma_2}x\underbrace{\left(f^{\gamma_1}\left(\frac{a_1}{b_1}\right)\right)^{\gamma_2}}_{=:h_3} + d_1^{\gamma_2}\underbrace{\left(f^{\gamma_1}\left(\frac{c_1}{d_1}\right)\right)^{\gamma_2}}_{=:h_4}\Bigg]. \end{aligned} \tag{2.8}$$

We now manipulate the terms individually.

$$\begin{aligned} h_1 &= \left((a_1d_1 + b_1c_1)^{-\frac{1}{2}}\right)^{\gamma_2} = \left((a_1d_1 + b_1c_1)^{2^n-1-2^{n-1}}\right)^{\gamma_2} \\ &= (a_1^{\gamma_2}d_1^{\gamma_2} + b_1^{\gamma_2}c_1^{\gamma_2})^{2^n-1-2^{n-1}} = |A_1^{\gamma_2}|^{-\frac{1}{2}}\,. \end{aligned}$$

The other three terms may be handled very similarly.

$$\begin{aligned} h_2 &= \left(f^{\gamma_1}\left(\frac{a_1x^{\frac{1}{\gamma_2}} + c_1}{b_1x^{\frac{1}{\gamma_2}} + d_1}\right)\right)^{\gamma_2} = \left(f^{\gamma_1}\left(\left(\frac{a_1^{\gamma_2}x + c_1^{\gamma_2}}{b_1^{\gamma_2}x + d_1^{\gamma_2}}\right)^{\frac{1}{\gamma_2}}\right)\right)^{\gamma_2} = f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}x + c_1^{\gamma_2}}{b_1^{\gamma_2}x + d_1^{\gamma_2}}\right), \\ h_3 &= \left(f^{\gamma_1}\left(\frac{a_1}{b_1}\right)\right)^{\gamma_2} = \left(f^{\gamma_1}\left(\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right)^{\frac{1}{\gamma_2}}\right)\right)^{\gamma_2} = f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right), \\ h_4 &= \left(f^{\gamma_1}\left(\frac{c_1}{d_1}\right)\right)^{\gamma_2} = \left(f^{\gamma_1}\left(\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)^{\frac{1}{\gamma_2}}\right)\right)^{\gamma_2} = f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right). \end{aligned}$$

Plugging these expressions into (2.8), we obtain

$$\begin{aligned} g^{\gamma_2}(x) = |A_1^{\gamma_2}|^{-\frac{1}{2}}\Bigg[&(b_1^{\gamma_2}x + d_1^{\gamma_2})\, f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}x + c_1^{\gamma_2}}{b_1^{\gamma_2}x + d_1^{\gamma_2}}\right) \\ &+ b_1^{\gamma_2}x f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + {d_1}^{\gamma_2} f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg]. \end{aligned} \tag{2.9}$$

Now we are able to consider $(\psi_2 g)(x)$.

$$(\psi_2 g)(x) = |A_2|^{-\frac{1}{2}}\Bigg[\underbrace{(b_2x + d_2)g^{\gamma_2}\left(\frac{a_2x + c_2}{b_2x + d_2}\right)}_{=:T_1} + \underbrace{b_2xg^{\gamma_2}\left(\frac{a_2}{b_2}\right)}_{=:T_2} + \underbrace{d_2g^{\gamma_2}\left(\frac{c_2}{d_2}\right)}_{=:T_3}\Bigg]. \tag{2.10}$$

Applying Formula (2.9) directly results in very long expressions, so we consider the terms T_1, T_2, T_3 one by one. We proceed in an ascending order with respect to the effort involved, underlining terms colorfully that cancel in the sum.

$$\begin{aligned} T_3 &= d_2\,|A_1^{\gamma_2}|^{-\frac{1}{2}}\Bigg[\left(b_1^{\gamma_2}\frac{c_2}{d_2} + d_1^{\gamma_2}\right) f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}\frac{c_2}{d_2} + c_1^{\gamma_2}}{b_1^{\gamma_2}\frac{c_2}{d_2} + d_1^{\gamma_2}}\right) \\ &\qquad + b_1^{\gamma_2}\frac{c_2}{d_2} f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + d_1^{\gamma_2} f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg] \\ &= |A_1^{\gamma_2}|^{-\frac{1}{2}}\Bigg[(b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2)\, f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}c_2 + c_1^{\gamma_2}d_2}{b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2}\right) \\ &\qquad + \underline{b_1^{\gamma_2}c_2 f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right)} + \underline{d_1^{\gamma_2}d_2 f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)}\Bigg]. \end{aligned}$$

Next, we handle T_2.

$$\begin{aligned}
T_3 &= b_2 x \left|A_1^{\gamma_2}\right|^{-\frac{1}{2}} \Bigg[\left(b_1^{\gamma_2}\frac{a_2}{b_2} + d_1^{\gamma_2}\right) f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}\frac{a_2}{b_2} + c_1^{\gamma_2}}{b_1^{\gamma_2}\frac{a_2}{b_2} + d_1^{\gamma_2}}\right) \\
&\qquad + b_1^{\gamma_2}\frac{a_2}{b_2} f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + d_1^{\gamma_2} f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg] \\
&= \left|A_1^{\gamma_2}\right|^{-\frac{1}{2}} \Bigg[\left(b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2\right) x f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}a_2 + c_1^{\gamma_2}b_2}{b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2}\right) \\
&\qquad + b_1^{\gamma_2}a_2 x f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + d_1^{\gamma_2}b_2 x f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg].
\end{aligned}$$

And lastly, we handle T_1.

$$\begin{aligned}
T_1 &= (b_2x + d_2)\left|A_1^{\gamma_2}\right|^{-\frac{1}{2}} \Bigg[\left(b_1^{\gamma_2}\frac{a_2x + c_2}{b_2x + d_2} + d_1^{\gamma_2}\right) f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}\frac{a_2x+c_2}{b_2x+d_2} + c_1^{\gamma_2}}{b_1^{\gamma_2}\frac{a_2x+c_2}{b_2x+d_2} + d_1^{\gamma_2}}\right) \\
&\qquad + b_1^{\gamma_2}\frac{a_2x + c_2}{b_2x + d_2} f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + d_1^{\gamma_2} f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg] \\
&= \left|A_1^{\gamma_2}\right|^{-\frac{1}{2}} \Bigg[\left(b_1^{\gamma_2}(a_2x + c_2) + d_1^{\gamma_2}(b_2x + d_2)\right) f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}(a_2x + c_2) + c_1^{\gamma_2}(b_2x + d_2)}{b_1^{\gamma_2}(a_2x + c_2) + d_1^{\gamma_2}(b_2x + d_2)}\right) \\
&\qquad + b_1^{\gamma_2}(a_2x + c_2) f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + d_1^{\gamma_2}(b_2x + d_2) f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg] \\
&= \left|A_1^{\gamma_2}\right|^{-\frac{1}{2}} \Bigg[\left(\left(b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2\right) x + b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2\right) f^{\gamma_1\gamma_2}\left(\frac{\left(a_1^{\gamma_2}a_2 + c_1^{\gamma_2}b_2\right) x + a_1^{\gamma_2}c_2 + c_1^{\gamma_2}d_2}{\left(b_1^{\gamma_2}a_2 + d_1^{\gamma_2}b_2\right) x + b_1^{\gamma_2}c_2 + d_1^{\gamma_2}d_2}\right) \\
&\qquad + b_1^{\gamma_2}a_2 x f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + b_1^{\gamma_2}c_2 f^{\gamma_1\gamma_2}\left(\frac{a_1^{\gamma_2}}{b_1^{\gamma_2}}\right) + d_1^{\gamma_2}b_2 x f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right) \\
&\qquad + d_1^{\gamma_2}d_2 f^{\gamma_1\gamma_2}\left(\frac{c_1^{\gamma_2}}{d_1^{\gamma_2}}\right)\Bigg].
\end{aligned}$$

Now, by combining the determinants we see that Equation (2.7) and Equation (2.10) coincide. We have therefore proved that the group $\Gamma\mathrm{L}(2,q)$ acts on $\mathcal{F}$ via (2.6).

For the group $\mathrm{P\Gamma L}(2,q)$ to inherit this action, we need to show that the action does not depend on the chosen representation of elements of $\mathrm{P\Gamma L}(2,q)$. The elements of $\mathrm{P\Gamma L}(2,q)$ are uniquely determined by an automorphism $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$ and a matrix $A \in \mathrm{GL}(2,q)$, up to scalar multiples. We thus need to prove that the action is invariant under taking scalar multiples of A. We may represent a scalar multiple of A as $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) A$ with $a \in \mathbb{F}_q^*$. So far we have shown $(\psi_2\psi_1)f = \psi_2(\psi_1 f)$ for $\psi_1, \psi_2 \in \Gamma\mathrm{L}(2,q)$. So, let $\psi_1 \in \Gamma\mathrm{L}(2,q)$ be a representation of $\psi \in \mathrm{P\Gamma L}(2,q)$ and let $\psi_2 : x \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) x \in \Gamma\mathrm{L}(2,q)$.

Then we have

$$(\psi_2 f)(x) = a^{-1}\left(af\left(\frac{ax}{a}\right)\right) = f(x)$$

and thus $(\psi_2\psi_1)f = \psi_1 f$ for all $f \in \mathcal{F}$ and the action is independent of the chosen representation. □

The first important property is the semilinearity of the magic action. The second important property, one of the reasons the magic action is interesting to us, is that the magic action maps o-permutations to os-equivalent o-permutations. Moreover, a collineation mapping the oval $\mathcal{O}(f)$ to $\mathcal{O}(\psi f)$, for an o-permutation f and a collineation $\psi \in \mathrm{P\Gamma L}(2,q)$, can be given explicitly.

After proving these facts, we will be able to give an example easily. Also note that $\mathrm{P\Gamma L}(2,q)$ acts on the sets of o-permutations and o-polynomials as well, since we identify maps and polynomials.

2.2.13 Lemma. *The magic action of* $\mathrm{P\Gamma L}(2,q)$ *on* $\mathcal{F}$ *is semilinear, that is, for* $k \in \mathbb{F}_q$, $f, g \in \mathcal{F}$, *and* $\psi : x \mapsto Ax^\gamma \in \mathrm{P\Gamma L}(2,q)$ *we have*

$$\psi(kf) = k^\gamma \psi f,$$
$$\psi(f+g) = \psi f + \psi g.$$

Proof. Let $k \in \mathbb{F}_q$, $f, g \in \mathcal{F}$, and $\psi : x \mapsto Ax^\gamma \in \mathrm{P\Gamma L}(2,q)$. Firstly, we have

$$(kf)^\gamma(x) = \left((kf)\left(x^{\frac{1}{\gamma}}\right)\right)^\gamma = \left(k \cdot f\left(x^{\frac{1}{\gamma}}\right)\right)^\gamma = k^\gamma f^\gamma(x),$$

so

$$\begin{aligned}(\psi(kf))(x) &= |A|^{-\frac{1}{2}}\left((bx+d)(kf)^\gamma\left(\frac{ax+c}{bx+d}\right) + bx(kf)^\gamma\left(\frac{a}{b}\right) + d(kf)^\gamma\left(\frac{c}{d}\right)\right)\\ &= k^\gamma |A|^{-\frac{1}{2}}\left((bx+d)f^\gamma\left(\frac{ax+c}{bx+d}\right) + bxf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right) = k^\gamma(\psi f)(x).\end{aligned}$$

Furthermore, we have

$$(f+g)^\gamma = \left((f+g)\left(x^{\frac{1}{\gamma}}\right)\right)^\gamma = \left(f\left(x^{\frac{1}{\gamma}}\right) + g\left(x^{\frac{1}{\gamma}}\right)\right)^\gamma = f^\gamma(x) + g^\gamma(x)$$

and thus

$$\begin{aligned}(\psi(g+f))(x) &= |A|^{-\frac{1}{2}}\left((bx+d)(f+g)^\gamma\left(\frac{ax+c}{bx+d}\right) + bx(f+g)^\gamma\left(\frac{a}{b}\right) + d(f+g)^\gamma\left(\frac{c}{d}\right)\right)\\ &= |A|^{-\frac{1}{2}}\left((bx+d)f^\gamma\left(\frac{ax+c}{bx+d}\right) + bxf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right)\\ &\quad + |A|^{-\frac{1}{2}}\left((bx+d)g^\gamma\left(\frac{ax+c}{bx+d}\right) + bxg^\gamma\left(\frac{a}{b}\right) + dg^\gamma\left(\frac{c}{d}\right)\right)\\ &= (\psi f)(x) + (\psi g)(x).\end{aligned}$$

□

2.2.14 Theorem. *Let $f \in \mathbb{F}_q[x]$ be an o-permutation and let $\psi : x \mapsto Ax^\gamma \in \mathrm{P\Gamma L}(2,q)$, where $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,q)$ and $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$. Then ψf is an o-permutation os-equivalent to f and $\varphi\mathcal{O}(f) = \mathcal{O}(\psi f)$, where $\varphi \in \mathrm{P\Gamma L}(3,q)$, $\varphi : x \mapsto \overline{\psi}_f x^\gamma$ with*

$$\overline{\psi}_f = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ a(\psi f)\left(\frac{c}{a}\right) & b(\psi f)\left(\frac{d}{b}\right) & |A|^{\frac{1}{2}} \end{pmatrix} \in \mathrm{GL}(3,q).$$

Proof. Our approach is as described in the remarks after Definition 2.2.1: We calculate $\varphi\mathcal{O}(f)$ explicitly and recover that ψf is an os-equivalent o-permutation. So let f, ψ, and φ be given as in the statement.

First, we note

$$\begin{aligned} a(\psi f)\left(\frac{c}{a}\right) &= a|A|^{-\frac{1}{2}}\left(\left(b\frac{c}{a}+d\right)\underbrace{f^\gamma\left(\frac{a\frac{c}{a}+c}{b\frac{c}{a}+d}\right)}_{=0} + b\frac{c}{a}f^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right) \\ &= |A|^{-\frac{1}{2}}\left(bcf^\gamma\left(\frac{a}{b}\right) + adf^\gamma\left(\frac{c}{d}\right)\right) \end{aligned} \tag{2.11}$$

and

$$\begin{aligned} b(\psi f)\left(\frac{d}{b}\right) &= b|A|^{-\frac{1}{2}}\left(\underbrace{\left(b\frac{d}{b}+d\right)}_{=0} f^\gamma\left(\frac{a\frac{d}{b}+c}{b\frac{d}{b}+d}\right) + b\frac{d}{b}f^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right) \\ &= |A|^{-\frac{1}{2}}\left(bdf^\gamma\left(\frac{a}{b}\right) + bdf^\gamma\left(\frac{c}{d}\right)\right). \end{aligned} \tag{2.12}$$

We start by calculating

$$\begin{aligned} \varphi\mathcal{O}(f) &= \left\{\overline{\psi}_f(1, s^\gamma, (f(s))^\gamma) : s \in \mathbb{F}_q\right\} \cup \{\overline{\psi}_f(0,1,0)\} \\ &= \left\{\overline{\psi}_f(1, s, f^\gamma(s)) : s \in \mathbb{F}_q\right\} \cup \{\overline{\psi}_f(0,1,0)\} \\ &= \left\{\left(a+bs, c+ds, a(\psi f)\left(\frac{c}{a}\right) + bs(\psi f)\left(\frac{d}{b}\right) + |A|^{\frac{1}{2}}f^\gamma(s)\right) : s \in \mathbb{F}_q\right\} \\ &\quad \cup \left\{\left(b, d, b(\psi f)\left(\frac{d}{b}\right)\right)\right\} \\ &= \left\{\left(1, \frac{c+ds}{a+bs}, \underbrace{\frac{a(\psi f)\left(\frac{c}{a}\right) + bs(\psi f)\left(\frac{d}{b}\right) + |A|^{\frac{1}{2}}f^\gamma(s)}{a+bs}}_{=:y(s)}\right) : s \in \mathbb{F}_q \setminus \left\{\frac{a}{b}\right\}\right\} \\ &\quad \cup \left\{\left(0, c+d\frac{a}{b}, \underbrace{a(\psi f)\left(\frac{c}{a}\right) + b\frac{a}{b}(\psi f)\left(\frac{d}{b}\right) + |A|^{\frac{1}{2}}f^\gamma\left(\frac{a}{b}\right)}_{=:T}\right), \left(b, d, b(\psi f)\left(\frac{d}{b}\right)\right)\right\}, \end{aligned}$$

where in the second step we have replaced s by $s^{\frac{1}{\gamma}}$ and in the fourth step we scaled

each point by $\frac{1}{a+bs}$, after swapping the problematic point out.

We handle T first by applying Formulas (2.11) and (2.12). We need $T = 0$, so the corresponding point is $(0, 1, 0)$, the only allowed point from the line at infinity.

$$\begin{aligned}
T &= |A|^{-\frac{1}{2}} \left(bcf^\gamma\left(\frac{a}{b}\right) + adf^\gamma\left(\frac{c}{d}\right)\right) + a|A|^{-\frac{1}{2}} \left(df^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right) + |A|^{\frac{1}{2}} f^\gamma\left(\frac{a}{b}\right) \\
&= |A|^{\frac{1}{2}} f^\gamma\left(\frac{a}{b}\right) + |A|^{-\frac{1}{2}} \left(bcf^\gamma\left(\frac{a}{b}\right) + adf^\gamma\left(\frac{a}{b}\right) + adf^\gamma\left(\frac{c}{d}\right) + adf^\gamma\left(\frac{c}{d}\right)\right) \\
&= |A|^{\frac{1}{2}} f^\gamma\left(\frac{a}{b}\right) + |A|^{-\frac{1}{2}} f^\gamma\left(\frac{a}{b}\right) \underbrace{(ad+bc)}_{=|A|} = 0.
\end{aligned}$$

To handle $y(s)$, we substitute $t = \frac{c+ds}{a+bs}$ for $s \in \mathbb{F}_q \setminus \left\{\frac{a}{b}\right\}$, or equivalently, $s = \frac{at+c}{bt+d}$ for $t \in \mathbb{F}_q \setminus \left\{\frac{b}{d}\right\}$. We first look into the denominator of $y(s)$, where we have substituted $s = \frac{at+c}{bt+d}$, by calculating

$$a + bs = a + b\frac{at+c}{bt+d} = \frac{abt + ad + abt + bc}{bt+d} = \frac{|A|}{bt+d}.$$

Thus we obtain

$$y(s) = \frac{\overbrace{(bt+d)a(\psi f)\left(\frac{c}{a}\right) + (at+c)b(\psi f)\left(\frac{d}{b}\right)}^{=:S} + (bt+d)|A|^{\frac{1}{2}} f^\gamma\left(\frac{at+c}{bt+d}\right)}{|A|}.$$

Further applications of Formulas (2.11) and (2.12) give

$$\begin{aligned}
S &= (bt+d)|A|^{-\frac{1}{2}} \left(bcf^\gamma\left(\frac{a}{b}\right) + adf^\gamma\left(\frac{c}{d}\right)\right) + (at+c)|A|^{-\frac{1}{2}} \left(bdf^\gamma\left(\frac{a}{b}\right) + bdf^\gamma\left(\frac{c}{d}\right)\right) \\
&= |A|^{-\frac{1}{2}} \Bigg(b^2ctf^\gamma\left(\frac{a}{b}\right) + bcdf^\gamma\left(\frac{a}{b}\right) + abdtf^\gamma\left(\frac{c}{d}\right) + ad^2f^\gamma\left(\frac{c}{d}\right) \\
&\qquad + abdtf^\gamma\left(\frac{a}{b}\right) + bcdf^\gamma\left(\frac{a}{b}\right) + abdtf^\gamma\left(\frac{c}{d}\right) + bcdf^\gamma\left(\frac{c}{d}\right)\Bigg) \\
&= |A|^{-\frac{1}{2}} \left(f^\gamma\left(\frac{a}{b}\right) \underbrace{(b^2ct + abdt)}_{=bt|A|} + f^\gamma\left(\frac{c}{d}\right) \underbrace{(ad^2 + bcd)}_{=d|A|}\right) \\
&= |A|^{\frac{1}{2}} \left(btf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right).
\end{aligned}$$

So, all in all, we get

$$\begin{aligned}
y(s) &= \frac{|A|^{\frac{1}{2}} \left(btf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right) + (bt+d)|A|^{\frac{1}{2}} f^\gamma\left(\frac{at+c}{bt+d}\right)}{|A|} \\
&= |A|^{-\frac{1}{2}} \left((bt+d)|A|^{\frac{1}{2}} f^\gamma\left(\frac{at+c}{bt+d}\right) + btf^\gamma\left(\frac{a}{b}\right) + df^\gamma\left(\frac{c}{d}\right)\right) = (\psi f)(t).
\end{aligned}$$

The yet remaining point $\left(b, d, b(\psi f)\left(\frac{d}{b}\right)\right)$ is, scaled by $\frac{1}{b}$, of the same form, so it follows that

$$\varphi\mathcal{O}(f) = \{(1, t, (\psi f)(t)) : t \in \mathbb{F}_q\} \cup \{(0, 1, 0)\} = \mathcal{O}(\psi f). \qquad \square$$

2.2.15 Example. Let $f \in \mathbb{F}_q[x]$ be an o-permutation and let $\bar{f}$ denote the reciprocal polynomial $\bar{f}(x) = xf(x^{q-2})$. Consider $\phi : x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x \in \mathrm{P\Gamma L}(2, q)$. Then we have

$$(\phi f)(x) = 1\left((1x+0)f\left(\frac{0x+1}{1x+0}\right) + 1xf\left(\frac{0}{1}\right) + 0f\left(\frac{1}{0}\right)\right) = xf(x^{q-2}) = \bar{f}(x),$$

so $\bar{f}$ is an o-permutation os-equivalent to f by Theorem 2.2.14. Using its notation we have

$$\overline{\phi} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so $\mathcal{O}(\phi f)$ is an oval attainable from $\mathcal{O}(f)$ by swapping the first and second coordinates.

Note that this is just Example 2.2.3 for ovals written in the language of the magic action. Importantly, Example 2.2.2 cannot be adapted in this context because the nucleus $(0, 0, 1)$ would be mapped to $(0, 1, 0)$, but Lemma 2.2.8 prohibits that. Consequently, the map inv taking permutations to their inverses is not an os-equivalence preserving map.

Our next goal is to prove a converse statement to Theorem 2.2.14, namely that for any two os-equivalent o-permutations there is an element $\psi \in \mathrm{P\Gamma L}(2, q)$ mapping one to the other, up to a scalar multiple. Equivalently, two os-equivalent o-permutations are in the same orbit, up to a scalar multiple, under the action of $\mathrm{P\Gamma L}(2, q)$.

The following lemma is the crucial observation that if the matrix of a projectivity mapping ovals corresponding to two os-equivalent o-permutations onto each other looks sufficiently enough like the matrix given in Theorem 2.2.14, the matrices coincide. Thus the work necessary for the converse statement reduces to ensuring that the matrices describing the projectivities are of the correct form. This is why everything is only up to a scalar multiple, we need this additional degree of freedom for this task.

2.2.16 Lemma. *Let f be an o-permutation of $\mathrm{PG}(2, q)$, $a, b, c, d \in \mathbb{F}_q$ with $ad + bc \neq 0$ and $z, y \in \mathbb{F}_q$. Let*

$$A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ z & y & (ad+bc)^{\frac{1}{2}} \end{pmatrix}$$

and $\psi : x \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} x \in \mathrm{PGL}(2, q)$. Then $A\mathcal{O}(f)$ is an oval of the form $\mathcal{O}(g)$ for an o-permutation $g \in \mathbb{F}_q[x]$ if and only if $z = a(\psi f)\left(\frac{a}{c}\right)$ and $y = b(\psi f)\left(\frac{d}{b}\right)$.

Proof. If $z = a(\psi f)\left(\frac{a}{c}\right)$ and $y = b(\psi f)\left(\frac{d}{b}\right)$, then by Theorem 2.2.14 we have

$$\overline{\psi}_f = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ a(\psi f)\left(\frac{c}{a}\right) & b(\psi f)\left(\frac{d}{b}\right) & (ad+bc)^{\frac{1}{2}} \end{pmatrix} = A$$

and $A\mathcal{O}(f) = \mathcal{O}(\psi f)$ and thus $g := \psi f$ is an o-permutation.

Now assume we have an o-permutation g such that $A\mathcal{O}(f) = \mathcal{O}(g)$. Let $\overline{\psi}_f$ be given as in Theorem 2.2.14 and consider

$$v := \overline{\psi}_f^{-1} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ and } w := \overline{\psi}_f^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Then we have $\langle v \rangle, \langle w \rangle \in \mathcal{O}(f)$ as well as

$$Av = \begin{pmatrix} 0 \\ 1 \\ \alpha \end{pmatrix} \text{ and } Aw = \begin{pmatrix} 1 \\ 0 \\ \beta \end{pmatrix}$$

for some $\alpha, \beta \in \mathbb{F}_q$ because the first two rows of A and $\overline{\psi}_f$ coincide. Now, $A\mathcal{O}(f)$ may only be an oval of the desired form $\mathcal{O}(g)$ if $\alpha = 0$ and $\beta = 0$. Indeed, $(0,1,0)$ is the only point of the line at infinity of $\mathcal{O}(g)$ and $(1,0,0)$ is the only point of $\mathcal{O}(g)$, where the second coordinate is 0. So we obtain the linear system

$$\begin{cases} v_1 z & + & v_2 y & = & v_3(ad+bc)^{\frac{1}{2}}, \\ w_1 z & + & w_2 y & = & w_3(ad+bc)^{\frac{1}{2}}. \end{cases}$$

One solution, $z = a(\psi f)\left(\frac{a}{c}\right)$ and $y = b(\psi f)\left(\frac{d}{b}\right)$, is already known by Theorem 2.2.14, so we only need to show the uniqueness of the solution. This, however, follows because $\langle v \rangle$ and $\langle w \rangle$ are different points of $\mathcal{O}(f)$. Indeed, if one of the points is $(0,1,0)$, assume $\langle v \rangle = (0,1,0)$, then $\langle w \rangle = (1,t,f(t))$ for some $t \in \mathbb{F}_q$, so $w_1 \neq 0$ and

$$\det \begin{pmatrix} 0 & v_2 \\ w_1 & w_2 \end{pmatrix} \neq 0.$$

If both points are not $(0,1,0)$, then $v_1, w_1 \neq 0$. In this case we have

$$\det \begin{pmatrix} v_1 & v_2 \\ w_1 & w_2 \end{pmatrix} = \frac{1}{v_1 w_1} \det \begin{pmatrix} 1 & \frac{v_2}{v_1} \\ 1 & \frac{w_2}{w_1} \end{pmatrix} \neq 0$$

because the second coordinate differs for two different points of $\mathcal{O}(f)$ if the first coordinate is fixed as 1. □

2.2.17 Theorem. *Let $f, g \in \mathbb{F}_q[x]$ be os-equivalent o-permutations. Then there is an element $k \in \mathbb{F}_q^*$ and a collineation $\psi \in \mathrm{P\Gamma L}(2,q)$ with $\psi f = k \cdot g$.*

Proof. First of all, $\mathcal{O}(g)$ and $\mathcal{O}(kg)$ are equivalent by the projectivity

$$x \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & k \end{pmatrix} x,$$

so f and kg are os-equivalent as well. Now, let $\eta \in \mathrm{P\Gamma L}(3,q)$, $\eta : x \mapsto Ax^\gamma$ be a collineation mapping $\mathcal{O}(f)$ to $\mathcal{O}(kg)$. Then $A\mathcal{O}(f^\gamma) = \mathcal{O}(kg)$ because

$$\begin{aligned} \eta\mathcal{O}(f) &= A\left\{(1, s^\gamma, (f(s))^\gamma) : s \in \mathbb{F}_q\right\} \cup A\left\{(0, 1^\gamma, 0)\right\} \\ &= A\{(1, s, f^\gamma(s)) : s \in \mathbb{F}_q\} \cup A\{(0,1,0)\} = A\mathcal{O}(f^\gamma). \end{aligned}$$

So if we have $\psi_2 \in \mathrm{PGL}(2,q), \psi_2 : x \mapsto Ax$ with $\overline{\psi_2}_{f^\gamma}\mathcal{O}(f^\gamma) = \mathcal{O}(kg)$, then $\psi : x \mapsto Ax^\gamma$ fulfills

$$\mathcal{O}(\psi f) = \mathcal{O}(\psi_2 f^\gamma) = \overline{\psi_2}_{f^\gamma}\mathcal{O}(f^\gamma) = \mathcal{O}(kg).$$

Thus it suffices assume that $\mathcal{O}(f)$ and $\mathcal{O}(kg)$ are equivalent via a projectivity φ with associated matrix A.

We can also rewrite our problem to $\mathcal{O}(kf)$ and $\mathcal{O}(g)$ being equivalent via a projectivity φ: If we have an element $\psi \in \mathrm{PGL}(2,q)$ with $\mathcal{O}(\psi(kf)) = \mathcal{O}(g)$, by Lemma 2.2.13 we also have

$$\mathcal{O}(\psi(kf)) = \mathcal{O}(k\psi f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & k \end{pmatrix} \mathcal{O}(\psi f) = \mathcal{O}(g),$$

so

$$\mathcal{O}(\psi f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{k} \end{pmatrix} \mathcal{O}(g) = \mathcal{O}\left(\frac{1}{k}g\right).$$

The plan is to find the matrix A and choose a value for k such that Lemma 2.2.16 is applicable. Since a projectivity is determined by its images on a frame of $\mathrm{PG}(2,q)$, we select a particularly easy frame and consider its image under φ. Let $u_i, v_i, s_i \in \mathbb{F}_q$ for $i = 1,2,3$ such that

$$\begin{array}{cccccc} & \mathcal{O}(kf) & \overset{\varphi}{\mapsto} & \mathcal{O}(g) & & \\ B_1 := & (1,0,0) & \mapsto & (u_1,u_2,u_3) & =: & C_1, \\ B_2 := & (0,1,0) & \mapsto & (v_1,v_2,v_3) & =: & C_2, \\ B_3 := & (0,0,1) & \mapsto & (0,0,1) & =: & C_3, \\ B_4 := & (1,1,1) & \mapsto & (s_1,s_2,s_3) & =: & C_4. \end{array}$$

We may select the representatives

$$b_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, \quad b_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad b_3 = \begin{pmatrix}0\\0\\kf(t)\end{pmatrix}, b_4 = \begin{pmatrix}1\\1\\kf(t)\end{pmatrix},$$
$$c_1 = a\begin{pmatrix}u_1\\u_2\\u_3\end{pmatrix}, c_2 = b\begin{pmatrix}v_1\\v_2\\v_3\end{pmatrix}, c_3 = c\begin{pmatrix}0\\0\\1\end{pmatrix}, \quad c_4 = \begin{pmatrix}s_1\\s_2\\s_3\end{pmatrix}$$

with $a, b, c \in \mathbb{F}_q^*$ such that $c_1 + c_2 + c_3 = c_4$ holds. This guarantees $\varphi B_4 = C_4$ as well. These constants exist, as C_1, C_2, C_3, and C_4 also constitute a frame, since they are four points of the oval $\mathcal{O}(g)$. Then we find that the matrix

$$A := \begin{pmatrix} a\,u_1 & b\,v_1 & 0 \\ a\,u_2 & b\,v_2 & 0 \\ a\,u_3 & b\,v_3 & \frac{c}{k\cdot f(t)} \end{pmatrix}$$

induces the projectivity φ. In particular, we have $A \in \mathrm{GL}(3, q)$. Set

$$D := \begin{pmatrix} a\,u_1 & b\,v_1 \\ a\,u_2 & b\,v_2 \end{pmatrix}.$$

Note that $0 \neq |A| = \frac{c}{k\cdot f(t)}|D|$ and thus $|D| \neq 0$, since $c \neq 0$. Now choose

$$k = \frac{c}{|D|^{\frac{1}{2}} f(t)} \text{ and } \psi : x \mapsto Dx \in \mathrm{PGL}(2, q).$$

Then the matrices A and $\overline{\psi}_{kf}$ from Theorem 2.2.14 coincide by Lemma 2.2.16, so we have

$$\mathcal{O}(g) = A\mathcal{O}(kf) = \overline{\psi}_{kf}\mathcal{O}(kf) = \mathcal{O}(\psi(kf))$$

and thus $g = \psi(kf)$. □

Note that in [35] the crucial argument involving Lemma 2.2.16 is employed only implicitly and is not given directly.

2.2.3 Application to Hyperovals

The goal of this subsection is to lift the results about the magic action to o-polynomials and to obtain a set of transformations explaining the equivalence classes of o-equivalence for o-polynomials in general and for o-monomials in particular.

We start by giving a set of generators of $\mathrm{P\Gamma L}(2, q)$ taken from [35], utilizing a subset of the elementary matrices. These generators correspond to a set of transformations of o-permutations, which can be seen as building blocks for all possible transformations of o-permutations, up to a scalar multiple.

The following lemma holds for arbitrary characteristic, so we state it for the general case, although we only need it for characteristic two.

2.2.18 Lemma (Generators of $\mathrm{P\Gamma L}(2,q)$)**.** *The following elements of* $\mathrm{P\Gamma L}(2,q)$ *generate* $\mathrm{P\Gamma L}(2,q)$*:*

- $\sigma_a : x \mapsto \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} x$, *where* $a \in \mathbb{F}_q^*$,
- $\tau_c : x \mapsto \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} x$, *where* $c \in \mathbb{F}_q$,
- $\phi : x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x$, *and*
- $\rho_\gamma : x \mapsto x^\gamma$, *where* $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$.

In fact, for $\psi \in \mathrm{P\Gamma L}(2,q)$, $\psi : x \mapsto Ax^\gamma$ *with* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *we have*

$$\psi = \begin{cases} \sigma_a\tau_c\sigma_{\frac{1}{d}}\rho_\gamma & : \ b = 0, \\ \sigma_b\tau_d\sigma_{\frac{1}{c}}\phi\rho_\gamma & : \ a = 0, \\ \sigma_b\tau_d\phi\tau_{\frac{-a}{|A|}}\sigma_{\frac{-|A|}{b}}\rho_\gamma & : \ a, b \neq 0. \end{cases}$$

Proof. Let $x \in \mathrm{PG}(2,q)$. We consider the case $b = 0$ first. Because $|A| = ad - bc \neq 0$, we have $d \neq 0$. Then

$$\begin{aligned} \sigma_a\tau_c\sigma_{\frac{1}{d}}\rho_\gamma x = \sigma_a\tau_c\sigma_{\frac{1}{d}}x^\gamma &= \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{d} & 0 \\ 0 & 1 \end{pmatrix} x^\gamma \\ &= \begin{pmatrix} a & 0 \\ c & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{d} & 0 \\ 0 & 1 \end{pmatrix} x^\gamma = \begin{pmatrix} \frac{a}{d} & 0 \\ \frac{c}{d} & 1 \end{pmatrix} x^\gamma = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} x^\gamma = \psi x. \end{aligned}$$

The case $a = 0$ can be dealt with using the first case, as we have

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}\rho_\gamma x = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x^\gamma = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix}\phi x^\gamma = \sigma_b\tau_d\sigma_{\frac{1}{c}}\phi x^\gamma.$$

If $a, b \neq 0$, then

$$\begin{aligned}
\sigma_b\tau_d\phi\tau_{\frac{-a}{|A|}}\sigma_{\frac{-|A|}{b}}\rho_\gamma x &= \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \frac{-a}{|A|} & 1 \end{pmatrix}\begin{pmatrix} \frac{-|A|}{b} & 0 \\ 0 & 1 \end{pmatrix} x^\gamma \\
&= \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{-|A|}{b} & 0 \\ \frac{a}{b} & 1 \end{pmatrix} x^\gamma \\
&= \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}\begin{pmatrix} \frac{a}{b} & 1 \\ \frac{-|A|}{b} & 0 \end{pmatrix} x^\gamma = \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{a}{b} & 1 \\ \frac{-|A|}{b} + \frac{ad}{b} & d \end{pmatrix} x^\gamma \\
&= \begin{pmatrix} a & b \\ \frac{-ad+bc+ad}{b} & d \end{pmatrix} x^\gamma = \psi x. \qquad \square
\end{aligned}$$

2.2.19 Corollary. *The following transformations on the set of o-permutations induced by the maps in Lemma 2.2.18 map o-permutations to os-equivalent o-permutations. Furthermore, up to a scalar, any two os-equivalent o-permutations arise from each other using the following transformations. For an o-permutation $f \in \mathbb{F}_q[x]$, define*

- $(\sigma_a f)(x) = a^{-\frac{1}{2}} f(ax)$, *where* $a \in \mathbb{F}_q^*$,
- $(\tau_c f)(x) = f(x+c) + f(c)$, *where* $c \in \mathbb{F}_q$,
- $(\phi f)(x) = xf(\frac{1}{x})$, *and*
- $(\rho_\gamma f)(x) = f^\gamma(x)$, *where* $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$.

Proof. The elements σ_a, τ_c, ϕ, and $\rho_\gamma \in \mathrm{P\Gamma L}(2,q)$ with $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, and $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$ act on $\mathcal{F}$ as described in Theorem 2.2.12 and map o-permutations to os-equivalent o-permutations, by Theorem 2.2.14. Moreover, given two os-equivalent o-permutations $f, g \in \mathbb{F}_q[x]$, Theorem 2.2.17 guarantees the existence of a scalar factor $k \in \mathbb{F}_q$ and an element $\psi \in \mathrm{P\Gamma L}(2,q)$ with $\psi f = kg$. Now Lemma 2.2.18 gives a representation of ψ as a product of the elements σ_a, τ_c, ϕ, and ρ_γ. Thus g arises, up to a scalar factor, from the transformations induced by σ_a, τ_c, ϕ, and ρ_γ. Finally, we calculate

$$\begin{aligned}
(\sigma_a f)(x) &= a^{-\frac{1}{2}}\left((0x+1)\, f\left(\frac{ax+1}{0x+1}\right) + 0xf\left(\frac{1}{0}\right) + 1f\left(\frac{0}{1}\right)\right) = a^{-\frac{1}{2}} f(ax), \\
(\tau_c f)(x) &= 1\left((0x+1)\, f\left(\frac{1x+c}{0x+1}\right) + 0xf\left(\frac{1}{0}\right) + 1f\left(\frac{c}{1}\right)\right) = f(x+c) + f(c), \\
(\phi f)(x) &= 1\left((1x+0)\, f\left(\frac{0x+1}{1x+0}\right) + 1xf\left(\frac{0}{x}\right) + 0f\left(\frac{1}{0}\right)\right) = xf\left(\frac{1}{x}\right), \\
(\rho_\gamma f)(x) &= \left((0x+1)\, f^\gamma\left(\frac{1x+0}{0x+1}\right) + 0xf^\gamma\left(\frac{1}{0}\right) + 1f^\gamma\left(\frac{0}{1}\right)\right) = f^\gamma(x). \qquad \square
\end{aligned}$$

Geometrically speaking, the different decompositions described in Lemma 2.2.18 translate to where the points $(1,0,0)$ and $(0,1,0)$ are mapped under the collineation given in Theorem 2.2.14: Either to an affine point $(1, s, f(s))$ or to $(0,1,0)$.

Our next goal is to lift these results to hyperovals and to the o-equivalence relation for o-polynomials. For that purpose we need to ensure that the transformations preserve the property of o-polynomials that $f(1) = 1$. Our argumentation follows [15, Chapter 5].

2.2.20 Definition (Modified Magic Action)**.** For $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, and an o-polynomial $f \in \mathbb{F}_q[x]$ define the transformations

$$(\tilde{\sigma}_a f)(x) = \frac{a^{\frac{1}{2}}}{f(a)}(\sigma_a f)(x) = \frac{1}{f(a)} f(ax),$$
$$(\tilde{\tau}_c f)(x) = \frac{1}{f(1+c)+f(c)}(\tau_c f)(x) = \frac{f(x+c)+f(c)}{f(1+c)+f(c)}.$$

2.2.21 Theorem. *Two o-polynomials $f, g \in \mathbb{F}_q[x]$ are o-equivalent if and only if they arise from each other using the transformations $\tilde{\sigma}_a$, $\tilde{\tau}_c$, ϕ, ρ_γ,* inv *with $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, and $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$.*

Proof. Firstly, let f be an o-polynomial. By Theorem 2.2.14 $\sigma_a f$, $\tau_c f$, ϕf, and $\rho_\gamma f$ are o-permutations os-equivalent to f. Then $\tilde{\sigma}_a f$ and $\tilde{\tau}_c f$ are o-permutations os-equivalent to f because they are scalar multiples of $\sigma_a f$ and $\tau_c f$. So $\tilde{\sigma}_a f$, $\tilde{\tau}_c f$, ϕf, and $\rho_\gamma f$ are o-polynomials because they all evaluate to 1 at 1. Furthermore, they are os-equivalent to f, so by Corollary 2.2.9 they are o-equivalent to f. Finally, Example 2.2.2 shows that $\mathrm{inv} f$ is an o-polynomial o-equivalent to f.

Now assume f and g are o-equivalent o-polynomials and let $\varphi \in \mathrm{P\Gamma L}(3,q)$ denote a collination with $\varphi\mathcal{H}(f) = \mathcal{H}(g)$. We proceed by distinguishing between the values of $\varphi^{-1}((0,0,1))$.

Case 1: Assume $\varphi^{-1}((0,0,1)) = (0,0,1)$. Then we have $\varphi\mathcal{O}(f) = \mathcal{O}(g)$, so f and g are os-equivalent o-permutations. Thus Corollary 2.2.19 and Lemma 2.2.18 yield the existence of $k \in \mathbb{F}_q$, $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$, and

$$\alpha_1, \ldots, \alpha_5 \in \{\mathrm{id}, \sigma_a, \tau_c, \phi : a \in \mathbb{F}_q^*, c \in \mathbb{F}_q\}$$

with

$$\alpha_5 \ldots \alpha_1 \rho_\gamma f = kg.$$

To replace α_i with its modified version $\tilde{\alpha}_i$, if necessary, we just multiply by an appropriate factor. Now, ϕ and id need no modification, that is, $\tilde{\phi} = \phi$ and $\tilde{\mathrm{id}} = \mathrm{id}$. Because the magic action is semilinear (Lemma 2.2.13), we may swap the new factors all the way to the left and obtain a single constant factor, which we denote by $b \in \mathbb{F}_q^*$. All in all, we have

$$kg = \alpha_5 \ldots \alpha_1 \rho_\gamma f = b\tilde{\alpha}_5 \ldots \tilde{\alpha}_1 \rho_\gamma f.$$

Because g and $\tilde{\alpha}_5 \ldots \tilde{\alpha}_1 \rho_\gamma f$ are o-polynomials, $k = b$ follows by evaluating at 1. Thus g arises from f through the transformations $\tilde{\sigma}_a, \tilde{\tau}_c, \phi$, and ρ_γ, where $a \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$.

Case 2: Assume $\varphi^{-1}((0,0,1)) = (0,1,0)$. We reduce this case to the first case utilizing inv. As described in Example 2.2.2, one collineation mapping $\mathcal{H}(f)$ to $\mathcal{H}(\mathrm{inv} f)$ swaps the second and the third coordinate. Because $\mathrm{inv}\,\mathrm{inv} f = f$, we have

$$\begin{array}{ccccc} \mathcal{H}(\mathrm{inv}f) & & \mathcal{H}(f) & & \mathcal{H}(g) \\ (0,0,1) & \mapsto & (0,1,0) & \mapsto & (0,0,1). \end{array}$$

Thus the first case yields that g arises from f using the transformations $\tilde{\sigma}_a$, $\tilde{\tau}_c$, ϕ, inv, and ρ_γ, where $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$ and $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$.

Case 3: Assume $\varphi^{-1}((0,0,1)) = (1,t,f(t))$, where $t \in \mathbb{F}_q$. We reduce this case to the second case along the following scheme.

$$\begin{array}{ccccccc} \mathcal{O}(\phi\tilde{\tau}_t f) = \mathcal{O}\left(\frac{1}{f(1+t)+f(t)}\phi\tau_t f\right) & \overset{\varphi_1}{\to} & \mathcal{O}(\phi\tau_t f) & \overset{\varphi_2}{\to} & \mathcal{O}(\tau_t f) & \overset{\varphi_3}{\to} & \mathcal{O}(f) \\ (0,1,0) & \mapsto & (0,1,0) & \mapsto & (1,0,0) & \mapsto & (1,t,f(t)) \end{array}$$

Note that $\frac{1}{f(1+t)+f(t)}\phi\tau_t f = \phi\tilde{\tau}_t f$, as the magic action is semilinear. For φ_1 we may use the projectivity induced by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & f(1+t)+f(t) \end{pmatrix}.$$

For φ_2 and φ_3 we may use, as indicated in Theorem 2.2.14, the projectivities induced by the matrices

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ f(t) & 0 & 1 \end{pmatrix}.$$

All in all, we have the following situation.

$$\begin{array}{ccccc} \mathcal{H}(\phi\tilde{\tau}_c f) & & \mathcal{H}(f) & & \mathcal{H}(g) \\ (0,1,0) & \mapsto & (1,t,f(t)) & \mapsto & (0,0,1), \end{array}$$

so the second case applies and g arises from f using the transformations $\tilde{\sigma}_a$, $\tilde{\tau}_c$, ϕ, inv, and ρ_γ, where $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, and $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$. □

Note that the reduction in the third case differs from what is described in [15], as their reduction does not define a collineation.

Our next goal, and highlight of this section, is to consider when o-monomials are o-equivalent. We need Lucas' Theorem about congruences of binomial coefficients, with an adapted proof taken from [20].

2.2.22 Lemma (Lucas' Theorem)**.** *Let $q = 2^n$ and $0 \le b \le a < q$. Then $\binom{a}{b} \equiv 1 \bmod 2$ if and only if a covers b.*

Proof. Write $a = \sum_{i\in I_a} 2^i$ and $b = \sum_{i\in I_b} 2^i$ with $I_a, I_b \subseteq \{0,\dots,n-1\}$. Then we have

$$\sum_{t=0}^{a}\binom{a}{t}x^t = (1+x)^a = (1+x)^{\sum_{i\in I_a} 2^i} = \prod_{i\in I_a}\left(1+x^{2^i}\right) = \sum_{I\subseteq I_a}\prod_{i\in I}x^{2^i} = \sum_{I\subseteq I_a}x^{\sum_{i\in I}2^i}$$

in $\mathbb{F}_q$, so $\binom{a}{b} \equiv 1 \mod 2$ if and only if $I_b \subseteq I_a$. □

The next lemma yields some information about how some transformations take effect on o-monomials. The lemma afterwards shows that some naturally appearing terms never vanish. This is a special case of the more general 2-to-1 characterization explored in Section 4.1.1.

2.2.23 Lemma. *Let $f(x) = \sum_{i=1}^{\frac{q-2}{2}} a_{2i}x^{2i}$ be an o-polynomial. Then the transformations σ_a, τ_c, and ρ_γ leave the degree of f invariant for $a \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, and $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$.*

Proof. Let d denote the degree of f. We calculate in ascending difficulty:

$$\begin{aligned}
(\rho_\gamma f)(x) &= \sum_{i=1}^{\frac{d}{2}} a_{2i}^\gamma x^{2i},\\
(\sigma_a f)(x) &= a^{-\frac{1}{2}} \sum_{i=1}^{\frac{d}{2}} a_{2i}(ax)^{2i} = \sum_{i=1}^{\frac{d}{2}} a_{2i}a^{2i-\frac{1}{2}}x^{2i},\\
(\tau_c f)(x) &= \sum_{i=1}^{\frac{d}{2}} a_{2i}(x+c)^{2i} + \sum_{i=1}^{\frac{d}{2}} a_{2i}c^{2i} = a_d(x+c)^d + \sum_{i=1}^{\frac{d-2}{2}} a_{2i}(x+c)^{2i} + \sum_{i=1}^{\frac{d}{2}} a_{2i}c^{2i}\\
&= a_d x^d + \sum_{k=0}^{d-1} \binom{d}{k} c^{d-k}x^l + \sum_{i=1}^{\frac{d-2}{2}} a_{2i}(x+c)^{2i} + \sum_{i=1}^{\frac{d}{2}} a_{2i}c^{2i}.
\end{aligned}$$

□

2.2.24 Lemma. *Let $f(x) = x^e$ be an o-monomial and $t \in \mathbb{F}_q \setminus \{0,1\}$. Then $t^e + t \neq 0$.*

Proof. If $t^e + t$ were equal to zero, we would either have $t = 0$ or $t^{e-1} = 1$. Because e is an o-exponent, $e-1$ also defines a permutation on $\mathbb{F}_q$, so $t^{e-1} = 1$ implies $t = 1$. □

2.2.25 Theorem (o-Equivalence for o-Monomials)**.** *Let $f(x) = x^e$ and $g(x) = x^j$ be o-monomials. Then f and g are o-equivalent if and only if*

$$j \in B_e := \left\{e, \frac{1}{e}, 1-e, \frac{1}{1-e}, \frac{e}{e-1}, \frac{e-1}{e}\right\}, \tag{2.13}$$

where the elements of B_e are meant to be taken modulo $q-1$.

Proof. For an o-monomial $f(x) = x^e$ we have the o-equivalent o-monomials $(\mathrm{inv} f)(x) = x^{\frac{1}{e}}$, $(\phi f)(x) = x^{1-e}$, $(\mathrm{inv}\,\phi f)(x) = x^{\frac{1}{1-e}}$, $(\phi\,\mathrm{inv} f)(x) = x^{1-\frac{1}{e}} = x^{\frac{e-1}{e}}$ and $(\mathrm{inv}\,\phi\,\mathrm{inv} f)(x) = x^{\frac{e}{e-1}}$. Thus B_e has to contain the elements $e, \frac{1}{e}, 1-e, \frac{1}{1-e}, \frac{e}{e-1}, \frac{e-1}{e}$.

Now the transformations inv and ϕ (and in particular their effect on o-polynomials) can be described using the projectivities given in the Examples 2.2.2 and 2.2.3. Since these projectivities correspond to permutations of the coordinates, there are only those six o-monomials attainable using inv and ϕ.

To show that the six elements of B_e are indeed the only o-exponents inducing o-monomials o-equivalent to f, we mimic the proof of Theorem 2.2.21. So, let $g(x) = x^j$

be an o-monomial o-equivalent to f and let $\varphi \in \mathrm{P\Gamma L}(3,q)$ denote a collineation mapping $\mathcal{H}(f)$ to $\mathcal{H}(g)$. Because

$$(\rho_\gamma f)(x) = x^e = f(x)$$

for any automorphism $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$, we may assume $\varphi \in \mathrm{PGL}(3,q)$. Now we distinguish again between the possible preimages of $(0,0,1)$ under φ.

Case 1: Assume $\varphi^{-1}((0,0,1)) = (0,0,1)$. Then $\varphi\mathcal{O}(f) = \mathcal{O}(g)$, so f and g are os-equivalent o-permutations. So by Theorem 2.2.17 we obtain $k \in \mathbb{F}_q^*$ and $\psi \in \mathrm{P\Gamma L}(2,q)$ with $\psi f = kg$. Because $\varphi \in \mathrm{PGL}(3,q)$, we may assume that $\psi \in \mathrm{PGL}(2,q)$ as well.

Now apply Lemma 2.2.18 to ψ. If $\psi = \sigma_a\tau_c\sigma_d$ with appropriate $a,d \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$, then

$$kg = \sigma_a\tau_c\sigma_d f$$

has the same degree as f by Lemma 2.2.23, so $\deg kg = j = e$ and $j \in B_e$.

If $\psi = \sigma_a\tau_c\sigma_d\phi$ with appropriate $a,d \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$, then ϕf has degree $1-e$, so

$$kg = \sigma_a\tau_c\sigma_d\phi f$$

has degree $1-e$ as well. Thus $j = 1-e \in B_e$.

Now suppose that $\psi = \sigma_b\tau_d\phi\tau_c\sigma_a$ with appropriate $b,a \in \mathbb{F}_q^*$, $c,d \in \mathbb{F}_q$, and

$$kg = \psi f = \sigma_b\tau_d\phi\tau_c\sigma_a f,$$

which we may rewrite as $\phi\tau_c\sigma_a f = k\tau_d\sigma_{b^{-1}}g$. Lemma 2.2.23 yields that applying σ_a to a monomial introduces only a factor. Renaming b^{-1} to b and collecting all the factors in a new constant $k \in \mathbb{F}_q$, we have

$$\begin{aligned}(\phi\tau_c f)(x) \overset{!}{=} k(\tau_d g)(x) = k\left((x+d)^j + d^j\right) = \sum_{i=1}^{j}\binom{j}{i}kd^{j-1}x^i \\ = x\left(\left(\frac{1}{x}+c\right)^e + c^e\right) = x\sum_{i=1}^{e}\binom{e}{i}c^{e-i}x^{-i} = \sum_{i=1}^{e}\binom{e}{i}c^{e-i}x^{q-i}.\end{aligned} \tag{2.14}$$

Let $e = \sum_{i\in I_e} 2^i$ and $j = \sum_{i\in I_j} 2^i$ be the binary expansions of e and j. Now, let $i = 2^{i_1}$ with $i_1 \in I_j$ minimal. Then by Lemma 2.2.22 $\binom{j}{i} = 1$, so on the right-hand side there is a term of degree i. So, if we are to have equality in Equation (2.14), there needs to be a term of degree i on the left-hand side too. That means $\binom{e}{q-i}$ needs to be 1. We have

$$q - i = \sum_{l=i_1}^{n-1} 2^l,$$

thus $i_1, \ldots, n-1$ are necessarily in I_e. On the other hand, let $i = 2^{i_2}$ with $i_2 \in I_e$ minimal. Then on the left-hand side there is a term of degree $q-i$, so for equality we

need a term of degree $q-i$ on the right-hand side as well. As

$$q-i=\sum_{l=i_2}^{n-1}2^l,$$

we therefore need $i_2,\dots,n-1\in I_j$. All in all, we have $i_1\le i_2\le i_1$, so $i_1=i_2$ and $e=j$ and thus $j\in B_e$.

Case 2: Let $A_1=(1,0,0)$, $A_2=(0,1,0)$ and $A_3=(0,0,1)$ and assume $\varphi(A_i)=A_k$ for a pair $(i,k)\in\{1,2,3\}^2$. Because S_3 acts transitively on $\{A_1,A_2,A_3\}$, we can find a composition ψ_1 of inv and ϕ transformations so that there is projectivity φ_1 mapping $\mathcal{H}(\psi_1 f)$ to $\mathcal{H}(f)$ with $\varphi_1(A_3)=A_i$ (cf. Examples 2.2.2 and 2.2.3). Similarly, we can find a composition ψ_2 of inv and ϕ, so that there is a projectivity φ_2 mapping $\mathcal{H}(g)$ to $\mathcal{H}(\psi_2 g)$ with $\varphi_2(A_k)=A_3$. Now $\psi_1 f$ and $\psi_2 g$ are o-monomials with exponents $\tilde{e}\in B_e$, respectively $\tilde{j}\in B_j$. Therefore, the first case, applied to $\mathcal{H}(\psi_1 f)$ and $\mathcal{H}(\psi_2 g)$, yields $\tilde{j}\in B_{\tilde{e}}=B_e$ and since $j\in B_{\tilde{j}}$ also $j\in B_e$.

Case 3: Assume $\varphi^{-1}(A_i)\notin\{A_1,A_2,A_3\}$ for $i=1,2,3$, that is, there are distinct $\tilde{s}_1,\tilde{s}_2,\tilde{s}_3\in\mathbb{F}_q^*$ with $\varphi^{-1}(A_i)=(1,\tilde{s}_i,\tilde{s}_i^e)$ for $i=1,2,3$. Then there are also distinct $\tilde{t}_1,\tilde{t}_2,\tilde{t}_3\in\mathbb{F}_q^*$ with $\varphi(A_i)=(1,\tilde{t}_i,\tilde{t}_i^j)$. Our aim is to show that this cannot actually happen.

The projectivity φ_1 induced by the matrix

$$\begin{pmatrix}1&0&0\\0&\tilde{s}_1&0\\0&0&\tilde{s}_1^e\end{pmatrix}\tag{2.15}$$

stabilizes $\mathcal{H}(f)$. Indeed,

$$\varphi_1\mathcal{H}(f)=\{(1,\tilde{s}_1 s,(\tilde{s}_1 s)^e):s\in\mathbb{F}_q\}\cup\{(0,1,0),(0,0,1)\}=\mathcal{H}(f).$$

Usefully, φ_1 maps $(1,1,1)$ to $(1,\tilde{s}_1,\tilde{s}_1^j)$. Analogously, let the projectivity φ_2 map $(1,1,1)$ to $(1,\tilde{t}_1,\tilde{t}_1^j)$, while stabilizing $\mathcal{H}(g)$. All in all, we obtain the following situation.

$$\begin{array}{ccccccc}
\mathcal{H}(f)&\overset{\varphi_1^{-1}}{\to}&\mathcal{H}(f)&\overset{\varphi}{\to}&\mathcal{H}(g)&\overset{\varphi_2^{-1}}{\to}&\mathcal{H}(g)\\
(1,0,0)&\mapsto&(1,0,0)&\mapsto&(1,\tilde{t}_1,\tilde{t}_1^j)&\mapsto&(1,1,1)\\
(0,1,0)&\mapsto&(0,1,0)&\mapsto&(1,\tilde{t}_2,\tilde{t}_2^j)&\mapsto&(1,r,r^j)\\
(0,0,1)&\mapsto&(0,0,1)&\mapsto&(1,\tilde{t}_3,\tilde{t}_3^j)&\mapsto&(1,u,u^j)\\
(1,1,1)&\mapsto&(1,\tilde{s}_1,\tilde{s}_1^e)&\mapsto&(1,0,0)&\mapsto&(1,0,0)\\
(1,v,v^e)&\mapsto&(1,\tilde{s}_2,\tilde{s}_2^e)&\mapsto&(0,1,0)&\mapsto&(0,1,0)\\
(1,w,w^e)&\mapsto&(1,\tilde{s}_3,\tilde{s}_3^e)&\mapsto&(0,0,1)&\mapsto&(0,0,1),
\end{array}$$

with distinct $v,w\in\mathbb{F}_q\setminus\{0,1\}$ and also distinct $r,u\in\mathbb{F}_q\setminus\{0,1\}$. Thus we may replace

φ by $\varphi_2^{-1}\varphi\varphi_1^{-1}$. Then φ is induced by the matrix

$$A = \begin{pmatrix} a & b & c \\ a & br & cu \\ a & br^j & cu^j \end{pmatrix},$$

with $a, b, c \in \mathbb{F}_q^*$ being appropriate constants. Because $\varphi((1,1,1)) = (1,0,0)$ and $\varphi((1,w,w^e)) = (0,0,1)$ we obtain the linear system

$$\begin{cases} a + br + cu = 0, \\ a + br^j + cu^j = 0, \\ a + bwr + cw^e u = 0, \\ a + bwr^j + cw^e u^j = 0 \end{cases} \tag{2.16}$$

for a, b, and c. The corresponding matrix

$$\begin{pmatrix} 1 & r & u \\ 1 & r^j & u^j \\ 1 & wr & w^e u \\ 1 & wr^j & w^e u^j \end{pmatrix}$$

has full rank: After adding the first row to the second and the third row to the fourth, adding the new second row, scaled with w, to the new fourth row yields

$$\begin{pmatrix} 1 & r & u \\ 0 & r + r^j & u + u^j \\ 1 & wr & w^e u \\ 0 & w(r + r^j) & w^e(u + u^j) \end{pmatrix} \sim \begin{pmatrix} 1 & r & u \\ 0 & r + r^j & u + u^j \\ 1 & wr & w^e u \\ 0 & 0 & (w + w^e)(u + u^j) \end{pmatrix}.$$

The entries $(w + w^e)(u + u^j)$ and $r + r^j$ are never zero, as indicated by Lemma 2.2.24. But then the linear system in (2.16) has only the trivial solution $a = b = c = 0$, which is a contradiction to φ being a projectivity. So this case is impossible. □

Remark. In essence, when obtaining the equivalent monomial hyperovals to a monomial hyperoval one needs to only consider permutations of the coordinates. So for o-monomials we have that o-equivalence is the same as equivalence under the group action of S_3 on the set of o-monomials, which we mentioned after Example 2.2.2. However, and this is the point making the proof difficult, this does not mean that a collineation φ taking $\mathcal{H}(x^e)$ to $\mathcal{H}(x^j)$ for e and j o-exponents necessarily maps the points $(1,0,0)$, $(0,1,0)$, and $(0,0,1)$ onto each other: If a collineation in the stabilizer maps one of those points to some affine point $(1,s,s^e)$ for $s \in \mathbb{F}_q^*$, then φ is not guaranteed to have this property. In Subsection 3.1.3 we survey the stabilizers of monomial hyperovals and one takeaway from there is that only translation hyperovals are affected by this. Indeed, the bulk of the work for the first case in the proof of Theorem 2.2.25 was concerned with a translation o-exponent being transformed into itself.

Another interesting aspect of Theorem 2.2.25 is its origin. The first implication is easy and a quick reference is [22, Theorem 8.4.3]. In the survey [42] about ovals Penttila

attributes this result to Segre and Bartocci [45, 46], but we have not been able to confirm this independently. The proof we have given is to the best of our knowledge new, as its central tool, the magic action, has had yet to be developed in the times of [45, 46].

To conclude this subsection, we aim to utilize the $\tilde{\sigma}_a$ transformation to gain insight about binomial o-polynomials. In fact, there are no known o-binomials. We follow [34] and start with a theorem that allows assuming that two coefficients of an o-polynomial coincide.

2.2.26 Theorem. *Let $f(x) = \sum_{k=1}^{\frac{q-2}{2}} a_{2k}x^{2k}$ be an o-polynomial, with a pair (i, j), $1 \leq i \neq j \leq \frac{q-1}{2}$, $i - j$ and $q - 1$ coprime, and $a_{2i}, a_{2j} \neq 0$. Then f is o-equivalent to an o-polynomial $g(x) = \sum_{k=1}^{\frac{q-2}{2}} b_{2k}x^{2k}$ with $b_{2i} = b_{2j}$ and $b_{2k} = 0$ if and only if $a_{2k} = 0$ for $1 \leq k \leq \frac{q-2}{2}$.*

Proof. Let $b \in \mathbb{F}_q^*$. Then $g := \tilde{\sigma}_b f$ is an o-polynomial o-equivalent to f by Theorem 2.2.14 and we have $g(x) = \frac{1}{f(b)} f(bx)$. Then

$$g(x) = \sum_{k=1}^{\frac{q-2}{2}} \underbrace{\left(\sum_{l=1}^{\frac{q-2}{2}} a_{2l} b^{2l} \right)^{-1} a_{2k} b^{2k}}_{=:c_k} x^{2k}.$$

Therefore, we have

$$\frac{c_{2i}}{c_{2j}} = \frac{a_{2i}b^{2i}}{a_{2j}b^{2j}} = b^{2(i-j)} \frac{a_{2i}}{a_{2j}}.$$

Because $\gcd(i-j, q-1) = 1$ and $x \mapsto x^2$ is bijective over $\mathbb{F}_q$, there is a choice for $b \in \mathbb{F}_q^*$ satisfying $\frac{c_{2i}}{c_{2j}} = 1$. □

2.2.27 Corollary. *If $f(x) = ax^{2i} + bx^{2j}$ is an o-binomial, then $\gcd(i - j, q - 1) \neq 1$. Also, there are no o-binomials if $q - 1$ is prime.*

Proof. Assume $f(x) = ax^{2i} + bx^{2j}$ is an o-binomial with $\gcd(i - j, q - 1) = 1$. Then Theorem 2.2.26 would yield an o-binomial $g(x) = \hat{a}x^{2i} + \hat{a}x^{2j}$. Then $g(1) = \hat{a} + \hat{a} = 0 = g(0)$, so g is not an o-polynomial.

If $q - 1$ is prime, then $\gcd(i - j, q - 1) = 1$, so there are no o-binomials then. □

3 Known Families and Formulas for o-Monomials

In this chapter we survey the known families of hyperovals. Because we continue our investigation into the o-monomials in Subsection 3.3, we reproduce proofs for the o-monomials in the first subsection. Theorem 2.2.25 indicates that for each o-monomial, there are at most six different o-equivalent o-monomials. Our aim is to give formulas for these six o-equivalent monomials for the known families. For this, assume q to be a power of 2 throughout this chapter.

When we speak of a hyperoval of a type, we mean a hyperoval equivalent to the hyperoval induced by the o-polynomial of said type, e.g. a Segre hyperoval is a hyperoval equivalent to the hyperoval induced by the Segre o-polynomial x^6.

Let us also mention that for small values of q the different families may intersect, but (often with arguments involving the stabilizer) it can be shown that the families are indeed distinct.

Before beginning, we turn to some classification results. A lot of effort has been put in this topic and for small fields it is possible to do an exhaustive search of the corresponding plane. For $q = 2^6 = 64$ this has been done in [48], where earlier endeavors for smaller fields are described as well. In short, all known hyperovals, except for one sporadic one, belong to one of infinite families described later. The sporadic one is due to Penttila and O'Keefe [31] in PG$(2, 32)$ and can be described via the o-polynomial

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

where $\omega \in \mathbb{F}_{32}$ is a primitive root of $\mathbb{F}_{32}$ satisfying $\omega^5 = \omega^2 + 1$.

Another kind of classification result concerns o-monomials and o-exponents of a specific form. In [14] Cherowitzo proves the only o-exponents of the form $2^i + 2^j$ are the ones already known. Similarly, o-exponents of the form $2^i + 2^j + 2^k$ are also classified in [49], as indicated in [8], although we were not able to check this independently.

Further, there are also results about the classification of o-polynomials with low degree. Concerning them we have the following theorem.

3.0.1 Theorem ([8, Theorem 1.2])**.** *Let $f \in \mathbb{F}_q[x]$ be an o-polynomial of degree less than $\frac{1}{2}q^{\frac{1}{4}}$. Then f is o-equivalent to either x^6 or x^{2^k} with $k \in \mathbb{N}$, that is, $\mathcal{H}(f)$ is either a Segre hyperoval or a translation hyperoval.*

The special case of f being an o-monomial had been proved earlier in [21] and later with a different proof also in [50]. In the preprint [17] Theorem 3.0.1 is strengthened to also cover polynomials with degree up to $q^{\frac{1}{4}}$ using an alternative approach.

An interesting corollary is that the only exceptional o-polynomials, that is, polynomials that are o-polynomials for infinitely many planes, are x^6 and x^{2^k} with $k \in \mathbb{N}$.

Finally, we mention that there are other surveys covering the known families in a more condensed way. See, for example, [2, Section 15].

3.1 Monomial Families

Monomial hyperovals are interesting for a number of reasons, the simplicity of the corresponding o-polynomials being only the first. Their stabilizers are well understood and are surveyed in the last subsection. A second interesting application arises in Chapter 4, where we investigate the connection between o-monomials and 2-to-1 binomials. A long standing conjecture by Glynn [18] states that there are no further o-monomials other than the ones described in this section. The conjecture is supported by a computer search employing Theorem 2.1.19 up to $n = 30$ by Glynn in [19].

3.1.1 Regular, Translation and Segre Hyperovals

We begin with a simple condition based on Theorem 2.1.15 for a monomial to be an o-monomial.

3.1.1 Theorem. *The monomial $f(x) = x^e \in \mathbb{F}_q[x]$ is an o-polynomial if and only if*

(i) $\gcd(e, q-1) = 1$, $\gcd(e-1, q-1) = 1$, *and*

(ii) $((x+1)^e + 1)\, x^{q-2}$ *is a permutation polynomial of* $\mathbb{F}_q$.

Proof. For monomials $f(x) = x^e$ we always have $f(0) = 0$ and $f(1) = 1$. The condition $\gcd(e, q-1) = 1$ is equivalent to f being a permutation polynomial and $\gcd(e-1, q-1) = 1$ is equivalent to

$$f_0(x) = ((x+0)^e + 0^e)\, x^{q-2} = x^{e-1}$$

being a permutation polynomial. Finally, for $a \in \mathbb{F}_q^*$ we have

$$\begin{aligned} f_a(x) = ((x+a)^e + a^e)x^{q-2} &= \left(a^e \left(\frac{x}{a} + 1\right)^e + a^e\right) x^{q-2} \\ &= a^e \left(\left(\frac{x}{a} + 1\right)^e + 1\right) x^{q-2} = a^{e+q-2} \left(\left(\frac{x}{a} + 1\right)^e + 1\right) \left(\frac{x}{a}\right)^{q-2} \\ &= a^{e-1} \left(\left(\frac{x}{a} + 1\right)^e + 1\right) \left(\frac{x}{a}\right)^{q-2} = a^{e-1} f_1\left(\frac{x}{a}\right), \end{aligned}$$

so f_a is a permutation polynomial if and only if f_1 is. □

The first and easiest hyperoval is the regular hyperoval, which we have already seen in Example 2.1.16. Its first description appeared in [4, Section 5.3].

3.1.2 Theorem (Regular Hyperoval)**.** *For q even, the polynomial $f(x) = x^2 \in \mathbb{F}_q[x]$ is an o-polynomial.*

This hyperoval $\mathcal{H}(x^2)$ arises from the conic $\{(x,y,z) \in \mathrm{PG}(2,q) : xz = y^2\}$ by adding its nucleus. Since in odd characteristic every oval is a conic by Segre's Theorem and other families of hyperovals do not arise from conics, hyperovals of this family are called regular. See Subsection 4.2.3 for conics and Segre's Theorem.

The next family is the family of translation hyperovals, which also contains the regular hyperovals. Their discovery is due to Segre [44]. We have not been able to check this specific reference, but it is widely attributed to him (see, for example, [2, 21]).

3.1.3 Theorem (Translation Hyperoval)**.** *For $q = 2^n$ and $i \in \mathbb{N}$ with $\gcd(n,i) = 1$, the monomial $f(x) = x^{2^i} \in \mathbb{F}_q[x]$ is an o-polynomial.*

Proof. We apply Theorem 3.1.1. Firstly, $e = 2^i$ is only divisible by powers of 2, while $q-1$ is not divisible by 2 at all. Hence $\gcd(e, q-1) = 1$. Further, we have

$$\gcd(2^i - 1, 2^n - 1) = \gcd(i,n) = 1.$$

Finally,

$$f_1(x) = ((x+1)^e + 1)x^{q-2} = x^{e-1},$$

so f_1 is a permutation polynomial too. □

These o-polynomials f are precisely the ones inducing additive maps on $\mathbb{F}_q$ (see [22, Section 8.5] or [36]), or equivalently, they are precisely those o-polynomials remaining fixed under the transformations τ_c and $\tilde{\tau}_c$ with $c \in \mathbb{F}_q$. Hence the corresponding hyperoval $\mathcal{H}(f)$ is stabilized by the projectivity $\varphi : \mathrm{PG}(2,q) \to \mathrm{PG}(2,q)$ with $(x,y,z) \mapsto (x, y+cx, z+f(c)x)$ induced by the matrix

$$\overline{\tau_{cf}} = \begin{pmatrix} 1 & 0 & 0 \\ c & 1 & 0 \\ f(c) & 0 & 1 \end{pmatrix}.$$

When restricting φ to the affine plane $\{(1,s,t) : s,t \in \mathbb{F}_q\}$ embedded in $\mathrm{PG}(2,q)$, one obtains a translation, since

$$\begin{pmatrix} 1 & 0 & 0 \\ c & 1 & 0 \\ f(c) & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ s \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ c \\ f(c) \end{pmatrix} + \begin{pmatrix} 1 \\ s \\ t \end{pmatrix}$$

and for this reason the hyperovals are called translation hyperovals. Note that sometimes (a generalization) of this property is used to define translation hyperovals, see for example [42].

Next we have the Segre-Bartocci hyperovals, introduced in [46].

3.1.4 Theorem (Segre o-Monomials)**.** *For $q = 2^n$ with $n \geq 3$ odd, the monomial $f(x) = x^6 \in \mathbb{F}_q[x]$ is an o-polynomial.*

An easy way to prove this is to utilize a connection to the Dickson polynomials, for which we refer to [23, Section 2.4]. They make up classical examples of permutation polynomials, as it is well understood under which conditions they induce permutations.

3.1.5 Definition. Let q be a prime power. Let $a \in \mathbb{F}_q$ and $k \in \mathbb{N}$. The polynomial

$$D_k(x,a) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-i} \binom{k-i}{i} (-1)^i a^i X^{k-2i} \in \mathbb{F}_q[x]$$

is called the kth *Dickson polynomial* with parameter a.

3.1.6 Theorem ([23, Theorem 2.24])**.** *Let q be a prime power. Let $a \in \mathbb{F}_q^*$ and $k \in \mathbb{N}$. Then the Dickson polynomial $D_k(x,a) \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if* $\gcd(k, q^2-1) = 1$.

Proof (of the Segre o-Monomials). We have $\gcd(6, 2^n-1) = \gcd(3, 2^n-1)$, as 2 is not a divisor of $2^n - 1$. Further, letting $n = 2l+1$ with $l \in \mathbb{N}$,

$$2^{2l+1} - 1 \equiv 2 \cdot 4^l - 1 \equiv 2 \cdot 1 - 1 = 1 \mod 3$$

and thus $\gcd(3, q-1) = 1$.

Similarly, 5 is not a divisor of $2^n - 1$, as

$$2^{2l+1} - 1 = 2 \cdot 4^l - 1 \equiv \pm 2 - 1 \neq 0 \mod 5,$$

so $\gcd(5, q-1) = 1$.

Lastly, we need

$$f_1(x) = ((x+1)^6 + 1)x^{q-2} = (x^6 + x^4 + x^2)x^{q-2} = x^5 + x^3 + x$$

to be a permutation polynomial. To this end, notice $D_5(x,1) = x^5 + x^3 + x$. By Theorem 3.1.6 the Dickson polynomial $D_5(x,1)$ is a permutation polynomial if and only if $\gcd(5, q^2-1) = 1$. But we have

$$q^2 - 1 = 2^{4l+2} - 1 = 4 \cdot 16^l - 1 \equiv 4 - 1 = 3 \mod 5. \qquad \square$$

3.1.2 Glynn Hyperovals

In this subsection we treat the Glynn_1 and Glynn_2 hyperovals, originally found by Glynn in 1985 [18], using a computer search to find monomial hyperovals. Although Glynn considered the Glynn_2 o-exponent first, it is the more complicated one and is thus now known as the Glynn_2 o-exponent.

The long proofs we give are the ones given by Glynn himself. As far as we know, there is only one other known direct proof due to Cherowitzo [10, Appendix], which itself is also very long and requires some additional machinery.

3.1.7 Definition. Let $q = 2^n$ with n odd and let $\sigma = 2^{\frac{n+1}{2}}$, that is, σ is the unique least positive residue $\bmod q-1$ satisfying

$$\sigma^2 \equiv 2 \mod q-1.$$

Let

$$\gamma = \begin{cases} 2^{\frac{3n+1}{4}} & : n \equiv 1 \mod 4, \\ 2^{\frac{n+1}{4}} & : n \equiv 3 \mod 4, \end{cases}$$

that is, γ is the unique least positive residue satisfying

$$\gamma^4 \equiv 2 \mod q-1.$$

3.1.8 Theorem (Glynn_1 Hyperovals)**.** *Let $q = 2^n$ with n odd and let $e = 3\sigma + 4 = 3 \cdot 2^{\frac{n+1}{2}} + 4$. Then the polynomial $f(x) = x^e \in \mathbb{F}_q[x]$ is an o-polynomial.*

The proof is of geometric nature: Instead of utilizing Theorem 3.1.1 (as usual), we show that every line of $\text{PG}(2,q)$ meets the Glynn_1 hyperoval in at most two points. The crucial part will be the lines that do not contain the points $(0,1,0)$ or $(0,0,1)$, which we handle in the following lemma.

3.1.9 Lemma. *Let $q = 2^n$ with n odd. Then, for all $m \in \mathbb{F}_q$, the equation*

$$y^{\sigma+2} + y^3 + m = 0 \tag{3.1}$$

over $\mathbb{F}_q$ has at most two solutions.

Proof. Suppose Equation (3.1) has at least two solutions in $\mathbb{F}_q$. The idea is to show that for any two distinct solutions $\alpha, \beta \in \mathbb{F}_q$ the trace equality $\text{Tr}(\alpha+\beta) = 1$ holds. Indeed, if we had three distinct solutions $\alpha, \beta, \delta \in \mathbb{F}_q$, we would have

$$\begin{aligned} 1 &= \text{Tr}(\alpha+\beta) + \text{Tr}(\alpha+\delta) + \text{Tr}(\beta+\delta) \\ &= \text{Tr}(\alpha+\alpha+\beta+\beta+\delta+\delta) = 0. \end{aligned}$$

So, let $\alpha, \beta \in \mathbb{F}_q$ be distinct solutions of Equation (3.1) for the remainder of the proof.

Step 1: Reduce (3.1) to a linear equation holding for $y \in \{\alpha, \beta\}$. Firstly, we have

$$(y+\alpha)(y+\beta) = y^2 + (\alpha+\beta)y + \alpha\beta = 0$$

for $y \in \{\alpha, \beta\}$, so

$$y^2 = (\alpha+\beta)y + \alpha\beta. \tag{3.2}$$

Secondly, by choosing $a, b \in \mathbb{F}_q$ to be the solutions of the linear system

$$\begin{cases} \alpha a + b = \alpha^\sigma, \\ \beta a + b = \beta^\sigma, \end{cases}$$

we have that α and β are solutions of

$$y^\sigma + ay + b = 0. \tag{3.3}$$

Note that $a \neq 0$, as that would imply a unique solution of Equation (3.3). Raising (3.3) to the σth power yields

$$y^2 + a^\sigma y^\sigma + b^\sigma = 0,$$

since $\sigma^2 \equiv 2 \mod q-1$. Applying (3.3) again, one gets

$$y^2 + a^\sigma(ay + b) + b^\sigma = 0,$$

so

$$y^2 + a^{\sigma+1}y + a^\sigma b + b^\sigma = 0. \tag{3.4}$$

Since Equation (3.2) and (3.4) are two quadratic equations with agreeing solutions, we must have $\alpha + \beta = a^{\sigma+1}$ and $\alpha\beta = a^\sigma b + b^\sigma$. Equation (3.2) now takes the form

$$y^2 = a^{\sigma+1}y + a^\sigma b + b^\sigma. \tag{3.5}$$

We use Equation (3.3) and (3.5) to reduce Equation (3.1), where we hide the constant terms in a (from line to line changing) constant $C \in \mathbb{F}_q$.

$$\begin{aligned} y^{\sigma+2} + y^3 + m &= y^2\left(y^\sigma + y\right) + m = \left(a^{\sigma+1}y + a^\sigma b + b^\sigma\right)(ay + b + y) + m \\ &= \left(a^{\sigma+1}y + a^\sigma b + b^\sigma\right)((a+1)y + b) + m \\ &= (a+1)a^{\sigma+1}y^2 + \left(a^{\sigma+1}b + a^\sigma b(a+1) + b^\sigma(a+1)\right)y + C \\ &= (a+1)a^{\sigma+1}\left(a^{\sigma+1}y + a^\sigma b + b^\sigma\right) + \left(a^\sigma b + b^\sigma(a+1)\right)y + C \\ &= \left((a+1)a^{2\sigma+2} + a^\sigma b + (a+1)b^\sigma\right)y + C. \end{aligned}$$

Step 2: Obtain $\mathrm{Tr}(\alpha + \beta) = 1$. Since we have a linear equation with two distinct roots, each coefficient has to be zero. In particular, we have

$$(a+1)a^{2\sigma+2} = a^\sigma b + (a+1)b^\sigma. \tag{3.6}$$

As $a \neq 0$, we may multiply (3.6) by $(a+1)^{\sigma+1}a^{-2\sigma-2}$ to obtain

$$\begin{aligned} (a+1)^{\sigma+2} &= a^{-\sigma-2}(a+1)^{\sigma+1}b + a^{-2\sigma-2}(a+1)^{\sigma+2}b^\sigma \\ &= a^{-\sigma-2}(a+1)^{\sigma+1}b + \left(a^{-\sigma-2}(a+1)^{\sigma+1}b\right)^\sigma \end{aligned}$$

using $\sigma^2 \equiv 2 \mod q-1$ again. Therefore, $\mathrm{Tr}\left((a+1)^{\sigma+2}\right) = 0$. As

$$(a+1)^{\sigma+2} = \left(a^\sigma + 1\right)\left(a^2 + 1\right) = a^{\sigma+2} + a^\sigma + a^2 + 1$$

and $\mathrm{Tr}(1) = 1$ (since n is odd) and $\mathrm{Tr}(a^\sigma + a^2) = 0$ we may conclude $\mathrm{Tr}\left(a^{\sigma+2}\right) = 1$. Finally, we have

$$\left(a^{\sigma+2}\right)^{\frac{\sigma}{2}} = a^{1+\sigma} = \alpha + \beta$$

and therefore $\mathrm{Tr}(\alpha + \beta) = 1$. □

Proof (of the Glynn$_1$ hyperovals). By Theorem 2.2.25 we may prove that $\tilde{e} = \frac{e}{e-1}$ (taken mod $q-1$) defines an o-monomial instead. Using the formulas we derive in Theorem 3.3.2, we obtain

$$\tilde{e} = \begin{cases} \frac{2\cdot 2^n + 2^{\frac{n+1}{2}}}{3} & n \equiv 1 \mod 4, \\ \frac{2^{\frac{n+1}{2}}+2}{3} & n \equiv 3 \mod 4 \end{cases} \equiv \frac{\sigma+2}{3} \mod q-1$$

and that $x^{\tilde{e}}$ is a permutation polynomial of $\mathbb{F}_q$. Also note that the derivations of the formulas in Theorem 3.3.2 do not depend on e actually being an o-exponent!

Firstly, only the points $(0,1,0)$ and $(0,0,1)$ are on $l_\infty = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle^\perp$. On the lines $l_a = \left\langle \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix} \right\rangle^\perp$ for $a \in \mathbb{F}_q$ we have $(0,0,1)$ and one other point from $\mathcal{H}(x^{\tilde{e}})$, since $x \mapsto x$ is a permutation of $\mathbb{F}_q$. Similarly, on the lines $l_{a,0} = \left\langle \begin{pmatrix} a \\ 0 \\ 1 \end{pmatrix} \right\rangle^\perp$ we have $(0,1,0)$ and one other point from $\mathcal{H}(x^{\tilde{e}})$, since $x \mapsto x^{\tilde{e}}$ is a permutation of $\mathbb{F}_q$.

So, we only need to handle the lines $l_{a,b}$ with $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. A point $(1, x, x^{\tilde{e}}) \in \mathcal{H}(x^{\tilde{e}})$ with $x \in \mathbb{F}_q$ is on $l_{a,b} = \left\langle \begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \right\rangle^\perp$ if and only if

$$a + bx + x^{\tilde{e}} = 0. \tag{3.7}$$

As n is odd, we may substitute $x = b^{3(\sigma+1)}y^3$ in (3.7) to obtain

$$\begin{aligned} 0 &= \left(b^{3(\sigma+1)}y^3\right)^{\frac{\sigma+2}{3}} + b^{3(\sigma+1)+1}y^3 + a, \\ &= b^{\sigma^2+3\sigma+2}y^{\sigma+2} + b^{3\sigma+4}y^3 + a \end{aligned}$$

and setting $m = \frac{a}{b^{3\sigma+4}}$ thus

$$y^{\sigma+2} + y^3 + m = 0. \tag{3.8}$$

By Lemma 3.1.9 Equation (3.8) has at most two solutions. □

Remark. Interestingly, now that we know that $e = 3\sigma + 4$ is an o-exponent, we can sharpen the statement of Lemma 3.1.9 a bit: By Lemma 2.1.3 we know that each line meeting $\mathcal{H}(x^{\tilde{e}})$ contains exactly two points of the hyperoval. Therefore, Equation (3.1) has exactly two or zero solutions, depending on the corresponding line of $\mathrm{PG}(2,q)$.

Next, we turn to the Glynn$_2$ hyperovals.

3.1.10 Theorem (Glynn$_2$ Hyperovals)**.** *Let $q = 2^n$ with n odd and let*

$$e = \gamma + \sigma = \begin{cases} 2^{\frac{3n+1}{4}} + 2^{\frac{n+1}{2}} & : n \equiv 1 \mod 4, \\ 2^{\frac{n+1}{4}} + 2^{\frac{n+1}{2}} & : n \equiv 3 \mod 4. \end{cases}$$

Then $f(x) = x^e \in \mathbb{F}_q[x]$ is an o-polynomial.

The crucial part of the proof is establishing that $f_1(x)$ is an o-polynomial and the key ingredient is the following generalization to the classical trace condition for the solvability of quadratic equations, given by Glynn [18, Result 5].

3.1.11 Theorem. *Let $n, k \in \mathbb{N}$ with $\gcd(n, k) = 1$, $a, b \in \mathbb{F}_{2^n}$ and let $g \in \mathbb{N}$ with $g \equiv (2^k - 1)^{-1} \mod 2^n - 1$. Then the equation*

$$x^{2^k} + ax + b = 0 \tag{3.9}$$

over $\mathbb{F}_{2^n}$ has either

- *one unique solution if $a = 0$,*
- *no solution if $a \neq 0$ and $\mathrm{Tr}\left(\frac{b}{a^{g+1}}\right) = 1$, or*
- *exactly two solutions if $a \neq 0$ and $\mathrm{Tr}\left(\frac{b}{a^{g+1}}\right) = 0$.*

Proof. For our purposes the weaker statement that Equation (3.9) having a solution implies $\mathrm{Tr}\left(\frac{b}{a^{g+1}}\right) = 0$ when $a \neq 0$ suffices, so we only prove that. Assume that $a \neq 0$.

We have

$$2^k \cdot g = (2^k - 1)g + g \equiv 1 + g \mod 2^n - 1,$$

so dividing Equation (3.9) by a^{g+1} yields

$$\left(\frac{x}{a^g}\right)^{2^k} + \frac{x}{a^g} + \frac{b}{a^{g+1}} = 0.$$

Suppose there is an element $t \in \mathbb{F}_q$ satisfying $t^{2^k} + t + \frac{b}{a^{g+1}} = 0$. Then

$$0 = \mathrm{Tr}\left(t^{2^k} + t + \frac{b}{a^{g+1}}\right) = \mathrm{Tr}\left(t^{2^k} + t\right) + \mathrm{Tr}\left(\frac{b}{a^{g+1}}\right) = \mathrm{Tr}\left(\frac{b}{a^{g+1}}\right). \qquad \square$$

Now, the general strategy is as follows. We assume two elements $s, t \in \mathbb{F}_q$ get mapped to the same element under f_1. Using this relation, we derive an equation of the type $x^\gamma + Ax + B = 0$, which has at least one solution coming from s and t. We can then infer by Theorem 3.1.11 that some trace equation holds and use the specific properties of σ and γ to show that this trace equation, in fact, cannot hold. The details are highly technical and we begin with a lemma that helps to establish the equation.

3.1.12 Notation. Let $q = 2^n$ with n odd and let $s, t \in \mathbb{F}_q^*$ be two distinct elements. Define

1. $S := S(s,t) := s + t$,
2. $T := T(s,t) := st$,
3. $Y := Y(s,t) := TS^{-2} = \frac{st}{s^2+t^2}$,
4. $\beta_a := \beta_a(s,t) := (s^a + t^a)YS^{-a} = \frac{s^a+t^a}{(s+t)^a}\frac{st}{s^2+t^2}$ for $a \in \mathbb{N}$, and
5. $K := K(s,t) := \beta_{\gamma-1}$.

3.1.13 Lemma. *Let $q = 2^n$ with n odd and let $s, t \in \mathbb{F}_q^*$ be two distinct elements. Then we have*

1. $\beta_{\sigma-1} = K + K^\gamma$,
2. $\beta_{\sigma+\gamma-1} = K + K^2 + K^\gamma + K^{\gamma+1} + K^\sigma + K^{\gamma\sigma}$, *and*
3. $\mathrm{Tr}(K) = 0$.

Proof. This proof is done mostly by direct computations. We begin with some auxiliary statements. Firstly, we have $\beta_0 = (s^0 + t^0)YS^{-2} = 0$ and for $m \in \mathbb{N}$ we have

$$\beta_{2^m} = \frac{s^{2^m} + t^{2^m}}{(s+t)^{2^m}} Y = Y.$$

Furthermore, for any $a \in \mathbb{N}$ and $l \in \{1, \ldots, a\}$ we have

$$\beta_a = Y^{-1}\beta_l\beta_{a-l+1} + \beta_{l-1}\beta_{a-l}, \tag{3.10}$$

proven by direct computation, denoting the right-hand side by L:

$$\begin{aligned}
L &= Y^{-1}\left(s^l + t^l\right) YS^{-l}\left(s^{a-l+1} + t^{a-l+1}\right) YS^{-a+l-1} \\
&\quad + \left(s^{l-1} + t^{l-1}\right) YS^{-l+1}\left(s^{a-l} + t^{a-l}\right) YS^{-a+l} \\
&= \left(s^l + t^l\right)\left(s^{a-l+1} + t^{a-l+1}\right) YS^{-a-1} + \left(s^{l-1} + t^{l-1}\right)\left(s^{a-l} + t^{a-l}\right) Y^2S^{-a+1} \\
&= YS^{-a-1}\left(s^{a+1} + s^l t^{a-l+1} + t^l s^{a-l+1} + t^{a+1}\right) \\
&\quad + YS^2 \cdot YS^{-a-1}\left(s^{a-1} + s^{l-1}t^{a-l} + s^{a-l}t^{l-1} + t^{a-1}\right).
\end{aligned}$$

By recalling $YS^2 = T = st$ we arrive at

$$\begin{aligned}
L &= YS^{-a-1}\left(s^{a+1} + \underline{s^l t^{a-l+1}} + \underline{t^l s^{a-l+1}} + t^{a+1} + ts^a + \underline{s^l t^{a-l+1}} + \underline{s^{a-l+1}t^l} + st^a\right) \\
&= YS^{-a-1}\left(s^{a+1} + t^{a+1} + ts^a + st^a\right) = YS^{-a-1}\left((s+t)\left(s^a + t^a\right)\right) \\
&= YS^{-a}\left(s^a + t^a\right) = \beta_a.
\end{aligned}$$

Next, for $m \in \mathbb{N}_0$ we have

$$\beta_{2^m-1} = \sum_{i=0}^{m-1} Y^{2^i}, \tag{3.11}$$

proven via induction. For $m = 0$ there is nothing to do, as $\beta_0 = 0$. For the induction step $m - 1 \mapsto m$ we utilize Formula (3.10) using $a = 2^m - 1$ and $l = 2^{m-1}$. We then obtain

$$\begin{aligned}\beta_{2^m-1} &= Y^{-1}\beta_{2^{m-1}}\beta_{2^{m-1}} + \beta_{2^{m-1}-1}\beta_{2^{m-1}-1} \\ &= Y^{-1}Y^2 + \left(\sum_{i=0}^{m-2} Y^{2^i}\right)^2 = \sum_{i=0}^{m-1} Y^{2^i}.\end{aligned}$$

In particular, we have $\beta_{q-1} = \mathrm{Tr}(Y)$.

Now, since

$$Y = \frac{st}{s^2+t^2} = \frac{s}{s+t} + \left(\frac{s}{s+t}\right)^2,$$

we have $\beta_{q-1} = \mathrm{Tr}(Y) = 0$.

And as the last auxiliary statement, we have $Y = K + K^\sigma + K^\gamma + K^{\sigma\gamma}$. Consider the case $n \equiv 1 \mod 4$ first by writing $n = 4l + 1$ with $l \in \mathbb{N}$. Then $\sigma = 2^{2l+1}$ and $\gamma = 2^{3l+1}$. As $K = \beta_{\gamma-1}$, we have

$$K + K^\sigma + K^\gamma + K^{\gamma\sigma} = \underbrace{\sum_{i=0}^{3l} Y^{2^i}}_{=:B_0} + \underbrace{\sum_{i=0}^{3l} Y^{2^i \cdot 2^{2l+1}}}_{=:B_1} + \underbrace{\sum_{i=0}^{3l} Y^{2^i \cdot 2^{3l+1}}}_{=:B_2} + \underbrace{\sum_{i=0}^{3l} Y^{2^i \cdot 2^{5l+2}}}_{=:B_3}.$$

By applying $Y^{2^{4l+1}} = 1$, while coloring those terms which will combine to $\mathrm{Tr}(Y) = 0$ in the sum, we may calculate

$$\begin{aligned}B_1 &= \sum_{i=0}^{3l} Y^{2^{i+2l+1}} = \sum_{i=2l+1}^{5l+1} Y^{2^i} = \sum_{i=2l+1}^{4l} Y^{2^i} + \sum_{i=0}^{l} Y^{2^i}, \\ B_2 &= \sum_{i=0}^{3l} Y^{2^{i+3l+1}} = \sum_{i=3l+1}^{6l+1} Y^{2^i} = \sum_{i=3l+1}^{4l} Y^{2^i} + \sum_{i=0}^{2l} Y^{2^i}, \\ B_3 &= \sum_{i=0}^{3l} Y^{2^{i+5l+2}} = \sum_{i=5l+2}^{8l+2} Y^{2^i} = \sum_{i=l+1}^{4l} Y^{2^i} + Y.\end{aligned}$$

Since B_0 and B_3 sum to $\mathrm{Tr}(Y) + Y = Y$, we have $Y = K + K^\sigma + K^\gamma + K^{\gamma\sigma}$. In this case, we can continue by showing $\beta_{\sigma-1} = K + K^\gamma$. We have

$$\begin{aligned}\beta_{\sigma-1} = \mathrm{Tr}(Y) + \beta_{\sigma-1} &= \sum_{i=0}^{4l} Y^{2^i} + \sum_{i=0}^{2l} Y^{2^i} = \sum_{i=0}^{3l} Y^{2^i} + \sum_{i=3l+1}^{4l} Y^{2^i} + \sum_{i=0}^{2l} Y^{2^i} \\ &= \beta_{\gamma-1} + \sum_{i=3l+1}^{6l+1} Y^{2^i} = \beta_{\gamma-1} + \sum_{i=0}^{3l} Y^{2^{3l+1}} \\ &= \beta_{\gamma-1} + \left(\sum_{i=0}^{3l} Y^{2^i}\right)^{2^{3l+1}} = \beta_{\gamma-1} + \beta_{\gamma-1}^\gamma = K + K^\gamma.\end{aligned}$$

The other case $n \equiv 3 \mod 4$ is a little more straightforward: We write $n = 4l + 3$ with $l \in \mathbb{N}_0$. Then $\sigma = 2^{2l+2}$ and $\gamma = 2^{l+1}$, leading to

$$\begin{aligned} K + K^\sigma + K^\gamma + K^{\gamma\sigma} &= \sum_{i=0}^{l} Y^{2^i} + \sum_{i=0}^{l} Y^{2^i \cdot 2^{2l+2}} + \sum_{i=0}^{l} Y^{2^i \cdot 2^{l+1}} + \sum_{i=0}^{l} Y^{2^i \cdot 2^{3l+3}} \\ &= \sum_{i=0}^{l} Y^{2^i} + \sum_{i=2l+2}^{3l+2} Y^{2^i} + \sum_{i=l+1}^{2l+1} Y^{2^i} + \sum_{i=3l+3}^{4l+2} Y^{2^i} + Y \\ &= \mathrm{Tr}(Y) + Y = Y. \end{aligned}$$

Continuing with proving $\beta_{\sigma-1} = K + K^\gamma$, we have

$$\beta_{\sigma-1} = \sum_{i=0}^{2l+1} Y^{2^i} = \sum_{i=0}^{l} Y^{2^i} + \sum_{i=l+1}^{2l+1} Y^{2^i} = \beta_{\gamma-1} + \sum_{i=0}^{l} Y^{2^i \cdot 2^{l+1}} = \beta_{\gamma-1} + \beta_{\gamma-1}^{\gamma} = K + K^\gamma.$$

To verify the statement regarding $\beta_{\sigma+\gamma-1}$, we use Formula (3.10) with $a = \sigma + \gamma - 1$ and $l = \sigma$ to obtain

$$\begin{aligned} \beta_{\sigma+\gamma-1} &= Y^{-1}\beta_\sigma\beta_{\sigma+\gamma-1-\sigma+1} + \beta_{\sigma-1}\beta_{\gamma-1} \\ &= Y + (K + K^\gamma)\, K \\ &= K^\sigma + K^{\gamma+1} + K^\gamma + K^{\gamma\sigma} + K^2 + K. \end{aligned}$$

Finally, K is a sum of Y^{2^i} terms, so $\mathrm{Tr}(K) = 0$, as $\mathrm{Tr}(Y) = 0$. □

The next two lemmas are needed to rewrite the equation in question in a more convenient form.

3.1.14 Lemma. *For $q = 2^n$ with n odd and $s, t \in \mathbb{F}_q^*$ distinct,*

$$(\gamma - 1)^{-1} \equiv \gamma\sigma + \sigma + \gamma + 1 \mod q - 1$$

holds. In particular, $x \mapsto x^{\gamma-1}$ is a permutation of $\mathbb{F}_q$.

Proof. We have

$$\begin{aligned} (\gamma - 1)(\gamma\sigma + \sigma + \gamma + 1) &\equiv 2 + \gamma\sigma + \sigma + \gamma - \gamma\sigma - \sigma - \gamma - 1 \mod q - 1 \\ &= 1. \end{aligned}$$

□

3.1.15 Lemma. *For $q = 2^n$ with n odd and $s, t \in \mathbb{F}_q^*$ distinct, we have $K \neq 0$ and $K^{\gamma-1} + 1 \neq 0$.*

Proof. By the definition of K, we have

$$K = \beta_{\gamma-1} = \frac{s^{\gamma-1} + t^{\gamma-1}}{(s+t)^{\gamma+1}} st \neq 0,$$

as $s^{\gamma-1} \neq t^{\gamma-1}$ by Lemma 3.1.14.

Further, if $K^{\gamma-1}+1=0$ were to hold, we would have $K=1$. Then, since n is odd, $\mathrm{Tr}(K)=1$ would follow. This, however, is ruled out by Lemma 3.1.13, stating $\mathrm{Tr}(K)=0$. □

We are now ready to tackle the proof of Theorem 3.1.10.

Proof (of Glynn$_2$ hyperovals). Firstly, the formulas obtained in Theorem 3.3.3 and Theorem 3.3.4 are valid independent of whether e is an o-exponent, so we can conclude that $\gcd(e,q-1)=\gcd(e-1,q-1)=1$ holds.

By Theorem 3.1.1 only $h(x)=((x+1)^e+1)x^{q-2}$ being a permutation polynomial remains to be shown. For a contradiction, suppose there are two distinct elements $s,t\in\mathbb{F}_q$ satisfying $h(s)=h(t)$. Since $x\mapsto x^e$ is a permutation of $\mathbb{F}_q$, we have $h^{-1}(\{0\})=\{0\}$. Therefore, s and t are not zero.

Step 1: Deriving the equation in terms of K. We have

$$\begin{aligned}h(s)&=((s+1)^{\sigma+\gamma}+1)s^{q-2}=\left(\left(s^\sigma+1\right)\left(s^\gamma+1\right)+1\right)s^{q-2}\\&=\left(s^{\sigma+\gamma}+s^\sigma+s^\gamma\right)s^{q-2}=s^{\sigma+\gamma-1}+s^{\sigma-1}+s^{\gamma-1}.\end{aligned}$$

Multiplying $0=h(s)+h(t)$ by $YS^{-(\sigma+\gamma-1)}$ gives

$$\begin{aligned}&\underbrace{\left(s^{\sigma+\gamma-1}+t^{\sigma+\gamma-1}\right)YS^{-(\sigma+\gamma-1)}}_{=\beta_{\sigma+\gamma-1}}+\underbrace{\left(s^{\sigma-1}+t^{\sigma-1}\right)YS^{-(\sigma+\gamma-1)}}_{=\beta_{\sigma-1}S^{-\gamma}}\\&+\underbrace{\left(s^{\gamma-1}+t^{\gamma-1}\right)YS^{-(\sigma+\gamma-1)}}_{=\beta_{\gamma-1}S^{-\sigma}}=0.\end{aligned}$$

Substituting $x=S^{-\gamma}$ and using the formulas given in Lemma 3.1.13 yields

$$Kx^\gamma+\left(K+K^\gamma\right)x+K+K^2+K^\gamma+K^{\gamma+1}+K^\sigma+K^{\gamma\sigma}=0.$$

Since $K\neq 0$ by Lemma 3.1.15, we might divide by K to arrive at

$$x^\gamma+\left(K^{\gamma-1}+1\right)x+K+K^{\gamma-1}+K^\gamma+K^{\sigma-1}+K^{\gamma\sigma-1}+1=0. \tag{3.12}$$

Step 2: Reformulating Equation (3.12) *in terms of* $A:=K^{\gamma-1}+1$. By Lemma 3.1.15 we have $A\neq 0$ and by setting

$$g:=\gamma\sigma+\sigma+\gamma+1\equiv(\gamma-1)^{-1}\mod q-1$$

we have $K=(A+1)^g$ by Lemma 3.1.14.

Next, we rewrite the constant parts of Equation (3.12) in terms of A.

$$\begin{aligned} B :&= K + K^{\gamma-1} + K^{\gamma} + K^{\sigma-1} + K^{\gamma\sigma-1} + 1 \\ &= A + K(1 + K^{\gamma-1}) + K^{\sigma-1} + K^{\gamma\sigma-1} \\ &= A + (A+1)^g A + K^{\sigma-1}\left(1 + K^{(\gamma-1)\sigma}\right) \\ &= A + A(A+1)^g + (A+1)^{g(\sigma-1)}\left(1 + K^{\gamma-1}\right)^{\sigma} \\ &= A + A(A+1)^g + A^{\sigma}(A+1)^{g(\sigma-1)}. \end{aligned}$$

Calculating

$$\begin{aligned} g(\sigma-1) &= (\gamma\sigma + \sigma + \gamma + 1)(\sigma - 1) \\ &= \gamma\sigma^2 + \sigma^2 + \gamma\sigma + \sigma - \gamma\sigma - \sigma - \gamma - 1 \\ &\equiv 2\gamma + 2 - \gamma - 1 = \gamma + 1 \mod q - 1 \end{aligned}$$

then yields

$$B = A + A(A+1)^g + A^{\sigma}(A+1)^{\gamma+1}.$$

Equation (3.12) is now of the form

$$x^{\gamma} + Ax + B = 0. \tag{3.13}$$

Step 3: Reaching the contradiction with the trace equality. Equation (3.13) has at least one solution $x = S^{-\gamma}$ by construction. Therefore, since $A \neq 0$, by Theorem 3.1.11 we must have

$$\mathrm{Tr}\left(\frac{B}{A^{g+1}}\right) = 0.$$

We calculate $\mathrm{Tr}\left(\frac{B}{A^{g+1}}\right)$ to be 1 now and thus reach a contradiction. We begin by examining

$$\frac{B}{A^{g+1}} = A^{-g}\underbrace{\left(1 + (A+1)^g + (A+1)^{\gamma+1}A^{\sigma-1}\right)}_{:=L}.$$

We have

$$\begin{aligned} L &= 1 + (A+1)^{\gamma\sigma}(A+1)^{\sigma}(A+1)^{\gamma}(A+1) + (A+1)^{\gamma}(A+1)A^{\sigma-1} \\ &= 1 + \left(A^{\gamma\sigma+\sigma} + A^{\gamma\sigma} + A^{\sigma} + 1 + A^{\sigma-1}\right)(A+1)^{\gamma}(A+1) \\ &= 1 + \left(A^{\gamma\sigma+\sigma} + A^{\gamma\sigma} + A^{\sigma} + A^{\sigma-1} + 1\right)\left(A^{\gamma+1} + A^{\gamma} + A + 1\right). \end{aligned}$$

Expanding yields

$$\begin{aligned}L = &\underline{1} + A^{\gamma\sigma+\sigma+\gamma+1} + A^{\gamma\sigma+\sigma+\gamma} + A^{\gamma\sigma+\sigma+1} + A^{\gamma\sigma+\sigma}\\ &+ A^{\gamma\sigma+\gamma+1} + A^{\gamma\sigma+\gamma} + A^{\gamma\sigma+1} + A^{\gamma\sigma}\\ &+ A^{\gamma+\sigma+1} + \underline{A^{\sigma+\gamma}} + A^{\sigma+1} + \underline{A^{\sigma}} + \underline{A^{\sigma+\gamma}} + A^{\sigma+\gamma-1} + \underline{A^{\sigma}} + A^{\sigma-1}\\ &+ A^{\gamma+1} + A^{\gamma} + A + \underline{1}.\end{aligned}$$

Cancelling and artificially creating a g summand in the exponents gives

$$\begin{aligned}L = &A^{g} + A^{g-1} + A^{g-\gamma} + A^{g-\gamma-1} + A^{g-\sigma} + A^{g-\sigma-1} + A^{g-\gamma-\sigma} + A^{g-\gamma-\sigma-1}A^{g-\gamma\sigma}\\ &+ A^{g-\gamma\sigma-\gamma} + A^{g-\gamma\sigma-2} + A^{g-\gamma\sigma-\gamma-2} + A^{g-\gamma\sigma-\sigma} + A^{g-\gamma\sigma-\sigma-1} + A^{g-\gamma\sigma-\gamma-\sigma}.\end{aligned}$$

Next we group the terms of $\frac{B}{A^{g+1}}$ into parts which will amount to 0 when taking the trace by underlining them in the same color. Note the relations

$$\begin{aligned}A^{\gamma\sigma-2} &= A^{\sigma(-\gamma-\sigma)},\\ A^{-2-\gamma\sigma-\gamma} &= A^{\gamma(-\gamma\sigma-\sigma-1)},\\ A^{-\sigma-\gamma\sigma-\gamma} &= A^{\gamma(-\gamma-\sigma-1)}.\end{aligned}$$

We have

$$\begin{aligned}\frac{B}{A^{g+1}} = 1 &+ \underline{A^{-1}} + \underline{A^{-\gamma}} + \underline{A^{-\gamma-1}} + \underline{A^{-\sigma}} + \underline{A^{-\sigma-1}} + \underline{A^{-\gamma-\sigma}} + \underline{A^{-\gamma-\sigma-1}}\\ &+ \underline{A^{-\gamma\sigma}} + \underline{A^{-\gamma\sigma-\gamma}} + \underline{A^{-\gamma\sigma-2}} + \underline{A^{-\gamma\sigma-\gamma-2}} + \underline{A^{-\gamma\sigma-\sigma}} + \underline{A^{-\gamma\sigma-\sigma-1}} + \underline{A^{-\gamma\sigma-\gamma-\sigma}}\end{aligned}$$

and, therefore,

$$\begin{aligned}\operatorname{Tr}\left(\frac{B}{A^{g+1}}\right) &= \operatorname{Tr}(1) + \underline{\operatorname{Tr}\left(A^{-1} + \left(A^{-1}\right)^{\gamma}\right)} + \underline{\operatorname{Tr}\left(A^{-\gamma-1} + \left(A^{-\gamma-1}\right)^{\sigma}\right)}\\ &\quad + \underline{\operatorname{Tr}\left(A^{-\sigma} + \left(A^{-\sigma}\right)^{\gamma}\right)} + \underline{\operatorname{Tr}\left(A^{-\sigma-1} + \left(A^{-\sigma-1}\right)^{\gamma}\right)}\\ &\quad + \underline{\operatorname{Tr}\left(A^{-\gamma-\sigma} + \left(A^{-\gamma-\sigma}\right)^{\sigma}\right)} + \underline{\operatorname{Tr}\left(A^{-\gamma\sigma-\sigma-1} + \left(A^{-\gamma\sigma-\sigma-1}\right)^{\gamma}\right)}\\ &\quad + \underline{\operatorname{Tr}\left(A^{-\gamma-\sigma-1} + \left(A^{-\gamma-\sigma-1}\right)^{\gamma}\right)}\\ &= \operatorname{Tr}(1) + 0 = 1,\end{aligned}$$

as n is odd. □

3.1.3 Stabilizers of Monomial Hyperovals

This subsection is interesting to us mostly for its interplay with Theorem 2.2.25. In the remark after its proof we already discussed how the stabilizers affect its conclusions. Furthermore, in the third case of its proof we used a specific projectivity (given by the matrix in (2.15)) always present in the stabilizer of $\mathcal{H}(x^e)$ to simplify the given situation.

First of all, any collineation induced by an automorphism of $\mathbb{F}_q$ stabilizes the monomial hyperoval $\mathcal{H}(x^e)$, as monomials have 1 as their coefficient. Therefore, we only need to consider their homography stabilizer, that is, the set of projectivities from $\mathrm{PGL}(3,q)$ stabilizing the hyperoval. The results surveyed here have been obtained in [32], if not indicated otherwise.

We begin with the regular hyperovals and continue with the irregular translation hyperovals.

3.1.16 Theorem. *Let $q = 2^n$ with $n \in \mathbb{N}$. Then*

- *for $n = 1$ a regular hyperoval has a transitive homography stabilizer of order 24 isomorphic to the symmetric group S_4,*
- *for $n = 2$ a regular hyperoval has a transitive homography stabilizer of order 360 isomorphic to the alternating group A_6, and*
- *for $n \geq 3$ a regular hyperoval has a homography stabilizer of order $(q+1)q(q-1)$ isomorphic to $\mathrm{PGL}(2,q)$ (see [22, Theorem 8.4.2 Corollary 6]).*

3.1.17 Theorem. *Let $n, h \in \mathbb{N}$ with $n \geq 3$, $2 \leq h \leq n-2$, $\gcd(n,h) = 1$ and set $q = 2^n$ and $e = 2^h$. Then the translation hyperoval $\mathcal{H}(x^e)$ has a homography stabilizer of order $q(q-1)$, which fixes the points $(0,1,0)$ and $(0,0,1)$ and has $\{(1,s,s^e) : s \in \mathbb{F}_q\}$ as the remaining orbit.*

Interestingly, there is no need to distinguish between Segre and Glynn hyperovals (or other types if they exist).

3.1.18 Theorem. *Let $e \in \mathbb{N}$ such that $\mathcal{H}(x^e)$ is a hyperoval of $\mathrm{PG}(2,q)$, though not a translation hyperoval. Then*

- *if $e^2 - e + 1 \equiv 0 \mod q-1$, the homography stabilizer of $\mathcal{H}$ has order $3(q-1)$ and has the orbits $\{(1,s,s^e) : s \in \mathbb{F}_q^*\}$ and $\{(1,0,0),(0,1,0),(0,0,1)\}$,*
- *otherwise the homography stabilizer of $\mathcal{H}$ has order $q-1$ and has $\{(1,s,s^e) : s \in \mathbb{F}_q^*\}$ as one orbit, while fixing the points $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$.*

The only o-exponents e known to satisfy $e^2 - e + 1 \equiv 0 \mod q-1$ are $e = 6$, the Segre o-exponent, for $q = 32$ and $e = 20$, the Glynn_2 o-exponent, for $q = 128$. From the known families these are the only possible examples, as $6^2 - 6 + 1$ is constant,

$$(3\sigma+4)^2 - 3\sigma - 4 + 1 \equiv 21\sigma + 31 \mod q-1$$

grows slower than $q-1$, and

$$(\sigma+\gamma)^2 - \sigma - \gamma + 1 \equiv 0 \mod q-1$$

implies $9 \equiv 7\sigma + 6\gamma \mod q-1$ by squaring, which also can happen only finitely many times, since $7\sigma + 6\gamma$ grows slower than $q-1$.

3.2 Non-Monomial Families

3.2.1 q-Clans

In order to appreciate the construction of the Subiaco and Adelaide hyperovals we make a quick detour to the theory of q-clans, as they are fundamentally connected to those hyperovals. We only sketch their construction and follow [13, Section 2], where also proofs for the given statements and further connections to other objects of finite geometry can be found.

3.2.1 Definition (q-Clan)**.** Let $C = \{A_t \in \mathbb{F}_q^{2\times 2} : t \in \mathbb{F}_q\}$ be a family of 2×2 matrices over $\mathbb{F}_q$. Then C is a called a *q-clan* if the quadratic forms

$$Q_{st}(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A_s - A_t \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

for distinct $s, t \in \mathbb{F}_q$ are anisotropic, that is, $Q_{st}(x, y) = 0$ if and only if $x = y = 0$ for all distinct $s, t \in \mathbb{F}_q$.

For each q-clan there is also a normalized q-clan obtainable via a normalization process.

3.2.2 Definition (Normalized q-Clan)**.** A q-clan C with $A_0 = 0$, $A_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & c_1 \end{smallmatrix}\right)$ and $A_t = \left(\begin{smallmatrix} a_t & t^{\frac{1}{2}} \\ 0 & c_t \end{smallmatrix}\right)$ for $t \in \mathbb{F}_q$ is called a *normalized q-clan.*

When writing $a = c_1$, $f(t) = a_t$ and $g(t) = \frac{c_t}{a}$, the following, although only noted in [13], is a consequence of Theorem 3.1.11.

3.2.3 Theorem. *Let $a \in \mathbb{F}_q$ and let $f, g \in \mathbb{F}_q[x]$. Then*

$$C = \left\{ \begin{pmatrix} f(t) & t^{\frac{1}{2}} \\ 0 & ag(t) \end{pmatrix} : t \in \mathbb{F}_q \right\}$$

is a normalized q-clan if and only if

$$\operatorname{Tr}\left(\frac{a(f(s) + f(t))(g(s) + g(t))}{s + t} \right) = 1$$

holds for all distinct $s, t \in \mathbb{F}_q$.

The next theorem is the reason that q-clans are interesting to us: A normalized q-clan induces $q + 1$ o-polynomials, which induce a so-called herd of ovals.

3.2.4 Theorem. *Let $a \in \mathbb{F}_q$ and let $f, g \in \mathbb{F}_q[x]$ with $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$. Then*

$$\operatorname{Tr}\left(\frac{a(f(s) + f(t))(g(s) + g(t))}{s + t} \right) = 1$$

holds if and only if $\mathrm{Tr}(a) = 1$, *g is an o-polynomial and the map*

$$f_s(x) = \frac{f(x) + asg(x) + s^{\frac{1}{2}}x^{\frac{1}{2}}}{1 + as + s^{\frac{1}{2}}}$$

describes an o-polynomial for all distinct $s \in \mathbb{F}_q$.

3.2.2 Subiaco and Adelaide Hyperovals

We begin by describing the Subiaco q-clan.

3.2.5 Theorem ([13, Theorem 5])**.** *Let* $d \in \mathbb{F}_q$ *such that* $d^2+d+1 \neq 0$ *and* $\mathrm{Tr}\left(\frac{1}{d}\right) = 1$. *Set*

$$\begin{aligned} a &= \frac{d^2 + d^5 + d^{\frac{1}{2}}}{d(1 + d + d^2)}, \\ f(x) &= \frac{d^2(x^4 + x) + d^2(1 + d + d^2)(x^3 + x^2)}{(x^2 + dx + 1)^2} + x^{\frac{1}{2}}, \\ g(x) &= \frac{d^4x^4 + d^3(1 + d^2 + d^4)x^3 + d^3(1 + d^2)x}{(d^2 + d^5 + d^{\frac{1}{2}})(x^2 + dx + 1)^2} + \frac{d^{\frac{1}{2}}}{d^2 + d^5 + d^{\frac{1}{2}}}x^{\frac{1}{2}}. \end{aligned}$$

Then

$$S = S_d = \left\{ \begin{pmatrix} f(t) & t^{\frac{1}{2}} \\ 0 & ag(t) \end{pmatrix} : t \in \mathbb{F}_q \right\}$$

is a q-clan, called the Subiaco q-clan.

In [40] various properties and a different representation of the Subiaco q-clan are shown, for example it is proven that different choices for $d \in \mathbb{F}_q$ lead to equivalent q-clans by giving an explicit isomorphism in their Theorem 4.4. Furthermore, it is established that for $q = 2^n$ with $n \not\equiv 2 \mod 4$ only one hyperoval, up to equivalence, arises from the Subiaco q-clan. This hyperoval may be described by the o-polynomial given by the map

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

where again $d \in \mathbb{F}_q$ such that $d^2+d+1 \neq 0$ and $\mathrm{Tr}\left(\frac{1}{d}\right) = 1$. In [33, Corollary 14 and 17] its stabilizer is worked out to be a cyclic group of order $2n$ for $q \geq 32$.

If $n \equiv 2 \mod 4$, the situation is a little more delicate, as there are two inequivalent hyperovals arising from the Subiaco q-clan [40, Theorem 6.13]. Let $\omega \in \mathbb{F}_q$ with $\omega^2 + \omega + 1 = 0$. Such an element ω exists, since $2|n$ and thus $\mathbb{F}_4 \leq \mathbb{F}_q$. Then the polynomial describing the map

$$f(x) = \frac{\omega^2x^4 + \omega^2x}{x^4 + \omega^2x^2 + 1} + x^{\frac{1}{2}}$$

is an o-polynomial for the first kind [40, Eq. 53 or Theorem 6.6]. It has a stabilizer of order $10n$ for $q \geq 64$ [40, Theorem 6.13]. The other hyperoval is explicitly described in [38, Eq. 50]. Let ζ be a primitive element of $\mathbb{F}_{q^2}$ and let $\lambda = \zeta^{q-1}$. Then $\delta := \lambda + \lambda^{-1}$ is an element of $\mathbb{F}_q$, since

$$\begin{aligned}\delta^q &= \zeta^{q^2-q} + \zeta^{-q^2+q} = \zeta^{q^2-1}\zeta^{1-q} + \left(\frac{1}{\zeta}\right)^{q^2-1}\left(\frac{1}{\zeta}\right)^{1-q} \\ &= \lambda^{-1} + \lambda = \delta.\end{aligned}$$

The polynomial given by the map

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

is an o-polynomial for the second kind, whose associated hyperoval has a stabilizer of order $5\frac{n}{2}$ for $q \geq 64$ (see [40, Theorem 6.13] again).

The Adelaide q-clan has been described in [11].

3.2.6 Theorem ([11, Theorem 3.1])**.** *Let $q = 2^n$ with $n > 2$ even and let $\beta \in \mathbb{F}_{q^2} \setminus \{1\}$ with $\beta^{q+1} = 1$. Let further $m \in \mathbb{N}$ with $m \equiv \pm\frac{q-1}{3} \mod q+1$. Let $T : \mathbb{F}_{q^2} \to \mathbb{F}_q$ be the trace map, that is, $T(x) = x + x^q$ for $x \in \mathbb{F}_{q^2}$. Define $a \in \mathbb{F}_q$ and functions $f, g : \mathbb{F}_q \to \mathbb{F}_q$ by*

$$\begin{aligned}a &= \frac{T(\beta^m)}{T(\beta)} + \frac{1}{T(\beta^m)} + 1, \\ f(t) &= \frac{T(\beta^m)(t+1)}{T(\beta)} + \frac{T\left((\beta t + \beta^q)^m\right)}{T(\beta)\left(t + T(\beta)t^{\frac{1}{2}} + 1\right)^{m-1}} + t^{\frac{1}{2}}, \\ ag(t) &= \frac{T(\beta^m)}{T(\beta)}t + \frac{T\left((\beta^2 t + 1)^m\right)}{T(\beta)T(\beta^m)\left(t + T(\beta)t^{\frac{1}{2}} + 1\right)^{m-1}} + \frac{t^{\frac{1}{2}}}{T(\beta^m)}.\end{aligned}$$

Then

$$C = \left\{ \begin{pmatrix} f(t) & t^{\frac{1}{2}} \\ 0 & ag(t) \end{pmatrix} : t \in \mathbb{F}_q \right\}$$

is a q-clan, called the Adelaide q-clan.

Remarkably, when choosing other values for m such that different congruences are satisfied, one can obtain other q-clans as well, including the Subiaco q-clan. In [12] it is shown that there is, up to equivalence, only one Adelaide hyperoval, in particular it is shown that the concrete values of β and m do not matter. One suitable o-polynomial is given by the map $t \mapsto f(t)$ from Theorem 3.2.6. For $q \geq 64$ the Adelaide hyperoval has a cyclic stabilizer of order $2n$ [41, Corollary 7.3].

3.2.3 Payne and Cherowitzo Hyperovals

The Payne hyperoval was found by Payne in 1985 [37], while investigating generalized quadrangles, which are geometric spaces with quadrangles but no triangles (see, e.g. [1]). We include a proof, as it is short and provides an explicit example to the usage of q-clans. The original work is also hard to find. Furthermore, we also yield another proof for the Segre o-monomial as a byproduct. We give the proof found in [7] or alternatively in [39, Section 2.4].

3.2.7 Theorem (Payne Hyperovals)**.** *Let $q = 2^n$ with n odd. Then the polynomial over $\mathbb{F}_q$ describing the map*

$$f(x) = x^{\frac{1}{6}} + x^{\frac{3}{6}} + x^{\frac{5}{6}}$$

is an o-polynomial and its hyperoval is called the Payne hyperoval.

Proof. Letting $a = 1$, $f(x) = x^{\frac{1}{6}}$ and $g(x) = x^{\frac{5}{6}}$, we prove that

$$\left\{ \begin{pmatrix} t^{\frac{1}{6}} & t^{\frac{1}{2}} \\ 0 & t^{\frac{5}{6}} \end{pmatrix} : t \in \mathbb{F}_q \right\}$$

is a q-clan. By Theorem 3.2.3 we need to show that

$$\mathrm{Tr}\left(\frac{(s+t)(s^5+t^5)}{s^6+t^6} \right) = 1, \tag{3.14}$$

where we already substituted $s \mapsto s^6$ and $t \mapsto t^6$, for all distinct $s, t \in \mathbb{F}_q$. Using the relations

$$s^3 + t^3 = (s+t)(s^2+st+t^2) \text{ and } s^5 + t^5 = (s+t)(s^4+s^3t+s^2t^2+st^3+t^4)$$

we have that

$$\begin{aligned} 1 + \frac{(s+t)(s^5+t^5)}{s^6+t^6} &= 1 + \frac{s^4+s^3t+s^2t^2+st^3+t^4}{(s^2+st+t^2)^2} = \frac{s^3t+st^3}{s^4+s^2t^2+t^2} \\ &= \frac{st}{s^2+st+t^2} + \left(\frac{st}{s^2+st+t^2} \right)^2 \end{aligned}$$

has trace zero. Since n is odd and therefore $\mathrm{Tr}(1) = 1$, Equation (3.14) must hold. Then by Theorem 3.2.4 the polynomial describing the map

$$f_1(x) = x^{\frac{1}{6}} + x^{\frac{5}{6}} + x^{\frac{1}{2}}$$

is an o-polynomial. □

The Payne hyperoval has a cyclic stabilizer of order $2n$ for $q \geq 32$ [47].

The Cherowitzo o-polynomial has long been conjectured to be an o-polynomial (see for example [9, Section 4]) and has been finally proven to be one by Cherowitzo in 1998 in [10] using a generalization of q-clans called α-clans.

3.2.8 Theorem ([10, Corollary 20]). *Let $q = 2^n$ with n odd and let $\sigma = 2^{\frac{n+1}{2}}$, that is, σ is the unique least positive residue* $\mod q-1$ *satisfying*

$$\sigma^2 \equiv 2 \mod q-1.$$

Then the polynomial

$$f(x) = x^\sigma + x^{\sigma+2} + x^{3\sigma+4} = x^{2^{\frac{n+1}{2}}} + x^{2^{\frac{n+1}{2}}+2} + x^{3\cdot 2^{\frac{n+1}{2}}+4}$$

is an o-polynomial.

When $q \geq 32$, the associated hyperoval has a stabilizer of order n, consisting of only the automorphisms of $\mathbb{F}_q$ [3, Corollary 4.4].

3.3 Explicit Formulas for the Known Monomial Hyperovals

Our examinations in Chapter 2 culminated in Theorem 2.2.25, stating that for each o-monomial, there are exactly five more o-equivalent o-monomials. Our goal is now to give explicit formulas for those o-monomials o-equivalent to the known o-exponents we dealt with in Section 3.1.

The strategy is generally as follows. We use computer calculated examples in small fields to search for a general pattern in the binary expansion of the exponents. These patterns are usually quick to spot and may be exploited to obtain a formula using the geometric series. Note that this approach ensures that the formulas found require only division in $\mathbb{Z}$ and always give the least positive residue modulo $q-1$. Obtaining formulas for $(1-e)^{-1}$, when e is the exponent in question, requires some more work, as $(1-e)^{-1}$ is dependent on $n \mod 4$ (and even on $n \mod 8$ for Glynn_2) as well. Afterwards, one has to check by brute calculation that the formulas are indeed valid. Note that we only need to calculate e^{-1} and $(1-e)^{-1}$, as the others follow easily then.

Finally, we would like to mention that some of these formulas are already known. For the Glynn o-exponents Glynn himself gives the equivalent o-monomials in [18], although only in terms of γ and σ and not as explicit as we do it here. In [5, Table 1] some relations are given, sometimes explicit, sometimes as a series. Series representations are also given in [14, Tables 1 and 2]. These references, however, were found only after the following work was already done. Also, in [16, Section 2.2.2] explicit formulas for $1-e$ and e^{-1} of the Segre and translation o-exponents are given, which were the starting point of the following work.

3.3.1 Segre Exponents

3.3.1 Theorem (Transformations of the Segre o-Exponent). *Let $n \in \mathbb{N}$ be odd, that is, $n = 2l+1$ with $l \in \mathbb{N}$. Then for $e = 6$, the Segre o-exponent, the following relations,*

taken $\mod 2^n-1$ *each, hold.*

$$\begin{aligned}
1-e &= 2^n-6,\\
\frac{1}{e} &= \frac{5\cdot 2^{n-1}-2}{3},\\
\frac{e-1}{e} &= \frac{2^{n-1}+2}{3},\\
\frac{1}{1-e} &= \begin{cases} \frac{2^n-2}{5} & : n\equiv 1 \mod 4,\\ \frac{3\cdot 2^n-4}{5} & : n\equiv 3 \mod 4,\end{cases}\\
\frac{e}{e-1} &= \begin{cases} \frac{4\cdot 2^n+2}{5} & : n\equiv 1 \mod 4,\\ \frac{2\cdot 2^n+4}{5} & : n\equiv 3 \mod 4.\end{cases}
\end{aligned}$$

Proof. The first relation is clear, since $2^n-6\equiv 1-6 \mod q-1$. By consideration of the binary expansions of e^{-1} for small values of l, one can extrapolate the following form.

$$\begin{aligned}
x_l :&= (110\underbrace{10\,10\,\ldots\,10}_{l-1\ 10\text{ blocks}})_2\\
&= 2^{2l}+2^{2l-1}+\sum_{j=0}^{l-2}2^{1+2j} = 2^{2l}+2^{2l-1}+2\sum_{j=0}^{l-2}4^j\\
&= 2^{2l}+2^{2l-1}+2\frac{4^{l-1}-1}{3} = \frac{9\cdot 2^{2l-1}}{3}+\frac{2^{2l-1}-2}{3}\\
&= \frac{10\cdot 2^{2l-1}-2}{3} = \frac{5\cdot 2^{2l}-2}{3} = \frac{5\cdot 2^{n-1}-2}{3}.
\end{aligned}$$

We can verify this formula by computing

$$\frac{5\cdot 2^{n-1}-2}{3}\cdot 6 = 5\cdot 2^n-4\equiv 1 \mod 2^n-1.$$

For the third relation we may resort to the second via

$$\frac{e-1}{e} = 1-\frac{1}{e}\equiv 2^n-\frac{5\cdot 2^{n-1}-2}{3} = \frac{3\cdot 2^n-5\cdot 2^{n-1}+2}{3} = \frac{2^{n-1}+2}{3} \mod 2^n-1.$$

Next we consider the case $n\equiv 1 \mod 4$ first, writing $n=4\tilde{l}+1$ with $\tilde{l}\in\mathbb{N}$. Examples

of $(1-e)^{-1}$ for small sizes of l lead to

$$\begin{aligned} x_{\tilde{l}} &:= (\underbrace{1100\,1100\,\ldots\,1100}_{\tilde{l}-1\ 1100\text{ blocks}}\,110)_2 \\ &= 2 + 2^2 + \sum_{j=0}^{\tilde{l}-2} 2^{5+4j} + 2^{6+4j} = 2 + 2^2 + 2^5 \sum_{j=0}^{\tilde{l}-2} 16^j + 2^6 \sum_{j=0}^{\tilde{l}-2} 16^j \\ &= 6 + \left(2^5 + 2^6\right) \frac{16^{\tilde{l}-1} - 1}{15} = 6 + 3 \cdot 2^5 \frac{2^{4\tilde{l}-4} - 1}{15} = 6 + \frac{2^{4\tilde{l}+1} - 2^5}{5} \\ &= \frac{2^{4\tilde{l}+1} - 2}{5} = \frac{2^n - 2}{5}. \end{aligned}$$

This is indeed the general form of $(1-e)^{-1}$, since

$$\frac{2^n - 2}{5} \cdot (1 - 6) = 2 - 2^n \equiv 2 - 1 = 1 \mod 2^n - 1.$$

Furthermore,

$$\frac{e}{e-1} = 1 - \frac{1}{1-e} \equiv 2^n - \frac{2^n - 2}{5} = \frac{4 \cdot 2^n + 2}{5} \mod 2^n - 1.$$

So, only the case $n \equiv 3 \mod 4$ remains. We write $n = 4\tilde{l} + 3$ with $\tilde{l} \in \mathbb{N}_0$. If we look at the binary expansions of $(1-e)^{-1}$ for small values of l again, we may suggest the following form:

$$\begin{aligned} x_{\tilde{l}} &:= (100\,\underbrace{1100\,1100\,\ldots\,1100}_{\tilde{l}\ 1100\text{ blocks}})_2 \\ &= 2^{4\tilde{l}+2} + \sum_{j=0}^{\tilde{l}-1} 2^{2+4j} + 2^{3+4j} = 2^{4\tilde{l}+2} + 2^2 \sum_{j=0}^{\tilde{l}-1} 16^j + 2^3 \sum_{j=0}^{\tilde{l}-1} 16^j \\ &= 2^{4\tilde{l}+2} + 12\frac{16^{\tilde{l}} - 1}{15} = 2^{4\tilde{l}+2} + \frac{4 \cdot 2^{4\tilde{l}} - 4}{5} = \frac{6 \cdot 2^{4\tilde{l}+2} - 4}{5} = \frac{3 \cdot 2^n - 4}{5}. \end{aligned}$$

This is indeed the general form, as

$$\frac{3 \cdot 2^n - 4}{5} \cdot (1 - 6) = 4 - 3 \cdot 2^n \equiv 4 - 3 = 1 \mod 2^n - 1.$$

Finally, we have

$$\frac{e}{e-1} = 1 - \frac{1}{1-e} \equiv 2^n - \frac{3 \cdot 2^n - 4}{5} = \frac{2 \cdot 2^n + 4}{5} \mod 2^n - 1. \qquad \square$$

3.3.2 Glynn Exponents

3.3.2 Theorem (Transformations of the Glynn$_1$ Exponent)**.** *Let n be odd, so $n = 2l+1$ with $l \in \mathbb{N}$. Then for $e = 3 \cdot 2^{\frac{n+1}{2}} + 4 = 3 \cdot 2^{l+1} + 4$, the Glynn$_1$ o-exponent, the following*

relations, each taken $\mod 2^n-1$*, hold.*

$$\begin{aligned}
1-e &= 2^n - 3\cdot 2^{\frac{n+1}{2}} - 4,\\
\frac{1}{e} &= 3\cdot 2^{\frac{n-1}{2}} - 2,\\
\frac{e-1}{e} &= 2^n - 3\cdot 2^{\frac{n-1}{2}} + 2,\\
\frac{1}{1-e} &= \begin{cases} \frac{2^n - 2^{\frac{n+1}{2}}}{3} & : n \equiv 1 \mod 4,\\ 2^n - \frac{2^{\frac{n+1}{2}}+2}{3} & : n \equiv 3 \mod 4,\end{cases}\\
\frac{e}{e-1} &= \begin{cases} \frac{2\cdot 2^n + 2^{\frac{n+1}{2}}}{3} & : n \equiv 1 \mod 4,\\ \frac{2^{\frac{n+1}{2}}+2}{3} & : n \equiv 3 \mod 4.\end{cases}
\end{aligned}$$

Proof. The first relation is clear, as $2^n - 3\cdot 2^{\frac{n+1}{2}} - 4 \equiv 1 - 3\cdot 2^{\frac{n+1}{2}} - 4 \mod 2^n-1$. By consideration of the binary expansions of e^{-1} for small values of l, one can extrapolate the following form.

$$\begin{aligned}
x_l :&= (10\,\underbrace{1\,1\ldots 1}_{l-1\ \text{1s}}\,0)\\
&= 2^{l+1} + \sum_{j=0}^{l-2} 2^{1+j} = 2^{l+1} + 2\sum_{j=0}^{l-2} 2^{1+j}\\
&= 2^{l+1} + 2\cdot(2^{l-1}-1) = 3\cdot 2^l - 2 = 3\cdot 2^{\frac{n-1}{2}} - 2.
\end{aligned}$$

Direct computation verifies the validity of the formula:

$$\begin{aligned}
x_l \cdot e &= \left(3\cdot 2^l - 2\right)\cdot\left(3\cdot 2^{l+1}+4\right) = 9\cdot 2^{2l+1} + 12\cdot 2^l - 6\cdot 2^{l+1} - 8\\
&= 9\cdot 2^n + 12\cdot 2^l - 12\cdot 2^l - 8 \equiv 9 - 8 = 1 \mod 2^n - 1.
\end{aligned}$$

Further, it follows that

$$\frac{e-1}{e} = 1 - \frac{1}{e} \equiv 2^n - 3\cdot 2^{\frac{n-1}{2}} + 2 \mod 2^n - 1.$$

First, we consider the case $n \equiv 1 \mod 4$ by writing $n = 4\tilde{l}+1$ with $n \in \mathbb{N}$. Examples of $(1-e)^{-1}$ for small sizes of $\tilde{l}$ again lead to

$$\begin{aligned}
x_{\tilde{l}} :&= (\underbrace{10\,10\ldots 10}_{\tilde{l}\ \text{10 blocks}}\,\underbrace{0\,0\ldots 0}_{2\tilde{l}\ \text{0s}})_2\\
&= \sum_{j=0}^{\tilde{l}-1} 2^{2\tilde{l}+1+2j} = 2^{2\tilde{l}+1}\cdot\frac{4^{\tilde{l}}-1}{3}\\
&= \frac{2^{4\tilde{l}+1} - 2^{2\tilde{l}+1}}{3} = \frac{2^n - 2^{\frac{n+1}{2}}}{3}.
\end{aligned}$$

That is indeed the general form of $(1-e)^{-1}$, because

$$\begin{aligned}(1-e)\cdot x_{\tilde{l}} &\equiv \left(1-3\cdot 2^{2\tilde{l}+1}-4\right)\frac{1-2^{2\tilde{l}+1}}{3} = \left(-2^{2\tilde{l}+1}-1\right)\left(-2^{2\tilde{l}-1}+1\right)\\ &= 2^{4\tilde{l}+2}-1 \equiv 1 \mod 2^n-1.\end{aligned}$$

And we also have

$$\frac{e}{e-1} = 1-\frac{1}{1-e} \equiv 2^n - \frac{2^n-2^{\frac{n+1}{2}}}{3} = \frac{2\cdot 2^n+2^{\frac{n+1}{2}}}{3} \mod 2^n-1.$$

So, only the case $n \equiv 3 \mod 4$ remains and for that matter we write $n = 4\tilde{l}+3$ with $\tilde{l} \in \mathbb{N}_0$. By looking at the binary expansions of $(1-e)^{-1}$ for small values of $\tilde{l}$, we arrive at the following conjectured form:

$$\begin{aligned}x_{\tilde{l}} :&= (\underbrace{1\,1\,\ldots\,1}_{2\tilde{l}+1\ \text{1s}}\ \underbrace{10\,10\,\ldots\,10}_{\tilde{l}+1\ \text{10 blocks}})\\ &= \sum_{j=0}^{2\tilde{l}} 2^{2\tilde{l}+2+j} + \sum_{j=0}^{\tilde{l}} 2^{1+2j} = 2\cdot\frac{4^{\tilde{l}+1}-1}{3} + 2^{2\tilde{l}+2}\cdot\left(2^{2\tilde{l}+1}-1\right)\\ &= \frac{2^{2\tilde{l}+3}-2+3\cdot 2^{4\tilde{l}+3}-3\cdot 2^{2\tilde{l}+2}}{3}\\ &= \frac{3\cdot 2^n-2^{2\tilde{l}+2}-2}{3} = 2^n - \frac{2^{\frac{n+1}{2}}+2}{3}.\end{aligned}$$

This is the general form of $(1-e)^{-1}$, which can be verified by calculating

$$\begin{aligned}(1-e)\cdot x_{\tilde{l}} &\equiv \left(1-3\cdot 2^{2\tilde{l}+2}-4\right)\frac{1-2^{2\tilde{l}+2}}{3} = \left(-1-2^{2\tilde{l}+2}\right)\left(1-2^{2\tilde{l}+2}\right)\\ &= 2^{4\tilde{l}+4}-1 \equiv 1 \mod 2^n-1.\end{aligned}$$

Finally, we have

$$\frac{e}{e-1} = 1-\frac{1}{1-e} \equiv \frac{2^{\frac{n+1}{2}}+2}{3} \mod 2^n-1. \qquad \square$$

For the Glynn_2 o-exponent a distinction between $n \equiv 1 \mod 4$ and $n \equiv 3 \mod 4$ is necessary.

3.3.3 Theorem (Transformations of the Glynn_2 o-Exponent with $n \equiv 1 \mod 4$)**.** *Let $n = 4\tilde{l}+1$ with $\tilde{l} \in \mathbb{N}$. Then for $e = 2^{\frac{n+1}{2}}+2^{\frac{3n+1}{4}} = 2^{2\tilde{l}+1}+2^{3\tilde{l}+1}$, the Glynn_2 o-exponent,*

the following relations, each taken $\mod 2^n-1$*, hold.*

$$\begin{aligned}
1-e &= 2^n - 2^{\frac{3n+1}{4}} - 2^{\frac{n+1}{2}},\\
\frac{1}{e} &= 2^n - 2^{\frac{3n+1}{4}} + 2^{\frac{n+1}{2}} - 2^{\frac{n-1}{4}},\\
\frac{e-1}{e} &= 2^{\frac{3n+1}{4}} - 2^{\frac{n+1}{2}} + 2^{\frac{n-1}{4}},\\
\frac{1}{1-e} &= \begin{cases} 2^n - \frac{2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}+2}{3} & : n \equiv 1 \mod 8,\\ \frac{2^n-2^{\frac{3n+1}{4}}-2^{\frac{n+3}{4}}}{3} & : n \equiv 5 \mod 8, \end{cases}\\
\frac{e}{e-1} &= \begin{cases} \frac{2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}+2}{3} & : n \equiv 1 \mod 8,\\ \frac{2\cdot 2^n+2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}}{3} & : n \equiv 5 \mod 8. \end{cases}
\end{aligned}$$

Proof. The first relation is clear, since $2^n-2^{\frac{3n+1}{4}}-2^{\frac{n+1}{2}} \equiv 1-2^{\frac{n+1}{2}}+2^{\frac{3n+1}{4}} \mod 2^n-1$. Considering the binary expansion of e^{-1} for small values of l, one can conjecture the following form for e^{-1}:

$$\begin{aligned}
x_{\tilde{l}} :&= (\underbrace{1\ldots1}_{\tilde{l}\ 1\text{s}}\ \underbrace{0\ldots0}_{\tilde{l}\ 0\text{s}}\ \underbrace{1\ldots1}_{\tilde{l}+1\ 1\text{s}}\ \underbrace{0\ldots0}_{\tilde{l}\ 0\text{s}})\\
&= \sum_{j=0}^{\tilde{l}-1} 2^{3\tilde{l}+1+j} + \sum_{j=0}^{\tilde{l}} 2^{\tilde{l}+j} = 2^{4\tilde{l}+1} - 2^{3\tilde{l}+1} + 2^{2\tilde{l}+1} - 2^{\tilde{l}}\\
&= 2^n - 2^{\frac{3n+1}{4}} + 2^{\frac{n+1}{2}} - 2^{\frac{n-1}{4}}.
\end{aligned}$$

This can be verified by calculating

$$\begin{aligned}
e\cdot x_{\tilde{l}} &\equiv 2^{2\tilde{l}+1}\left(1+2^{\tilde{l}}\right)\left(1-2^{3\tilde{l}+1}+2^{2\tilde{l}+1}-2^{\tilde{l}}\right)\\
&= 2^{2\tilde{l}+1}\left(1-2^{3\tilde{l}+1}+2^{2\tilde{l}+1}-2^{\tilde{l}}+2^{2\tilde{l}}-2^{4\tilde{l}+1}+2^{3\tilde{l}+1}-2^{2\tilde{l}}\right)\\
&\equiv 2^{2\tilde{l}+1}\left(1+2^{2\tilde{l}}-1\right) = 2^{4\tilde{l}+1} \equiv 1 \mod 2^n-1.
\end{aligned}$$

Then we also have

$$\frac{e-1}{e} = 1-\frac{1}{e} \equiv 2^{3\tilde{l}+1}-2^{2\tilde{l}+1}+2^{\tilde{l}} = 2^{\frac{3n+1}{4}}-2^{\frac{n+1}{2}}+2^{\frac{n-1}{4}} \mod 2^n-1.$$

To obtain $(1-e)^{-1}$ we first start with the case that $n \equiv 1 \mod 8$ by writing $n = 8\hat{l}+1$

with $\hat{l} \in \mathbb{N}$. Sample binary expansions yield the following presumed form.

$$\begin{aligned} x_{\hat{l}} :&= (\underbrace{1 \ldots 1}_{2\hat{l}+1 \text{ 1s}} \underbrace{01\,01 \ldots 01}_{2\hat{l}-1 \text{ 01 blocks}} 00 \underbrace{10\,10 \ldots 10}_{\hat{l} \text{ 10 blocks}})_2 \\ &= \sum_{j=0}^{\hat{l}-1} 2^{1+2j} + \sum_{j=0}^{2\hat{l}-2} 2^{2\hat{l}+2+2j} + \sum_{j=0}^{2\hat{l}} 2^{6\hat{l}+j} \\ &= 2 \cdot \frac{4^{\hat{l}}-1}{3} + 2^{2\hat{l}+2} \cdot \frac{4^{2\hat{l}-1}-1}{3} + 2^{6\hat{l}} \cdot \left(2^{2\hat{l}+1}-1\right) \\ &= 2^{8\hat{l}+1} + \frac{1}{3}\left(2^{2\hat{l}+1} - 2 + 2^{6\hat{l}} - 2^{2\hat{l}+2} - 3 \cdot 2^{6\hat{l}}\right) \\ &= 2^n - \frac{2^{6\hat{l}+1} + 2^{2\hat{l}+1} + 2}{3} = 2^n - \frac{2^{\frac{3n+1}{4}} + 2^{\frac{n+3}{4}} + 2}{3}. \end{aligned}$$

Then we can calculate its validity as follows.

$$\begin{aligned} x_{\hat{l}} \cdot (1-e) &\equiv \frac{3 - 2^{6\hat{l}+1} - 2^{2\hat{l}+1} - 2}{3}\left(1 - 2^{6\hat{l}+1} - 2^{4\hat{l}+1}\right) \\ &= -\frac{1}{3}\left(2^{2\hat{l}+1} + 2^{2\hat{l}+1} - 1\right)\left(1 - 2^{6\hat{l}+1} - 2^{4\hat{l}+1}\right) \\ &= -\frac{1}{3}\left(\underline{2^{6\hat{l}+1}} - 2^{12\hat{l}+2} - 2^{10\hat{l}+2} + 2^{2\hat{l}+1} - 2^{8\hat{l}+2} \underline{-2^{6\hat{l}+2}} - 1 + \underline{2^{6\hat{l}+1}} + 2^{4\hat{l}+1}\right) \\ &\equiv -\frac{1}{3}\left(-2^{4\hat{l}+1} - 2^{2\hat{l}+1} + 2^{2\hat{l}+1} - 2 - 1 + 2^{4\hat{l}+1}\right) = 1 \mod 2^n - 1. \end{aligned}$$

Furthermore, we have

$$\frac{e}{e-1} = 1 - \frac{1}{1-e} \equiv \frac{2^{\frac{3n+1}{4}} + 2^{\frac{n+3}{4}} + 2}{3} \mod 2^n - 1.$$

Now, only the case $n \equiv 5 \mod 8$ remains. We write $n = 8\hat{l} + 5$ with $\hat{l} \in \mathbb{N}_0$. Considerations of the binary expansions of $(1-e)^{-1}$ for small values of $\hat{l}$ point to the following conjectured form.

$$\begin{aligned} x_{\hat{l}} :&= (\underbrace{10\,10 \ldots 10}_{\hat{l} \text{ 10 blocks}} \underbrace{01\,01 \ldots 01}_{2\hat{l}+1 \text{ 01 blocks}} \underbrace{0 \ldots 0}_{2\hat{l}+2 \text{ 0s}})_2 \\ &= \sum_{j=0}^{2\hat{l}} 2^{2\hat{l}+2+2j} + \sum_{j=0}^{\hat{l}-1} 2^{6\hat{l}+5+2j} = 2^{2\hat{l}+2} \cdot \frac{4^{2\hat{l}+1}-1}{3} + 2^{6\hat{l}+5} \cdot \frac{4^{\hat{l}}-1}{3} \\ &= \frac{2^{6\hat{l}+4} - 2^{2\hat{l}+2} + 2^{8\hat{l}+5} - 2^{6\hat{l}+5}}{3} \\ &= \frac{2^{8\hat{l}+5} - 2^{6\hat{l}+4} - 2^{2\hat{l}+2}}{3} = \frac{2^n - 2^{\frac{3n+1}{4}} - 2^{\frac{n+3}{4}}}{3}. \end{aligned}$$

That is the general form of $(1-e)^{-1}$, as

$$\begin{aligned} x_{\hat{l}} \cdot (1-e) &\equiv \frac{1}{3}\left(1-2^{6\hat{l}+4}-2^{2\hat{l}+2}\right)\left(1-2^{6\hat{l}+4}-2^{4\hat{l}+3}\right) \\ &= \frac{1}{3}\left(1\underline{-2^{6\hat{l}+4}}-2^{4\hat{l}+3}\underline{-2^{6\hat{l}+4}}+2^{12\hat{l}+8}+2^{10\hat{l}+7}-2^{2\hat{l}+2}+2^{8\hat{l}+6}+\underline{2^{6\hat{l}+5}}\right) \\ &\equiv \frac{1}{3}\left(1-2^{4\hat{l}+3}+2^{4\hat{l}+3}+2^{2\hat{l}+2}-2^{2\hat{l}+2}+2\right)=1 \mod 2^n-1. \end{aligned}$$

We also have

$$\frac{e}{e-1} = 1-\frac{1}{1-e} \equiv \frac{2\cdot 2^n+2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}}{3} \mod 2^n-1. \qquad \square$$

3.3.4 Theorem (Transformations of the Glynn$_2$ o-Exponent with $n \equiv 3 \mod 4$)**.** *Let $n = 4\tilde{l}+3$ with $\tilde{l} \in \mathbb{N}_0$. Then for $e = 2^{\frac{n+1}{2}}+2^{\frac{n+1}{4}} = 2^{2\tilde{l}+2}+2^{\tilde{l}+1}$, the Glynn$_2$ o-exponent, the following relations, each taken $\mod 2^n-1$, hold.*

$$\begin{aligned} 1-e &= 2^n-2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}}, \\ \frac{1}{e} &= 2^n-2^{\frac{3n-1}{4}}+2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}}, \\ \frac{e-1}{e} &= 2^{\frac{3n-1}{4}}-2^{\frac{n+1}{2}}+2^{\frac{n+1}{4}}, \\ \frac{1}{1-e} &= \begin{cases} 2^n-\frac{2^{\frac{3n+3}{4}}+2^{\frac{n+1}{4}}+2}{3} & : n \equiv 3 \mod 8, \\ \frac{2^n-2^{\frac{3n+3}{4}}-2^{\frac{n+1}{4}}}{3} & : n \equiv 7 \mod 8, \end{cases} \\ \frac{e}{e-1} &= \begin{cases} \frac{2^{\frac{3n+3}{4}}+2^{\frac{n+1}{4}}+2}{3} & : n \equiv 3 \mod 8, \\ \frac{2\cdot 2^n+2^{\frac{3n+3}{4}}+2^{\frac{n+1}{4}}}{3} & : n \equiv 7 \mod 8. \end{cases} \end{aligned}$$

Proof. The first relation is clear, as $2^n-2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}} \equiv 1-2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}} \mod 2^n-1$. For the second relation, the binary expansions of e^{-1} for small values of $\tilde{l}$ suggest the following general form.

$$\begin{aligned} x_{\tilde{l}} &:= (\underbrace{1\ldots1}_{\tilde{l}+1\ 1\mathrm{s}}\ \underbrace{0\ldots0}_{\tilde{l}\ 0\mathrm{s}}\ \underbrace{1\ldots1}_{\tilde{l}+1\ 1\mathrm{s}}\ \underbrace{0\ldots0}_{\tilde{l}+1\ 0\mathrm{s}})_2 \\ &= \sum_{j=0}^{\tilde{l}} 2^{\tilde{l}+1+j}+\sum_{j=0}^{\tilde{l}} 2^{3\tilde{l}+2+j} = 2^{\tilde{l}+1}\sum_{j=0}^{\tilde{l}} 2^j + 2^{3\tilde{l}+2}\sum_{j=0}^{\tilde{l}} 2^j \\ &= 2^{4\tilde{l}+3}-2^{3\tilde{l}+2}+2^{2\tilde{l}+2}-2^{\tilde{l}+1} = 2^n-2^{\frac{3n-1}{4}}+2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}}. \end{aligned}$$

This is indeed the general form, as the following computation shows.

$$\begin{aligned} x_{\tilde{l}} \cdot e &\equiv \left(1 - 2^{3\tilde{l}+2} + 2^{2\tilde{l}+2} - 2^{\tilde{l}+1}\right)\left(2^{2\tilde{l}+2} + 2^{\tilde{l}+1}\right) \\ &= 2^{2\tilde{l}+2} + 2^{\tilde{l}+1} - 2^{5\tilde{l}+4} - 2^{4\tilde{l}+3} + 2^{4\tilde{l}+4} + 2^{3\tilde{l}+3} - 2^{3\tilde{l}+3} - 2^{2\tilde{l}+2} \\ &\equiv 2^{\tilde{l}+1} - 2^{\tilde{l}+1} - 1 + 2 = 1 \mod 2^n - 1. \end{aligned}$$

Thus we also have

$$\frac{e-1}{e} = 1 - \frac{1}{e} \equiv 2^{\frac{3n-1}{4}} - 2^{\frac{n+1}{2}} + 2^{\frac{n+1}{4}} \mod 2^n - 1.$$

To obtain $(1-e)^{-1}$, we consider the case $n \equiv 3 \mod 8$ first by writing $n = 8\hat{l}+3$ with $\hat{l} \in \mathbb{N}_0$. Sample binary expansions for small values of $\hat{l}$ indicate the following general form.

$$\begin{aligned} x_{\hat{l}} :&= (\underbrace{1 \ldots 1}_{2\hat{l}+1 \text{ 1s}} \underbrace{01 \ldots 01}_{2\hat{l} \text{ 01 blocks}} 00 \underbrace{10 \ldots 10}_{\hat{l} \text{ 10 blocks}})_2 \\ &= \sum_{j=0}^{\hat{l}-1} 2^{1+2j} + \sum_{j=0}^{2\hat{l}-1} 2^{2\hat{l}+2+2j} + \sum_{j=0}^{2\hat{l}} 2^{6\hat{l}+2+j} \\ &= 2 \cdot \frac{4^{\hat{l}} - 1}{3} + 2^{2\hat{l}+2}\frac{4^{2\hat{l}} - 1}{3} + 2^{6\hat{l}+2} \cdot \left(2^{2\hat{l}+1} - 1\right) \\ &= 2^{8\hat{l}+3} + \frac{1}{3}\left(2^{2\hat{l}+1} - 2 + 2^{6\hat{l}+2} - 2^{2\hat{l}+2} - 3 \cdot 2^{6\hat{l}+2}\right) \\ &= 2^{8\hat{l}+3} - \frac{2^{6\hat{l}+3} + 2^{2\hat{l}+1} + 2}{3} = 2^n - \frac{2^{\frac{3n+3}{4}} + 2^{\frac{n+1}{4}} + 2}{3}. \end{aligned}$$

This is indeed the general form of $(1-e)^{-1}$, since we have

$$\begin{aligned} (1-e) \cdot x_{\hat{l}} &\equiv \left(1 - 2^{4\hat{l}+2} - 2^{2\hat{l}+1}\right)\frac{1 - 2^{6\hat{l}+3} - 2^{2\hat{l}+1}}{3} \\ &= \frac{1}{3}\left(1 - \underline{2^{6\hat{l}+3}} - \underline{2^{2\hat{l}+1}} - \underline{2^{4\hat{l}+2}} + \underline{2^{10\hat{l}+5}} + \underline{2^{6\hat{l}+3}} - \underline{2^{2\hat{l}+1}} + 2^{8\hat{l}+4} + \underline{2^{4\hat{l}+2}}\right) \\ &\equiv \frac{1}{3}(1+2) = 1 \mod 2^n - 1. \end{aligned}$$

Therefore we also have

$$\frac{e}{e-1} = 1 - \frac{1}{1-e} \equiv \frac{2^{\frac{3n+3}{4}} + 2^{\frac{n+1}{4}} + 2}{3} \mod 2^n - 1.$$

Now, only the case $n \equiv 7 \mod 8$ remains to be considered. We write $n = 8\hat{l}+7$ with

$\hat{l} \in \mathbb{N}_0$ and binary expansions of $(1-e)^{-1}$ for small $\hat{l}$ reveal the following form.

$$\begin{aligned} x_{\hat{l}} :&= (\underbrace{10\,10\,\ldots\,10}_{\hat{l}\text{ 10 blocks}}\,\underbrace{01\,01\,\ldots\,01}_{2\hat{l}+2\text{ 01 blocks}}\,\underbrace{0\,0\,\ldots\,0}_{2\hat{l}+2\text{ 0s}})_2 \\ &= \sum_{j=0}^{2\hat{l}+1} 2^{2\hat{l}+2+2j} + \sum_{j=0}^{\hat{l}-1} 2^{6\hat{l}+7+2j} \\ &= 2^{2\hat{l}+2}\frac{4^{2\hat{l}+2}-1}{3} + 2^{6\hat{l}+7}\frac{4^{\hat{l}}-1}{3} \\ &= \frac{2^{8\hat{l}+7} - 2^{6\hat{l}+7} + 2^{6\hat{l}+6} - 2^{2\hat{l}+2}}{3} \\ &= \frac{2^{8\hat{l}+7} - 2^{6\hat{l}+6} - 2^{2\hat{l}+2}}{3} = \frac{2^n - 2^{\frac{3n+3}{4}} - 2^{\frac{n+1}{4}}}{3}. \end{aligned}$$

That is indeed the general form, as we have

$$\begin{aligned} (1-e)\cdot x_{\hat{l}} &\equiv \frac{1}{3}\left(1 - 2^{4\hat{l}+4} - 2^{2\hat{l}+2}\right)\left(1 - 2^{6\hat{l}+6} - 2^{2\hat{l}+2}\right) \\ &= \frac{1}{3}\left(1 - \underline{2^{6\hat{l}+6}} - \underline{2^{2\hat{l}+2}} - \underline{2^{4\hat{l}+4}} + \underline{2^{10\hat{l}+10}} + \underline{2^{6\hat{l}+6}} - \underline{2^{2\hat{l}+2}} + 2^{8\hat{l}+8} + \underline{2^{4\hat{l}+4}}\right) \\ &\equiv \frac{1}{3}(1+2) = 1 \mod 2^n - 1. \end{aligned}$$

Finally, we have

$$\frac{e}{e-1} = 1 - \frac{1}{1-e} \equiv \frac{2\cdot 2^n + 2^{\frac{3n+3}{4}} + 2^{\frac{n+1}{4}}}{3} \mod 2^n - 1. \qquad \square$$

3.3.3 Translation Exponents

Here the situation is somewhat trickier, at least for the $(1-e)^{-1}$ case. The reason is that if $e = 2^h$ with $\gcd(n,h) = 1$, the least positive residue of $(1-e)^{-1} \mod 2^n - 1$ carries a lot of information about $h^{-1} \mod n$ as well. We begin with some general observations about $(1-e)^{-1}$.

3.3.5 Lemma. *Let $n \in \mathbb{N}$ and $h \in \mathbb{N}$ with $\gcd(n,h) = 1$. Then for $e = 2^h$ there exists a unique number $a(n,h) \in \{1, \ldots, 2^h - 2\}$ such that*

$$x_{n,h} := \frac{a(n,h)\cdot 2^n - (a(n,h)+1)}{2^h - 1} \in \{1, \ldots, 2^n - 2\}$$

is the least positive residue of $(1-e)^{-1} \mod 2^n - 1$.

Proof. We first show that there is a number $a(n,h)$ such that $a(n,h)\cdot 2^n - (a(n,h)+1)$ is divisible by $2^h - 1$, or equivalently, that $a(n,h)\cdot 2^n - (a(n,h)+1) \equiv 0 \mod 2^h - 1$ holds. Since $\gcd(n,h) = 1$ implies $\gcd(2^n - 1, 2^h - 1) = 1$, we have that

$$a(n,h) \equiv (2^n - 1)^{-1} \mod 2^h - 1$$

has a unique solution $a(n,h) \in \{1,\ldots,2^h-2\}$.

That $(1-e)^{-1}$ is given by $x_{n,h}$ is immediate from

$$\left(1-2^h\right)\frac{a(n,h)\cdot 2^n-(a(n,h)+1)}{2^h-1} \equiv a(n,h)+1-a(n,h)=1 \mod 2^n-1.$$

And finally, we have

$$0<\frac{a(n,h)\cdot 2^n-(a(n,h)+1)}{2^h-1}=\frac{a(n,h)\cdot(2^n-1)-1}{2^h-1}<2^n-1-\frac{1}{2^h-1}<2^n-1$$

and thus that $x_{n,h}$ is the least positive residue. □

3.3.6 Lemma (Special Cases)**.** *Let $n,h \in \mathbb{N}$ with $\gcd(n,h)=1$. Then for $a(n,h)$ from Lemma 3.3.5 the following statements hold.*

1. $a(n,h)=1$ *if* $n \equiv 1 \mod h$.
2. $a(n,h)=2^h-3$ *if* $n \equiv -1 \mod h$.
3. $a(n,h)=\frac{2\cdot 2^h-1}{3}$ *if* $n \equiv 2 \mod h$.

Proof. We verify by computation that $a(n,h)\cdot 2^n-(a(n,h)+1)$ is divisible by 2^h-1 in each case.

1. We have $n=l\cdot h+1$ with $l \in \mathbb{N}$. Then we have
$$2^{l\cdot h+1}-2 \equiv 2\cdot\left(2^h\right)^l-2 \equiv 2-2=0 \mod 2^h-1.$$
2. We have $n=l\cdot h-1$ with $l \in \mathbb{N}$ and thus
$$\left(2^h-3\right)2^{l\cdot h-1}-2^h+2 \equiv (-2)\cdot 2^{l\cdot h-1}-1+2 \equiv -1-1+2=0 \mod 2^h-1.$$
3. We have $n=l\cdot h+2$ with $l \in \mathbb{N}$ and h must be odd, since $\gcd(n,h)=1$. Then $2^{h+1}-1$ is divisible by 3, since $2^{h+1}-1 \equiv (-1)^{h+1}-1 \equiv 1-1=0 \mod 3$. Therefore,
$$\begin{aligned}\frac{2\cdot 2^{h-1}-1}{3}\cdot 2^h-\left(\frac{2\cdot 2^h-1}{3}+1\right) &\equiv \frac{2-1}{3}\cdot 2^2-\frac{2-1}{3}-1\\ &\equiv 1-1\equiv 0 \mod 2^h-1.\end{aligned}$$
□

One way of calculating $a(n,h)$ could be via recursion.

3.3.7 Lemma. *Let $n,h \in \mathbb{N}$ with $\gcd(n,h)=1$ and $n \equiv t \mod h$. Then for $a(n,h)$ from Lemma 3.3.5*

$$a(n,h) \equiv \left(2^t-1\right)^{-1} \equiv 2^h-1-\frac{a(h,t)\cdot 2^h-(a(h,t)+1)}{2^t-1} \mod 2^h-1$$

holds.

Proof. The condition $a(n,h)2^n - (a(n,h)+1) \equiv 0 \mod 2^h - 1$ implies

$$a(n,h) \equiv (2^n - 1)^{-1} \mod 2^h - 1,$$

so it is the same problem (with a flipped sign and smaller modulus). □

Very conveniently for us, Kyureghyan and Suder [27] give a more explicit result.

3.3.8 Theorem ([27, Theorem 3.12])**.** *Let $n, h \in \mathbb{N}$ with $\gcd(n,h) = 1$ and let h_n^{-1} be least positive residue of $h^{-1} \mod n$. Then*

$$(1-2^h)^{-1} \equiv 2^n - 1 - \sum_{i=0}^{h_n^{-1}-1} 2^{hi} \mod n \mod 2^n - 1$$

holds.

3.3.9 Theorem (Transformations of the Translation o-Exponents)**.** *Let $n, h \in \mathbb{N}$ with $\gcd(n,h) = 1$ and let $h_n^{-1} \in \{1, \ldots, n-1\}$ be the least positive residue of $h^{-1} \mod n$. Then for the translation o-exponent $e = 2^h$ the following relations, taken $\mod 2^n - 1$ each, hold.*

$$\begin{aligned}
1 - e &= 2^n - 2^h \\
e^{-1} &= 2^{n-h} \\
\frac{e-1}{e} &= 2^n - 2^{n-h} \\
(1-e)^{-1} &= 2^n - 1 - \sum_{i=0}^{h_n^{-1}-1} 2^{hi} \mod n \\
\frac{e}{e-1} &= 1 + \sum_{i=0}^{h_n^{-1}-1} 2^{hi} \mod n.
\end{aligned}$$

Proof. The first relation is clear, since $2^n - 2^h \equiv 1 - 2^h \mod 2^n - 1$, the second relation is also clear, as $2^{n-h} \cdot 2^h = 2^n \equiv 1 \mod 2^n - 1$, and the third follows from $\frac{e-1}{e} = 1 - e^{-1}$. Theorem 3.3.8 yields the fourth relation and the last one follows from $\frac{e}{e-1} = 1 - \frac{1}{1-e}$. □

4 Application: 2-to-1 Binomials

This last chapter deals with an application of o-polynomials: They are naturally related to the 2-to-1 polynomials and thus allow constructing 2-to-1 polynomials.

This connection stems from the property that no three points of the corresponding hyperoval are collinear, meaning that we can generalize it to ovals in odd characteristic as well, allowing for similar investigations in that case in the second section.

As we deal with both even and odd characteristic in this chapter, we carefully specify whether q is an odd or even prime power when necessary.

A central tool in this chapter is examining specific lines of $\mathrm{PG}(2,q)$. For that purpose, recall the lines of $\mathrm{PG}(2,q)$ and their representations:

- $l_{a,b} = \left\langle \begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \right\rangle^{\perp}$ for $a, b \in \mathbb{F}_q$,
- $l_a = \left\langle \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix} \right\rangle^{\perp}$ for $a \in \mathbb{F}_q$, and
- $l_\infty = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle^{\perp}$.

4.1 Even Characteristic

The goal of this section is to find many different 2-to-1 binomials using o-monomials. To that matter, we first relate o-polynomials to a family of 2-to-1 polynomials, show that one 2-to-1 binomial already induces such a family of 2-to-1 binomials and thus an o-monomial and finally apply this to the results of Section 3.3.

4.1.1 The 2-to-1 Characterization

In this subsection we give a characterization of o-polynomials using 2-to-1 polynomials, employing mostly combinatorial arguments.

4.1.1 Definition. Let q be even. The polynomial $f \in \mathbb{F}_q[x]$ is called *2-to-1* if every element of $\mathbb{F}_q$ has either zero or two preimages under f.

An equivalent formulation is that the equation $f(x) = a$ has either zero or two solutions for each $a \in \mathbb{F}_q$. In relation to this property we have the following characterization: A polynomial f is an o-polynomial if and only if the polynomial $f(x) + bx$ is 2-to-1 for all $b \in \mathbb{F}_q$.

The key idea is that the solutions of the equation

$$f(x) + bx = a$$

correspond to the points of $\mathcal{H}(f)$ on the lines $l_{a,b}$ of $\mathrm{PG}(2,q)$. Intuitively, $f(x)+bx$ being 2-to-1 for all $b \in \mathbb{F}_q^*$ is equivalent to on most lines being exactly zero or two points.

To make the argument rigorous we need a converse statement to Lemma 2.1.3, characterizing hyperovals by the number of their external lines. Before proving this we start by giving a counting lemma, which continues to be useful in Subsection 4.2.2 as well. This argumentation is due to Maschietti [29].

4.1.2 Lemma. *Let q be a prime power, S be a set of m points in $\mathrm{PG}(2,q)$ and k be the maximal number of collinear points from S. Further, let τ_i be the number of lines containing exactly i points for $i = 0, 1, \ldots, k$. Then the following equalities hold.*

$$\sum_{i=0}^{k} \tau_i = q^2 + q + 1, \tag{4.1}$$

$$\sum_{i=1}^{k} i\tau_i = m(q+1), \tag{4.2}$$

$$\sum_{i=2}^{k} (i-1)i\tau_i = m(m-1). \tag{4.3}$$

Further, for the tangents of S we have

$$\tau_1 = m(q+1) - m(m-1) + \sum_{i=2}^{k} (i^2 - 2i)\tau_i. \tag{4.4}$$

Proof. Equation (4.1) is obtained by counting every line of $\mathrm{PG}(2,q)$ exactly once.

Let us introduce some more notation. Let T_i be the set of lines containing exactly i points of S. Then $|T_i| = \tau_i$.

For Equation (4.2) we count the pairs (l, P), where $P \in S$ and l is a line containing the point P. On the one hand, for $l \in T_i$, there are i different points on l, so we can count the number of pairs to be $\sum_{i=1}^{k} i\tau_i$. On the other hand, each point of S lies on exactly $q+1$ lines, so we obtain $m(q+1)$ pairs.

For Equation (4.3) we count the pairs (l, P_1, P_2), where P_1 and P_2 are distinct points of S and l is a line containing both points. On a line $l \in T_i$ we can choose two points from the i points available, so we have $\sum_{i=2}^{k} i(i-1)\tau_i$ pairs overall. But we may also choose two distinct points P_1 and P_2 from S, fixing the unique line connecting them. Thus we obtain $m(m-1)$ pairs.

Finally, subtracting (4.3) from (4.2) yields

$$\sum_{i=1}^{k} i\tau_i - \sum_{i=2}^{k} (i-1)i\tau_i = \tau_1 + \sum_{i=2}^{k} (-i^2 + 2i)\tau_i = m(q+1) - m(m-1)$$

and thus Equation (4.4). □

4.1.3 Theorem. *A set $\mathcal{H}$ of $q+2$ points of $\mathrm{PG}(2,q)$, q even, is a hyperoval if and only if there are $\tau_0 = \frac{q(q-1)}{2}$ external lines to $\mathcal{H}$.*

Proof. The if part has already been covered in Lemma 2.1.3, so let $\mathcal{H}$ be a $(q+2)$-set of points of $\mathrm{PG}(2,q)$ with exactly $\tau_0 = \frac{q(q-1)}{2}$ external lines. Reusing the notation from Lemma 4.1.2 and applying it with $m = q+2$ yields

$$\sum_{i=1}^{k} \tau_i = q^2 + q + 1, \tag{4.5}$$

$$\sum_{i=2}^{k} i(i-1)\tau_i = (q+2)(q+1), \tag{4.6}$$

$$\tau_1 = \sum_{i=2}^{k} (i^2 - 2i)\tau_i. \tag{4.7}$$

Substituting τ_0 and τ_1 into (4.5), one obtains

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

and thus

$$\sum_{i=2}^{k} (2i^2 - 4i + 2)\tau_i = q^2 + 3q + 2 = (q+2)(q+1). \tag{4.8}$$

Finally, by subtracting Equation (4.6) from (4.8) we get

$$\sum_{i=3}^{k} (i^2 - 3i + 2)\tau_i = 0,$$

as $2^2 - 3 \cdot 2 + 2 = 0$. Since $i^2 - 3i + 2 > 0$ for $i \geq 3$, we have $\tau_i = 0$ for $i \geq 3$. So, no three points of $\mathcal{H}$ are collinear and $\mathcal{H}$ is therefore a hyperoval. □

We are now able to prove the already mentioned characterization.

4.1.4 Theorem. *Let q be even. The polynomial $f \in \mathbb{F}_q[x]$ is an o-polynomial if and only if the polynomial $f(x) + bx$ is 2-to-1 for all $b \in \mathbb{F}_q^*$.*

Proof. Let f be an o-polynomial and consider the lines $l_{a,b}$ for $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. Then $(0,1,0), (0,0,1) \notin l_{a,b}$. A point $(1, t, f(t)) \in \mathcal{H}(f)$ with $t \in \mathbb{F}_q$ is on $l_{a,b}$ if and only if

$$\begin{pmatrix} 1 \\ t \\ f(t) \end{pmatrix} \in \left\langle \begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \right\rangle^{\perp},$$

that is, if and only if

$$a + bt + f(t) = 0.$$

Since $\mathcal{H}(f)$ is a hyperoval, this equation has exactly zero or two solutions for each $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$, so the polynomials $f(x) + bx$ are 2-to-1 for all $b \in \mathbb{F}_q^*$.

Now let $f \in \mathbb{F}_q[x]$ so that the polynomial $f(x) + bx$ is 2-to-1 for each $b \in \mathbb{F}_q^*$. Then $\mathcal{H}(f)$ is a $(q+2)$-set, so we may apply Theorem 4.1.3. We have $(0,0,1) \in l_\infty, l_a$ and $(0,1,0) \in l_{a,0}$. Consider a fixed $b \in \mathbb{F}_q^*$. Since $f(x) + bx$ is 2-to-1, there are exactly $\frac{q}{2}$ values for $a \in \mathbb{F}_q$ such that

$$a + bx + f(x) = 0$$

has no solution in $\mathbb{F}_q$. For those values of a the line $l_{a,b}$ is an external line. All in all, we obtain $\frac{q(q-1)}{2}$ external lines. Therefore $\mathcal{H}(f)$ is a hyperoval and f an o-polynomial. □

4.1.2 Equivalence of 2-to-1 Binomials and o-Monomials

In this subsection we show that every 2-to-1 binomial may be traced back to an o-monomial. The important idea is that the property of $x^e + bx^d$ being 2-to-1 for some $b \in \mathbb{F}_q^*$ is already strong enough to imply that $x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. Once this is established, we may conclude using the characterization from Theorem 4.1.3 proved in the last subsection. This subsection follows very closely [25].

4.1.5 Lemma. *Let q be even, $0 < e \neq d$, $b \in \mathbb{F}_q^*$ and assume that $f(x) = x^e + bx^d \in \mathbb{F}_q[x]$ is 2-to-1. Then* $\gcd(e-d, q-1) = 1$.

Proof. We have $f(0) = 0$, so there is exactly one more element $t \in \mathbb{F}_q^*$ satisfying $f(t) = 0$. So, consider

$$f(t) = t^d \left(t^{e-d} + b\right) \stackrel{!}{=} 0.$$

This equation has either one or $1 + \gcd(e-d, q-1)$ solutions, so $\gcd(e-d, q-1) = 1$ follows. □

4.1.6 Theorem. *Let q be even, $0 < e \neq d$, $b \in \mathbb{F}_q^*$ and assume that $f_b(x) = x^e + bx^d \in \mathbb{F}_q[x]$ is 2-to-1. Then* $\gcd(e, q-1) = \gcd(d, q-1) = 1$ *and $f_{b'}(x) = x^e + b'x^d$ is 2-to-1 for all $b' \in \mathbb{F}_q^*$.*

Proof. Take $b' \in \mathbb{F}_q^*$. The goal is to show that $f_{b'}(x)$ is 2-to-1.

Firstly, because $f_b(x)$ is 2-to-1, by Lemma 4.1.5 we have $\gcd(e-d, q-1) = 1$. Since we have

$$f_{b'}(x) = x^e \left(1 + b'x^{d-e}\right)$$

it follows that $f_{b'}(x) = 0$ if and only if $x = 0$ or x is the unique nonzero solution of $b'x^{d-e} = 1$, so 0 has exactly two preimages under $f_{b'}$. Thus we will assume $x \neq 0$ and $b'x^{d-e} \neq 1$ from now on.

Consider for a fixed $x \in \mathbb{F}_q$ with $x \neq 0$ and $b'x^{d-e} \neq 1$ the equation

$$f_{b'}(x) = f_{b'}(\alpha x) \tag{4.9}$$

in $\alpha \in \mathbb{F}_q^*$. Then the polynomial $f_{b'}(x)$ is 2-to-1 if and only if Equation (4.9) has exactly two solutions: $\alpha = 1$ and one other solution $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$. Since $x \neq 0$, by dividing

through x^d Equation (4.9) is seen to be equivalent to

$$1 + b'x^{d-e} \stackrel{!}{=} \alpha^e \left(1 + b'\alpha^{d-e}x^{d-e}\right) = \alpha^e + b'\alpha^d x^{d-e}$$

and thus equivalent to

$$1 + \alpha^e = (1 + \alpha^d)b'x^{d-e}. \tag{4.10}$$

Next we show $\gcd(d, q-1) = \gcd(e, q-1) = 1$. For a contradiction, assume $\gcd(e, q-1) > 1$ for now. Then there is an element $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ such that the left-hand side of (4.10) vanishes. Thus we also have $1+\alpha^d = 0$, since $b'x^{d-e} \neq 0$ for $x \neq 0$. In particular, we have $\alpha^e = 1$ and $\alpha^d = 1$, so $\alpha^{e-d} = 1$ as well. Because $\gcd(e-d, q-1) = 1$, this is only possible for $\alpha = 1$, hence $\gcd(e, q-1) = 1$. Then $\alpha^d = 1$ if and only if $\alpha = 1$, since the left-hand side vanishes only for $\alpha = 1$. Therefore, $\alpha \mapsto \alpha^d$ is a permutation of $\mathbb{F}_q$ and we have $\gcd(d, q-1) = 1$ as well.

Now, if $\alpha \neq 1$, then $\alpha^e \neq 1$, so by dividing Equation (4.10) by $\alpha^d + 1$ we obtain the following: The polynomial $f_{b'}(x)$ is 2-to-1 if and only if for each fixed $x \in \mathbb{F}_q$ with $x \neq 0$ and $b'x^{d-e} \neq 1$ the equation

$$b'x^{d-e} = \frac{\alpha^e + 1}{\alpha^d + 1} \tag{4.11}$$

has exactly one solution $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$. Defining $T := \left\{\frac{\alpha^e+1}{\alpha^d+1} : \alpha \in \mathbb{F}_q \setminus \{0, 1\}\right\}$, this is equivalent to $T = \mathbb{F}_q \setminus \{0, 1\}$, since $\gcd(e-d, q-1) = 1$.

Fortunately, T does not depend on b', so we may take $b' = b$ to determine T completely. As $f_b(x)$ is 2-to-1 by assumption, $T = \mathbb{F}_q \setminus \{0, 1\}$ follows. We conclude that $f_{b'}(x)$ is 2-to-1 for all $b' \in \mathbb{F}_q^*$. □

4.1.7 Corollary. *For $0 < e \neq d$ the following three statements are equivalent:*

1. *The polynomial $f_b(x) = x^e + bx^d$ is 2-to-1 for a value $b \in \mathbb{F}_q^*$.*
2. *The polynomial $f_b(x) = x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$.*
3. *The monomial $x^{\frac{e}{d}}$ is an o-monomial, provided $\gcd(d, q-1) = 1$.*

Proof. The equivalence of the first two statements is immediate from Theorem 4.1.6. If $f_b(x)$ is 2-to-1 for all $b \in \mathbb{F}_q$, then by Theorem 4.1.6 $\gcd(d, q-1) = 1$. Therefore, we can substitute $x \mapsto x^{\frac{1}{d}}$ and obtain that $g_b(x) = x^{\frac{e}{d}} + bx$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. By the characterization of Theorem 4.1.4 this is equivalent to $x^{\frac{e}{d}}$ being an o-monomial.

Conversely, $x^{\frac{e}{d}}$ being an o-monomial implies that $g_b(x) = x^{\frac{e}{d}} + bx$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. The reverse substitution $x \mapsto x^d$ now yields $f_b(x) = x^e + bx^d$ being 2-to-1 for all $b \in \mathbb{F}_q^*$. □

4.1.3 2-to-1 Binomials from o-Monomials

To obtain many different families of 2-to-1 binomials we now apply Corollary 4.1.7 to the explicit formulas given in Section 3.3.

4.1.8 Theorem (2-to-1 Binomials Induced by Segre o-Monomials)**.** *Let $n \in \mathbb{N}$ be odd and let $e = 6$ be the Segre o-exponent. Then the following binomials are 2-to-1 for all $b \in \mathbb{F}_q^*$.*

o-exponent	*induced 2-to-1 binomials*
e	$x^6 + bx$
$1-e$	$x^{2^n-6} + bx$
$\frac{1}{e}$	$x^{\frac{5\cdot 2^{n-1}-2}{3}} + bx$
$\frac{e-1}{e}$	$x^{\frac{2^{n-1}+2}{3}} + bx$
$\frac{1}{1-e}$	$x^{\frac{2^n-2}{5}} + bx$ *if* $n \equiv 1 \mod 4$ $x^{\frac{3\cdot 2^n-4}{5}} + bx$ *if* $n \equiv 3 \mod 4$
$\frac{e}{e-1}$	$x^{\frac{4\cdot 2^n+2}{5}} + bx$ *if* $n \equiv 1 \mod 4$ $x^{\frac{2\cdot 2^n+4}{5}} + bx$ *if* $n \equiv 3 \mod 4$

4.1.9 Theorem (2-to-1 Binomials Induced by Glynn_1 o-Monomials)**.** *Let $n \in \mathbb{N}$ be odd and let $e = 3 \cdot 2^{\frac{n+1}{2}} + 4$ be the Glynn₁ o-exponent. Then the following binomials are 2-to-1 for all $b \in \mathbb{F}_q^*$.*

o-exponent	*induced 2-to-1 binomials*
e	$x^{3\cdot 2^{\frac{n+1}{2}}+4} + bx$
$1-e$	$x^{2^n-3\cdot 2^{\frac{n+1}{2}}-4} + bx$
$\frac{1}{e}$	$x^{3\cdot 2^{\frac{n-1}{2}}-2} + bx$
$\frac{e-1}{e}$	$x^{2^n-3\cdot 2^{\frac{n-1}{2}}+2} + bx$
$\frac{1}{1-e}$	$x^{\frac{2^n-2^{\frac{n+1}{2}}}{3}} + bx$ *if* $n \equiv 1 \mod 4$ $x^{2^n-\frac{2^{\frac{n+1}{2}}+2}{3}} + bx$ *if* $n \equiv 3 \mod 4$
$\frac{e}{e-1}$	$x^{\frac{2\cdot 2^n+2^{\frac{n+1}{2}}}{3}} + bx$ *if* $n \equiv 1 \mod 4$ $x^{\frac{2^{\frac{n+1}{2}}+2}{3}} + bx$ *if* $n \equiv 3 \mod 4$

4.1.10 Theorem (2-to-1 Binomials Induced by Glynn_2 o-Monomials)**.** *Let n be odd*

and e be the Glynn$_2$ o-exponent. Then the following binomials are 2-to-1 for all $b \in \mathbb{F}_q^*$.

o-exponent	*induced 2-to-1 binomials*
e	$x^{2^{\frac{n+1}{2}}+2^{\frac{3n+1}{4}}} + bx$ *if* $n \equiv 1 \mod 4$
	$x^{2^{\frac{n+1}{2}}+2^{\frac{n+1}{4}}} + bx$ *if* $n \equiv 3 \mod 4$
$1-e$	$x^{2^n-2^{\frac{3n+1}{4}}-2^{\frac{n+1}{2}}} + bx$ *if* $n \equiv 1 \mod 4$
	$x^{2^n-2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}}} + bx$ *if* $n \equiv 3 \mod 4$
$\frac{1}{e}$	$x^{2^n-2^{\frac{3n+1}{4}}+2^{\frac{n+1}{2}}-2^{\frac{n-1}{4}}} + bx$ *if* $n \equiv 1 \mod 4$
	$x^{2^n-2^{\frac{3n-1}{4}}+2^{\frac{n+1}{2}}-2^{\frac{n+1}{4}}} + bx$ *if* $n \equiv 3 \mod 4$
$\frac{e-1}{e}$	$x^{2^{\frac{3n+1}{4}}-2^{\frac{n+1}{2}}+2^{\frac{n-1}{4}}} + bx$ *if* $n \equiv 1 \mod 4$
	$x^{2^{\frac{3n-1}{4}}-2^{\frac{n+1}{2}}+2^{\frac{n+1}{4}}} + bx$ *if* $n \equiv 3 \mod 4$
$\frac{1}{1-e}$	$x^{2^n-\frac{2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}+2}{3}} + bx$ *if* $n \equiv 1 \mod 8$
	$x^{2^n-\frac{2^{\frac{3n+3}{4}}+2^{\frac{n+1}{4}}+2}{3}} + bx$ *if* $n \equiv 3 \mod 8$
	$x^{\frac{2^n-2^{\frac{3n+1}{4}}-2^{\frac{n+3}{4}}}{3}} + bx$ *if* $n \equiv 5 \mod 8$
	$x^{\frac{2^n-2^{\frac{3n+3}{4}}-2^{\frac{n+1}{4}}}{3}} + bx$ *if* $n \equiv 7 \mod 8$
$\frac{e}{e-1}$	$x^{\frac{2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}+2}{3}} + bx$ *if* $n \equiv 1 \mod 8$
	$x^{\frac{2^{\frac{3n+3}{4}}+2^{\frac{n+1}{4}}+2}{3}} + bx$ *if* $n \equiv 3 \mod 8$
	$x^{\frac{2\cdot 2^n+2^{\frac{3n+1}{4}}+2^{\frac{n+3}{4}}}{3}} + bx$ *if* $n \equiv 5 \mod 8$
	$x^{\frac{2\cdot 2^n+2^{\frac{3n+3}{4}}+2^{\frac{n+1}{4}}}{3}} + bx$ *if* $n \equiv 7 \mod 8$

4.1.11 Theorem (2-to-1 Binomials Induced by Translation o-Monomials)**.** *Let $n, h \in \mathbb{N}$ with $\gcd(n,h) = 1$ and let $h_n^{-1} \in \{1, \ldots, n-1\}$ be the least positive residue of $h^{-1} \mod n$. Then for the translation o-exponent $e = 2^h$, setting $t = \sum_{i=0}^{h_n^{-1}-1} 2^{hi \mod n}$, the following binomials are 2-to-1 for all $b \in \mathbb{F}_q^*$.*

o-exponent	*induced 2-to-1 binomials*
e	$x^{2^h} + bx$
$1 - e$	$x^{2^n - 2^h} + bx$
$\frac{1}{e}$	$x^{2^{n-h}} + bx$
$\frac{e-1}{e}$	$x^{2^n - 2^{n-h}} + bx$
$\frac{1}{1-e}$	$x^{2^n - 1 - t} + bx$
$\frac{e}{e-1}$	$x^{1+t} + bx$

4.2 Odd Characteristic

The previous section deals with 2-to-1 binomials in even characteristic. Now we transfer the arguments and results to the case of odd characteristic. Although by Theorem 2.1.6 there are no hyperovals in $\mathrm{PG}(2, q)$ for q odd, the existing ovals can still be linked to 2-to-1 polynomials just as it is done in the case of even characteristic. This is done in the first subsection.

The greatest difference is that no odd characteristic version of Lemma 4.1.5 holds. Consequently, a single 2-to-1 binomial $x^e + bx^d$ does not yet define an oval, so we use the additional assumption that the binomial $x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. This situation is investigated in the second subsection.

An advantage of working in odd characteristic is that ovals are very well understood using Segre's Theorem. Using this powerful tool we conclude this thesis by obtaining a complete classification of those 2-to-1 binomials.

Finally, we would like to mention that this section was motivated mainly by research group meetings held by Professor Gohar Kyureghyan in Rostock about 2-to-1 binomials. The idea that it might be worthwhile to consider the statements of what is now Theorem 4.2.8 and Theorem 4.2.11 originated there, after the statement of Lemma 4.2.7 was established. Considerable contributions were made by Lucas Krompholz, especially regarding the definition, what kind of 2-to-1 binomials should be studied, and which properties they possess.

4.2.1 Ovals in Odd Characteristic

An oval in odd characteristic has exactly $q + 1$ points and in this subsection we obtain an algebraic description of an oval analogous to Theorem 2.1.15, while the algebraic condition is in the spirit of the characterization of Theorem 4.1.4.

When the characteristic is odd, we also have an odd number of elements in $\mathbb{F}_q$, which has to be accounted for when considering the 2-to-1 property.

4.2.1 Definition. Let q be odd. A polynomial $f \in \mathbb{F}_q[x]$ is *2-to-1*, if $|f^{-1}(\{t\})| \in \{0,1,2\}$ for all $t \in \mathbb{F}_q$ and if there is exactly one element $t \in \mathbb{F}_q$ with $|f^{-1}(\{t\})| = 1$.

First we justify why ovals may be assumed to be of a specific form, similar to the assumption that a hyperoval contains the fundamental quadrangle. Afterwards, the main characterization is proved.

4.2.2 Lemma. *Let q be odd and let $\mathcal{O}$ be an oval of $\mathrm{PG}(2,q)$. Then there is an equivalent oval $\mathcal{O}'$ of $\mathrm{PG}(2,q)$ containing the points $(1,0,0),(1,1,1),(0,0,1)$ and no other points from l_∞.*

Proof. By Lemma 2.1.3 we know that $\mathcal{O}$ has $q+1$ tangents. Fix l to be one of those and let $P \in \mathcal{O}$ be the tangent point.

Let S and T be other points of $\mathcal{O}$. Further, let Q be a point of $l \setminus \{P\}$ not contained in $S \vee T$. Since $q \geq 3$ it is always possible to select such a point. Finally, let $Q' \in l_\infty \setminus \{(0,0,1)\}$.

By construction, the points P, Q, S and T constitute a frame. Therefore, we can define a projectivity $\mathrm{PG}(2,q) \to \mathrm{PG}(2,q)$ by setting

- $\varphi(P) = (0,0,1)$,
- $\varphi(Q) = Q'$,
- $\varphi(S) = (1,0,0)$, and
- $\varphi(T) = (1,1,1)$.

Then $\varphi\mathcal{O}$ is an oval containing the three prescribed points. Additionally, φ preserves incidence relations, so $\varphi l = l_\infty$ and l_∞ is a tangent of $\mathcal{O}' := \varphi\mathcal{O}$. □

4.2.3 Theorem. *Let q be odd and let $\mathcal{O}$ be an oval of $\mathrm{PG}(2,q)$ containing the points $(1,0,0),(1,1,1)$ and $(0,0,1)$, which has l_∞ as a tangent. Then $\mathcal{O}$ may be represented via a polynomial $f \in \mathbb{F}_q[x]$ as*

$$\mathcal{O} = \mathcal{O}_o(f) := \{(1,s,f(s)) : s \in \mathbb{F}_q\} \cup \{(0,0,1)\},$$

where f satisfies the conditions

(i) $f(0) = 0$ and $f(1) = 1$ and

(ii) the polynomial $f(x) + bx$ is 2-to-1 for every $b \in \mathbb{F}_q$.

Conversely, every such polynomial $f \in \mathbb{F}_q[x]$ defines an oval $\mathcal{O}_o(f)$.

Proof. Firstly, if l_∞ is a tangent of $\mathcal{O}$, then every point of $\mathcal{O}$ besides $(0,0,1)$ must have a non-vanishing first coordinate. The q remaining points are thus of the form $(1,c_i,d_i)$ with $c_i, d_i \in \mathbb{F}_q$ for $i = 1,\ldots,q$. Assume now for a contradiction that $c_i = c_j$ for a pair (i,j) with $1 \leq i \neq j \leq q$. Consider the line

$$h = l_{-c_i} = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ c_i \\ d_i \end{pmatrix} \right\rangle.$$

We have $(1, c_j, d_j) \in h$, as

$$\begin{pmatrix} 1 \\ c_j \\ d_j \end{pmatrix} = \begin{pmatrix} 1 \\ c_i \\ d_i \end{pmatrix} + (d_j - d_i) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

so three points on the line h, a contradiction. Therefore $\{c_i : i = 1, \ldots, q\} = \mathbb{F}_q$.

Let f be the polynomial describing the map $c_i \mapsto d_i$ for $i = 1, ..., q$. Then $\mathcal{O} = \mathcal{O}_o(f)$. We prove next that f satisfies the claimed properties. From $(1, 0, 0)$ and $(1, 1, 1)$ being points of $\mathcal{O}$ it is immediate that $f(0) = 0$ and $f(1) = 1$. Consider the lines $l_{a,b}$ of PG$(2, q)$: For $a, b \in \mathbb{F}_q$ the line $l_{a,b} = \left\langle \begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \right\rangle^{\perp}$ does not contain the point $(0, 0, 1)$ and for $t \in \mathbb{F}_q$ contains the point $(1, t, f(t))$ if and only if

$$a + bt + f(t) = 0.$$

So the equation $f(x) + bx = -a$ has at most two solutions in $\mathbb{F}_q$.

What remains to be shown is that there is exactly one element a for fixed $b \in \mathbb{F}_q$ such that the equation $f(x) + bx = -a$ has exactly one solution. Such lines are precisely the tangents and there are exactly $q+1$ tangents overall, one of which is l_∞. Suppose there is an element $b \in \mathbb{F}_q$ such that for no $a \in \mathbb{F}_q$ the equation $f(x) + bx = -a$ has exactly one solution, e.g. no line $l_{a,b}$ is a tangent for this fixed b. Then every $a \in \mathbb{F}_q$ has exactly zero or two preimages under $f(x) + bx$, so $|\mathbb{F}_q|$ is even, a contradiction. Therefore, for every $b \in \mathbb{F}_q$, there is at least one element $a \in \mathbb{F}_q$ such that $l_{a,b}$ is a tangent. As there are only q tangents left to be accounted for, we have $f(x) + bx$ is 2-to-1 for all $b \in \mathbb{F}_q$.

Finally, for the converse, only the lines l_a for $a \in \mathbb{F}_q$ remain to be handled. For $t \in \mathbb{F}_q$ the point $(1, t, f(t))$ is on l_a if and only if

$$a + t = 0,$$

so only the points $(1, -a, f(-a))$ and $(0, 0, 1)$ from $\mathcal{O}(f)$ are on l_a. □

Notice that, in contrast to the even case, the polynomial f is not required to be bijective, but has to be 2-to-1. Lastly, we give an example of a family satisfying the conditions of Theorem 4.2.3, so that no concerns about the existence of the families dealt with in the next subsection may arise. This is analogous to Example 2.1.16 about the regular hyperoval and also provides an additional proof idea for that example.

4.2.4 Example. Take $f(x) = x^2$ with q odd. We show that $\mathcal{O}_o(f)$ is an oval and thus $f_b(x) = x^2 + bx$ is 2-to-1 for all $b \in \mathbb{F}_q^*$:

- A line $l_{a,b}$ with $a, b \in \mathbb{F}_q$ contains a point $(1, s, s^2)$ with $s \in \mathbb{F}_q$ if and only if

  $$a + bs + s^2 = 0$$

  holds. This quadratic equation has at most two solutions, so no such line contains more than two points from $\mathcal{O}_o(f)$.

- A line l_a with $a \in \mathbb{F}_q$ contains the point $(1, s, s^2)$ for $s \in \mathbb{F}_q$ if and only if

$$a + s = 0.$$

  They also contain the point $(0, 0, 1)$, so those lines contain exactly two points from $\mathcal{O}_o(f)$.

- The line l_∞ is a tangent by construction.

As there are no three collinear points, $\mathcal{O}_o(f)$ is an oval.

4.2.2 Families of 2-to-1 Binomials

We now turn to the odd characteristic version of Subsection 4.1.2, characterizing specific families of 2-to-1 binomials, which relate to (monomial) ovals. We specifically look at the families $(f_b)_{b\in\mathbb{F}_q}$ with $f_b(x) = x^e + bx^d$ and fixed $e \neq d$, where the binomial is 2-to-1 for all $b \in \mathbb{F}_q^*$. The main result of this subsection is that in this situation we must have either $\gcd(e, q-1) = 2$ and $\gcd(d, q-1) = 1$ or the other way round.

The primary idea consists in associating an oval-like structure $\mathcal{O}(e, d)$ to the exponents e and d and examining it using Lemma 4.1.2 to show that it actually is an oval.

4.2.5 Definition. Let q be odd and $0 < e \neq d$. Define

$$\mathcal{O}(e, d) := \{(1, s^d, s^e) : s \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}.$$

Note that $\mathcal{O}(e, d)$ is chosen exactly so that the 2-to-1 property corresponds to how many points of $\mathcal{O}(e, d)$ lie on the lines $l_{a,b}$. For Lemma 4.1.2 to be effective, we need to ensure that $\mathcal{O}(e, d)$ has the right number of points. Afterwards we collect some basic facts about e and d before continuing to prove the main result of this subsection.

4.2.6 Lemma. *Let q be odd and $0 < e \neq d$. Assume that $f_b(x) = x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. Then $|\mathcal{O}(e, d)| = q + 1$.*

Proof. We need to prove that the points $(1, s^d, s^e)$ are actually distinct. For a contradiction, assume that there are distinct $s, t \in \mathbb{F}_q$ satisfying

$$s^d = t^d \text{ and } s^e = t^e,$$

so

$$\left(\frac{s}{t}\right)^d = 1 = \left(\frac{s}{t}\right)^e.$$

Now take $b = -1$, then $f_{-1}(0) = 0$, $f_{-1}(1) = 0$, and $f_{-1}\left(\frac{s}{t}\right) = 0$. In particular, the polynomial f_{-1} is not 2-to-1. □

4.2.7 Lemma. *Let q be odd and $0 < e \neq d$. Assume that $x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. Then $\gcd(e - d, q - 1) = 1$. Also, $\gcd(e, q - 1)$ is even and $\gcd(d, q - 1)$ odd or the other way round.*

Proof. We have

$$f_b(x) = x^d \left(x^{e-d} + b\right).$$

Now, for some primitive element ξ of $\mathbb{F}_q^*$, choose $b \in -\left\langle \xi^{e-d} \right\rangle$. Then $x^{e-d} = -b$ has $\gcd(e-d, q-1)$ solutions in $\mathbb{F}_q^*$, so 0 has $1 + \gcd(e-d, q-1)$ preimages under the map induced by f_b. Since f_b is 2-to-1, $\gcd(e-d, q-1) = 1$ follows.

As $q-1$ is even, either e is even and d odd or the other way round. □

A converse statement is also true: If $f_b(x) = x^e + bx$ is 2-to-1 for some $b \in \mathbb{F}_q^*$ and $\gcd(e-d, q-1) = 1$, then for some primitive element ξ of $\mathbb{F}_q^*$ the polynomials

$$\left(\xi^i\right)^{-e} f_b\left(\xi^i x\right) = \left(\xi^i\right)^{-e} \left(\left(\xi^i\right)^e x^e + \left(\xi^i\right)^d b x^d\right) = x^e + \left(\xi^{d-e}\right)^i b x^d$$

for $i \in \mathbb{N}$ are also 2-to-1. Then $f_{b'}$ is 2-to-1 for all $b' \in \mathbb{F}_q^*$. However, not all $e \neq d$ with $\gcd(e-d, q-1) = 1$, $\gcd(e, q-1) = 2$, and $\gcd(d, q-1) = 1$ define such families.

4.2.8 Theorem. *Let q be odd and $0 < e \neq d$. Assume that $f_b(x) = x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. Then $\gcd(e, q-1) = 2$ and $\gcd(d, q-1) = 1$ or the other way round.*

Proof. Lemma 4.2.7 implies that either $\gcd(e, q-1)$ or $\gcd(d, q-1)$ is even. Without loss of generality (by multiplying the binomials by b^{-1} if necessary), assume that $\gcd(e, q-1)$ is even. Set

$$h := \gcd(e, q-1) \text{ and } m := \gcd(d, q-1).$$

Now we count the number of lines containing a specific number of points of $\mathcal{O}(e, d)$. Let k equal the maximum number of collinear points of $\mathcal{O}(e, d)$. Consider the lines $l_{a,b}$ for $a \in \mathbb{F}_q$ and fixed $b \in \mathbb{F}_q^*$ first. As f_b is 2-to-1, we have one tangent, $\frac{q-1}{2}$ bisecants and $\frac{q-1}{2}$ external lines among those lines. So from $b \in \mathbb{F}_q^*$ we obtain $\frac{(q-1)^2}{2}$ external lines, $q-1$ tangents, and $\frac{(q-1)^2}{2}$ bisecants overall.

A point $(1, t^d, t^e)$ for $t \in \mathbb{F}_q$ is on $l_{a,0}$ if and only if

$$a + t^e = 0.$$

So, with $a = 0$ we have another tangent and $a \in \mathbb{F}_q^*$ yields $\frac{q-1}{h}$ lines containing h points from $\mathcal{O}(e, d)$ as well as $q - 1 - \frac{q-1}{h}$ external lines.

The point $(0, 0, 1)$ is always on l_a for $a \in \mathbb{F}_q$ and the point $(1, t^d, t^e)$ for $t \in \mathbb{F}_q$ is on l_a if and only if

$$a + t^d = 0.$$

So, for $a = 0$ we get another bisecant and $a \in \mathbb{F}_q^*$ yields $\frac{q-1}{m}$ lines with exactly $m+1$ points from $\mathcal{O}(e, d)$ and $q - 1 - \frac{q-1}{m}$ tangents.

Finally, l_∞ is another tangent. Overall, we have

$$\tau_0 = \frac{(q-1)^2}{2} + q - 1 - \frac{q-1}{h}$$

external lines. Lemma 4.1.2 implies

$$\begin{aligned}\tau_1 &= (q+1)^2 - (q+1)q + \sum_{i=2}^{k}(i^2-2i)\tau_i \\ &= q + 1 + \sum_{i=2}^{k}(i^2-2i)\tau_i\end{aligned}$$

and substituting τ_0 and τ_1 into $\sum_{i=0}^{k}\tau_i = q^2+q+1$ yields

$$\begin{aligned}q^2+q+1 &= \tau_0 + \tau_1 + \sum_{i=2}^{k}\tau_i \\ &= \frac{(q-1)^2}{2} + q - 1 - \frac{q-1}{h} + q + 1 + \sum_{i-2}^{k}(i^2-2i+1)\tau_i \qquad (4.12) \\ &= \frac{(q-1)^2}{2} + 2q - \frac{q-1}{h} + \sum_{i=2}^{k}(i-1)^2\tau_i.\end{aligned}$$

We avoid giving an explicit expression for τ_2, as it depends on both h and m. However,

$$\sum_{i=2}^{k}(i-1)^2\tau_i = \frac{(q-1)^2}{2} + 1 + (h-1)^2\frac{q-1}{h} + m^2\frac{q-1}{m} \qquad (4.13)$$

holds. Combining (4.12) and (4.13) then yields

$$\begin{aligned}q^2+q+1 &= \frac{(q-1)^2}{2} + 2q - \frac{q-1}{h} + \frac{(q-1)^2}{2} + 1 + (h-1)^2\frac{q-1}{h} + m(q-1) \\ &= q^2 + (h^2-2h)\frac{q-1}{h} + m(q-1) + 2 \\ &= q^2 + (h+m-2)(q-1) + 2,\end{aligned}$$

leading to

$$0 = (h+m-3)(q-1).$$

As $q-1 \neq 0$, we must have $h+m=3$ and thus $h=2$ and $m=1$, since $h, m \in \mathbb{N}$ and $h \geq 2$. □

A similar proof in the even case for the main statement of Subsection 4.1.2 is also feasible: From the remarks after Lemma 4.2.7 and Lemma 4.1.5 we get that $x^e + b'x^d$ is 2-to-1 for all $b' \in \mathbb{F}_q$, provided it is for a specific $b \in \mathbb{F}_q$. Then the same line counting arguments takes effect and forces $\gcd(e, q-1) = \gcd(d, q-1) = 1$.

4.2.3 Segre's Theorem and Application to 2-to-1 Binomials

Finally, we use Segre's Theorem about ovals to show that the families $(f_b)_{b\in\mathbb{F}_q^*}$, where $f_b(x) = x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$, originate from the family $x^2 + bx$, which we examined in Example 4.2.4.

We are following [6, Section 9.7] for the definition of conics and Segre's Theorem, where also proofs for the statements we give can be found. As our focus has been mainly on the even case, we omit the details.

4.2.9 Definition (Non-Singular Conic)**.** A *conic* $\mathcal{C}$ is the set of points of $\mathrm{PG}(2,q)$ satisfying a non-singular quadratic equation, that is,

$$\mathcal{C} = \{(x,y,z) \in \mathrm{PG}(2,q) : ax^2 + by^2 + cz^2 + fyz + gzx + hxy = 0\}$$

with $a,b,c,f,g,h \in \mathbb{F}_q$ such that no linear substitution involving x, y and z leads to an equivalent equation in less than three variables.

Conics make up for simple examples for ovals. For odd characteristic though, Segre showed the remarkable converse statement.

4.2.10 Theorem (Segre [43])**.** *If q is odd, then any oval of $\mathrm{PG}(2,q)$ is a conic.*

In the last subsection we proved that $\mathcal{O}(e,d)$ is an oval if $f_b(x) = x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. Now knowing that it is also a conic, we can infer more about e and d by examining the associated non-singular quadratic equation.

4.2.11 Theorem. *Let q be odd and let $0 < e \neq d$, such that $f_b(x) = x^e + bx^d$ is 2-to-1 for all $b \in \mathbb{F}_q^*$. Then, assuming $\gcd(d, q-1) = 1$, we have $\frac{e}{d} \equiv 2 \mod q-1$, that is, $f_b(x)$ can be traced back to $x^2 + bx$ using the substitution $x \mapsto x^{\frac{1}{d}}$.*

Proof. By Theorem 4.2.8 we can assume without loss of generality that $\gcd(e, q-1) = 2$ and $\gcd(d, q-1) = 1$. Then

$$\mathcal{O}(e,d) = \mathcal{O}\left(\frac{e}{d}, 1\right) = \left\{\left(1, s, s^{\frac{e}{d}}\right) : s \in \mathbb{F}_q\right\} \cup \{(0,0,1)\} =: \mathcal{O},$$

using the substitution $x \mapsto x^{\frac{1}{d}}$. By Segre's Theorem $\mathcal{O}$ is a conic, so let

$$G(x,y,z) := ax^2 + by^2 + cz^2 + fyz + gzx + hxy$$

with $a,b,c,f,g,h \in \mathbb{F}_q$ be the associated quadratic form.

Since $(0,0,1) \in \mathcal{O}$, we have $c = 0$ and from $(1,0,0) \in \mathcal{O}$ it follows that $a = 0$. Letting k be the least positive residue of $\frac{e}{d} \mod q-1$, define

$$F(x) := G(1, x, x^k) = bx^2 + fx^{k+1} + gx^k + hx \in \mathbb{F}_q[x].$$

Note that by Theorem 4.2.8 $\gcd(k, q-1) = 2$, as $\mathcal{O} = \mathcal{O}(k,1)$ holds.

Then $F(t) = 0$ for all $t \in \mathbb{F}_q$, so $\deg F = q$ or $\deg F = -\infty$. In the first case, we must have $k = q-1$. Unless $q = 3$, we would have $\gcd(k, q-1) = q-1 \neq 2$. If $q = 3$, we have $k = 2$ and are done.

Thus only the case $F(x) = 0$ remains. As G is non-singular, not all coefficients vanish. This rules out $k \geq 3$, as all monomials in F would have a different degree. And finally, $\gcd(1, q-1) = 1$, so $k = 1$ cannot happen either. We therefore conclude that $k = 2$. □

Bibliography

[1] Simeon Ball. "Geometries". In: *Finite geometry and combinatorial applications*. London Mathematical Society Student Texts. Cambridge University Press, 2015, pp. 51–92. DOI: 10.1017/CBO9781316257449.005.

[2] Simeon Ball and Michel Lavrauw. "Arcs in finite projective spaces". In: *EMS Surveys in Mathematical Sciences* 6 (2019). DOI: 10.4171/emss/33.

[3] Luke Bayens, William E. Cherowitzo, and Tim Penttila. "Groups of hyperovals in Desarguesian planes". In: *Innovations in Incidence Geometry* 6+7.1 (Jan. 2008), pp. 37–51. DOI: 10.2140/iig.2008.6.37.

[4] Raj C. Bose. "Mathematical theory of the symmetrical factorial design". English. In: *Sankhyā* 8 (1947), pp. 107–166.

[5] Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Alexander Kholosha. "On o-equivalence of Niho bent functions". In: *Arithmetic of Finite Fields*. Ed. by Çetin Kaya Koç, Sihem Mesnager, and Erkay Savaş. Cham: Springer International Publishing, 2015, pp. 155–168. DOI: 10.1007/978-3-319-16277-5_9.

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

[7] Ilaria Cardinali and Stanley E. Payne. "The Payne q-clans". In: *q-clan geometries in characteristic 2*. Basel: Birkhäuser Basel, 2007, pp. 141–148. DOI: 10.1007/978-3-7643-8508-8_8.

[8] Florian Caullery and Kai-Uwe Schmidt. "On the classification of hyperovals". In: *Advances in Mathematics* 283 (2015), pp. 195–203. DOI: 10.1016/j.aim.2015.07.016.

[9] William E. Cherowitzo. "Hyperovals in Desarguesian planes of even order". In: *Combinatorics '86*. Ed. by A. Barloti, M. Marchi, and G. Tallini. Vol. 37. Annals of Discrete Mathematics. Elsevier, 1988, pp. 87–94. DOI: https://doi.org/10.1016/S0167-5060(08)70228-0.

[10] William E. Cherowitzo. "α-flocks and hyperovals". In: *Geometriae Dedicata* 72.3 (Oct. 1998), pp. 221–245. DOI: 10.1023/A:1005022808718.

[11] William E. Cherowitzo, Christine M. O'Keefe, and Tim Penttila. "A unified construction of finite geometries associated with q-clans in characteristic 2". In: *Advances in Geometry* 3.1 (2003), pp. 1–21. DOI: doi:10.1515/advg.2003.002.

[12] William E. Cherowitzo and Stanley E. Payne. "The cyclic q-clans with $q = 2^e$". In: *Advances in Geometry* 3.s1 (2003), pp. 158–185. DOI: doi:10.1515/advg.2003.2003.s1.158.

[13] William E. Cherowitzo, Tim Penttila, I. Pinneri, and G. F. Royle. "Flocks and ovals". In: *Geometriae Dedicata* 60.1 (Mar. 1996), pp. 17–37. DOI: 10.1007/BF00150865.

[14] William E. Cherowitzo and Leo Storme. "α-flocks with oval herds and monomial hyperovals". In: *Finite Fields and Their Applications* 4.2 (1998), pp. 185–199. DOI: 10.1006/ffta.1998.0210.

[15] Diana Davidova, Lilya Budaghyan, Claude Carlet, Tor Helleseth, Ferdinand Ihringer, and Tim Penttila. "Relation between o-equivalence and EA-equivalence for Niho bent functions". In: *Finite Fields and Their Applications* 72 (2021), p. 101834. DOI: 10.1016/j.ffa.2021.101834.

[16] Cunsheng Ding and Chunming Tang. "Infinite families of 3-designs from o-polynomials". In: *Advances in Mathematics of Communications* 15.4 (2021), pp. 557–573. DOI: 10.3934/amc.2020082.

[17] Zhiguo Ding and Michael E. Zieve. *Determination of hyperovals by lines through a few points*. 2023. arXiv: 2309.10866 [math.CO].

[18] David G. Glynn. "Two new sequences of ovals in finite Desarguesian planes of even order". In: *Combinatorial Mathematics X*. Ed. by Louis Reynolds Antoine Casse. Berlin, Heidelberg: Springer Berlin Heidelberg, 1983, pp. 217–229. DOI: 10.1007/BFb0071521.

[19] David G. Glynn. "A condition for the existence of ovals in PG(2, q), q even". In: *Geometriae Dedicata* 32.2 (Nov. 1989), pp. 247–252. DOI: 10.1007/BF00147433.

[20] Andrew Granville. "Arithmetic properties of binomial coefficients. I: Binomial coefficients modulo prime powers". English. In: *Organic mathematics. Proceedings of the workshop, Simon Fraser University, Burnaby, Canada, December 12-14, 1995*. Providence, RI: American Mathematical Society, 1997, pp. 253–276.

[21] Fernando Hernando and Gary McGuire. "Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes". In: *Designs, Codes and Cryptography* 65.3 (Dec. 2012), pp. 275–289. DOI: 10.1007/s10623-012-9624-3.

[22] James W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford mathematical monographs. Clarendon Press, 1979.

[23] Xiang-dong Hou. *Lectures on finite fields*. Graduate Studies in Mathematics. American Mathematical Society, 2018. DOI: 10.1090/gsm/190.

[24] Daniel R. Hughes and Frederick C. Piper. *Projective planes*. Graduate Texts in Mathematics. Springer New York, 1983.

[25] Lukas Kölsch and Gohar Kyureghyan. "The classifications of o-monomials and of 2-to-1 binomials are equivalent". In: *Designs, Codes and Cryptography* (July 2024). DOI: 10.1007/s10623-024-01463-1.

[26] Hans Kurzweil and Bernd Stellmacher. "Operieren und Konjugieren". In: *Theorie der endlichen Gruppen: Eine Einführung*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 51–70. DOI: 10.1007/978-3-642-58816-7_3.

[27] Gohar Kyureghyan and Valentin Suder. "On inversion in $\mathbb{Z}_{2^n-1}$". In: *Finite Fields and Their Applications* 25 (2014), pp. 234–254. DOI: 10.1016/j.ffa.2013.10.002.

[28] Rudolf Lidl and Harald Niederreiter. "Applications of finite fields". In: *Finite fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1996, pp. 470–540. DOI: 10.1017/CBO9780511525926.

[29] Antonio Maschietti. "Difference sets and hyperovals". In: *Designs, Codes and Cryptography* 14.1 (Apr. 1998), pp. 89–98. DOI: 10.1023/A:1008264606494.

[30] Sihem Mesnager and Longjiang Qu. "On two-to-one mappings over finite fields". In: *IEEE Transactions on Information Theory* 65.12 (2019), pp. 7884–7895. DOI: 10.1109/TIT.2019.2933832.

[31] Christine M. O'Keefe and Tim Penttila. "A new hyperoval in PG(2, 32)". In: *Journal of Geometry* 44.1 (July 1992), pp. 117–139. DOI: 10.1007/BF01228288.

[32] Christine M. O'Keefe and Tim Penttila. "Symmetries of arcs". In: *Journal of Combinatorial Theory, Series A* 66.1 (1994), pp. 53–67. DOI: 10.1016/0097-3165(94)90050-7.

[33] Christine M. O'Keefe and Joseph A. Thas. "Collineations of Subiaco and Cherowitzo hyperovals". In: *Bulletin of the Belgian Mathematical Society - Simon Stevin* 3.2 (1996), pp. 177–192. DOI: 10.36045/bbms/1105540790.

[34] Christine M. O'Keefe and Tim Penttila. "Polynomials for hyperovals of Desarguesian planes". In: *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics* 51.3 (1991), pp. 436–447. DOI: 10.1017/S1446788700034601.

[35] Christine M. O'Keefe and Tim Penttila. "Automorphism groups of generalized quadrangles via an unusual action of PΓL $(2, 2^h)$". In: *European Journal of Combinatorics* 23.2 (2002), pp. 213–232. DOI: 10.1006/eujc.2001.0550.

[36] Stanley E. Payne. "A complete determination of translation ovoids in finite Desarguian planes". eng. In: *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti* 51.5 (Nov. 1971), pp. 328–331.

[37] Stanley E. Payne. "A new infinite family of generalized quadrangles". In: *Proceedings of the sixteenth Southeastern international conference on combinatorics, graph theory and computing (Boca Raton, Fla., 1985)*. Vol. 49. 1985, pp. 115–128.

[38] Stanley E. Payne. "A tensor product action on q-clan generallzed quadrangles with q = 2^e". In: *Linear Algebra and its Applications* 226-228 (1995). Honoring J.J.Seidel, pp. 115–137. DOI: 10.1016/0024-3795(94)00345-E.

[39] Stanley E. Payne. *The Subiaco notebook*. 1997. URL: https://web.archive.org/web/20091113052840/http://www-math.cudenver.edu/~spayne/publications/nroot.ps.

[40] Stanley E. Payne, Tim Penttila, and Ivano Pinneri. "Isomorphisms between Subiaco q-clan geometries". In: *Bulletin of the Belgian Mathematical Society - Simon Stevin* 2.2 (1995), pp. 197–222. DOI: 10.36045/bbms/1103408755.

[41] Stanley E. Payne and Joseph A. Thas. "The stabilizer of the Adelaide oval". In: *Discrete Mathematics* 294.1 (2005). Finite Geometries, pp. 161–173. DOI: 10.1016/j.disc.2004.04.045.

[42] Tim Penttila. "Configurations of ovals". In: *Journal of Geometry* 76.1 (June 2003), pp. 233–255. DOI: 10.1007/s00022-003-1700-4.

[43] Beniamino Segre. "Ovals in a finite projective plane". In: *Canadian Journal of Mathematics* 7 (1955), pp. 414–416. DOI: 10.4153/CJM-1955-045-x.

[44] Beniamino Segre. "Sui k-archi nei piani finiti di caratteristica due". Italian. In: *Acad. Republ. Popul. Roum., Rev. Math. Pur. Appl.* 2 (1957), pp. 288–300.

[45] Beniamino Segre. "Ovali e curve σ nei piani di Galois di caratteristica due". Italian. In: *Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat.* 32 (1962), pp. 785–790.

[46] Beniamino Segre and Ugo Bartocci. "Ovali ed altre curve nei piani di Galois di caratteristica due". Italian. In: *Acta Arith.* 18 (1971), pp. 423–449. DOI: 10.4064/aa-18-1-423-449.

[47] Joseph A. Thas, H. Gevaert, and Stanley E. Payne. "A family of ovals with few collineations". In: *European Journal of Combinatorics* 9.4 (1988), pp. 353–362. DOI: 10.1016/S0195-6698(88)80065-9.

[48] Peter Vandendriessche. "Classification of the hyperovals in PG(2,64)". In: *The Electronic Journal of Combinatorics* 26 (May 2019). DOI: 10.37236/7589.

[49] Timothy L. Vis. "Monomial hyperovals in Desarguesian planes". PhD thesis. University of Colorado at Denver, 2010.

[50] Michael E. Zieve. "Planar functions and perfect nonlinear monomials over finite fields". In: *Designs, Codes and Cryptography* 75.1 (Apr. 2015), pp. 71–80. DOI: 10.1007/s10623-013-9890-8.