# 2-to-1 binomials from ovals and hyperovals

Alexander Oertel

11.10.2024

## Definition

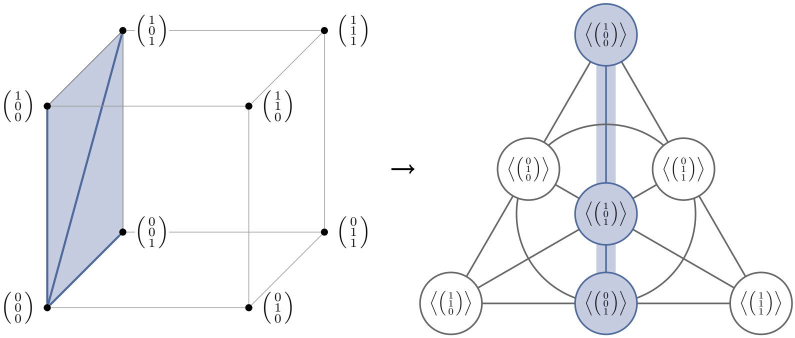
The Desarguesian projective plane $\mathrm{PG}(2, q)$ is defined as the set of the subspaces of $\mathbb{F}_q^3$. Further,

- the one dimensional subspaces are called the points and
- the two dimensional subspaces are called the lines.

Incidence is defined by the inclusion in $\mathbb{F}_q^3$.

# Definitions

## Example: Fano Plane



**Definition**

An *arc* of $\mathrm{PG}(2, q)$ is a set of points of $\mathrm{PG}(2, q)$ of which no three are collinear.

**Definition**

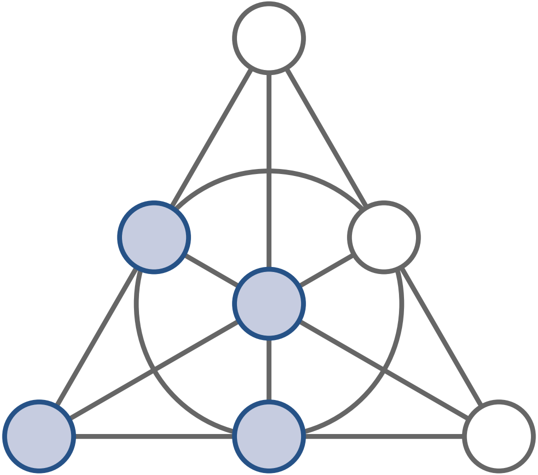
Let $q$ be even. A *hyperoval* of $\mathrm{PG}(2, q)$ is a set of $q + 2$ points of $\mathrm{PG}(2, q)$ of which no three are collinear.

**Definition**

An *oval* of $\mathrm{PG}(2, q)$ is a set of $q + 1$ points of $\mathrm{PG}(2, q)$ of which no three are collinear.

# Definitions

## Example: Regular Hyperoval in the Fano Plane



### Definition

Let $q = 2^n$. A polynom $f \in \mathbb{F}_q[x]$ 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 points $(1, 0, 0)$ und $(1, 1, 1)$.

### Example

The polynomial $f(x) = x^2$ is an o-polynomial.

# o-Polynomials

## Example

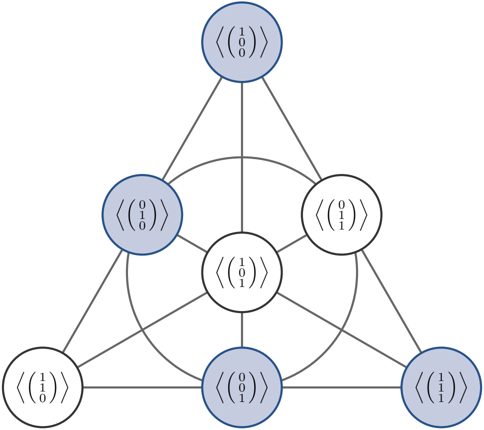



Figure: $f(x) = x^2$ for $q = 2$

**Theorem**

*Let $q = 2^n$. A polynomial $f \in \mathbb{F}_q[x]$ is an o-polynomial 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 as well for each $a \in \mathbb{F}_q$.*

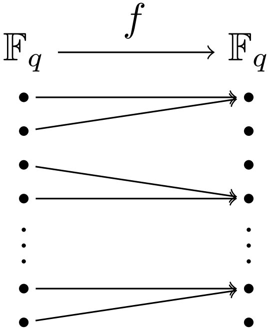
*Moreover, every hyperoval containing the points $(1,0,0)$, $(1,1,1)$, $(0,1,0)$ and $(0,0,1)$ may be written as $\mathcal{H}(f)$ with an o-polynomial $f$.*

| name | o-exponent | condition |
|---|---|---|
| Regular | $2$ | |
| Translation | $2^h$ | $\gcd(n,h)=1$ |
| Segre | $6$ | $n$ odd |
| $\text{Glynn}_1$ | $3\sigma+4=3\cdot 2^{\frac{n+1}{2}}+4$ | $n$ odd |
| $\text{Glynn}_2$ | $\sigma+\gamma=2^{\frac{n+1}{2}}+2^{\frac{3n+1}{4}}$ | $n\equiv 1 \mod 4$ |
| | $\sigma+\gamma=2^{\frac{n+1}{2}}+2^{\frac{n+1}{4}}$ | $n\equiv 3 \mod 4$ |

| name | o-polynomial | condition |
|---|---|---|
| Payne | $f(x) = x^{\frac{1}{6}} + x^{\frac{3}{6}} + x^{\frac{5}{6}}$ | $n$ odd |
| Cherowitzo | $f(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$ <br> $= x^{2^{\frac{n+1}{2}}} + x^{2^{\frac{n+1}{2}}+2} + x^{3\cdot 2^{\frac{n+1}{2}}+4}$ | $n$ odd |
| Subiaco | ... | |
| Adelaide | ... | $n$ even |

## Definition

Let $q$ be even. A 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.



**Theorem**

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

**Idea**

$$\left\langle \begin{pmatrix} 1 \\ t \\ f(t) \end{pmatrix} \right\rangle \in \left\langle \begin{pmatrix} a \\ b \\ 1 \end{pmatrix} \right\rangle^{\perp} \Leftrightarrow a + bt + f(t) = 0$$

## Theorem (Kölsch and Kyureghyan (2024))

*Let $q$ be even, $0 < e \neq d$, $b \in \mathbb{F}_q^*$ and let $f_b(x) = x^e + bx^d$ be 2-to-1. Then $\gcd(e, q-1) = \gcd(d, q-1) = 1$. Furthermore, the following statements are equivalent:*

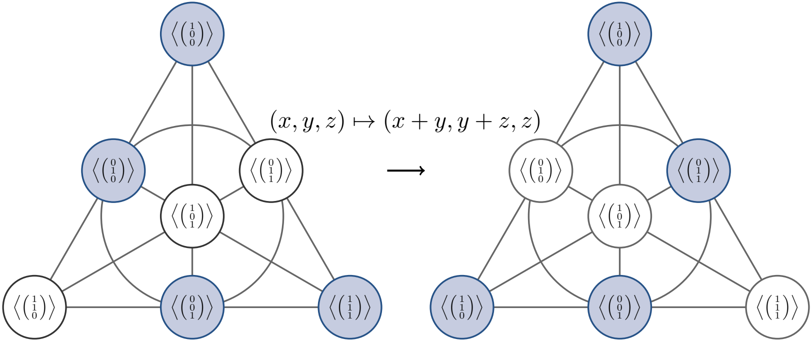
1. *The polynomial $f_b(x) = x^e + bx^d$ is 2-to-1.*
2. *The polynomial $f_{b'}(x) = x^e + b'x^d$ is 2-to-1 for every $b' \in \mathbb{F}_q^*$.*
3. *The monomial $x^{\frac{e}{d}}$ is an o-monomial.*

## Corollary

*2-to-1 binomials and o-monomials are equivalent. In particular, one can use the known o-monomials to construct 2-to-1 binomials.*

# o-Equivalence

## Example



**Definition**

Two o-polynomials $f$, $g$ are *o-equivalent* if the hyperovals $\mathcal{H}(f)$ and $\mathcal{H}(g)$ are equivalent under $\mathrm{P\Gamma L}(3, q)$.

**Goal:** Description of equivalence class for a given o-polynomial

1. Solve smaller problem for ovals induced by o-permutations
   - $\mathcal{O}(f) = \{(1, s, f(s)) : s \in \mathbb{F}_q\} \cup \{(0, 1, 0)\}$
   - *Magic Action* of Penttila und O'Keefe (2002): Group action of $\mathrm{P\Gamma L}(2, q)$ on the o-permutations
   - Generators of $\mathrm{P\Gamma L}(2, q) \rightsquigarrow$ Transformations explaining the equivalence classes
2. Lift results to hyperovals
   - Reduction to previous case by introduction of one more transformation
   - Due to Davidova, Budaghyan, Carlet, Helleseth, Ihringer, and Penttila (2021)

**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*

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

*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.*

**Theorem**

*Two o-polynomials $f, g \in \mathbb{F}_q[x]$ are o-equivalent if and only if they arise from each other by the transformations*

1. $(\tilde{\sigma}_a f)(x) = \frac{1}{f(a)} f(ax)$ *with* $a \in \mathbb{F}_q^*$,
2. $(\tilde{\tau}_c f)(x) = \frac{f(x+c)+f(c)}{f(1+c)+f(c)}$ *with* $c \in \mathbb{F}_q^*$,
3. $(\phi f)(x) = xf\left(\frac{1}{x}\right)$,
4. $(\rho_\gamma) = f^\gamma(x)$ *for* $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$ *and*
5. $(\mathrm{inv} f)(x) = f^{-1}(x)$.

**Theorem**

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

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

*where the elements of $B_e$ are meant to be taken $\mod q-1$.*

**Conclusion:** To find the to $\mathcal{H}(f)$ equivalent hyperovals with monomial o-polynomials, one has to only consider permutations of the coordinates.

| o-exponent | induced 2-to-1 binomial, $b \in \mathbb{F}_q^*$ |
|---|---|
| $e$ | $x^6 + bx$ |
| $1 - e$ | $x^{2^n - 6} + bx$ |
| $\frac{1}{e}$ | $x^{\frac{5 \cdot 2^{n-1} - 2}{3}} + bx$ |
| $\frac{e-1}{e}$ | $x^{\frac{2^{n-1} + 2}{3}} + bx$ |
| $\frac{1}{1-e}$ | $x^{\frac{2^n - 2}{5}} + bx$ if $n \equiv 1 \mod 4$<br>$x^{\frac{3 \cdot 2^n - 4}{5}} + bx$ if $n \equiv 3 \mod 4$ |
| $\frac{e}{e-1}$ | $x^{\frac{4 \cdot 2^n + 2}{5}} + bx$ if $n \equiv 1 \mod 4$<br>$x^{\frac{2 \cdot 2^n + 4}{5}} + bx$ if $n \equiv 3 \mod 4$ |

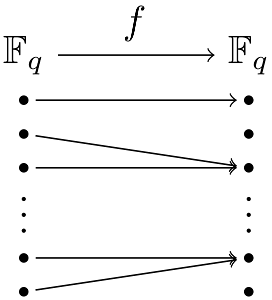
**Goal:** Generalize equivalence of 2-to-1 binomials and o-monomials in even characteristic to odd characteristic.

**Theorem**

*Let $q$ be odd and $0 < e \neq d$. Let further $f_b(x) = x^e + bx^d$ be 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.*
*Moreover, $\frac{e}{d} \equiv 2 \mod q-1$ or the other way round.*

## 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 $|f^{-1}(\{t\})| = 1$.



1. Associate oval structure to $e$ and $d$:

$$\mathcal{O}(e,d) := \{(1, s^d, s^e) : s \in \mathbb{F}_q\} \cup \{(0,0,1)\}$$

2. Count how many lines contain how many points of $\mathcal{O}(e,d)$

$$\left\langle \begin{pmatrix} 1 \\ t^d \\ t^e \end{pmatrix} \right\rangle \in \left\langle \begin{pmatrix} 1 \\ 0 \\ b \end{pmatrix} \right\rangle^{\perp} \Leftrightarrow 1 + bt^e = 0$$

$\rightsquigarrow \mathcal{O}(e,d)$ is an oval

### Lemma

*Let $k$ be the maximal number of collinear points of $\mathcal{O}(e, d)$ and let $\tau_i$ denote the number of lines of $\mathrm{PG}(2, q)$ containing exactly $i$ points of $\mathcal{O}(e, d)$. Then the following equalities hold.*

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

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

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

**Definition**

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.

**Theorem (Segre's Theorem)**

*If $q$ is odd, then any oval of $\mathrm{PG}(2,q)$ is a conic.*

# 2-to-1 binomials from ovals and hyperovals

Alexander Oertel

11.10.2024