On Quadratic Functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$

Wilfried Meidl
(joint works with Nurdagül Anbar, Ayça Çeşmelioğlu, Canan Kasikci, Sankhadip Roy, Alev Topuzoğlu)

International Workshop on Boolean Functions and Their Applications, September 2 – September 7 2014, Bergen

Quadratic functions

A quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can uniquely be represented as

$$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}).$$

with $a_i \in \mathbb{F}_{p^n}$, $0 \leq i < n/2$, and if n is even the coefficient $a_{n/2}$ is taken modulo $K = \{a \in \mathbb{F}_{p^n} \mid \mathrm{Tr_{n/(n/2)}}(a) = 0\}$.

Property: For all $a \in \mathbb{F}_{p^n}$ the derivative in direction a

$$D_a Q(x) = Q(x+a) - Q(x)$$

is either balanced or constant. Quadratic functions are partially bent functions.

Definition: The set Ω of elements $a \in \mathbb{F}_{p^n}$ for which $D_a Q(x)$ is constant is a subspace of $\mathbb{F}_{p^n}$, the linear space of Q.

Quadratic functions

A quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can uniquely be represented as

$$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}).$$

with $a_i \in \mathbb{F}_{p^n}$, $0 \leq i < n/2$, and if n is even the coefficient $a_{n/2}$ is taken modulo $K = \{a \in \mathbb{F}_{p^n} \mid \mathrm{Tr_{n/(n/2)}}(a) = 0\}$.

Property: For all $a \in \mathbb{F}_{p^n}$ the derivative in direction a

$$D_a Q(x) = Q(x+a) - Q(x)$$

is either balanced or constant. Quadratic functions are partially bent functions.

Definition: The set Ω of elements $a \in \mathbb{F}_{p^n}$ for which $D_a Q(x)$ is constant is a subspace of $\mathbb{F}_{p^n}$, the linear space of Q.

Quadratic functions

A quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can uniquely be represented as

$$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}).$$

with $a_i \in \mathbb{F}_{p^n}$, $0 \leq i < n/2$, and if n is even the coefficient $a_{n/2}$ is taken modulo $K = \{a \in \mathbb{F}_{p^n} \mid \mathrm{Tr_{n/(n/2)}}(a) = 0\}$.

Property: For all $a \in \mathbb{F}_{p^n}$ the derivative in direction a

$$D_a Q(x) = Q(x+a) - Q(x)$$

is either balanced or constant. Quadratic functions are partially bent functions.

Definition: The set Ω of elements $a \in \mathbb{F}_{p^n}$ for which $D_a Q(x)$ is constant is a subspace of $\mathbb{F}_{p^n}$, the linear space of Q.

Quadratic functions and Walsh transform

The Walsh transform $\widehat{Q}$ of Q is the complex valued function

$$\widehat{Q}(b) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x) - \mathrm{Tr}_n(bx)} \text{ with } \epsilon_p = e^{2\pi i/p} .$$

$\widehat{Q}(b)$ is called the Walsh coefficient of Q at b.

Parially bent functions are always plateaued. For a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ we have:

$p = 2$: $\widehat{Q}(b) \in \{0, \pm 2^{\frac{n+s}{2}}\}$

p odd:

$$\widehat{Q}(b) \in \{0, \pm i p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ if } n-s \text{ odd } p \equiv 3 \bmod 4$$
$$\widehat{Q}(b) \in \{0, \pm p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ otherwise.}$$

The value for s is exactly the dimension of the linear space Ω of Q.

Quadratic functions and Walsh transform

The Walsh transform $\widehat{Q}$ of Q is the complex valued function

$$\widehat{Q}(b) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x) - \mathrm{Tr}_n(bx)} \text{ with } \epsilon_p = e^{2\pi i/p} .$$

$\widehat{Q}(b)$ is called the Walsh coefficient of Q at b.

Parially bent functions are always plateaued. For a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ we have:

$p = 2$: $\widehat{Q}(b) \in \{0, \pm 2^{\frac{n+s}{2}}\}$

p odd:

$$\widehat{Q}(b) \in \{0, \pm i p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ if } n-s \text{ odd } p \equiv 3 \bmod 4$$
$$\widehat{Q}(b) \in \{0, \pm p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ otherwise.}$$

The value for s is exactly the dimension of the linear space Ω of Q.

Quadratic functions and Walsh transform

The Walsh transform $\widehat{Q}$ of Q is the complex valued function

$$\widehat{Q}(b) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x) - \mathrm{Tr}_n(bx)} \quad \text{with} \quad \epsilon_p = e^{2\pi i/p} \ .$$

$\widehat{Q}(b)$ is called the Walsh coefficient of Q at b.

Parially bent functions are always plateaued. For a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ we have:

$p = 2$: $\widehat{Q}(b) \in \{0, \pm 2^{\frac{n+s}{2}}\}$

p odd:

$$\begin{aligned} \widehat{Q}(b) &\in \{0, \pm i p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ if } n - s \text{ odd } p \equiv 3 \bmod 4 \\ \widehat{Q}(b) &\in \{0, \pm p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ otherwise.} \end{aligned}$$

The value for s is exactly the dimension of the linear space Ω of Q.

Quadratic functions and Walsh transform

The Walsh transform $\widehat{Q}$ of Q is the complex valued function

$$\widehat{Q}(b) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x) - \mathrm{Tr}_n(bx)} \quad \text{with} \quad \epsilon_p = e^{2\pi i/p} \ .$$

$\widehat{Q}(b)$ is called the Walsh coefficient of Q at b.

Parially bent functions are always plateaued. For a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ we have:

$p = 2$: $\widehat{Q}(b) \in \{0, \pm 2^{\frac{n+s}{2}}\}$

p odd:

$$\begin{aligned} \widehat{Q}(b) &\in \{0, \pm i p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ if } n - s \text{ odd } p \equiv 3 \bmod 4 \\ \widehat{Q}(b) &\in \{0, \pm p^{\frac{n+s}{2}} \epsilon_p^{f^*(b)}\} \text{ otherwise.} \end{aligned}$$

The value for s is exactly the dimension of the linear space Ω of Q.

The linear space Ω and its dimension s

$$Q(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\right) \xrightarrow[\text{squaring method}]{} L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i^{p^{n-i}} x^{p^{n-i}}$$

The linear space Ω is the kernel (in $\mathbb{F}_{p^n}$) of $L(x)$.

$s = \dim_{\mathbb{F}_p} \mathrm{Ker}(L(x))$; i.e.

$$\deg(\gcd(x^{p^n} - x, L(x))) = p^s \ .$$

The linear space Ω and its dimension s

$$Q(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\right) \xrightarrow[\text{squaring method}]{} L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i^{p^{n-i}} x^{p^{n-i}}$$

The linear space Ω is the kernel (in $\mathbb{F}_{p^n}$) of $L(x)$.

$s = \dim_{\mathbb{F}_p} \mathrm{Ker}(L(x))$; i.e.

$$\deg(\gcd(x^{p^n} - x, L(x))) = p^s \ .$$

Some explicitly known Walsh coefficients:

$p = 2$:

- $Q(x) = \mathrm{Tr}_n(ax^{2^\ell+1})$ with $a \in \mathbb{F}_{p^n}$
  Wolfmann (1989), Coulter (1999), Hou (2007)
- $Q(x) = \mathrm{Tr}_n(x^{2^k+1} + x^{2^\ell+1})$ with n odd and $\gcd(k+\ell, n) = \gcd(k-\ell, n) = 1$
  Lahtonen-McGuire-Ward (2007) which are semi bent functions!
- All $(n-2)$-plateaued quadratic functions
  $Q(x) = \mathrm{Tr}_n(\sum a_i x^{2^i+1})$ with $a_i \in \mathbb{F}_2$ by Fitzgerald (2005)
  and with $a_i \in \mathbb{F}_4$ by Özbudak-E. Saygı-Z. Saygı (2011-2012)

p odd:

- $Q(x) = \mathrm{Tr}_n(ax^{p^\ell+1})$ with $a \in \mathbb{F}_{p^n}$
  Wolfmann (1989), Coulter (1999), Helleseth-Kholosha (2006)

Quadratic Functions with Coefficients in the Prime Field

Our interest: Quadratic functions

$$Q(x) = \mathrm{Tr_n}\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} \right), \; a_i \in \mathbb{F}_p.$$

Some previous results:

- Khoo, Gong, Stinson 2006: Determine n for which all quadratic functions are near-bent for $p = 2$.
- Yul, Gong 2006: Number of quadratic binary bent functions for $n = 2^v p$, p prime, $ord_p 2 = p - 1$ or $(p-1)/2$.
- Hu, Feng 2007: Number of quadratic binary bent functions for $n = 2^v p^n$, p prime, $ord_p 2 = p - 1$ or $(p-1)/2$.
- Li, Hu, Zeng 2008: Number of quadratic p-ary bent functions for $n = p^v q^n$, $n = 2p^v q^n$, q prime, $ord_q p = q - 1$ or $(q-1)/2$.
- Fitzgerald 2009: Enumeration of binary quadratic functions, prescribed s, for $n = p$ and $n = pq$, p, q prime.

Outline

- Quadratic Functions, Definitions, Properties
- Enumeration of s-plateaued Quadratic Functions with given s
  - Method I: Discrete Fourier Transform
    - Enumeration results
    - Subcodes of the second order Reed-Muller code
  - Method II: Number theoretical approach
- Quadratic Functions and Artin-Schreier Curves

Outline

- Quadratic Functions, Definitions, Properties
- Enumeration of s-plateaued Quadratic Functions with given s
  - Method I: Discrete Fourier Transform
    - Enumeration results
    - Subcodes of the second order Reed-Muller code
  - Method II: Number theoretical approach
- Quadratic Functions and Artin-Schreier Curves

Outline

- Quadratic Functions, Definitions, Properties
- Enumeration of s-plateaued Quadratic Functions with given s
  - Method I: Discrete Fourier Transform
    - Enumeration results
    - Subcodes of the second order Reed-Muller code
  - Method II: Number theoretical approach
- Quadratic Functions and Artin-Schreier Curves

Associates

If $Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_p$, then $L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}}$.

By Lidl, Niederreiter, Finite Fields, Theorem 6.62:

The linear space Ω of Q has dimension

$$s = \deg(\gcd(A(x), x^n - 1)),$$

where

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i}$$

is the associate of $L(x)$.

Note: $\gcd(A(x), x^n - 1) = (x-1)^{\epsilon} f(x)$, $\epsilon \in \{0, 1\}$, for a self-reciprocal polynomial $f(x)$.

Associates

If $Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_p$, then
$L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}}$.

By Lidl, Niederreiter, Finite Fields, Theorem 6.62:

The linear space Ω of Q has dimension

$$s = \deg(\gcd(A(x), x^n - 1)),$$

where

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i}$$

is the associate of $L(x)$.

Note: $\gcd(A(x), x^n - 1) = (x-1)^\epsilon f(x)$, $\epsilon \in \{0, 1\}$, for a self-reciprocal polynomial $f(x)$.

Associates

If $Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_p$, then $L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}}$.

By Lidl, Niederreiter, Finite Fields, Theorem 6.62:

The linear space Ω of Q has dimension

$$s = \deg(\gcd(A(x), x^n - 1)),$$

where

$$A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i}$$

is the associate of $L(x)$.

Note: $\gcd(A(x), x^n - 1) = (x-1)^\epsilon f(x)$, $\epsilon \in \{0, 1\}$, for a self-reciprocal polynomial $f(x)$.

Prime self-reciprocal factorization of $x^n - 1$

Definition

A prime self-reciprocal polynomial $f \in \mathbb{F}_q[x]$ is a self-reciprocal polynomial which is

(i) irreducible over $\mathbb{F}_q$ or,

(ii) $f = ugg^*$, where g is irreducible over $\mathbb{F}_q$, the polynomial $g^* \neq g$ is the reciprocal of g and $u \in \mathbb{F}_q^*$ is a constant.

Factorization of $x^n - 1$, $\gcd(n, p) = 1$.

$$x^n - 1 = f_{j_1} f_{j_2} \cdots f_{j_k} \text{ with } f_{j_t} = \prod_{j \in C_{j_t}} (x - \alpha^j),$$

where α is a primitive nth root of unity, and C_{j_t} are the cyclotomic cosets modulo n relative to powers of p.

If $C_{j_t} = C_{-j_t}$, then f_{j_t} is (prime) self-reciprocal, otherwise $f_{j_t} f_{-j_t}$ is prime self-reciprocal.

Prime self-reciprocal factorization of $x^n - 1$

Definition

A prime self-reciprocal polynomial $f \in \mathbb{F}_q[x]$ is a self-reciprocal polynomial which is

(i) irreducible over $\mathbb{F}_q$ or,

(ii) $f = ugg^*$, where g is irreducible over $\mathbb{F}_q$, the polynomial $g^* \neq g$ is the reciprocal of g and $u \in \mathbb{F}_q^*$ is a constant.

Factorization of $x^n - 1$, $\gcd(n, p) = 1$.

$$x^n - 1 = f_{j_1} f_{j_2} \cdots f_{j_k} \text{ with } f_{j_t} = \prod_{j \in C_{j_t}} (x - \alpha^j),$$

where α is a primitive nth root of unity, and C_{j_t} are the cyclotomic cosets modulo n relative to powers of p.

If $C_{j_t} = C_{-j_t}$, then f_{j_t} is (prime) self-reciprocal, otherwise $f_{j_t} f_{-j_t}$ is prime self-reciprocal.

Prime self-reciprocal factorization of $x^n - 1$

Definition

A prime self-reciprocal polynomial $f \in \mathbb{F}_q[x]$ is a self-reciprocal polynomial which is

(i) irreducible over $\mathbb{F}_q$ or,

(ii) $f = ugg^*$, where g is irreducible over $\mathbb{F}_q$, the polynomial $g^* \neq g$ is the reciprocal of g and $u \in \mathbb{F}_q^*$ is a constant.

Factorization of $x^n - 1$, $\gcd(n, p) = 1$.

$$x^n - 1 = f_{j_1} f_{j_2} \cdots f_{j_k} \text{ with } f_{j_t} = \prod_{j \in C_{j_t}} (x - \alpha^j),$$

where α is a primitive nth root of unity, and C_{j_t} are the cyclotomic cosets modulo n relative to powers of p.

If $C_{j_t} = C_{-j_t}$, then f_{j_t} is (prime) self-reciprocal, otherwise $f_{j_t} f_{-j_t}$ is prime self-reciprocal.

Prime self-reciprocal factorization of $x^n - 1$

Example: $p = 2$, $n = 3^2 \cdot 5 = 45$.
Cyclotomic cosets: $(C_0 = \{0\})$, $C_5 = C_{40} = \{5, 10, 20, 40, 35, 25\}$,
$C_9 = C_{36} = \{9, 18, 36, 27\}$, $C_{15} = C_{30} = \{15, 30\}$.
$C_1 = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23\}$,
$C_{-1} = \{7, 14, 28, 11, 22, 44, 43, 41, 37, 29, 13, 26\}$,
$C_3 = \{3, 6, 12, 24\}$, $C_{-3} = \{21, 42, 39, 33\}$.

Degrees: 1, 2 4, 6, 8, and 24.

Factorization of $x^n - 1$ into prime self-reciprocal polynomials:
$x^n - 1 = (x-1) f_{j_1} f_{j_2} \cdots f_{j_r} g_{j_{r+1}} \cdots g_{j_{r+l}}$ with

$$f_{j_t} = \prod_{j \in C_{j_t}} (x - \alpha^j), \quad g_{j_s} = \prod_{j \in C_{j_s} \cup C_{-j_s}} (x - \alpha^j),$$

where C_{j_t}, $1 \le t \le r$ are the cyclotomic cosets different from $\{0\}$ with $C_{j_t} = C_{-j_t}$ and C_{j_s}, C_{-j_s}, $r+1 \le s \le r+l$, are the cyclotomic cosets with $C_{j_s} \ne C_{-j_s}$.

Prime self-reciprocal factorization of $x^n - 1$

Example: $p = 2$, $n = 3^2 \cdot 5 = 45$.
Cyclotomic cosets: $(C_0 = \{0\})$, $C_5 = C_{40} = \{5, 10, 20, 40, 35, 25\}$,
$C_9 = C_{36} = \{9, 18, 36, 27\}$, $C_{15} = C_{30} = \{15, 30\}$.
$C_1 = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23\}$,
$C_{-1} = \{7, 14, 28, 11, 22, 44, 43, 41, 37, 29, 13, 26\}$,
$C_3 = \{3, 6, 12, 24\}$, $C_{-3} = \{21, 42, 39, 33\}$.

Degrees: 1, 2 4, 6, 8, and 24.

Factorization of $x^n - 1$ into prime self-reciprocal polynomials:
$x^n - 1 = (x-1) f_{j_1} f_{j_2} \cdots f_{j_r} g_{j_{r+1}} \cdots g_{j_{r+l}}$ with

$$f_{j_t} = \prod_{j \in C_{j_t}} (x - \alpha^j), \quad g_{j_s} = \prod_{j \in C_{j_s} \cup C_{-j_s}} (x - \alpha^j),$$

where C_{j_t}, $1 \leq t \leq r$ are the cyclotomic cosets different from $\{0\}$ with $C_{j_t} = C_{-j_t}$ and C_{j_s}, C_{-j_s}, $r+1 \leq s \leq r+l$, are the cyclotomic cosets with $C_{j_s} \neq C_{-j_s}$.

Prime self-reciprocal factorization of $x^n - 1$

Example: $p = 2$, $n = 3^2 \cdot 5 = 45$.
Cyclotomic cosets: $(C_0 = \{0\})$, $C_5 = C_{40} = \{5, 10, 20, 40, 35, 25\}$,
$C_9 = C_{36} = \{9, 18, 36, 27\}$, $C_{15} = C_{30} = \{15, 30\}$.
$C_1 = \{1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23\}$,
$C_{-1} = \{7, 14, 28, 11, 22, 44, 43, 41, 37, 29, 13, 26\}$,
$C_3 = \{3, 6, 12, 24\}$, $C_{-3} = \{21, 42, 39, 33\}$.

Degrees: 1, 2 4, 6, 8, and 24.

Factorization of $x^n - 1$ into prime self-reciprocal polynomials:
$x^n - 1 = (x-1) f_{j_1} f_{j_2} \cdots f_{j_r} g_{j_{r+1}} \cdots g_{j_{r+l}}$ with

$$f_{j_t} = \prod_{j \in C_{j_t}} (x - \alpha^j), \quad g_{j_s} = \prod_{j \in C_{j_s} \cup C_{-j_s}} (x - \alpha^j),$$

where C_{j_t}, $1 \le t \le r$ are the cyclotomic cosets different from $\{0\}$ with $C_{j_t} = C_{-j_t}$ and C_{j_s}, C_{-j_s}, $r+1 \le s \le r+l$, are the cyclotomic cosets with $C_{j_s} \ne C_{-j_s}$.

Linear complexity and non-linearity

Linear complexity $L(S)$ of an n-periodic sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_p$ (Blahut's Theorem):

$$L(S) = n - \deg(\gcd(x^n - 1, S(x))),$$

where $S(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$.

Note that for $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i (x^i + x^{n-i})$

$$\gcd(x^n - 1, A(x)) = \gcd(x^n - 1, \bar{A}(x)), \quad \text{where}$$

$$\bar{A}(x) = \sum_{i=1}^{\lfloor n/2 \rfloor} a_i (x^i + x^{n-i}) + 2a_0.$$

Consequence: Let $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i (x^i + x^{n-i})$ be the polynomial associated with $Q(x)$. Then $Q(x)$ is s-plateaued with $s = n - L$, where L is the linear complexity of the n-periodic sequence over $\mathbb{F}_p$ with generating polynomial $\bar{A}(x) = \sum_{i=1}^{\lfloor n/2 \rfloor} a_i (x^i + x^{n-i}) + 2a_0$.

Linear complexity and non-linearity

Linear complexity $L(S)$ of an n-periodic sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_p$ (Blahut's Theorem):

$$L(S) = n - \deg(\gcd(x^n - 1, S(x))),$$

where $S(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$.

Note that for $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i})$

$$\gcd(x^n - 1, A(x)) = \gcd(x^n - 1, \bar{A}(x)), \quad \text{where}$$

$$\bar{A}(x) = \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i}) + 2a_0.$$

Consequence: Let $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i})$ be the polynomial associated with $Q(x)$. Then $Q(x)$ is s-plateaued with $s = n - L$, where L is the linear complexity of the n-periodic sequence over $\mathbb{F}_p$ with generating polynomial $\bar{A}(x) = \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i}) + 2a_0$.

Linear complexity and non-linearity

Linear complexity $L(S)$ of an n-periodic sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_p$ (Blahut's Theorem):

$$L(S) = n - \deg(\gcd(x^n - 1, S(x))),$$

where $S(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$.

Note that for $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i})$

$$\gcd(x^n - 1, A(x)) = \gcd(x^n - 1, \bar{A}(x)), \quad \text{where}$$

$$\bar{A}(x) = \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i}) + 2a_0.$$

Consequence: Let $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i})$ be the polynomial associated with $Q(x)$. Then $Q(x)$ is s-plateaued with $s = n - L$, where L is the linear complexity of the n-periodic sequence over $\mathbb{F}_p$ with generating polynomial $\bar{A}(x) = \sum_{i=1}^{\lfloor n/2 \rfloor} a_i(x^i + x^{n-i}) + 2a_0$.

Method I: Discrete Fourier Transform

$\gcd(p,n)=1$, $\alpha\in\mathbb{F}_p(\alpha)$ primitive nth root of unity.
DFT:$\mathbb{F}_p^n\to\mathbb{F}_p(\alpha)^n$ with $(s_0,s_1,\ldots,s_{n-1})\to\mathcal{S}=(\mathcal{S}_0,\ldots,\mathcal{S}_{n-1})$
where

$$\mathcal{S}_j=\sum_{i=0}^{n-1}s_i\alpha^{ji}=S(\alpha^j),$$

with $S(x)=s_0+s_1x+\cdots+s_{n-1}x^{n-1}$.

Note: $Hw((\mathcal{S}_0,\ldots,\mathcal{S}_{n-1}))=n-\deg(\gcd(x^n-1,S(x)))$.

$Q(x)=\mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2\rfloor}a_ix^{p^i+1})$, $a_i\in\mathbb{F}_p$, is s-partially bent with

$$s=n-Hw(DFT(\mathbf{a})),$$

$$\mathbf{a}=\begin{cases}(2a_0,a_1,\ldots,a_{(m-1)/2},a_{(m-1)/2},\ldots,a_1) & : \quad n \text{ odd}\\(2a_0,a_1,\ldots,a_{m/2-1},a_{m/2},a_{m/2-1},\ldots,a_1) & : \quad n \text{ even.}\end{cases} \quad (1)$$

Method I: Discrete Fourier Transform

$\gcd(p,n)=1$, $\alpha \in \mathbb{F}_p(\alpha)$ primitive nth root of unity.
DFT:$\mathbb{F}_p^n \to \mathbb{F}_p(\alpha)^n$ with $(s_0, s_1, \ldots, s_{n-1}) \to \mathcal{S} = (\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})$
where

$$\mathcal{S}_j = \sum_{i=0}^{n-1} s_i \alpha^{ji} = S(\alpha^j),$$

with $S(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$.

Note: $Hw((\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})) = n - \deg(\gcd(x^n - 1, S(x)))$.

$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_p$, is s-partially bent with

$$s = n - Hw(DFT(\mathbf{a})),$$

$$\mathbf{a} = \begin{cases} (2a_0, a_1, \ldots, a_{(m-1)/2}, a_{(m-1)/2}, \ldots, a_1) & : \quad n \text{ odd} \\ (2a_0, a_1, \ldots, a_{m/2-1}, a_{m/2}, a_{m/2-1}, \ldots, a_1) & : \quad n \text{ even.} \end{cases} \quad (1)$$

Method I: Discrete Fourier Transform

$\gcd(p,n)=1$, $\alpha \in \mathbb{F}_p(\alpha)$ primitive nth root of unity.
DFT:$\mathbb{F}_p^n \to \mathbb{F}_p(\alpha)^n$ with $(s_0, s_1, \ldots, s_{n-1}) \to \mathcal{S} = (\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})$
where

$$\mathcal{S}_j = \sum_{i=0}^{n-1} s_i \alpha^{ji} = S(\alpha^j),$$

with $S(x) = s_0 + s_1 x + \cdots + s_{n-1}x^{n-1}$.

Note: $Hw((\mathcal{S}_0, \ldots, \mathcal{S}_{n-1})) = n - \deg(\gcd(x^n - 1, S(x)))$.

$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$, $a_i \in \mathbb{F}_p$, is s-partially bent with

$$s = n - Hw(DFT(\mathbf{a})),$$

$$\mathbf{a} = \begin{cases} (2a_0, a_1, \ldots, a_{(m-1)/2}, a_{(m-1)/2}, \ldots, a_1) & : \quad n \text{ odd} \\ (2a_0, a_1, \ldots, a_{m/2-1}, a_{m/2}, a_{m/2-1}, \ldots, a_1) & : \quad n \text{ even.} \end{cases} \tag{1}$$

Lemma (Roy, Topuzoğlu, M.)

Let $\gcd(p, n) = 1$ *and* $\bar{A}(x)$ *be as above. Consider the cyclotomic coset* C_j *of* j *modulo* n *for* $0 \leq j \leq n-1$*. Suppose* $0 \leq k \leq n-1$ *is an element of* C_j*, i.e.,* $k \equiv jp^r \bmod n$ *for some* $r \geq 0$*. Then*

(i) $\bar{A}(\alpha^k) = \bar{A}(\alpha^j)^{p^r}$,

(ii) $\bar{A}(\alpha^{-j}) = \bar{A}(\alpha^j)$,

(iii) $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j}}$, *where* $l_j = |C_j|$*. If* $j \notin \{0, n/2\}$ *and* $-j \in C_j$*, then* $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j/2}}$*.*

(iv) $\bar{A}(1) = 0$*, if* $p = 2$*.*

We call n-tuples $\mathcal{A} = (\bar{A}(1), \bar{A}(\alpha), \ldots, \bar{A}(\alpha^{n-1}))$ of the form described in the Lemma n-tuples over $\mathbb{F}_p(\alpha)$ in sfdt-form.

Lemma (Roy, Topuzoğlu, M.)

Let $\gcd(p,n)=1$ *and* $\bar{A}(x)$ *be as above. Consider the cyclotomic coset* C_j *of* j *modulo* n *for* $0 \le j \le n-1$*. Suppose* $0 \le k \le n-1$ *is an element of* C_j*, i.e.,* $k \equiv jp^r \bmod n$ *for some* $r \ge 0$*. Then*

(i) $\bar{A}(\alpha^k) = \bar{A}(\alpha^j)^{p^r}$,

(ii) $\bar{A}(\alpha^{-j}) = \bar{A}(\alpha^j)$,

(iii) $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j}}$, *where* $l_j = |C_j|$*. If* $j \notin \{0, n/2\}$ *and* $-j \in C_j$*, then* $\bar{A}(\alpha^j) \in \mathbb{F}_{p^{l_j/2}}$*.*

(iv) $\bar{A}(1) = 0$*, if* $p = 2$*.*

We call n-tuples $\mathcal{A} = (\bar{A}(1), \bar{A}(\alpha), \ldots, \bar{A}(\alpha^{n-1}))$ of the form described in the Lemma n-tuples over $\mathbb{F}_p(\alpha)$ in sfdt-form.

Theorem (Roy, Topuzoğlu, M.)

There is a one to one correspondence between n-tuples over $\mathbb{F}_p$ of the form (1) and n-tuples $\mathcal{A}$ over $\mathbb{F}_p(\alpha)$ in sfdt-form.

Consequence: We can count s-plateaued quadratic functions with coefficients in the prime field by counting n-tuples over $\mathbb{F}_p(\alpha)$ in sfdt-form with Hamming weight $n - s$.

Theorem (Roy, Topuzoğlu, M.)

There is a one to one correspondence between n-tuples over $\mathbb{F}_p$ of the form (1) and n-tuples $\mathcal{A}$ over $\mathbb{F}_p(\alpha)$ in sfdt-form.

Consequence: We can count s-plateaued quadratic functions with coefficients in the prime field by counting n-tuples over $\mathbb{F}_p(\alpha)$ in sfdt-form with Hamming weight $n - s$.

Generating Function

Let $\mathcal{N}_n(s)$ be the number of s-plateaued quadratic functions with coefficients in the prime field and let $\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t) z^t$.

Theorem (Roy, Topuzoğlu, M., IEEE Trans. Inform. Theory 2014)

Let $p = 2$, n be odd, and let $x^n + 1 = (x+1) r_1 \cdots r_k$ be the factorization of $x^n - 1$ into prime self-reciprocal polynomials over $\mathbb{F}_2$. Then $\mathcal{G}_n(z)$ is given by

$$\mathcal{G}_n(z) = 2 \prod_{j=1}^{k} \left[1 + (2^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} \right].$$

Generating Function

Theorem (Roy, Topuzoğlu, M. and Çeşmelioğlu, M.)

Let $p \geq 3$*, n be odd,* $\gcd(n, p) = 1$*, and let* $x^n - 1 = (x-1)r_1 \cdots r_k$ *be the factorization of* $x^n - 1$ *over* $\mathbb{F}_p$ *with prime self-reciprocal polynomials* $r_1, \ldots, r_k$*. Then* $\mathcal{G}_n(z)$ *is given by*

$$\mathcal{G}_n(z) = (1 + (p-1)z) \prod_{j=1}^{k} \left[1 + (p^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} \right].$$

Let $p \geq 3$*, n be even,* $\gcd(n, p) = 1$*, and* $x^n - 1 = (x-1)(x+1)r_1 \cdots r_k$ *be the factorization of* $x^n - 1$ *over* $\mathbb{F}_p$ *with prime self-reciprocal polynomials* $r_1, \ldots, r_k$*. Then* $\mathcal{G}_n(z)$ *is given by*

$$\mathcal{G}_n(z) = (1 + (p-1)z)^2 \prod_{j=1}^{k} \left[1 + (p^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} \right].$$

Corollaries

- Explicit formulas for $\mathcal{N}_n(s)$ for all s, for several classes of integers n.
  (n prime; power of a prime; $p = 2,\ n = 2m - 1,\ m$ odd prime; $p = 2,\ n = 3q, ord_q 2 = 2k,\ k$ odd)
- Explicit formulas for the number of quadratic bent functions and semi-bent functions (coefficients in the prime field) for all n with $\gcd(n, p) = 1$.
- Expected value for s for all n with $\gcd(n, p) = 1$.

Second Order Reed-Muller Codes

Recall *rth order Reed-Muller code* $R(r,n)$ of length p^n:

$$R(r,n) = \{(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_{p^n})) \mid f \in P_r\},$$

where P_r is the set of all polynomials over $\mathbb{F}_p$ in n variables (or polynomial functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$) of algebraic degree at most r.

$R(2,n)$:

For $p=2$ the dimension is $(n^2+n+2)/2$.

For p odd the dimension is $(n^2+3n+2)/2$.

Weight distribution in Mc Elliece (1969), Sloane, Berlekamp (1970), v.d. Geer, v.d Vlught (1992).

Our interest: Subcodes of $R(2,n)$ from functions with coefficients in the prime field.

Second Order Reed-Muller Codes

Recall rth order Reed-Muller code $R(r, n)$ of length p^n:

$$R(r, n) = \{(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_{p^n})) \mid f \in P_r\},$$

where P_r is the set of all polynomials over $\mathbb{F}_p$ in n variables (or polynomial functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$) of algebraic degree at most r.

$R(2, n)$:

For $p = 2$ the dimension is $(n^2 + n + 2)/2$.

For p odd the dimension is $(n^2 + 3n + 2)/2$.

Weight distribution in Mc Elliece (1969), Sloane, Berlekamp (1970), v.d. Geer, v.d Vlught (1992).

Our interest: Subcodes of $R(2, n)$ from functions with coefficients in the prime field.

Second Order Reed-Muller Codes

Recall rth order Reed-Muller code $R(r, n)$ of length p^n:

$$R(r, n) = \{(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_{p^n})) \mid f \in P_r\},$$

where P_r is the set of all polynomials over $\mathbb{F}_p$ in n variables (or polynomial functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$) of algebraic degree at most r.

$R(2, n)$:

For $p = 2$ the dimension is $(n^2 + n + 2)/2$.

For p odd the dimension is $(n^2 + 3n + 2)/2$.

Weight distribution in Mc Elliece (1969), Sloane, Berlekamp (1970), v.d. Geer, v.d Vlught (1992).

Our interest: Subcodes of $R(2, n)$ from functions with coefficients in the prime field.

Weight of code words and Walsh transform

If c_f is the codeword corresponding to $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, then

$$wt(c_f) = p^n - \frac{1}{p} \sum_{a \in \mathbb{F}_p} \widehat{af}(0) \ .$$

In particular, for a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$

$$\begin{aligned} wt(c_Q) &= p^n - p^{n-1} \quad \text{if } p \text{ is odd } n-s \text{ is odd} \\ wt(c_Q) &= p^n - p^{n-1} - \frac{p-1}{p}\widehat{Q}(0) \quad \text{if } p \text{ is odd } n-s \text{ is even} \\ wt(c_Q) &= 2^{n-1} - \frac{1}{2}\widehat{Q}(0) \quad \text{if } p = 2. \end{aligned}$$

Weight of code words and Walsh transform

If c_f is the codeword corresponding to $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, then

$$wt(c_f) = p^n - \frac{1}{p} \sum_{a \in \mathbb{F}_p} \widehat{af}(0) .$$

In particular, for a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$

$$\begin{aligned} wt(c_Q) &= p^n - p^{n-1} \quad \text{if } p \text{ is odd } n-s \text{ is odd} \\ wt(c_Q) &= p^n - p^{n-1} - \frac{p-1}{p}\widehat{Q}(0) \quad \text{if } p \text{ is odd } n-s \text{ is even} \\ wt(c_Q) &= 2^{n-1} - \frac{1}{2}\widehat{Q}(0) \quad \text{if } p = 2. \end{aligned}$$

A subcode of $R(2, n)$

$C = \{c_Q \mid Q(x) = \mathrm{Tr}_n(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1} + bx + c)\}$ with $a_1, \ldots, a_{(n-1)/2} \in \mathbb{F}_2$, $b \in \mathbb{F}_{2^n}$ and $c \in \{0, \gamma\}$, where $\mathrm{Tr}_n(\gamma) = 1$.

Let A_i be the number of codewords in C of weight i. Then

$$\begin{aligned}\sum_{i=0}^{2^n} A_i x^i &= \sum_{k=0}^{n} \mathcal{N}_n(n-k) 2^k (x^{2^{n-1} - 2^{n-1-\frac{k}{2}}} + x^{2^{n-1} + 2^{n-1-\frac{k}{2}}}) \\ &\quad + \mathcal{N}_n(n-k)(2^{n+1} - 2^{k+1}) x^{2^{n-1}} .\end{aligned}$$

A subcode of $R(2, n)$

$C = \{c_Q \mid Q(x) = \mathrm{Tr}_n(\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1} + bx + c)\}$ with $a_1, \ldots, a_{(n-1)/2} \in \mathbb{F}_2, b \in \mathbb{F}_{2^n}$ and $c \in \{0, \gamma\}$, where $\mathrm{Tr}_n(\gamma) = 1$.

Let A_i be the number of codewords in C of weight i. Then

$$\sum_{i=0}^{2^n} A_i x^i = \sum_{k=0}^{n} \mathcal{N}_n(n-k) 2^k (x^{2^{n-1} - 2^{n-1-\frac{k}{2}}} + x^{2^{n-1} + 2^{n-1-\frac{k}{2}}}) + \mathcal{N}_n(n-k)(2^{n+1} - 2^{k+1}) x^{2^{n-1}} .$$

Observations

- Solely $x^{2^{n-1}\mp 2^{n-1-\frac{k}{2}}}$ and $x^{2^{n-1}}$ can have nonzero coefficients.
- The coefficient of $x^{2^{n-1}\mp 2^{n-1-\frac{k}{2}}}$ is equal to the coefficient of z^k in $\frac{1}{2}\mathcal{G}_n(2z)$.
- The coefficient of $x^{2^{n-1}}$ is $\sum_{k=0}^{n} \mathcal{N}_n(n-k)(2^{n+1}-2^{k+1}) = 2^n\mathcal{G}_n(1) - \mathcal{G}_n(2)$.
- If n is odd or $n = 2k$, k odd, then C is a $[2^n, (3n+1)/2, 2^{n-1} - 2^{n-1-\frac{r}{2}}]$ code, where r is the minimal degree of a prime self-reciprocal divisor of $x^n - 1$ different from $x + 1$.

Observations

- Solely $x^{2^{n-1}\mp 2^{n-1-\frac{k}{2}}}$ and $x^{2^{n-1}}$ can have nonzero coefficients.
- The coefficient of $x^{2^{n-1}\mp 2^{n-1-\frac{k}{2}}}$ is equal to the coefficient of z^k in $\frac{1}{2}\mathcal{G}_n(2z)$.
- The coefficient of $x^{2^{n-1}}$ is $\sum_{k=0}^{n}\mathcal{N}_n(n-k)(2^{n+1}-2^{k+1}) = 2^n\mathcal{G}_n(1)-\mathcal{G}_n(2)$.
- If n is odd or $n=2k$, k odd, then C is a $[2^n,(3n+1)/2,2^{n-1}-2^{n-1-\frac{r}{2}}]$ code, where r is the minimal degree of a prime self-reciprocal divisor of x^n-1 different from $x+1$.

Observations

- Solely $x^{2^{n-1}\mp 2^{n-1-\frac{k}{2}}}$ and $x^{2^{n-1}}$ can have nonzero coefficients.
- The coefficient of $x^{2^{n-1}\mp 2^{n-1-\frac{k}{2}}}$ is equal to the coefficient of z^k in $\frac{1}{2}\mathcal{G}_n(2z)$.
- The coefficient of $x^{2^{n-1}}$ is $\sum_{k=0}^{n}\mathcal{N}_n(n-k)(2^{n+1}-2^{k+1}) = 2^n\mathcal{G}_n(1)-\mathcal{G}_n(2)$.
- If n is odd or $n=2k$, k odd, then C is a $[2^n,(3n+1)/2,2^{n-1}-2^{n-1-\frac{r}{2}}]$ code, where r is the minimal degree of a prime self-reciprocal divisor of x^n-1 different from $x+1$.

Method II: Number Theoretical Approach

$$
\begin{aligned}
R_p &= \{f \in \mathbb{F}_p[x] \ : \ f \text{ is self-reciprocal}\}, \\
& \text{For } f \in \mathbb{F}_p[x] \\
C(f) &= \{g \in R_p \ : \ \deg(g) \text{ is even}, \ \deg(g) < \deg(f)\}, \\
K(f) &= \{g \in C(f) \ : \ \gcd(g(x), f(x)) = 1\}, \text{ and} \\
\phi_p(f) &= |K(f)|.
\end{aligned}
$$

Let $p = 2$. Define

$$\mathcal{N}_n(f;t) := \sum_{\substack{d|f \\ \deg(d)=t}} \phi_2(d),$$

where the summation is over all divisors d of f, $d \in R_{2,t}$, $\mathcal{N}_n(f;0) = 1$, and

$$\mathcal{G}_n(f;z) = \sum_{t \geq 0} \mathcal{N}_n(f;t) z^t.$$

Method II: Number Theoretical Approach

$$
\begin{aligned}
R_p &= \{f \in \mathbb{F}_p[x] \ : \ f \text{ is self-reciprocal}\}, \\
& \quad \text{For } f \in \mathbb{F}_p[x] \\
C(f) &= \{g \in R_p \ : \ \deg(g) \text{ is even}, \ \ \deg(g) < \deg(f)\}, \\
K(f) &= \{g \in C(f) \ : \ \gcd(g(x), f(x)) = 1\}, \text{ and} \\
\phi_p(f) &= |K(f)|.
\end{aligned}
$$

Let $p = 2$. Define

$$\mathcal{N}_n(f;t) := \sum_{\substack{d|f \\ \deg(d)=t}} \phi_2(d),$$

where the summation is over all divisors d of f, $d \in R_{2,t}$, $\mathcal{N}_n(f;0) = 1$, and

$$\mathcal{G}_n(f;z) = \sum_{t \geq 0} \mathcal{N}_n(f;t) z^t.$$

Express $\mathcal{N}_n(s)$

$A(x) = a_0 + a_1 x + \cdots + a_1 x^{n-1} + a_0 x^n$, $\bar{A}(x) = a_1 x + \cdots + a_1 x^{n-1}$.

n odd, then for a self-reciprocal polynomial $f_1(x)$, $\deg(f_1) = s - 1$

$$\gcd(\bar{A}(x), x^n - 1) = (x+1)f_1(x) \Rightarrow \bar{A}(x) = (x+1)f_1(x)g(x).$$

Properties of g:

- g is self-reciprocal of even degree smaller than $n - s$,
- $\gcd(\frac{x^n-1}{(x+1)f_1(x)}, g(x)) = 1$.

Consequence: $g \in K(d)$ for $d(x) = \frac{x^n-1}{(x+1)f_1(x)}$. Recall $|K(d)| = \phi_2(d)$.

Hence

$$\mathcal{N}_n(s) = 2 \sum_{\substack{d \mid (x^n+1)/(x+1) \\ \deg(d) = n-s}} \phi_2(d) = 2\mathcal{N}_n\left(\frac{x^n+1}{x+1}; n-s\right).$$

Express $\mathcal{N}_n(s)$

$A(x) = a_0 + a_1 x + \cdots + a_1 x^{n-1} + a_0 x^n$, $\bar{A}(x) = a_1 x + \cdots + a_1 x^{n-1}$.

n odd, then for a self-reciprocal polynomial $f_1(x)$, $\deg(f_1) = s - 1$

$$\gcd(\bar{A}(x), x^n - 1) = (x+1) f_1(x) \Rightarrow \bar{A}(x) = (x+1) f_1(x) g(x).$$

Properties of g:

- g is self-reciprocal of even degree smaller than $n - s$,
- $\gcd(\frac{x^n-1}{(x+1)f_1(x)}, g(x)) = 1.$

Consequence: $g \in K(d)$ for $d(x) = \frac{x^n-1}{(x+1)f_1(x)}$. Recall $|K(d)| = \phi_2(d)$.

Hence

$$\mathcal{N}_n(s) = 2 \sum_{\substack{d \mid (x^n+1)/(x+1) \\ \deg(d) = n-s}} \phi_2(d) = 2\mathcal{N}_n\left(\frac{x^n+1}{x+1}; n-s\right).$$

Express $\mathcal{N}_n(s)$

$A(x) = a_0 + a_1 x + \cdots + a_1 x^{n-1} + a_0 x^n$, $\bar{A}(x) = a_1 x + \cdots + a_1 x^{n-1}$.
n odd, then for a self-reciprocal polynomial $f_1(x)$, $\deg(f_1) = s - 1$

$$\gcd(\bar{A}(x), x^n - 1) = (x+1) f_1(x) \Rightarrow \bar{A}(x) = (x+1) f_1(x) g(x).$$

Properties of g:

- g is self-reciprocal of even degree smaller than $n - s$,
- $\gcd(\frac{x^n-1}{(x+1)f_1(x)}, g(x)) = 1$.

Consequence: $g \in K(d)$ for $d(x) = \frac{x^n-1}{(x+1)f_1(x)}$. Recall $|K(d)| = \phi_2(d)$.

Hence

$$\mathcal{N}_n(s) = 2 \sum_{\substack{d | (x^n+1)/(x+1) \\ \deg(d) = n-s}} \phi_2(d) = 2\mathcal{N}_n\left(\frac{x^n+1}{x+1}; n-s\right).$$

Express $\mathcal{N}_n(s)$

$A(x) = a_0 + a_1 x + \cdots + a_1 x^{n-1} + a_0 x^n$, $\bar{A}(x) = a_1 x + \cdots + a_1 x^{n-1}$.
n odd, then for a self-reciprocal polynomial $f_1(x)$, $\deg(f_1) = s - 1$

$$\gcd(\bar{A}(x), x^n - 1) = (x+1) f_1(x) \Rightarrow \bar{A}(x) = (x+1) f_1(x) g(x).$$

Properties of g:

- g is self-reciprocal of even degree smaller than $n - s$,
- $\gcd(\frac{x^n-1}{(x+1)f_1(x)}, g(x)) = 1$.

Consequence: $g \in K(d)$ for $d(x) = \frac{x^n-1}{(x+1)f_1(x)}$. Recall $|K(d)| = \phi_2(d)$.

Hence

$$\mathcal{N}_n(s) = 2 \sum_{\substack{d \mid (x^n+1)/(x+1) \\ \deg(d) = n-s}} \phi_2(d) = 2\mathcal{N}_n\left(\frac{x^n+1}{x+1}; n-s\right).$$

Express $\mathcal{N}_n(s)$

$A(x) = a_0 + a_1 x + \cdots + a_1 x^{n-1} + a_0 x^n$, $\bar{A}(x) = a_1 x + \cdots + a_1 x^{n-1}$.
n odd, then for a self-reciprocal polynomial $f_1(x)$, $\deg(f_1) = s - 1$

$$\gcd(\bar{A}(x), x^n - 1) = (x+1)f_1(x) \Rightarrow \bar{A}(x) = (x+1)f_1(x)g(x).$$

Properties of g:

- g is self-reciprocal of even degree smaller than $n - s$,
- $\gcd(\frac{x^n-1}{(x+1)f_1(x)}, g(x)) = 1$.

Consequence: $g \in K(d)$ for $d(x) = \frac{x^n-1}{(x+1)f_1(x)}$. Recall $|K(d)| = \phi_2(d)$.

Hence

$$\mathcal{N}_n(s) = 2 \sum_{\substack{d \mid (x^n+1)/(x+1) \\ \deg(d) = n-s}} \phi_2(d) = 2\mathcal{N}_n\left(\frac{x^n+1}{x+1}; n-s\right).$$

Theorem

Consider $\mathcal{N}_n(s)$*, the number of s-plateaued functions* $\mathcal{F}_{2,n}$*.*

(i) *If n is odd, then* $\mathcal{N}_n(n) = 2$ *and*

$$\mathcal{N}_n(s) = 2\mathcal{N}_n\left(\frac{x^n+1}{x+1}; n-s\right) = 2\sum_{\substack{d|(x^n+1)/(x+1)\\ \deg(d)=n-s}} \phi_2(d),$$

for $0 \leq s \leq n-1$*.*

(ii) *If* $n = 2m$*, m is odd, then* $\mathcal{N}_n(n) = 2$ *and*

$$\begin{aligned} \mathcal{N}_n(s) &= 2\mathcal{N}_n\left(\frac{x^n+1}{(x+1)^2}; n-s\right) \\ &= 2\sum_{\substack{d|(x^n+1)/(x+1)^2\\ \deg(d)=n-s}} \phi_2(d), \end{aligned}$$

for $0 \leq s \leq n-1$*.*

Properties of $\phi_p(d)$

For monic $f \in R_p$, $\deg(f) > 0$, not divisible by $x+1$, we have

$$\sum_{d|f} \phi_p(d) = p^{\frac{\deg(f)}{2}} - 1,$$

$$\phi_p(f) = \sum_{d|f} \mu_p(d) p^{\frac{\deg(f)-\deg(d)}{2}},$$

where the sum is over all monic self-reciprocal divisors d of f.

Let $f, f_1, f_2 \in \mathbb{F}_p[x]$ be monic self-reciprocal polynomials of positive degree, not divisible by $x+1$. If $f = f_1 f_2$ and $\gcd(f_1, f_2) = 1$, then

$$\phi_p(f) = \phi_p(f_1)\phi_p(f_2).$$

If $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ is the canonical factorization of f into monic prime self-reciprocal polynomials, then

$$\phi_p(f) = p^{\frac{\deg(f)}{2}} \prod_{j=1}^{k} \left(1 - p^{-\frac{\deg(r_j)}{2}}\right).$$

Properties of $\phi_p(d)$

For monic $f \in R_p$, $\deg(f) > 0$, not divisible by $x+1$, we have

$$\sum_{d|f} \phi_p(d) = p^{\frac{\deg(f)}{2}} - 1,$$

$$\phi_p(f) = \sum_{d|f} \mu_p(d) p^{\frac{\deg(f)-\deg(d)}{2}},$$

where the sum is over all monic self-reciprocal divisors d of f.

Let $f, f_1, f_2 \in \mathbb{F}_p[x]$ be monic self-reciprocal polynomials of positive degree, not divisible by $x+1$. If $f = f_1 f_2$ and $\gcd(f_1, f_2) = 1$, then

$$\phi_p(f) = \phi_p(f_1)\phi_p(f_2).$$

If $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ is the canonical factorization of f into monic prime self-reciprocal polynomials, then

$$\phi_p(f) = p^{\frac{\deg(f)}{2}} \prod_{j=1}^{k} \left(1 - p^{-\frac{\deg(r_j)}{2}}\right).$$

Generating function (with Roy, Topuzoğlu)

Let $f = f_1 f_2 \in R_2$, $f_1, f_2 \in R_2$, not divisible by $x+1$. If $\gcd(f_1, f_2) = 1$, then

$$\mathcal{G}_n(f; z) = \mathcal{G}_n(f_1; z)\mathcal{G}_n(f_2; z).$$

Recall $\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t) z^t$.
If n is odd and $x^n + 1 = (x+1) r_1 \cdots r_k$ is the factorization of x^n+1 into prime self-reciprocal polynomials, then

$$\mathcal{G}_n(z) = 2\prod_{j=1}^{k}\left[1 + (2^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)}\right].$$

If $n = 2m$, m is odd, and $x^n + 1 = (x+1)^2 r_1^2 \cdots r_k^2$ is the factorization of $x^n + 1$ into prime self-reciprocal polynomials, then

$$\mathcal{G}_n(z) = 2\prod_{j=1}^{k}\left[1 + (2^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} + (2^{\deg(r_j)} - 2^{\frac{\deg(r_j)}{2}}) z^{2\deg(r_j)}\right].$$

Generating function (with Roy, Topuzoğlu)

Let $f = f_1 f_2 \in R_2$, $f_1, f_2 \in R_2$, not divisible by $x+1$. If $\gcd(f_1, f_2) = 1$, then

$$\mathcal{G}_n(f; z) = \mathcal{G}_n(f_1; z)\mathcal{G}_n(f_2; z).$$

Recall $\mathcal{G}_n(z) = \sum_{t=0}^{n} \mathcal{N}_n(n-t) z^t$.
If n is odd and $x^n + 1 = (x+1) r_1 \cdots r_k$ is the factorization of $x^n + 1$ into prime self-reciprocal polynomials, then

$$\mathcal{G}_n(z) = 2 \prod_{j=1}^{k} \left[1 + (2^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} \right].$$

If $n = 2m$, m is odd, and $x^n + 1 = (x+1)^2 r_1^2 \cdots r_k^2$ is the factorization of $x^n + 1$ into prime self-reciprocal polynomials, then

$$\mathcal{G}_n(z) = 2 \prod_{j=1}^{k} \left[1 + (2^{\frac{\deg(r_j)}{2}} - 1) z^{\deg(r_j)} + (2^{\deg(r_j)} - 2^{\frac{\deg(r_j)}{2}}) z^{2\deg(r_j)} \right].$$

Artin-Schreier curves (with N. Anbar)

Our object: Artin-Schreier curves $\mathcal{X}$ over $\mathbb{F}_{p^n}$, p odd prime, from quadratic functions,

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

Properties:

- By Hurwitz Genus Formula, the genus of $\mathcal{X}$ is $g(\mathcal{X}) = \frac{(p-1)}{2} p^l$, where l is the largest integer for which $a_l \neq 0$.

- By Hilbert's Theorem 90, the number of rational points of $\mathcal{X}$ is $N(\mathcal{X}) = 1 + p|\{x;\ \mathrm{Tr}_n(\sum_{i=0}^{l} a_i x^{p^i+1}) = 0\}|$.

Artin-Schreier curves (with N. Anbar)

Our object: Artin-Schreier curves $\mathcal{X}$ over $\mathbb{F}_{p^n}$, p odd prime, from quadratic functions,

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

Properties:

- By Hurwitz Genus Formula, the genus of $\mathcal{X}$ is $g(\mathcal{X}) = \frac{(p-1)}{2} p^l$, where l is the largest integer for which $a_l \neq 0$.
- By Hilbert's Theorem 90, the number of rational points of $\mathcal{X}$ is $N(\mathcal{X}) = 1 + p|\{x;\ \mathrm{Tr}_n(\sum_{i=0}^{l} a_i x^{p^i+1}) = 0\}|$.

Artin-Schreier curves (with N. Anbar)

Our object: Artin-Schreier curves $\mathcal{X}$ over $\mathbb{F}_{p^n}$, p odd prime, from quadratic functions,

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

Properties:

- By Hurwitz Genus Formula, the genus of $\mathcal{X}$ is $g(\mathcal{X}) = \frac{(p-1)}{2} p^l$, where l is the largest integer for which $a_l \neq 0$.
- By Hilbert's Theorem 90, the number of rational points of $\mathcal{X}$ is $N(\mathcal{X}) = 1 + p|\{x;\ \mathrm{Tr}_n(\sum_{i=0}^{l} a_i x^{p^i+1}) = 0\}|$.

Maximal and minimal curves

$N(\mathcal{X})$: the number of rational points of $\mathcal{X}$
$g(\mathcal{X})$: the genus of $\mathcal{X}$

The Hasse-Weil Bound

$$p^n + 1 - 2g(\mathcal{X})p^{n/2} \quad \leq \quad N(\mathcal{X}) \quad \leq \quad p^n + 1 + 2g(\mathcal{X})p^{n/2}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

minimal — maximal

Target: Construct maximal and minimal curves over $\mathbb{F}_{p^n}$ of the form

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

Maximal and minimal curves

$N(\mathcal{X})$: the number of rational points of $\mathcal{X}$
$g(\mathcal{X})$: the genus of $\mathcal{X}$

The Hasse-Weil Bound

$$p^n + 1 - 2g(\mathcal{X})p^{n/2} \quad \leq \quad N(\mathcal{X}) \quad \leq \quad p^n + 1 + 2g(\mathcal{X})p^{n/2}$$

$\Downarrow$ minimal (lower bound) ... $\Downarrow$ maximal (upper bound)

Target: Construct maximal and minimal curves over $\mathbb{F}_{p^n}$ of the form

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

Maximal and minimal curves

$N(\mathcal{X})$: the number of rational points of $\mathcal{X}$
$g(\mathcal{X})$: the genus of $\mathcal{X}$

The Hasse-Weil Bound

$$p^n + 1 - 2g(\mathcal{X})p^{n/2} \quad \leq \quad N(\mathcal{X}) \quad \leq \quad p^n + 1 + 2g(\mathcal{X})p^{n/2}$$

$\Downarrow$ minimal (lower bound) $\qquad$ $\Downarrow$ maximal (upper bound)

Target: Construct maximal and minimal curves over $\mathbb{F}_{p^n}$ of the form

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$$

Walsh transform and the number of points

Let

$$Q(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\right)$$

be a quadratic function with s-dimensional linear space Ω, and

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} .$$

$$N(\mathcal{X}) = 1 + pN_0(Q) \quad \text{with} \quad N_0(Q) = \left|\{x \in \mathbb{F}_{p^n};\ Q(x) = 0\}\right|.$$

Lemma:

$$N_0(Q) = \begin{cases} p^{n-1} + \frac{p-1}{p}\widehat{Q}(0) & \text{if } n - s \equiv 0 \mod 2 \\ p^{n-1} & \text{if } n - s \equiv 1 \mod 2 \end{cases}$$

Walsh transform and the number of points

Let

$$Q(x) = \mathrm{Tr}_n\Big(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\Big)$$

be a quadratic function with s-dimensional linear space Ω, and

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} \ .$$

$$N(\mathcal{X}) = 1 + pN_0(Q) \quad \text{with} \quad N_0(Q) = |\{x \in \mathbb{F}_{p^n};\ Q(x) = 0\}|.$$

Lemma:

$$N_0(Q) = \begin{cases} p^{n-1} + \frac{p-1}{p}\widehat{Q}(0) & \text{if } n - s \equiv 0 \mod 2 \\ p^{n-1} & \text{if } n - s \equiv 1 \mod 2 \end{cases}$$

Walsh transform and the number of points

Let

$$Q(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}\right)$$

be a quadratic function with s-dimensional linear space Ω, and

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1} .$$

$$N(\mathcal{X}) = 1 + pN_0(Q) \quad \text{with} \quad N_0(Q) = |\{x \in \mathbb{F}_{p^n};\ Q(x) = 0\}|.$$

Lemma:

$$N_0(Q) = \begin{cases} p^{n-1} + \frac{p-1}{p}\widehat{Q}(0) & \text{if } n - s \equiv 0 \mod 2 \\ p^{n-1} & \text{if } n - s \equiv 1 \mod 2 \end{cases}$$

Walsh transform and the number of points

Theorem:

Let $\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$ be a curve over $\mathbb{F}_{p^n}$ for an odd prime p. Then

$$N(\mathcal{X}) = \begin{cases} 1 + p^n + \Lambda(p-1)p^{\frac{n+s}{2}} & \text{if } n-s \text{ is even}, \\ 1 + p^n & \text{if } n-s \text{ is odd}, \end{cases}$$

where $\Lambda = \begin{cases} 1 & \text{if } \widehat{Q}(0) = p^{\frac{n+s}{2}} \\ -1 & \text{if } \widehat{Q}(0) = -p^{\frac{n+s}{2}} \end{cases}$.

Requirements for maximal and minimal curves:

I. $s = 2l$, where l is the largest integer for which a_l is nonzero. (curve is maximal or minimal)

II. $\Lambda = 1$ for maximal curve, $\Lambda = -1$ for minimal curve.

Walsh transform and the number of points

Theorem:

Let $\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1}$ be a curve over $\mathbb{F}_{p^n}$ for an odd prime p. Then

$$N(\mathcal{X}) = \begin{cases} 1 + p^n + \Lambda(p-1)p^{\frac{n+s}{2}} & \text{if } n-s \text{ is even,} \\ 1 + p^n & \text{if } n-s \text{ is odd,} \end{cases}$$

where $\Lambda = \begin{cases} 1 & \text{if } \widehat{Q}(0) = p^{\frac{n+s}{2}} \\ -1 & \text{if } \widehat{Q}(0) = -p^{\frac{n+s}{2}} \end{cases}$.

Requirements for maximal and minimal curves:

I. $s = 2l$, where l is the largest integer for which a_l is nonzero. (curve is maximal or minimal)

II. $\Lambda = 1$ for maximal curve, $\Lambda = -1$ for minimal curve.

Constructing maximal and minimal curves

Step I: Find a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$

$$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$$

and its linear space Ω such that the of dimension of Ω is $s = 2l$.

The corresponding curves is then maximal or minimal.

Step II: Determination of (the sign of) $\widehat{Q}(0) = \pm p^{\frac{n+s}{2}}$:

Find a complement Ω^c in $\mathbb{F}_{p^n}$ of Ω.

Determine $\widehat{Q}(0)$ as

$$\widehat{Q}(0) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x)} = (\sum_{y \in \Omega} \epsilon_p^{Q(y)})(\sum_{z \in \Omega^c} \epsilon_p^{Q(z)}) = p^s \sum_{z \in \Omega^c} \epsilon_p^{Q(z)}.$$

Hope for good luck!

i.e. $Q(z)$ is something simple when $z \in \Omega^c$, so that we can evaluate the character sum $\sum_{z \in \Omega^c} \epsilon_p^{Q(z)}$.

Constructing maximal and minimal curves

Step I: Find a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$

$$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$$

and its linear space Ω such that the of dimension of Ω is $s = 2l$.

The corresponding curves is then maximal or minimal.
Step II: Determination of (the sign of) $\widehat{Q}(0) = \pm p^{\frac{n+s}{2}}$:

Find a complement Ω^c in $\mathbb{F}_{p^n}$ of Ω.
Determine $\widehat{Q}(0)$ as

$$\widehat{Q}(0) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{Q(x)} = (\sum_{y \in \Omega} \epsilon_p^{Q(y)})(\sum_{z \in \Omega^c} \epsilon_p^{Q(z)}) = p^s \sum_{z \in \Omega^c} \epsilon_p^{Q(z)}.$$

Hope for good luck!

i.e. $Q(z)$ is something simple when $z \in \Omega^c$, so that we can evaluate the character sum $\sum_{z \in \Omega^c} \epsilon_p^{Q(z)}$.

Constructing maximal and minimal curves

Step I: Find a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$

$$Q(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$$

and its linear space Ω such that the of dimension of Ω is $s = 2l$.

The corresponding curves is then maximal or minimal.
Step II: Determination of (the sign of) $\widehat{Q}(0) = \pm p^{\frac{n+s}{2}}$:

Find a complement Ω^c in $\mathbb{F}_{p^n}$ of Ω.
Determine $\widehat{Q}(0)$ as

$$\widehat{Q}(0) = \sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{Q(x)} = (\sum_{y\in\Omega} \epsilon_p^{Q(y)})(\sum_{z\in\Omega^c} \epsilon_p^{Q(z)}) = p^s \sum_{z\in\Omega^c} \epsilon_p^{Q(z)}.$$

Hope for good luck!

i.e. $Q(z)$ is something simple when $z \in \Omega^c$, so that we can evaluate the character sum $\sum_{z\in\Omega^c} \epsilon_p^{Q(z)}$.

Achieving Step I

$Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$ with $a_i \in \mathbb{F}_p$
$\Longrightarrow L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}}$
Determine s by the associate of $L(x)$: $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i}$

$s = \deg(\gcd(A(x), x^n - 1)) = \deg(\frac{x^n-1}{h(x)})$ for some $h(x) \in \mathbb{F}_p[x]$

$\deg(h) = k = n - s$: the codimension of Q

Choose $h(x) = x^k - 1$ for some even divisor k of n.
Maximal or minimal curves can be obtained only if

- n/k even: $A(x) = c(x^{\frac{k}{2}} + x^{\frac{3k}{2}} + \cdots + x^{n-\frac{k}{2}})$, $c \in \mathbb{F}_p^*$
- n/k odd: $A(x) = c(1 + 2x^k + \cdots + 2x^{n-k} + x^n)$, $c \in \mathbb{F}_p^*$

- n/k even: $Q(x) = c\mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$
- n/k odd: $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$

Achieving Step I

$Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$ with $a_i \in \mathbb{F}_p$
$\implies L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}}$
Determine s by the associate of $L(x)$: $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i}$

$$s = \deg(\gcd(A(x), x^n - 1)) = \deg(\frac{x^n-1}{h(x)}) \text{ for some } h(x) \in \mathbb{F}_p[x]$$

$\deg(h) = k = n - s$: the codimension of Q

Choose $h(x) = x^k - 1$ for some even divisor k of n.
Maximal or minimal curves can be obtained only if

- n/k even: $A(x) = c(x^{\frac{k}{2}} + x^{\frac{3k}{2}} + \cdots + x^{n-\frac{k}{2}})$, $c \in \mathbb{F}_p^*$
- n/k odd: $A(x) = c(1 + 2x^k + \cdots + 2x^{n-k} + x^n)$, $c \in \mathbb{F}_p^*$

- n/k even: $Q(x) = c\mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$
- n/k odd: $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$

Achieving Step I

$Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i+1})$ with $a_i \in \mathbb{F}_p$
$\Longrightarrow L(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^{p^i} + a_i x^{p^{n-i}}$
Determine s by the associate of $L(x)$: $A(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} a_i x^i + a_i x^{n-i}$

$$s = \deg(\gcd(A(x), x^n - 1)) = \deg(\frac{x^n-1}{h(x)}) \text{ for some } h(x) \in \mathbb{F}_p[x]$$

$\deg(h) = k = n - s$: the codimension of Q

Choose $h(x) = x^k - 1$ for some even divisor k of n.
Maximal or minimal curves can be obtained only if

- n/k even: $A(x) = c(x^{\frac{k}{2}} + x^{\frac{3k}{2}} + \cdots + x^{n-\frac{k}{2}})$, $c \in \mathbb{F}_p^*$
- n/k odd: $A(x) = c(1 + 2x^k + \cdots + 2x^{n-k} + x^n)$, $c \in \mathbb{F}_p^*$

- n/k even: $Q(x) = c\mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$
- n/k odd: $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$

Performing Step II

If $\gcd(A(x), x^n - 1)) = \frac{x^n-1}{x^k-1}$ then Ω is the kernel in $\mathbb{F}_{p^n}$ of $L(x) = x + x^{p^k} + \cdots + x^{p^{n-2k}} + x^{p^{n-k}}$.

If $\gcd(n, p) = 1$, then $\Omega^c = \mathbb{F}_{p^k}$.

If n/k is even, where $Q(x) = \mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$ for $z \in \Omega^c = \mathbb{F}_{p^k}$ we have

$$Q(z) = \mathrm{Tr}_k\left(\alpha z^{p^{\frac{k}{2}}+1}\right) \quad \text{with} \quad \alpha = \frac{n}{k}\left(\frac{n}{2k}\right)^{p^{\frac{n}{2}}}.$$

GOOD LUCK!

$$\text{Then} \quad \widehat{Q}(0) = p^s \sum_{z \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\alpha z^{p^{\frac{k}{2}}+1})},$$

and the sign is obtained with the known results on quadratic monomials.

Performing Step II

If $\gcd(A(x), x^n - 1)) = \frac{x^n-1}{x^k-1}$ then Ω is the kernel in $\mathbb{F}_{p^n}$ of $L(x) = x + x^{p^k} + \cdots + x^{p^{n-2k}} + x^{p^{n-k}}$.

If $\gcd(n, p) = 1$, then $\Omega^c = \mathbb{F}_{p^k}$.

If n/k is even, where $Q(x) = \mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$ for $z \in \Omega^c = \mathbb{F}_{p^k}$ we have

$$Q(z) = \mathrm{Tr}_k\left(\alpha z^{p^{\frac{k}{2}}+1}\right) \quad \text{with} \quad \alpha = \frac{n}{k}\left(\frac{n}{2k}\right)^{p^{\frac{n}{2}}}.$$

GOOD LUCK!

$$\text{Then} \quad \widehat{Q}(0) = p^s \sum_{z \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\alpha z^{p^{\frac{k}{2}}+1})},$$

and the sign is obtained with the known results on quadratic monomials.

Performing Step II

If $\gcd(A(x), x^n - 1)) = \frac{x^n-1}{x^k-1}$ then Ω is the kernel in $\mathbb{F}_{p^n}$ of $L(x) = x + x^{p^k} + \cdots + x^{p^{n-2k}} + x^{p^{n-k}}$.

If $\gcd(n, p) = 1$, then $\Omega^c = \mathbb{F}_{p^k}$.

If n/k is even, where $Q(x) = \mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$ for $z \in \Omega^c = \mathbb{F}_{p^k}$ we have

$$Q(z) = \mathrm{Tr}_k\left(\alpha z^{p^{\frac{k}{2}}+1}\right) \quad \text{with} \quad \alpha = \frac{n}{k}\left(\frac{n}{2k}\right)^{p^{\frac{n}{2}}}.$$

GOOD LUCK!

$$\text{Then} \quad \widehat{Q}(0) = p^s \sum_{z \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\alpha z^{p^{\frac{k}{2}}+1})},$$

and the sign is obtained with the known results on quadratic monomials.

Performing Step II

If $\gcd(A(x), x^n - 1)) = \frac{x^n-1}{x^k-1}$ then Ω is the kernel in $\mathbb{F}_{p^n}$ of $L(x) = x + x^{p^k} + \cdots + x^{p^{n-2k}} + x^{p^{n-k}}$.

If $\gcd(n, p) = 1$, then $\Omega^c = \mathbb{F}_{p^k}$.

If n/k is even, where $Q(x) = \mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$ for $z \in \Omega^c = \mathbb{F}_{p^k}$ we have

$$Q(z) = \mathrm{Tr}_k\left(\alpha z^{p^{\frac{k}{2}}+1}\right) \quad \text{with} \quad \alpha = \frac{n}{k}\left(\frac{n}{2k}\right)^{p^{\frac{n}{2}}}.$$

GOOD LUCK!

$$\text{Then} \quad \widehat{Q}(0) = p^s \sum_{z \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\alpha z^{p^{\frac{k}{2}}+1})},$$

and the sign is obtained with the known results on quadratic monomials.

Performing Step II

Similar, for n/k odd, where

$Q(x) = \mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$ for $z \in \Omega^c = \mathbb{F}_{p^k}$ we have

$$Q(z) = \mathrm{Tr}_k\left(\alpha z^2\right) \quad \text{with} \quad \alpha = \left(\frac{n}{k}\right)^2.$$

GOOD LUCK again. The exact value for $\widehat{Q}(0)$ follows from results on quadratic monomials.

N. Anbar, W. Meidl, Quadratic functions and maximal Artin Schreier curves, Finite Fields Appl. 30 (2014), 49–71.

Performing Step II

Similar, for n/k odd, where

$Q(x) = \mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$ for $z \in \Omega^c = \mathbb{F}_{p^k}$ we have

$$Q(z) = \mathrm{Tr}_k\left(\alpha z^2\right) \quad \text{with} \quad \alpha = \left(\frac{n}{k}\right)^2.$$

GOOD LUCK again. The exact value for $\widehat{Q}(0)$ follows from results on quadratic monomials.

N. Anbar, W. Meidl, Quadratic functions and maximal Artin Schreier curves, Finite Fields Appl. 30 (2014), 49–71.

$\gcd(n, p) > 1$

$\gcd(n/k, p) = 1$ can be dealt with like the case that $\gcd(n, p) = 1$

If $\gcd(n/k, p) = p^e m$ then $\mathbb{F}_{p^k}$ is not a complement of Ω.

There exists $\alpha \in \mathbb{F}_{p^{p^e k}}$ for which $\alpha\mathbb{F}_{p^k}$ is a complement of Ω.

Show: One can choose α in $\mathbb{F}_{p^{p^{e+l}}}$, $k = p^l r$.

Example: Case n/k odd:

$$\widehat{Q}(0) = p^s \sum_{t \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(m\beta t^2)} = (-1)^{\frac{p+1}{2}} \eta(\beta) p^{\frac{s}{2}},$$

$$\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1}).$$

Show β is a square in $\mathbb{F}_{p^k}$.

$\gcd(n, p) > 1$

$\gcd(n/k, p) = 1$ can be dealt with like the case that $\gcd(n, p) = 1$

If $\gcd(n/k, p) = p^e m$ then $\mathbb{F}_{p^k}$ is not a complement of Ω.

There exists $\alpha \in \mathbb{F}_{p^{p^e k}}$ for which $\alpha\mathbb{F}_{p^k}$ is a complement of Ω.

Show: One can choose α in $\mathbb{F}_{p^{p^{e+l}}}$, $k = p^l r$.

Example: Case n/k odd:

$$\widehat{Q}(0) = p^s \sum_{t \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(m\beta t^2)} = (-1)^{\frac{p+1}{2}} \eta(\beta) p^{\frac{s}{2}},$$

$\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1})$.

Show β is a square in $\mathbb{F}_{p^k}$.

$\gcd(n,p) > 1$

$\gcd(n/k, p) = 1$ can be dealt with like the case that $\gcd(n,p) = 1$

If $\gcd(n/k, p) = p^e m$ then $\mathbb{F}_{p^k}$ is not a complement of Ω.

There exists $\alpha \in \mathbb{F}_{p^{p^e k}}$ for which $\alpha\mathbb{F}_{p^k}$ is a complement of Ω.

Show: One can choose α in $\mathbb{F}_{p^{p^{e+l}}}$, $k = p^l r$.

Example: Case n/k odd:

$$\widehat{Q}(0) = p^s \sum_{t \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(m\beta t^2)} = (-1)^{\frac{p+1}{2}} \eta(\beta) p^{\frac{s}{2}},$$

$$\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1}).$$

Show β is a square in $\mathbb{F}_{p^k}$.

$\gcd(n,p) > 1$

$\gcd(n/k,p)=1$ can be dealt with like the case that $\gcd(n,p)=1$

If $\gcd(n/k,p)=p^e m$ then $\mathbb{F}_{p^k}$ is not a complement of Ω.

There exists $\alpha \in \mathbb{F}_{p^{p^e k}}$ for which $\alpha\mathbb{F}_{p^k}$ is a complement of Ω.

Show: One can choose α in $\mathbb{F}_{p^{p^{e+l}}}$, $k = p^l r$.

Example: Case n/k odd:

$$\widehat{Q}(0) = p^s \sum_{t\in\mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(m\beta t^2)} = (-1)^{\frac{p+1}{2}}\eta(\beta)p^{\frac{s}{2}},$$

$\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1}).$

Show β is a square in $\mathbb{F}_{p^k}$.

$\gcd(n, p) > 1$

$\gcd(n/k, p) = 1$ can be dealt with like the case that $\gcd(n, p) = 1$

If $\gcd(n/k, p) = p^e m$ then $\mathbb{F}_{p^k}$ is not a complement of Ω.

There exists $\alpha \in \mathbb{F}_{p^{p^e k}}$ for which $\alpha \mathbb{F}_{p^k}$ is a complement of Ω.

Show: One can choose α in $\mathbb{F}_{p^{p^{e+l}}}$, $k = p^l r$.

Example: Case n/k odd:

$$\widehat{Q}(0) = p^s \sum_{t \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(m\beta t^2)} = (-1)^{\frac{p+1}{2}} \eta(\beta) p^{\frac{s}{2}},$$

$$\beta = \mathrm{Tr}_{\mathbb{F}_{p^{p^e k}}/\mathbb{F}_{p^k}}(\alpha^{p^{k/2}+1} + \alpha^{p^{3k/2}+1} + \cdots + \alpha^{p^{(n-k)/2}+1}).$$

Show β is a square in $\mathbb{F}_{p^k}$.

Theorem: (Anbar, M.)

Let k be an even divisor of n, and let $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a quadratic function with coefficients in $\mathbb{F}_p$ for which the associate $A(x) \in \mathbb{F}_p[x]$ of the corresponding linearized polynomial $L(x)$ satisfies that

$$\gcd(A(x), x^n - 1) = \frac{x^n - 1}{x^k - 1} = 1 + x^k + \cdots + x^{n-2k} + x^{n-k} \ .$$

The curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ obtained from Q is maximal if and only if

- $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$, $c \in \mathbb{F}_p^*$, $p \equiv 3 \mod 4$ and $n \equiv 2 \mod 4$.

The curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ obtained from Q is minimal if and only if

- n/k is odd, $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^k+1} + \cdots + 2x^{p^{\frac{n-k}{2}}+1})$, $c \in \mathbb{F}_p^*$, $p \equiv 1 \mod 4$, or $p \equiv 3 \mod 4$ and $n \equiv 0 \mod 4$;
- n/k is even and $Q(x) = c\mathrm{Tr}_n(x^{p^{\frac{k}{2}}+1} + x^{p^{\frac{3k}{2}}+1} + \cdots + x^{p^{\frac{n-k}{2}}+1})$, $c \in \mathbb{F}_p^*$.

Complete solution codimension 2 ($g(\mathcal{X}) = \frac{p-1}{2} p^{\frac{n-2}{2}}$)

Theorem: (Anbar, M.)

Let p be an odd prime and let $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a quadratic function with coefficients in $\mathbb{F}_p$ of codimension 2.
The curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ obtained from Q is maximal if and only if

- $n \equiv 2 \mod 4$, $p \equiv 3 \mod 4$, and
  $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^2+1} + \cdots + 2x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$.

The curve $\mathcal{X}$ over $\mathbb{F}_{p^n}$ obtained from Q is minimal if and only if

- $n \equiv 2 \mod 4$, $p \equiv 1 \mod 4$, and
  $Q(x) = c\mathrm{Tr}_n(x^2 + 2x^{p^2+1} + \cdots + 2x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$, or
- $n \equiv 0 \mod 4$, and
  $Q(x) = c\mathrm{Tr}_n(x^{p+1} + x^{p^3+1} + \cdots + x^{p^{\frac{n}{2}-1}+1})$, $c \in \mathbb{F}_p^*$.

Questions

- Can one use generalized discrete Fourier transform for the case $\gcd(n, p) > 1$?
- Find the "sign distribution" for the Walsh transform of quadratic function with coefficients in the prime field.
- Find the weight distribution of subcodes of R(2,n) also for odd characteristic.
- Apply the number theortical method to further classes of quadratic functions with coefficients in the prime field.
- Can one determine more quadratic character sums with our method?

Thank you!

Questions

- Can one use generalized discrete Fourier transform for the case $\gcd(n, p) > 1$?
- Find the "sign distribution" for the Walsh transform of quadratic function with coefficients in the prime field.
- Find the weight distribution of subcodes of R(2,n) also for odd characteristic.
- Apply the number theortical method to further classes of quadratic functions with coefficients in the prime field.
- Can one determine more quadratic character sums with our method?

Thank you!