Codes from bent functions over finite fields

Sihem Mesnager

University of Paris VIII, Department of mathematics
and University of Paris XIII LAGA and Telecom Paris-Tech, France

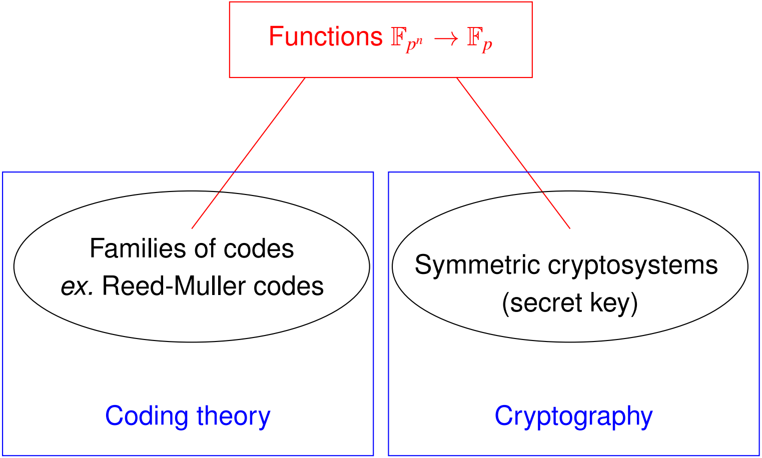
Seminar at Telecom
Paris
September 2016

Outline

1. Background on p-ary functions
2. Bent functions over finite fields
3. Two generic constructions of linear codes from bent functions
4. Explicit constructions of linear codes from bent functions
5. Conclusion

p-ary functions

- ☞ Functions from the finite field $\mathbb{F}_{p^n}$ to the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p-ary functions) play an important role in coding theory and cryptography !



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

Families of codes
ex. Reed-Muller codes

Coding theory

Symmetric cryptosystems
(secret key)

Cryptography

p-ary functions

- Algebraic Normal Form (A.N.F) of $f : \mathbb{F}_p^n \to \mathbb{F}_p$:
  $f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_p^n} a_u x^u$, with $x^u = \prod_{i=1}^n x_i^{u_i}$ and $a_u \in \mathbb{F}_p$.
- Polynomial form of $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$:

$$f(x) = \sum_{j \in \Gamma_n} Tr_{p^{o(j)}/p}(A_j x^j) + A_{p^n-1} x^{p^n-1}, x \in \mathbb{F}_{p^n}$$

  - Γ_n is the set of the integers obtained by choosing the smallest element in each cyclotomic class modulo $p^n - 1$,
  - cyclotomic class $C(j) = \{j, jp, jp^2, jp^3, \cdots, jp^{o(j)-1}\}$ containing j ;
  - $o(j)$ is the size of $C(j)$, c.a.d. $o(j)$ the smallest positive integer such that $jp^{o(j)} \equiv j \pmod{p^n - 1}$;
  - $A_j \in \mathbb{F}_{p^{o(j)}}$;
  - $A_{p^n-1} \in \mathbb{F}_p$;
  - $Tr_{p^n/p}(\cdot)$ the absolute trace function on $\mathbb{F}_{p^n}$: $Tr_{p^n/p}(x) = \sum_{i=0}^{n-1} x^{p^i}$.

Background on Boolean functions : representation

$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ an n-variable Boolean function.

Definition (Algebraic Normal Form (A.N.F))

Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. Then f can be expressed as :

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subset \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, a_I \in \mathbb{F}_2$$

where $I = \mathrm{supp}(u) = \{i = 1, \ldots, n \mid u_i = 1\}$ *and* $x^u = \prod_{i=1}^{n} x_i^{u_i}$.

The A.N.F exists and is unique.

Definition (The algebraic degree)

The algebraic degree $\deg(f)$ is the degree of the A.N.F.

Affine functions f $(\deg(f) \leq 1)$:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n, \; a_i \in \mathbb{F}_2$$

Background on Boolean functions : representation

Definition

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form :***

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n - 1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

Definition (Absolute trace over $\mathbb{F}_2$)

Let k be a positive integer. For $x \in \mathbb{F}_{2^k}$, the (absolute) trace $Tr_1^k(x)$ of x over $\mathbb{F}_2$ is defined by :

$$Tr_1^k(x) := \sum_{i=0}^{k-1} x^{2^i} = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}} \in \mathbb{F}_2$$

Background on Boolean functions : representation

Definition

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form :***

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

- Γ_n is the set obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$,
- $o(j)$ is the size of the cyclotomic coset containing j (that is $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \pmod{2^n - 1}$)
- $\epsilon = wt(f)$ modulo 2

Definition (The Hamming weight of a Boolean function)

$$wt(f) = \#supp(f) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$$

Background on Boolean functions : representation

Definition

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form*** *:*

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n - 1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

☞ **The algebraic degree** of f denoted by $\deg(f)$, is the maximum Hamming weight of the binary expansion of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and is n if $\epsilon = 1$.

- Affine functions : $Tr_1^n(ax) + \lambda$, $a \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_2$.

The discrete Fourier (Walsh) Transform of Boolean functions

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x}, \quad a \in \mathbb{F}_2^n$$

where "$\cdot$" is the canonical scalar product in $\mathbb{F}_2^n$ defined by $x \cdot y = \sum_{i=1}^n x_i y_i, \forall x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad \forall y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$.

Definition (The discrete Fourier (Walsh) Transform)

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)}, \quad a \in \mathbb{F}_{2^n}$$

where "Tr_1^n" is the absolute trace function on $\mathbb{F}_{2^n}$.

Characterization of bent functions

- **A main characterization of "bentness" :**

$$(f \text{ is bent }) \iff \widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}, \quad \forall \omega \in \mathbb{F}_{2^n}$$

Thanks to Parseval's identity, one can determine the number of occurrences of each value of the Walsh transform of a bent function.

TABLE: Walsh spectrum of bent functions f with $f(0) = 0$

Value of $\widehat{\chi_f}(\omega)$, $\omega \in \mathbb{F}_{2^n}$	Number of occurrences
$2^{\frac{n}{2}}$	$2^{n-1} + 2^{\frac{n-2}{2}}$
$-2^{\frac{n}{2}}$	$2^{n-1} - 2^{\frac{n-2}{2}}$

Bentness and nonlinearity

Definition (The Hamming distance)

$f, g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *two Boolean functions. The Hamming distance between* f *and* g *:* $d_H(f, g) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) \neq g(x)\}$*.*

Definition (Nonlinearity)

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *a Boolean function. The nonlinearity denoted by* $\mathrm{nl}(f)$ *of* f *is*

$$\mathrm{nl}(f) := min_{l \in A_n} d_H(f, l)$$

where $A_n := \{l : \mathbb{F}_{2^n} \to \mathbb{F}_2, \quad l(x) := a \cdot x + b\, ; a \in \mathbb{F}_{2^n}, \quad b \in \mathbb{F}_2$ *(where "·" is an inner product in* $\mathbb{F}_{2^n}$*)} is the set of affine functions on* $\mathbb{F}_{2^n}$*.*

➔ The nonlinearity of a function f is the minimum number of truth table entries that must be changed in order to convert f to an affine function.

General upper bound on the nonlinearity of Boolean functions

The nonlinearity of f equals :

$$\mathrm{nl}(f) \;=\; 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |\widehat{\chi_f}(a)|$$

➔Thanks to Parseval's relation : $\sum_{a\in\mathbb{F}_2^n} \widehat{\chi_f}^{\,2}(a) = 2^{2n}$
we have : $\max_{a\in\mathbb{F}_2^n} (\widehat{\chi_f}(a))^2 \geq 2^n$

Hence : for every n-variable Boolean function f, the nonlinearity is always upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$

➔It can reach this value if and only if n is even.

A main definition of a bent function

- **General upper bound on the nonlinearity of any n-variable Boolean function : $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$**

DEFINITION (BENT FUNCTION [ROTHAUS, 1975])

$f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ *(n even) is said to be a bent function if* $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$

Bent functions have been studied for more than 40 years (initiators : [Dillon, 1974], [Rothaus, 1975]).

☞ If f is bent then $\widehat{\chi_f}(\omega) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\omega)}$, $\forall \omega \in \mathbb{F}_2^n$, defines the dual function $\tilde{f}$ of f.

Bent Boolean functions in combinatorics

Bent functions are combinatorial objects :

Definition

- *Let G be a finite (abelian) group of order μ. A subset D of G of cardinality k is called (μ, k, λ)-difference set in G if every element $g \in G$, different from the identity, can be written as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly λ different ways.*
- *Hadamard difference set in elementary abelian 2-group :* $(\mu, k, \lambda) = (2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$.

Theorem (Dillon 74)

A Boolean function f over $\mathbb{F}_2^n$ is bent if and only if $supp(f) := \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ is a Hadamard difference set in $\mathbb{F}_2^n$.

Bent Boolean functions in combinatorics

Example : Let f a Boolean function defined on $\mathbb{F}_2^4$ ($n = 4$) by $f(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3$ The support of f is $Supp(f) = \{(1,0,0,1),(1,0,1,1),(1,1,0,1),(0,1,1,0),(0,1,1,1),(1,1,1,0)\}$ is a Hadamard $(16, 6, 2)$-difference set of $\mathbb{F}_2^4$.

d_1	d_2	$d_1 + d_2$
1001	1011	0010
1001	1101	0100
1001	0110	1111
1001	0111	1110
1001	1110	0111
1011	1101	0110
1011	0110	1101
1011	0111	1100
1011	1110	0101
1101	0110	1011
1101	0111	1010
1101	1110	0011
0110	0111	0001
0110	1110	1000
0111	1110	1001

Bent functions in characteristic p

The Walsh-Hadamard transform can be defined for p-ary functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$:

$$S_f(b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) - Tr_{p^n/p}(bx)},$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ is the complex primitive p^{th} root of unity and elements of $\mathbb{F}_p$ are considered as integers modulo p.

Definition

A p-ary function f is called bent if all its Walsh-Hadamard coefficients satisfy $|S_f(b)|^2 = p^n$. A bent function f is called regular bent if for every $b \in \mathbb{F}_{p^n}$, $p^{-\frac{n}{2}} S_f(b) = \zeta_p^{f^\star(b)}$ for some p-ary function $f^\star : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

Definition

The bent function f is called weakly regular bent if there exist a complex number u with $|u| = 1$ and a p-ary function $f^\star$ such that $up^{-\frac{n}{2}} S_f(b) = \zeta_p^{f^\star(b)}$ for all $b \in \mathbb{F}_{p^n}$.

Bent functions in characteristic p

[Kummar, Scholtz, Welch 1985] Walsh-Hadamard transform coefficients of a p-ary bent function f with odd p satisfy

$$p^{-\frac{n}{2}} S_f(b) = \begin{cases} \pm\zeta_p^{f^\star(b)}, & \text{if } n \text{ is even or } n \text{ is odd and } p \equiv 1 \pmod 4, \\ \pm i\zeta_p^{f^\star(b)}, & \text{if } n \text{ is odd and } p \equiv 3 \pmod 4, \end{cases} \tag{1}$$

where i is a complex primitive 4-th root of unity. Therefore, regular bent functions can only be found for even n and for odd n with $p \equiv 1 \pmod 4$. Moreover, for a weakly regular bent function, the constant u (defined above) can only be equal to ± 1 or $\pm i$.

Boolean functions in Error Correcting Coding

Definition (Linear codes)

A linear $[n,k,d]_q$ code $\mathcal{C}$ over a field $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d with $d := d(\mathcal{C}) = min_{\bar{a},\bar{b}\in\mathcal{C},\bar{a}\neq\bar{b}} d(\bar{a},\bar{b})$ where the distance $d(\bar{a},\bar{b})$ between two vectors $\bar{a}$ and $\bar{b}$ is the number of coordinates in which they differ.

$\mathcal{B}_n = \{f : \mathbb{F}_2^n \to \mathbb{F}_2\}$

- The Reed-Muller code $\mathcal{RM}(r,n)$ can be defined in terms of **Boolean functions** : $\mathcal{RM}(r,n)$ is the set of all n-variable Boolean functions $\mathcal{B}_n$ of algebraic degrees at most r. More precisely, it is the linear code of all binary words of length 2^n corresponding to the truth-tables of these functions.
- For every $0 \leq r \leq n$, $\mathcal{RM}(r,n)$ of order r, is a linear code :

$$\left[\underbrace{2^n}_{length}, \underbrace{\sum_{i=0}^{r}\binom{n}{i}}_{dimension}, \underbrace{2^{n-r}}_{\text{minimum distance}}\right]$$

The covering radius of $\mathcal{RM}(1,n)$ and bent functions

- The Covering radius $\rho(1,n)$ of the Reed-Muller code $\mathcal{RM}(1,n)$ coincides with the maximum nonlinearity $nl(f)$.
- General upper bound on the nonlinearity : $\mathrm{nl}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$

- When n is odd, $\rho(1,n) < 2^{n-1} - 2^{\frac{n}{2}-1}$
- When n is even, $\rho(1,n) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and the associated n-variable Boolean functions are the bent functions.

- The covering radius plays an important role in error correcting codes : measures the maximum errors to be corrected in the context of maximum-likelihood decoding.

Bent functions in coding theory

1. It is well-known that Kerdock codes are constructed from bent functions [MacWilliams-Sloane 1973].

Definition

The Kerdock codes of length 2^m consist of $\mathcal{RM}(1,m)$ together with $2^{m-1}-1$ cosets of $\mathcal{RM}(1,m)$ in $\mathcal{RM}(2,m)$

   The Boolean functions associated to these cosets are quadratic bent functions with the property that the sum of any two of them is a bent function.

2. Moreover, bent functions can also be used to construct linear codes. Such codes have applications in secret sharing, authentication codes, regular graphs.
3. Bent functions play a role even in very practical issues (memories with self error detection ; transmission and storage of multimedia data) through the so-called *robust error detecting codes* [Karpovsky-Kulikowski-Wang 2009].

A first generic construction

Let Ψ from $\mathbb{F}_q$ to $\mathbb{F}_q$ (where $q = p^m$). Let $\mathcal{C}(\Psi)$ be a linear code over $\mathbb{F}_p$ defined by

$$\mathcal{C}(\Psi) := \{\mathbf{c} = (Tr_{q/p}(\alpha\Psi(x) + \beta x))_{x\in\mathbb{F}_q^*}; \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q\}.$$

Then $\mathcal{C}(\Psi)$ is a $[q-1, k \leq 2m]$-code.

A construction of new good codes via p-ary bent functions

Let Ψ be a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ such that $\Psi(0) = 0$. Let $\alpha \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_{p^m}$. Let $g_{\alpha,\beta}$ be the p-ary function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ given by $g_{\alpha,\beta}(x) = \alpha Tr_{p^m/p}(\Psi(x)) - Tr_{p^m/p}(\beta x)$. Let us define a code as follows :

$$\mathcal{C} := \{\tilde{c}_{\alpha,\beta} = (g_{\alpha,\beta}(\zeta_1), g_{\alpha,\beta}(\zeta_2), \cdots, g_{\alpha,\beta}(\zeta_{p^m-1})), \alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_{p^m}\}, \qquad (2)$$

where $\zeta_1, \cdots, \zeta_{p^m-1}$ denote the nonzero elements of $\mathbb{F}_{p^m}$.

A construction of new good codes via p-ary bent functions

THEOREM (MESNAGER 2016)

Assume that $\psi_1 := Tr_{p^m/p}(\Psi)$ is bent or weakly regular bent if $p = 2$ or p odd, respectively. We denote by $\psi_1^\star$ its dual function. Then the weight distribution of $\mathcal{C}$ (which is of dimension $m+1$) is given as follows. In any characteristic, $wt(\tilde{c}_{0,0}) = 0$ and for $\beta \neq 0$, $wt(\tilde{c}_{0,\beta}) = p^m - p^{m-1}$. Moreover,

1. *when $p = 2$ then $wt(\tilde{c}_{1,\beta}) = 2^{m-1} - (-1)^{\psi_1^*(\beta)} 2^{\frac{m}{2}-1}$ ($\beta \in \mathbb{F}_{2^m}^\star$).*
2. *when p is odd then*
   - *if m is odd then $wt(\tilde{c}_{1,\beta})$ is given by (where $\epsilon = \pm 1$)*

$$\begin{cases} p^m - p^{m-1} \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) = 0; \\ p^m - p^{m-1} - \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}} \left(\frac{\psi_1^*(\bar{\alpha}\beta)}{p}\right) \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) \in \mathbb{F}_{p^m}^\star. \end{cases}$$

   - *if m is even then the Hamming weight of $\tilde{c}_{\alpha,\beta}$ is given by*

$$\begin{cases} p^m - p^{m-1} - p^{\frac{m}{2}-1}\epsilon(p-1) \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) = 0; \\ p^m - p^{m-1} + p^{\frac{m}{2}-1}\epsilon \text{ if } \alpha \in \mathbb{F}_p^\star \text{ and } \psi_1^*(\bar{\alpha}\beta) \in \mathbb{F}_{p^m}^\star. \end{cases}$$

A construction of new good codes via p-ary bent functions

Theorem (Mesnager 2016)

Hamming weight	*Multiplicity*
0	1
$p^m - p^{m-1}$	$2p^m - p^{m-1} - 1$
$p^m - p^{m-1} - \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}}$	$(p^{m-1} + \epsilon p^{\frac{m-1}{2}})\frac{(p-1)^2}{2}$
$p^m - p^{m-1} + \epsilon(\frac{-1}{p})^{\frac{m+1}{2}} p^{\frac{m-1}{2}}$	$(p^{m-1} - \epsilon p^{\frac{m-1}{2}})\frac{(p-1)^2}{2}$

Table: The weight distribution of $\mathcal{C}$ when m is odd

A construction of new good codes via p-ary bent functions

THEOREM (MESNAGER 2016)

Hamming weight	*Multiplicity*
0	1
$p^m - p^{m-1}$	$p^m - 1$
$p^m - p^{m-1} - \epsilon p^{\frac{m}{2}-1}(p-1)$	$p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}(p-1)^2$
$p^m - p^{m-1} + \epsilon p^{\frac{m}{2}-1}$	$(p^m - p^{m-1})(p-1) - \epsilon p^{\frac{m}{2}-1}(p-1)^2$

TABLE: Weight distribution of $\mathcal{C}$ when m is even, p odd

Hamming weight	*Multiplicity*
0	1
2^{m-1}	$2^m - 1$
$2^{m-1} - 2^{\frac{m}{2}-1}$	$2^{m-1} + 2^{\frac{m}{2}-1}$
$2^{m-1} + 2^{\frac{m}{2}-1}$	$2^{m-1} - 2^{\frac{m}{2}-1}$

TABLE: Weight distribution of $\mathcal{C}$ when m is even, $p = 2$

Outline of the proof (the Hamming weights of the codes-words)

- Let $a \in \mathbb{F}_{p^m}$. Let ψ_a a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ defined as : $\psi_a(x) = Tr_{p^m/p}(a\Psi(x))$. For $\tilde{c}_{\alpha,\beta} \in \mathcal{C}_\Psi$, we have : $wt(\tilde{c}_{\alpha,\beta}) = p^m - \frac{1}{q}\sum_{\omega\in\mathbb{F}_q} S_{\psi_{\omega\alpha}}(\omega\beta)$.
- Express the Walsh transform by means of S_{ψ_1} in terms of automorphism σ_α of cyclotomic field $\mathbb{Q}(\xi_p)$ where ξ_p is the primitive pth root of unity ($\sigma_a(\xi_p) = \xi_p^a$) : $wt(\tilde{c}_{\alpha,\beta}) = p^m - p^{m-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \sigma_\omega(\sigma_\alpha(S_{\psi_1}(\bar{\alpha}\beta)))$.
- Use Legendre symbols and identities in Galois field theory : the field $\mathbb{Q}(\xi_p)$ has a unique quadratic subfield $\mathbb{Q}(\sqrt{p^*})$ with $p^* = (\frac{-1}{p})p = (-1)^{(p-1)/2}p$ where $(\frac{a}{p})$ denotes the Legendre symbol for $1 \leq a \leq p-1$. Note that $p^m = (\frac{-1}{p})^m \sqrt{p^*}^{2m}$. For $1 \leq a \leq p-1$, $\sigma_a(\sqrt{p^*}) = (\frac{a}{p})\sqrt{p^*}$.

Outline of the proof (the weight distribution of the code $\mathcal{C}$ (1/2))

The weight distribution of the code $\mathcal{C}$ is closely is related to the bentness of the involved function ψ_1. Let g be a weakly regular bent function over $\mathbb{F}_{p^m}$:

$$S_g(\omega) = \epsilon u p^{\frac{m}{2}} \xi_p^{g^*(\omega)}, \omega \in \mathbb{F}_{p^m},\ \epsilon = \pm 1,\ u \in \{1, i\}.$$

Then g^* is a weakly regular bent function and

$$S_{g^*}(\omega) = \epsilon u^{-1} p^{\frac{m}{2}} \xi_p^{g(-\omega)}, \omega \in \mathbb{F}_{p^m}.$$

The Hamming weights depend if $\psi_1^*(\bar{\alpha}\beta) = 0$ or not. We have then to compute $N_0 := \#\{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m} \mid \psi_1^*(\bar{\alpha}\beta) = 0\} = (p-1)\#\{x \in \mathbb{F}_{p^m} \mid \psi_1^*(x) = 0\}$. Then
$\#\{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_{p^m} \mid \psi_1^*(\bar{\alpha}\beta) \neq 0\} = (p-1)(p^m - N_0)$.

Outline of the proof (the weight distribution of the code $\mathcal{C}$ (2/2))

Set

$$N_j := \#\{x \in \mathbb{F}_{p^m} \mid g(x) = j\}.$$

To complete the proof, we use :

Proposition

Assume $g^*(0) = 0$. Then

- *if m is even,*

$$N_0 = p^{m-1} - \epsilon p^{\frac{m}{2}-1} + \epsilon p^{\frac{m}{2}};$$

$$N_j = p^{m-1} - \epsilon p^{\frac{m}{2}-1}, 1 \leq j \leq p-1;$$

- *if m is odd, $N_0 = p^{m-1}; N_j = p^{m-1} + \epsilon p^{\frac{m-1}{2}}(\frac{j}{p}), 1 \leq j \leq p.$*

For which the proof uses identities of Gauss sums, in particular :

$$\sum_{j=1}^{p} (\frac{j}{p}) \xi_p^j = \begin{cases} p^{\frac{1}{2}}; & \text{if } p \equiv 1 \pmod 4; \\ ip^{\frac{1}{2}}, & \text{if } p \equiv 3 \pmod 4, \end{cases} \tag{3}$$

A second generic construction

Fix a set $D = \{d_1, d_2, \cdots, d_n\}$ in $\mathbb{F}_q$ (where $q = p^m$).
Let $\mathcal{C}_D$ be a linear code defined by

$$\mathcal{C}_D = \{\mathbf{c}_x = (Tr_{q/p}(xd_1), Tr_{q/p}(xd_2), \cdots, Tr_{q/p}(xd_n)), x \in \mathbb{F}_q\}.$$

The set D is usually called the *defining set* of the code $\mathcal{C}_D$.
Then, $\mathcal{C}_D$ is a $[n, k \leq m]$.

The Hamming weight of codeword from the second generic construction

Define for each $x \in \mathbb{F}_q$, $\mathbf{c}_x = (Tr_{q/p}(xd_1), Tr_{q/p}(xd_1), \cdots, Tr_{q/p}(xd_n))$. The Hamming weight $wt(\mathbf{c}_x)$ of $\mathbf{c}_x$ is n-N$_x(0)$, where

$$N_x(0) = \#\{1 \le i \le n \mid Tr_{q/p}(xd_i) = 0\}, \forall x \in \mathbb{F}_q.$$

Note that

$$\begin{aligned} pN_x(0) &= \sum_{i=1}^{n} \sum_{y \in \mathbb{F}_p} e^{\frac{2\pi\sqrt{-1}}{p} y Tr_{q/p}(xd_i)} \\ &= \sum_{i=1}^{n} \sum_{y \in \mathbb{F}_p} \chi_1(yxd_i) = n + \sum_{y \in \mathbb{F}_p^*} \chi_1(yxD), \end{aligned}$$

where χ_1 is the canonical additive character of $\mathbb{F}_q$, aD denotes the set $\{ad \mid d \in D\}$ and $\chi_1(S) := \sum_{x \in S} \chi_1(x)$ for any subset S of $\mathbb{F}_q$. Therefore,

$$wt(\mathbf{c}_x) = \frac{(p-1)}{p} n - \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \chi_1(yxD).$$

Explicit good linear codes based on the second generic construction

In 2015, bent functions have been used to construct linear codes from the second generic construction [Ding 2015], [Zhou-Li-Fan-Helleseth 2015], [Tang-Li-Qi-Zhou-Helleseth 2015].

Good linear codes based on the second generic construction

1) Let $p = 2$. We know that a function f from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is bent if and only if its support $D_f := \{x \in \mathbb{F}_{2^m} \mid f(x) = 1\}$ is a difference set in $(\mathbb{F}_{2^m}, +)$ with parameters

$$(2^m, 2^{m-1} \pm 2^{\frac{(m-2)}{2}}, 2^{m-2} \pm 2^{\frac{(m-2)}{2}}).$$

When f is bent, we have

$$n_f := |D_f| = 2^{m-1} \pm 2^{\frac{(m-2)}{2}}.$$

Theorem (Ding 2015)

Let f be a Boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ with $f(0) = 0$ where m even and $m \geq 4$. Then the code $\mathcal{C}_{D_f}$ is an $[n_f, m, (n_f - 2^{\frac{(m-2)}{2}})/2]$ two-weight binary code with weight distribution given by the next table.

Consequently, *any bent function can be plugged into the above theorem to obtain a two-weight binary linear code*.

Good linear codes based on the second generic construction

Weight	Multiplicity
0	1
$\frac{n_f}{2}-2^{\frac{m-4}{2}}$	$\frac{2^m-1+n_f 2^{-\frac{m-2}{2}}}{2}$
$\frac{n_f}{2}+2^{\frac{m-4}{2}}$	$\frac{2^m-1+n_f 2^{-\frac{m-2}{2}}}{2}$

Good linear codes based on the second generic construction

2) Using Ding's approach [Zhou-Li-Fan-Helleseth 2015] have derived several classes of p-ary linear codes with two or three weights constructed from quadratic bent functions over $\mathbb{F}_p$ where p is an odd prime.
Let Q be a quadratic bent function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Define $D_Q = \{x \in \mathbb{F}_{p^m}^* \mid Q(x) = 0\}$. Then if m is odd, we have $\#D_Q = p^{m-1} - 1$ and if m is even, we have $\#D_Q = p^{m-1} + \epsilon(p-1)p^{\frac{m-2}{2}}$ where $\epsilon \in \{-1, 1\}$.

THEOREM (ZHOU-LI-FAN-HELLESETH 2015)

If m is odd, then the associated code $\mathcal{C}_{D_Q}$ from the second generic construction. $\mathcal{C}_{D_Q}$ is a three-weight linear code with parameters $[p^{m-1} - 1, m]$ whose weight distribution has been given.

THEOREM (ZHOU-LI-FAN-HELLESETH 2015)

If m is even, then $\mathcal{C}_{D_Q}$ is a two- weight linear code with parameters $[p^{m-1} + \epsilon(p-1)p^{\frac{m-2}{2}} - 1, m]$ whose weight distribution has been given.

Good linear codes based on the second generic construction

3) Inspired by the work of C. Ding and K. Ding and C. Ding, Tang et al., [Tang-Li-Qi-Zhou-Helleseth 2015] have generalized their approach to weakly regular bent functions. More precisely, they derived linear codes with two or three weights from a sub-class of p-ary weakly regular bent functions ($\mathcal{WRB}$). Functions of the set $\mathcal{WRB}$ (p odd) vanish at 0 and satisfy the following condition :

$$\exists h \in \mathbb{N} \mid gcd(h-1, p-1) = 1 \text{ and } f(ax) = a^h f(x), \forall (a,x) \in \mathbb{F}_{p^m}^{\star} \times \mathbb{F}_{p^m}. \qquad (4)$$

Good linear codes based on the second generic construction

Given a p-ary function $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$. Define $D_f := \{x \in \mathbb{F}_{p^m} \mid f(x) = 0\}$. They proved the two following results.

THEOREM (TANG-LI-QI-ZHOU-HELLESETH 2015)

Let m be an even integer and f be a function in $\mathcal{WRB}$. Then $\mathcal{C}_{D_f}$ is a two-weight linear code with parameters $[p^{m-1} - 1 + \epsilon(p-1)p^{(m-2)/2}, m]$ (where ϵ denotes the sign of the Walsh transform of f) whose weight distribution has been given.

THEOREM (TANG-LI-QI-ZHOU-HELLESETH 2015)

Let m be a odd integer and f be a function in $\mathcal{WRB}$. Then $\mathcal{C}_{D_f}$ is a three-weight linear code with parameters $[p^{m-1} - 1, m]$ whose weight distribution has been given.

o-polynomials

Definition

Let m be any positive integer. A permutation polynomial G over $\mathbb{F}_{2^m}$ is called an o-polynomial if, for every $\gamma \in \mathbb{F}_{2^m}$, the function H_γ :
$z \in \mathbb{F}_{2^m} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} \text{ if } z \neq 0 \\ 0 \text{ if } z = 0 \end{cases}$ *is a permutation on $\mathbb{F}_{2^m}$.*

The notion of o-polynomial comes from Finite Projective Geometry :

- ☞ There is a close connection between "o-polynomials" and "hyperovals" :

Definition (A hyperoval of $PG_2(2^m)$)

Denote by $PG_2(2^m)$ the projective plane over $\mathbb{F}_{2^m}$.
A hyperoval of $PG_2(2^m)$ is a set of 2^m+2 points no three collinear.

A hyperoval of $PG_2(2^m)$ can then be represented by
$D(f) = \{(1,t,f(t)), t \in \mathbb{F}_{2^n}\} \cup \{(0,1,0),(0,0,1)\}$ or
$D(f) = \{(f(t),t,1), t \in \mathbb{F}_{2^n}\} \cup \{(0,1,0),(1,0,0)\}$ where f is an o-polynomial.

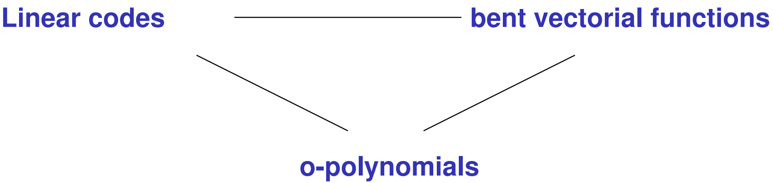
- ☞ There exists a list of only 9 classes of o-polynomials found by the geometers in 40 years

A construction of codes from bent vectorial functions via oval polynomials

New class of bent vectorial functions from oval polynomials

THEOREM (MESNAGER 2015)

Let m be a positive integer. Let G be an oval polynomial on $\mathbb{F}_{2^m}$. The $(2m,m)$-function : $F(x,y) = xG(yx^{2^m-2})$ is bent over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.



Linear codes

bent vectorial functions

o-polynomials

A construction of codes from bent vectorial functions via oval polynomials

Codes from oval polynomials

Let m be a positive integer and r a divisor of m. Let G be an o-polynomial over $\mathbb{F}_{2^m}$ such that $G(0)=0$. For any $\alpha \in \mathbb{F}_{2^m}$, we define the $(2m, r)$-function f_α as follows :

$$\begin{array}{rcccl} f_\alpha & : & \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} & \longrightarrow & \mathbb{F}_{2^r} \\ & & (x,y) & \longmapsto & f_\alpha(x,y) := Tr_r^m(\alpha x G(y x^{2^m-2})). \end{array}$$

Set $E_\delta := \{(x, \delta x) \mid x \in \mathbb{F}_{2^m}\}$ and $E_\infty := \{(0,y) \mid y \in \mathbb{F}_{2^m}\}$.
The set $(\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}) \setminus (E_0 \cup E_\infty)$ can be described as $\{(\gamma_i, \zeta_i) \mid 1 \leq i \leq (2^m-1)^2\}$.

$$\begin{aligned} \mathcal{C}_G &:= \{\bar{c}_\alpha = (f_\alpha(\gamma_1, \zeta_1), \cdots ,f_\alpha(\gamma_{(2^m-1)^2}, \zeta_{(2^m-1)^2})) \mid \alpha \in \mathbb{F}_{2^m}\} \\ &= \{\bar{c}_\alpha = (Tr_r^m(\alpha \gamma_i G(\zeta_i {\gamma_i}^{2^m-2})) \mid 1 \leq i \leq (2^m-1)^2); \alpha \in \mathbb{F}_{2^m}\}. \end{aligned} \tag{5}$$

A construction of codes from bent vectorial functions via oval polynomials

Theorem (Mesnager 2015)

For any o-polynomial G on $\mathbb{F}_{2^m}$ such that $G(0)=0$, the associated 2^r-ary linear code $\mathcal{C}_G$ defined above is a constant weight code with parameters $[(2^m-1)^2, \frac{m}{r}, 2^{m-r}(2^r-1)(2^m-1)]$.

Using [Cohen-Honkala-Litsyn-Lobstein 97], we finally deduce the following result which shows that the hyperovals of $PG_2(2^m)$ give rise to simplex codes.

Theorem (Mesnager 2015)

Let G be an o-polynomial on $\mathbb{F}_{2^m}$ such that $G(0)=0$. The associated code $\mathcal{C}_G$ defined by (5) is equivalent to a $(2^m-1)(2^r-1)$-multiple of 2^r-ary simplex codes $\mathcal{S}_{\frac{m}{r}}(2^r)$. Therefore, the hyperovals $D(G)=\{(1,t,G(t)) \mid t \in \mathbb{F}_{2^m}\} \cup \{(0,1,0),(0,0,1)\}$ in the projective space $PG_2(2^m)$ give rise to codes which are equivalent to $(2^m-1)(2^r-1)$- multiples of 2^r-ary simplex codes $\mathcal{S}_{\frac{m}{r}}(2^r)$ (where r is a divisor of m) whose duals are the 2^r-ary perfect single error-correcting Hamming codes.

Conclusion

In this talk, we have highlighted that bent functions lead to the construction of interesting linear codes (in particular, linear codes with few weights).
Further interesting constructions of linear codes could be obtained through

- other new generic constructions ;
- the know generic constructions using plateaued functions (our future work).