Constructions of linear codes from cryptographic functions over finite fields

Nian Li

Faculty of Mathematics and Statistics

Hubei University

Wuhan, 430062, China

The fourth International Workshop on
Boolean Functions and their Applications (BFA)
Florence, Italy

Outline

Outline

Linear Codes

Let $\mathbb{F}_{p^m}$ denote the finite field with p^m elements, where p is a prime and m is a positive integer.

- Linear code: An $[n,k,d]$ linear code over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum distance d.
- Optimal(resp. almost optimal) code: An $[n,k,d]$ code is called optimal(resp. almost optimal) if its parameters n, k and d (resp. $d+1$)meet a bound on linear codes.
- Weight distribution: The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the weight distribution of C, where A_i is the number of codewords with Hamming weight i in a code C of length n.
- t-weight code: A code C is said to be t-weight if the number of nonzero A_i in $(1, A_1, A_2, \cdots, A_n)$ is equal to t.

Linear Codes

Linear codes with good parameters can be employed in data storage systems and communication systems.

Weight distribution of a code

- allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms [T. Kløve, 2007].
- gives the minimum distance and the error correcting capability of a linear code C.

Main Research Problems:

1. Find new linear codes with good parameters $[n, k, d]$;
2. Determine the weight distribution for a code C.

Applications of Linear Codes

(1) Applications of linear codes:

- communication systems;
- consumer electronics;
- data storage systems;
- $\cdots$

(2) Applications of t-weight linear codes:

- secret sharing;
- authentication codes;
- association schemes;
- strongly regular graphs;
- $\cdots$

Cryptographic Functions

Let $F(x)$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ and $f(x)$ be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. The differential uniformity of $F(x)$ is defined by

$$\delta_F = \max_{a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^m}} \#\{x \in \mathbb{F}_{p^n} : F(x+a) - F(x) = b\}$$

and the Walsh transforms of $f(x)$ and $F(x)$ are defined by

$$\begin{aligned} W_f(a) &= \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{f(x) - \mathrm{Tr}_1^m(ax)}, \\ W_F(a,b) &= \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_1^m(bF(x)) - \mathrm{Tr}_1^n(ax)}, \end{aligned}$$

respectively, where ζ_p is a p-th primitive root of unity.

Cryptographic Functions

Let $f(x)$ and $F(x)$ be defined as above:

- F is perfect nonlinear (PN): $\delta_F = 1$.
- F is almost perfect nonlinear (APN): $\delta_F = 2$.
- f is bent: $|W_f(a)| = p^{m/2}$ for all $a \in \mathbb{F}_{p^m}$.
- F is vectorial bent: $|W_f(a)| = 2^{n/2}$, $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}^*$.
- f is weakly regular bent: $W_f(\lambda) = \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(\lambda)}$, $\varepsilon = \pm 1$.
- F is almost bent (AB): $W_F(a,b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^n}^*$.
- f is a plateaued: $W_f(a) \in \{0, \pm\mu\}$ for all $a \in \mathbb{F}_{p^n}$.
- F is plateaued: each $\mathrm{Tr}_1^m(bF(x))$, $b \neq 0$, is plateaued.
- f is weakly regular s-plateaued: $W_f(a) \in \{0, up^{\frac{m+s}{2}} \zeta_p^{g(a)}\}$, $|u|=1$.

Outline

The First Generic Construction of Linear Codes from Cryptographic Functions

The first generic construction of linear codes from cryptographic functions is given as follows:

$$C_F = \left\{ \mathbf{c}(a,b) = (\mathrm{Tr}_1^m(aF(x) + bx)_{x \in \mathbb{F}_{p^m}^*} : a, b \in \mathbb{F}_{p^m} \right\}$$

where $F(x)$ is a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ and $\mathrm{Tr}_1^m(\cdot)$ is the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$.

Research Problem:

- Select $F(x)$ such that C_F has good parameters.
- Determine the weight distribution of C_F.

The First Generic Construction of Linear Codes from Cryptographic Functions

The dual code $C_F^{\perp}$ of C_F is the code with parity check matrix

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{p^m-2} \\ F(1) & F(\alpha) & F\left(\alpha^2\right) & \ldots & F\left(\alpha^{p^m-2}\right) \end{pmatrix}$$

Theorem (Carlet, Charpin, Zinoviev, 1998) Let d be the minimal distance and $\Omega = \{j : A_i \neq 0, 1 \leq j \leq p^m - 1\}$ be the characteristic set of $C_F^{\perp}$, where $(1, A_1, \cdots, A_{p^m-1})$ is the weight distribution of C_F. If $p = 2$, then

(1) $C_F^{\perp}$ is such that $3 \leq d \leq 5$;

(2) $F(x)$ is APN if and only if $d = 5$;

(3) $F(x)$ is AB if and only if Ω looks as $\{2^{m-1}, 2^{m-1} \pm 2^{(m-1)/2}\}$.

The First Generic Construction of Linear Codes from Cryptographic Functions

$$
\begin{aligned}
C_F &= \left\{\mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x)+bx)_{x\in\mathbb{F}_{p^m}^*} : a,b\in\mathbb{F}_{p^m}\right\} \\
\overline{C}_F &= \left\{\mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x)+bx+c)_{x\in\mathbb{F}_{p^m}^*} : a,b,c\in\mathbb{F}_{p^m}\right\}
\end{aligned}
$$

Theorem (Carlet, Ding, Yuan, 2005) If $F(x)$is PN with $F(0)=0$, then C_F (resp. $\overline{C}_F$) has parameters $[p^m-1, 2m/h, d; p^h]$ (resp. $[p^m-1, 1+2m/h, d; p^h]$) with

$$
d \geq \frac{p^h-1}{p^h}(p^m - p^{m/2}).
$$

Remarks:

- The dual codes of C_F and $\overline{C}_F$ had also been investigated;
- Special cases: such as $h=1$ or $F(x)$ is a power function;
- Many optimal or best known codes were obtained.

The First Generic Construction of Linear Codes from Cryptographic Functions

$$C_F = \left\{ \mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x)) + bx)_{x \in \mathbb{F}_{p^m}^*} : a, b \in \mathbb{F}_{p^m} \right\}$$

The weight distribution of C_F for $h = 1$ was determined when $F(x)$ is a PN function of the form:

(1) $F(x) = x^{p^k+1}$ (Yuan, Carlet, Ding, 2006);

(2) $F(x) = x^{10} - ux^6 - u^2x^2$ (Yuan, Carlet, Ding, 2006);

(3) $F(x) = x^{(3^k+1)/2}$, m odd (Yuan, Carlet, Ding, 2006);

(4) $F(x) = x^{(3^k+1)/2}$ (Feng, Luo, 2007);

(5) $F(x)$ is DO type (Feng, Luo, 2007).

The First Generic Construction of Linear Codes from Cryptographic Functions

$$C_F = \left\{ \mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x) + bx)_{x \in \mathbb{F}_{p^m}^*} : a, b \in \mathbb{F}_{p^m} \right\}$$

In 2017 Mesnager investigated the linear code C_F and showed that it is a 3-weight linear code if

(1) $h = 1$;

(2) $a \in \mathbb{F}_p$; and

(3) $\mathrm{Tr}_1^m(F(x))$ is weakly regular bent.

The First Generic Construction of Linear Codes from Cryptographic Functions

$$C_F = \left\{ \mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x) + bx)_{x \in \mathbb{F}_{p^m}^*} : a, b \in \mathbb{F}_{p^m} \right\}$$

In 2017 Mesnager investigated the linear code C_F and showed that it is a 3-weight linear code if

(1) $h = 1$;

(2) $a \in \mathbb{F}_p$; and

(3) $\mathrm{Tr}_1^m(F(x))$ is weakly regular bent.

Problem

Determine the weight distribution of C_F if $h = 1$, $a \in \mathbb{F}_p$ and $\mathrm{Tr}_1^m(F(x))$ is non-weakly regular bent.

The First Generic Construction of Linear Codes from Cryptographic Functions

$$C_F = \left\{ \mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x) + bx)_{x \in \mathbb{F}_{p^m}^*} : a, b \in \mathbb{F}_{p^m} \right\}$$

In 2019 Mesnager, Özbudak, Sinak extended Mesnager's results and showed that C_F is a 3-weight linear code if

(1) $h = 1$;

(2) $a \in \mathbb{F}_p$; and

(3) $\mathrm{Tr}_1^m(F(x))$ is weakly regular plateaued.

The First Generic Construction of Linear Codes from Cryptographic Functions

$$C_F = \left\{ \mathbf{c}(a,b) = (\mathrm{Tr}_h^m(aF(x) + bx)_{x \in \mathbb{F}_{p^m}^*} : a, b \in \mathbb{F}_{p^m} \right\}$$

In 2019 Mesnager, Özbudak, Sinak extended Mesnager's results and showed that C_F is a 3-weight linear code if

(1) $h = 1$;
(2) $a \in \mathbb{F}_p$; and
(3) $\mathrm{Tr}_1^m(F(x))$ is weakly regular plateaued.

Problem

Determine the weight distribution of C_F if $h = 1$, $a \in \mathbb{F}_p$ and $\mathrm{Tr}_1^m(F(x))$ is non-weakly regular plateaued.

Remark: Research problems when $F(x)$ is a power function!

Outline

The Second Generic Construction of Linear Codes from Cryptographic Functions

The second generic construction of linear codes was proposed by Ding and Niederreiter in 2007 via defining set as follows:

$$C_D = \{(\mathrm{Tr}_1^m(xd_1), \mathrm{Tr}_1^m(xd_2), \cdots, \mathrm{Tr}_1^m(xd_n)) : x \in \mathbb{F}_{p^m}\},$$

where $D = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_{p^m}$.

This is an efficient way to construct linear codes with few weights and it has been showed that all linear codes can be obtained from this approach (C. Xiang, 2016).

Research Problems:

- Select D such that C_D has good parameters.
- Determine the weight distribution of C_D.

The Second Generic Construction of Linear Codes from Cryptographic Functions

The construction of linear codes of the form

$$C_D = \{(\mathrm{Tr}_1^m(xd_1), \mathrm{Tr}_1^m(xd_2), \cdots, \mathrm{Tr}_1^m(xd_n)) : x \in \mathbb{F}_{p^m}\}$$

reattracted researchers' attention due to Ding's work in 2015 in which Ding proposed 3 ways to define the defining set D via a Boolean function f from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$:

- Support of f: $D = \{x \in \mathbb{F}_{2^m} : f(x) = 1\}$;
- Image of f: $D = \{f(x) : x \in \mathbb{F}_{2^m}\}$;
- Preimage of f: $D = \{x \in \mathbb{F}_{2^m} : f(x) = b\}$, $b \in \mathbb{F}_2$.

The Second Generic Construction of Linear Codes from Cryptographic Functions

Let $F(x)$ be a mapping from $\mathbb{F}_{2^m}$ to itself and $f(x) = \mathrm{Tr}_1^m(F(x))$. Ding investigated the linear code C_D when $f(x)$ is one of the following cases:

(1) $f(x)$ is Boolean bent;

(2) $f(x)$ is semibent;

(3) $F(x)$ is AB;

(4) $f(x)$ is a quadratic Boolean function;

(5) $F(x)$ is an o-polynomial;

(6) $F(x)$ are some monomials;

(7) $F(x)$ are some trinomials.

The Second Generic Construction of Linear Codes from Cryptographic Functions

Let $F(x)$ be a mapping from $\mathbb{F}_{2^m}$ to itself and $f(x) = \mathrm{Tr}_1^m(F(x))$. Ding investigated the linear code C_D when $f(x)$ is one of the following cases:

(1) $f(x)$ is Boolean bent;

(2) $f(x)$ is semibent;

(3) $F(x)$ is AB;

(4) $f(x)$ is a quadratic Boolean function;

(5) $F(x)$ is an o-polynomial;

(6) $F(x)$ are some monomials;

(7) $F(x)$ are some trinomials.

Problem

Prove the conjectures proposed by Ding in his paper (Discrete Mathematics 339(2): 2288-2303, 2016).

The Second Generic Construction of Linear Codes from Cryptographic Functions

Motivated by Ding's work, many attempts have been made to construction linear codes of the form

$$C_D = \{(\mathrm{Tr}_1^m(xd_1), \mathrm{Tr}_1^m(xd_2), \cdots, \mathrm{Tr}_1^m(xd_n)) : x \in \mathbb{F}_{p^m}\}$$

by choosing defining sets from nonlinear functions:

$$D = D_f, \text{ where } f(x) = \mathrm{Tr}_1^m(F(x)).$$

The linear code C_D has been well studied if

- $F(x) \overset{\mathrm{PN}}{=} x^2$ (Ding, Ding, 2015);
- $F(x) \overset{\mathrm{PN}}{=} x^{3^k+1}$ or $F(x) = x^{(3^k+1)/2}$ (Heng, Yue, Li, 2016);
- f is quadratic bent (Zhou, L., Fan, Helleseth, 2016);
- f is weakly regular bent (Tang, L., Qi, Zhou, Helleseth, 2016);
- $\cdots$

The Second Generic Construction of Linear Codes from Cryptographic Functions

Ding and Niederreiter's construction of linear codes was extended in three directions:

The Second Generic Construction of Linear Codes from Cryptographic Functions

Ding and Niederreiter's construction of linear codes was extended in three directions:

Generalization I: Let $f:\mathbb{F}_{2^m}\mapsto\mathbb{F}_2$ with $f(ax)=f(x)$, where $a\in\mathbb{F}_{2^t}^*$ and $x\in\mathbb{F}_{2^m}$, $D=\{x\in\mathbb{F}_{2^m}^*:f(x)=0\}$, and C_D is given by

$$C_D=\{(\mathrm{Tr}_t^m(xd))_{d\in D}:x\in\mathbb{F}_{p^m}\}$$

The Second Generic Construction of Linear Codes from Cryptographic Functions

Ding and Niederreiter's construction of linear codes was extended in three directions:

Generalization I: Let $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_2$ with $f(ax) = f(x)$, where $a \in \mathbb{F}_{2^t}^*$ and $x \in \mathbb{F}_{2^m}$, $D = \{x \in \mathbb{F}_{2^m}^* : f(x) = 0\}$, and C_D is given by

$$C_D = \{(\mathrm{Tr}_t^m(xd))_{d \in D} : x \in \mathbb{F}_{p^m}\}$$

Generalization II: Let $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^s}$ and $D = \{d_1, \cdots, d_n\}$ be the support of $\mathrm{Tr}_1^s(\lambda F(x))$. A linear code over $\mathbb{F}_2$ is defined as

$$C_D = \{(\mathrm{Tr}_1^m(xd) + \mathrm{Tr}_1^s(yF(d)))_{d \in D} : x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^s}\}$$

The Second Generic Construction of Linear Codes from Cryptographic Functions

Ding and Niederreiter's construction of linear codes was extended in three directions:

Generalization I: Let $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_2$ with $f(ax) = f(x)$, where $a \in \mathbb{F}_{2^t}^*$ and $x \in \mathbb{F}_{2^m}$, $D = \{x \in \mathbb{F}_{2^m}^* : f(x) = 0\}$, and C_D is given by

$$C_D = \{(\mathrm{Tr}_t^m(xd))_{d \in D} : x \in \mathbb{F}_{p^m}\}$$

Generalization II: Let $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^s}$ and $D = \{d_1, \cdots, d_n\}$ be the support of $\mathrm{Tr}_1^s(\lambda F(x))$. A linear code over $\mathbb{F}_2$ is defined as

$$C_D = \{(\mathrm{Tr}_1^m(xd) + \mathrm{Tr}_1^s(yF(d)))_{d \in D} : x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^s}\}$$

Generalization III: Let $D = D_f \subset (\mathbb{F}_{p^m})^t$, where $f(x)$ is a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. A linear code over $\mathbb{F}_p$ is defined as

$$C_D = \{(\mathrm{Tr}_1^m(a_1x_1 + \cdots + a_tx_t)_{(a_1,\cdots,a_t) \in D} : x_1, \cdots, x_t \in \mathbb{F}_{p^m}\}$$

The Second Generic Construction: Generalization I

Let $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_2$ with $f(ax) = f(x)$, where $a \in \mathbb{F}_{2^t}^*$ and $x \in \mathbb{F}_{2^m}$, $D = \{x \in \mathbb{F}_{2^m}^* : f(x) = 0\}$. Define

$$C_D = \{(\mathrm{Tr}_t^m(xd_1), \mathrm{Tr}_t^m(xd_2), \cdots, \mathrm{Tr}_t^m(xd_n)) : x \in \mathbb{F}_{p^m}\}$$

Xiang, Feng and Tang in 2017 builded up the connection between the weight distribution of C_D and the Walsh spectrum of $f(x)$, and they further studied C_D when

- $f(x)$ is bent;
- $f(x)$ is simibent;
- $f(x)$ is quadratic;
- $f(x) = f_1(x_1) + f_2(x_2)$, where $x = (x_1, x_2)$.

The Second Generic Construction: Generalization II

Let $F: \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^s}$ and $D = \{d_1, \cdots, d_n\}$ be the support of $\mathrm{Tr}_1^s(\lambda F(x))$. Define

$$C_D = \{(\mathrm{Tr}_1^m(xd) + \mathrm{Tr}_1^s(yF(d)))_{d \in D} : x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^s}\}$$

Tang, Carlet and Zhou in 2017 studied C_D when

- $F(x)$ is vectorial Boolean bent $(m = 2s)$;
- $F(x)$ is AB

and further studied its a class of subcodes when

- $F(x)$ is vectorial Boolean bent $(m = 2s)$;
- $F(x)$ is Gold AB.

The Second Generic Construction: Generalization II

Let $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^s}$ and $D = \{d_1, \cdots, d_n\}$ be the support of $\mathrm{Tr}_1^s(\lambda F(x))$. Define

$$C_D = \{(\mathrm{Tr}_1^m(xd) + \mathrm{Tr}_1^s(yF(d)))_{d \in D} : x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^s}\}$$

Tang, Carlet and Zhou in 2017 studied C_D when

- $F(x)$ is vectorial Boolean bent $(m = 2s)$;
- $F(x)$ is AB

and further studied its a class of subcodes when

- $F(x)$ is vectorial Boolean bent $(m = 2s)$;
- $F(x)$ is Gold AB.

Problem

Determine the corresponding properties of the linear codes if $m \neq 2s$ or $F(x)$ is not Gold AB.

The Second Generic Construction: Generalization III

Let $F_i(x)(i = 1, 2, \cdots)$ be mappings from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$. Define

$$C_D = \{(\mathrm{Tr}_1^m(a_1x_1 + \cdots + a_tx_t)_{(a_1,\cdots,a_t)\in D} : x_1, \cdots, x_t \in \mathbb{F}_{p^m}\}$$

where the defining set D is defined as

$$D = \{(x_1, \cdots, x_t) : \mathrm{Tr}_1^m(F_1(x) + \cdots + F_t(x)) = 0\}.$$

The linear code C_D has been investigated when:

- $t = 2$: $F_i(x) = x^{d_i}$ are certain monomials (Li, Yue, Fu, 2016);
- $t \geq 1$: $F(x) = x^2$ (Li, Bae, Yang, 2019);
- $t = 2$: $F_1(x) = x$ and $F_2(x) = x^{p^k+1}$ (Jian, Lin, Feng, 2019);
- $t = 2$: $F_1(x) = x^2$ and $F_2(x) = x^{p^k+1}$ (Jian, Lin, Feng, 2019);
- $t = 2$: $F_i(x)$ is PN (Wu, L., Zeng, under review);
- $\cdots$

The Second Generic Construction: A Modified Construction

Ding and Niederreiter's construction: Let $F(x)$ be a mapping over $\mathbb{F}_{p^m}$, $D = \{\mathrm{Tr}_1^m(F(x)) = 0\}$ and C_D be defined as

$$C_D = \{(\mathrm{Tr}_1^m(xd_1), \mathrm{Tr}_1^m(xd_2), \cdots, \mathrm{Tr}_1^m(xd_n)) : x \in \mathbb{F}_{p^m}\}.$$

A modified construction: Let $F(x)$ be a mapping over $\mathbb{F}_{p^m}$, $D = \{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_1^m(x) = 0\}$ and $C_{F(D)}$ be defined as

$$C_{F(D)} = \{(\mathrm{Tr}_1^m(xF(d_1)), \mathrm{Tr}_1^m(xF(d_2)), \cdots, \mathrm{Tr}_1^m(xF(d_n))) : x \in \mathbb{F}_{p^m}\}.$$

Questions:

1 How to select $F(x)$ such that $C_{F(D)}$ has good parameters?

2 What's the relation between these two constructions?

The Second Generic Construction: A Modified Construction

For the modified construction of linear codes of the form

$$C_{F(D)} = \{(\mathrm{Tr}_1^m(xF(d_1)), \mathrm{Tr}_1^m(xF(d_2)), \cdots, \mathrm{Tr}_1^m(xF(d_n))) : x \in \mathbb{F}_{p^m}\},$$

the following functions were employed to obtain good codes:

- $F(x) = x^2$ (Wang, Li, Lin, 2015);
- $F(x) = x^2$ (Yang, Yao, 2017);
- $F(x) = x^d$, d is of Niho type (Luo, Cao, Xu, Mi, 2017);
- $F(x) = x^{2^h+1}$, (Li, Yan, Wang, Yan, 2019);
- $F(x) = x^d$, d is of Niho type (Hu, L., Zeng, under review);
- $F(x)$ is PN (Wu, L., Zeng, under review);
- $\cdots$

The Second Generic Construction of Linear Codes from Cryptographic Functions

$$\begin{tikzcd} D \arrow[r, "\text{linear code}"] \arrow[d, "F(x)"] & C_D \arrow[d, "?"] \\ F(D) \arrow[r, "\text{linear code}"] & C_{F(D)} \end{tikzcd}$$

Problem

Let $F(x)$ be a mapping over $\mathbb{F}_{p^m}$ and $D \subset \mathbb{F}_{p^m}$. Then

(1) *How to choose $F(x)$ such that $C_{F(D)}$ is good?*

(2) *What's the relation between C_D and $C_{F(D)}$?*

The Second Generic Construction of Linear Codes from Cryptographic Functions

$$\begin{array}{ccc} F(x) & \xrightarrow{\text{Equivalent?}} & G(x) \\ \Big\downarrow D & & \Big\downarrow D \\ C_{F(D)} & \xrightarrow{?} & C_{G(D)} \end{array}$$

Problem

Let $F(x)$ and $G(x)$ be two mappings over $\mathbb{F}_{p^m}$ and $D \subset \mathbb{F}_{p^m}$. Then what's the relation between $C_{F(D)}$ and $C_{G(D)}$ if $F(x)$ and $G(x)$ are equivalent?

Outline

Basic Concepts and Notations

Linear Codes From Cryptographic Functions: Approach I

Linear Codes From Cryptographic Functions: Approach II

Cyclic Codes From Cryptographic Functions: Approach I

Cyclic Codes From Cryptographic Functions: Approach II

Cyclic Codes From Cryptographic Functions: Minimal Polynomial Approach

Let α be a primitive element of $\mathbb{F}_{p^m}$ and $m_{\alpha^i}(x)$ denote the minimal polynomial of α^i over $\mathbb{F}_p$ for $1 \le i \le p^n - 1$. Define

$$C_{(d_1,d_2,\cdots,d_k)} = \langle m_{\alpha^{d_1}}(x) m_{\alpha^{d_2}}(x) \cdots m_{\alpha^{d_k}}(x) \rangle,$$

i.e., cyclic codes with generator polynomial

$$m_{\alpha^{d_1}}(x) m_{\alpha^{d_2}}(x) \cdots m_{\alpha^{d_k}}(x).$$

Research Topics

1. Find $C_{(d_1,d_2,\cdots,d_k)}$ with optimal or good parameters;
2. Determine the weight distribution of its dual code.

Cyclic Codes From Cryptographic Functions: Minimal Polynomial Approach

The cyclic code $C_{(d_1,d_2)}$ had been well studied and it has close connection with

- APN and AB functions;
- cross-correlation between m-sequences.

The details can be reached at

[1] Carlet, Charpin, Zinoviev, Des. Codes Cryptogr. 15: 125-156, 1998.

[2] Canteaut, Charpin, Dobbertin, SIAM J. Discrete Math. 13(1): 105-138, 2000.

[3] Hollmann, Xiang, Finite Fields Appl. 7: 253-286, 2001.

[4] Katz, J. Comb. Theory, Ser. A 119(8): 1644-1659, 2012.

[5] Ding, Li, L., Zhou, Discrete Math. 339: 415-427, 2016.

Cyclic Codes From Cryptographic Functions: Minimal Polynomial Approach

Known results on $C_{(d_1,d_2)}$:

- $p=2$: $C_{(1,e)}$ is optimal if and only if x^e is APN;
- $p=3$: $C_{(1,e)}$ is optimal if x^e is PN;
- $p>3$: $C_{(1,e)}$ cannot be optimal.

In 2013 Ding and Helleseth aimed to find new optimal ternary cyclic codes with parameters $[3^m-1, 3^m-2m-1, 4]$ and they

(1) proved that $C_{(1,e)}$ is optimal if x^e is APN;

(2) proved that $C_{(1,e)}$ is optimal if x^e satisfies certain conditions;

(3) proposed 9 open problems on the optimality of $C_{(1,e)}$.

Problem

What property of x^e leads to an optimal ternary code $C_{(1,e)}$?

Cyclic Codes From Cryptographic Functions: Minimal Polynomial Approach

Open problems proposed by Ding and Helleseth:

(1) $e = 2(3^h + 1)$ (solved by L., Zhou, Helleseth, 2015)

(2) $e = 2(3^{m-1} - 1)$ (solved by L., Li, Helleseth, Ding, Tang, 2014)

(3) $e = (3^h + 5)/2$, m odd (remains open)

(4) $e = (3^h - 5)/2$, m odd (remains open)

(5) $e = (3^h - 5)/2$, m even (remains open)

(6) $e = 3^h + 5$, m even (solved by Han, Yan, 2019)

(7) $e = 3^h + 5$, m prime (partially solved by Han, Yan, 2019)

(8) $e = 3^h + 13$, m prime (partially solved by Han, Yan, 2019)

(9) $e = (3^{m-1} - 1)/2 + 3^h + 1$ (partially solved by Han, Yan, 2019)

Cyclic Codes From Cryptographic Functions: Minimal Polynomial Approach

More results about the cyclic code $C_{(1,e)}$:

(1) Ternary optimal codes:

- $C_{(0,1,e)}$ when x^e is PN (Carlet, Ding, Yuan, 2005);
- $C_{(1,e,\frac{3^m-1}{2})}$ for some e (L., Li, Helleseth, Ding, Tang, 2014)

(2) The weight distribution of $C_{(1,e)}^{\perp}$ is determined when

- x^e is PN (Carlet, Ding, Yuan, 2005);
- x^e is APN (Li, L., Helleseth, Ding, 2014)

(3) Cyclic code $C_{(d_1,d_2)}$

- Ding, Li, L., Zhou, Discrete Math. 339: 415-427, 2016.
- $\cdots$

Outline

Cyclic Codes From Cryptographic Functions: Sequence Approach

Let $C =< g(x) >$ be a cyclic code of length n over $\mathbb{F}_p$. The polynomial $g(x)$ is called the generator polynomial of C and

$$\frac{x^n - 1}{g(x)}$$

is referred to as the parity-check polynomial.

Let $s = (s_i)$ be a sequence of period n over $\mathbb{F}_p$. The minimal polynomial of $s = (s_i)$ is given by

$$\frac{x^n - 1}{\gcd(s(x), x^n - 1)},$$

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

Cyclic Codes From Cryptographic Functions: Sequence Approach

$$s = (s_i) \xrightarrow{\text{minimal polynomial}} \frac{x^n - 1}{\gcd(s(x), x^n - 1)} \xrightarrow{\text{generator polynomial}} C_s$$

Ding in 2012 employed the sequence $s = (s_i)$ over $\mathbb{F}_p$ to construct cyclic code C_s when $s = (s_i)$ is the

- Two-prime sequence;
- Cyclotomic sequence of order 4

and obtained some (almost) optimal cyclic codes.

Problem

What property of the sequence s leads to an (almost) optimal cyclic code?

Cyclic Codes From Cryptographic Functions: Sequence Approach

Let $F(x)$ be a polynomial over $\mathbb{F}_{p^m}$ and α be a primitive element of $\mathbb{F}_{p^m}$. A sequence associated with $F(x)$ is defined by

$$s_i = \mathrm{Tr}_1^m(F(\alpha^i + 1)), \ \forall\, i \geq 0.$$

The following functions were employed to construct cyclic codes:

(1) $F(x) \stackrel{\text{APN}}{=} x^{-1}$ (Ding, 2013; Tang, Qi, Xu, 2014);

(2) $F(x) \stackrel{\text{PN}}{=} x^{p^k+1}$ (Ding, 2013);

(3) $F(x) \stackrel{\text{APN}}{=} x^{p^{2h}-p^h+1}$ (Ding, Zhou, 2014);

(4) $F(x) = x^{(p^h-1)/(p-1)}$ (Ding, Zhou, 2014);

(5) $F(x) \stackrel{\text{PN}}{=} x^{(3^k+1)/2}$ (Ding, 2013);

(6) $F(x) \stackrel{\text{APN}}{=} x^{2^k+3}$ (Ding, Zhou, 2014);

(7) $F(x) \stackrel{\text{APN}}{=} x^{2^{2t}+2^t-1}$, $m = 4t+1$ (Ding, Zhou, 2014);

(8) $F(x)$ are some Dickson polynomials; (Ding, 2012);

(9) $F(x) \stackrel{\text{APN}}{=}$ Dobbertin APN function (Tang, Qi, Xu, 2014).

Cyclic Codes From Cryptographic Functions: Sequence Approach

The details can be found at a nice survey paper:

C. Ding, Cryptogr. Commun. 10(2): 319-341, 2018.

Cyclic Codes From Cryptographic Functions: Sequence Approach

The details can be found at a nice survey paper:

C. Ding, Cryptogr. Commun. 10(2): 319-341, 2018.

Problem

Answer the open problems listed in the above Ding's survey paper.

Cyclic Codes From Cryptographic Functions: Sequence Approach

The details can be found at a nice survey paper:

C. Ding, Cryptogr. Commun. 10(2): 319-341, 2018.

Problem

Answer the open problems listed in the above Ding's survey paper.

Problem

How to determine or give a tight bound on the minimal distance of the cyclic code obtained from this sequence approach?

Cyclic Codes From Cryptographic Functions: Sequence Approach

The details can be found at a nice survey paper:

C. Ding, Cryptogr. Commun. 10(2): 319-341, 2018.

Problem

Answer the open problems listed in the above Ding's survey paper.

Problem

How to determine or give a tight bound on the minimal distance of the cyclic code obtained from this sequence approach?

Problem

Build up deeper connections among the pseudorandom properties of $s = (s_i)$, the cryptographic properties of $F(x)$ and the parameters of C_s.

Thank You !

Questions? Comments? Suggestions?