The skew reversible codes over finite fields

Ranya Djihad Boulanouar

University of Science and Technology Houari Boumediene
Joint work with Dr. **Aicha Batoul**, Dr. **Delphine Boucher**
NCRA-2021

July 6, 2021

Motivation

- Boucher, Geiselmann, and Ulmer.$\Longrightarrow$ Construction of skew cyclic codes .

Motivation

- Boucher, Geiselmann, and Ulmer.$\Longrightarrow$ Construction of skew cyclic codes .
- Ore.$\Longrightarrow$ If θ is not the identity, then $\mathbb{F}_q[x, \theta]$ is not a unique factorization ring.

Motivation

- Boucher, Geiselmann, and Ulmer. $\Longrightarrow$ Construction of skew cyclic codes .
- Ore. $\Longrightarrow$ If θ is not the identity, then $\mathbb{F}_q[x, \theta]$ is not a unique factorization ring.
- Massey. $\Longrightarrow$ Linear codes with complementary duals.

Motivation

- Boucher, Geiselmann, and Ulmer.$\Longrightarrow$ Construction of skew cyclic codes .
- Ore.$\Longrightarrow$ If θ is not the identity, then $\mathbb{F}_q[x,\theta]$ is not a unique factorization ring.
- Massey. $\Longrightarrow$ Linear codes with complementary duals.
- Massey and Yang. $\Longrightarrow$ Reversible codes.

Motivation

- Boucher, Geiselmann, and Ulmer.$\Longrightarrow$ Construction of skew cyclic codes .
- Ore.$\Longrightarrow$ If θ is not the identity, then $\mathbb{F}_q[x,\theta]$ is not a unique factorization ring.
- Massey. $\Longrightarrow$ Linear codes with complementary duals.
- Massey and Yang. $\Longrightarrow$ Reversible codes.

Question

What is the relationship between skew LCD codes and skew reversible codes?

Skew-Polynomial Rings

- $\mathbb{F}_q$, finite field.

Skew-Polynomial Rings

- $\mathbb{F}_q$, finite field.
- θ, automorphism of $\mathbb{F}_q$.

$$\mathbb{F}_q[x,\theta] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} | a_i \in \mathbb{F}_q \quad and \quad n \in \mathbb{N}\}.$$

Skew-Polynomial Rings

- $\mathbb{F}_q$, finite field.
- θ, automorphism of $\mathbb{F}_q$.

$$\mathbb{F}_q[x, \theta] = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} | a_i \in \mathbb{F}_q \quad and \quad n \in \mathbb{N}\}.$$

- Addition : like in $\mathbb{F}_q[x]$

Skew-Polynomial Rings

- $\mathbb{F}_q$, finite field.
- θ, automorphism of $\mathbb{F}_q$.

$$\mathbb{F}_q[x, \theta] = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} | a_i \in \mathbb{F}_q \quad and \quad n \in \mathbb{N}\}.$$

- Addition : like in $\mathbb{F}_q[x]$
- Multiplication : $x \cdot a = \theta(a)x, a \in \mathbb{F}_q$.

Skew-Polynomial Rings

- $\mathbb{F}_q$, finite field.
- θ, automorphism of $\mathbb{F}_q$.

$$\mathbb{F}_q[x, \theta] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} | a_i \in \mathbb{F}_q \quad and \quad n \in \mathbb{N}\}.$$

  - Addition : like in $\mathbb{F}_q[x]$
  - Multiplication : $x \cdot a = \theta(a)x, a \in \mathbb{F}_q$.

- The ring $\mathbb{F}_q[x, \theta]$ is noncommutative unless θ is the identity automorphism on $\mathbb{F}_q$(Ore, 1933).

Skew-Polynomial Rings

Example

Consider the finite field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ where $\alpha^2 + \alpha + 1 = 0$. Consider the Frobenius automorphism

$$\begin{array}{cccc} \theta: & \mathbb{F}_4 & \rightarrow & \mathbb{F}_4 \\ & a & \rightarrow & a^2 \end{array}$$

$$\left.\begin{array}{l} (\alpha x)\cdot(\alpha^2 x) = \alpha^2 x^2 \\ (\alpha^2 x)\cdot(\alpha x) = \alpha x^2 \end{array}\right. \Longrightarrow \quad (\alpha x)\cdot(\alpha^2 x) \neq (\alpha^2 x)\cdot(\alpha x) = \alpha x^2$$

Skew-Polynomial Rings

- A skew polynomial ring $\mathbb{F}_q[x, \theta]$ is a right Euclidean ring and a left Euclidean ring (McDonald).

Skew-Polynomial Rings

- A skew polynomial ring $\mathbb{F}_q[x,\theta]$ is a right Euclidean ring and a left Euclidean ring (McDonald).
- $h^* = \sum_{i=0}^{k} \theta^i(h_{k-i})x^i$: The skew reciprocal polynomial of $h(h_k \neq 0)$

Skew-Polynomial Rings

- A skew polynomial ring $\mathbb{F}_q[x, \theta]$ is a right Euclidean ring and a left Euclidean ring (McDonald).
- $h^* = \sum_{i=0}^{k} \theta^i(h_{k-i})x^i$: The skew reciprocal polynomial of $h(h_k \neq 0)$
- $h^\natural = (1/\theta^k(h_0))h^*$: The left monic skew reciprocal polynomial of $h(h_0 \neq 0)$

Skew-Polynomial Rings

- A skew polynomial ring $\mathbb{F}_q[x, \theta]$ is a right Euclidean ring and a left Euclidean ring (McDonald).
- $h^* = \sum_{i=0}^{k} \theta^i(h_{k-i})x^i$: The skew reciprocal polynomial of $h(h_k \neq 0)$
- $h^\natural = (1/\theta^k(h_0))h^*$: The left monic skew reciprocal polynomial of $h(h_0 \neq 0)$
- Let $\theta \in Aut(\mathbb{F}_q)$. Then the map :

$$\Theta : \begin{cases} \mathbb{F}_q[x, \theta] & \rightarrow & \mathbb{F}_q[x, \theta] \\ \sum_{i=0}^{n} a_i x^i & \mapsto & \sum_{i=0}^{n} \theta(a_i) x^i \end{cases}$$

is a morphism of rings.

Skew-Polynomial Rings

Example ((Boucher and Ulmer, 2009))

Consider $\mathbb{F}_4[x;\theta]$ where θ is the Frobenius automorphism .

$$\begin{aligned} x^4+x^2+1 &= (x^2+x+1)\cdot(x^2+x+1) \\ &= (x^2+\alpha^2)\cdot(x^2+\alpha) \\ &= (x^2+\alpha)\cdot(x^2+\alpha^2) \\ &= (x^2+\alpha^2x+1)\cdot(x^2+\alpha^2x+1) \end{aligned}$$

Linear codes

- A linear code C is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$.

Definitions

Linear codes

- A linear code C is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$.
- The minimum distance of a code C :

$$d_H(C) = \min\{d_H(c_i, c_j) | c_i, c_j \in C, c_i \neq c_j\}.$$

Definitions

Linear codes

- A linear code C is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$.
- The minimum distance of a code C :

$$d_H(C) = \min\{d_H(c_i, c_j) | c_i, c_j \in C, c_i \neq c_j\}.$$

Definitions

- C is **skew λ-constacyclic**, if C is for all $(c_0, c_1, \dots, c_{n-1}) \in C$, $(\lambda\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$.

Linear codes

- A linear code C is a k-dimensional vector subspace of $(\mathbb{F}_q)^n$.
- The minimum distance of a code C :

$$d_H(C) = \min\{d_H(c_i, c_j) | c_i, c_j \in C, c_i \neq c_j\}.$$

Definitions

- C is **skew λ-constacyclic**, if C is for all $(c_0, c_1, \dots, c_{n-1}) \in C$, $(\lambda\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$.
- C is **reversible**, if C is for all $(c_0, c_1, \dots, c_{n-1}) \in C$, $(c_{n-1}, c_{n-2}, \dots, c_0) \in C$.

Duals of skew constacyclic codes over $\mathbb{F}_q$

- The **Euclidean dual:**

$$C^{\perp_E} = \{x \in \mathbb{F}_q^n \mid \forall y \in C, < x, y >_E = 0\}$$

$< x, y >_E := \sum_{i=1}^{n} x_i y_i$

- The Euclidean dual $C^{\perp_E}$ of C is generated by $h^{\natural}$.
Assume that $q = r^2$ is an even power of an arbitrary prime and denote for a in $\mathbb{F}_q$, $\overline{a} = a^r$.
- The **Hermitian dual:**

$$C^{\perp_H} = \{x \in \mathbb{F}_q^n \mid \forall y \in C, < x, y >_H = 0\}$$

$< x, y >_H := \sum_{i=1}^{n} x_i \overline{y_i}$

- The Hermitian dual $C^{\perp_H}$ of C is generated by $\overline{h^{\natural}}$ where for $a(x) = \sum a_i x^i \in R$, $\overline{a(x)} := \sum \overline{a_i} x^i$.

$$\Theta^n(h) \cdot g = x^n - \lambda \Leftrightarrow g \cdot h = x^n - \theta^{-k}(\lambda). \tag{1}$$

h : *skew check polynomial* of C.

- The dual $C^\perp$ of C is a $(\theta, 1/\lambda)$-constacyclic code

Skew generator polynomials of LCD skew cyclic and negacyclic codes ($\lambda^2 = 1$)

Theorem ((Boulanouar, Batoul, and Boucher, 2020))

Consider a (θ, λ)-constacyclic code C with length n, skew generator polynomial g. Consider h in R such that $\Theta^n(h) \cdot g = x^n - \lambda$.

- *C is a Euclidean LCD code if and only if $\mathrm{GCRD}(g, h^{\natural}) = 1$.*

Skew generator polynomials of LCD skew cyclic and negacyclic codes ($\lambda^2 = 1$)

Theorem ((Boulanouar, Batoul, and Boucher, 2020))

Consider a (θ, λ)-constacyclic code C with length n, skew generator polynomial g. Consider h in R such that $\Theta^n(h) \cdot g = x^n - \lambda$.

- *C is a Euclidean LCD code if and only if $\mathrm{GCRD}(g, h^\natural) = 1$.*
- *If q is an even power of a prime number, $q = r^2$, C is a Hermitian LCD code if and only if $\mathrm{GCRD}(g, \overline{h^\natural}) = 1$.*

Reversible codes

In commutative case:

The cyclic code generated by the monic polynomial g is reversible if and only if $g(x)$ is self-reciprocal (i.e $g(x) = g^{\sharp}(x)$). Furthermore, if q is coprime with n, a cyclic code of length n is LCD if and only if C is reversible .

In noncommutative case:

Is it necessarily the case for skew cyclic codes when θ is not the identity?

Example

Let $\mathbb{F}_9 = \mathbb{F}_3(w)$ where $w^2 = w + 1$, θ the Frobenius automorphism and $R = \mathbb{F}_9[x; \theta]$. We have :

$$x^2 - 1 = (x + w^2)(x + w^2)$$

The skew polynomial $g = x + w^2$ is such that $g(x) = g^\sharp(x)$. The greatest common right divisor of $g(x)$ and $h^*(x)$ is $x + w^2$ (i.e $gcrd(g(x), h^*(x)) \neq 1$) therefore, C is not an LCD code.

Skew reversible codes

Definition

1. The code C is called a **skew reversible** code if

$$\forall c \in C \quad c = (c_0, \ldots, c_{n-1}) \in C \Longrightarrow \left(c_{n-1}, \ldots, \theta^{n-1}(c_0)\right) \in C$$

2. If q is an even power of a prime number, $q = p^2$, C is a **conjugate-skew reversible** code if

$$\forall c \in C \quad c = (c_0, \ldots, c_{n-1}) \in C \Longrightarrow \left(\overline{c_{n-1}}, \ldots, \theta^{n-1}(\overline{c_0})\right) \in C$$

Skew reversible codes

Theorem

If skew constacyclic code C is skew reversible(resp. conjugate-skew reversible), then $g = g^{\natural}$(resp. $g = \overline{g^{\natural}}$).

Example

For $\mathbb{F}_9 = \mathbb{F}_3(w)$ where $w^2 = w + 1$ and θ the Frobenius automorphism $\theta : a \mapsto a^3$. In $\mathbb{F}_9[x;\theta]$ the polynomial $x^6 - 1$ has two skew reversible codes generated by a proper central : $g_1(x) = x^2 + 2$ and $g_2(x) = x^4 + x^2 + 1$.

NOTATIONS

Let f, g in R such that $gcrd(f(x), g(x)) = 1$,
$A_{(f,g)} :=$
$\{(a(x), b(x)) \in R^2 \mid a(x)f(x) + b(x)g(x) = 1 \text{ and } b(x)g(x) = g(x)b(x)$

Tools

Consider g, h in R and $\lambda \in \{-1, 1\}$ such that $x^n - \lambda = g \cdot h = h \cdot g$ with $\deg(h) = k$.

- Assume that $A_{(g,\Theta^b(h^*))}$ is nonempty. Then $g = \Theta^{k+b}(g^\natural)$ for all b in $\{0, 1\}$.

Tools

Consider g, h in R and $\lambda \in \{-1, 1\}$ such that $x^n - \lambda = g \cdot h = h \cdot g$ with $\deg(h) = k$.

- Assume that $A_{(g,\Theta^b(h^*))}$ is nonempty. Then $g = \Theta^{k+b}(g^\natural)$ for all b in $\{0, 1\}$.
- If the greatest common right divisor of $h(x)$ and $g(x)$ is equal to 1, g_0 in $\mathbb{F}_q^\theta$ and $g = \Theta^{k+b}(g^\natural)$ then $gcrd(g(x), \Theta^b(h^\natural(x))) = 1$ for all b in $\{0, 1\}$.

Tools

Consider g, h in R and $\lambda \in \{-1, 1\}$ such that $x^n - \lambda = g \cdot h = h \cdot g$ with $\deg(h) = k$.

- Assume that $A_{(g,\Theta^b(h^*))}$ is nonempty. Then $g = \Theta^{k+b}(g^\natural)$ for all b in $\{0, 1\}$.
- If the greatest common right divisor of $h(x)$ and $g(x)$ is equal to 1, g_0 in $\mathbb{F}_q^\theta$ and $g = \Theta^{k+b}(g^\natural)$ then $gcrd(g(x), \Theta^b(h^\natural(x)))) = 1$ for all b in $\{0, 1\}$.
- If the greatest common left divisor of g and h is equal to 1 and if $g = \Theta^b(g^\natural)$, then $gcrd(g(x), \Theta^b(h^\natural(x))) = 1$ for all b in $\{0, 1\}$.

Main result

- If $A_{(g,h^*)}$ is nonempty and if C is an Euclidean LCD skew constacyclic code then $g = \Theta^k(g^\natural)$.

Main result

- If $A_{(g,h^*)}$ is nonempty and if C is an Euclidean LCD skew constacyclic code then $g = \Theta^k(g^\natural)$.
- If $A_{(g,\Theta(h^*))}$ is nonempty and if C is an Hermitian LCD skew constacyclic code then $g = \Theta^{k+1}(g^\natural)$.

Main result

- If $A_{(g,h^*)}$ is nonempty and if C is an Euclidean LCD skew constacyclic code then $g = \Theta^k(g^\natural)$.
- If $A_{(g,\Theta(h^*))}$ is nonempty and if C is an Hermitian LCD skew constacyclic code then $g = \Theta^{k+1}(g^\natural)$.
- If the greatest common right divisor of $h(x)$ and $g(x)$ is equal to 1, g_0 in $\mathbb{F}_q^\theta$ and $g(x) = \Theta^{k+b}(g^\natural(x))$ then C is an Euclidean LCD skew constacyclic code when $b = 0$ and C is an Hermitian LCD skew constacyclic code when $b = 1$.

- If the greatest common left divisor of $h(x)$ and $g(x)$ is equal to 1 and $g = \Theta^b(g^\natural)$ then C is an Euclidean LCD skew constacyclic code when $b = 0$ and C is an Hermitian LCD skew constacyclic code when $b = 1$.

- If the greatest common left divisor of $h(x)$ and $g(x)$ is equal to 1 and $g = \Theta^b(g^\natural)$ then C is an Euclidean LCD skew constacyclic code when $b = 0$ and C is an Hermitian LCD skew constacyclic code when $b = 1$.
- If the greatest common left divisor of $h(x)$ and $g(x)$ is equal to 1 and C is a skew reversible code (resp.conjugate-skew reversible code) then C is an Euclidean LCD skew constacyclic code (resp. C is an Hermitian LCD skew constacyclic code).

REFERENCES

Boucher, D., W. Geiselmann, and F. Ulmer (2007). "Skew cyclic codes". In: *Applicable Algebra in Engineering, Communication and Computing* 18, pp. 379–389.

Boulanouar, R. D., A. Batoul, and D. Boucher (2020). "An Overview on Skew Constacyclic Codes and their Subclass of LCD Codes". In: *Advances in Mathematics of Communications*. DOI: 10.3934/amc.2020085.

Massey, J. L. (1992). "Linear codes with complementary duals". In: *Discrete Mathematics* **106**, pp. 337–342.

Massey, J. L. and X. Yang (1994). "The condition for a cyclic code to have a complementary dual". In: *Discrete Mathematics* **126**, pp. 391–393.

*

Finaly

THANKS FOR
YOUR ATTENTION