Introduction to Space-Time Coding

Frédérique Oggier
frederique@ntu.edu.sg

Division of Mathematical Sciences
Nanyang Technological University, Singapore

Noncommutative Rings and their Applications V, Lens, 12-15 June 2017

Last Time

- 1. A fully diverse space-time code is a family $\mathcal{C}$ of (square) complex matrices such that $\det(\mathbf{X} - \mathbf{X}') \neq 0$ when $\mathbf{X} \neq \mathbf{X}'$.
  2. Division algebras whose elements can be represented as matrices satisfy full diversity by definition.

Last Time

- 1. A fully diverse space-time code is a family $\mathcal{C}$ of (square) complex matrices such that $\det(\mathbf{X} - \mathbf{X}') \neq 0$ when $\mathbf{X} \neq \mathbf{X}'$.
  2. Division algebras whose elements can be represented as matrices satisfy full diversity by definition.
- 1. For coding for MIMO slow fading channels, joint design of an inner and outer code.
  2. The outer code is a coset code, which addresses the problem of codes over matrices.
  3. Connection between codes over matrices and codes over finite fields.

Outline

Construction A

The non-commutative case

Non-associative Algebras

Construction A

- Let $\rho : \mathbb{Z}^N \mapsto \mathbb{F}_2^N$ be the reduction modulo 2 componentwise.
- Let $C \subset \mathbb{F}_2^N$ be an (N, k) linear binary code.
- Then $\rho^{-1}(C)$ is a lattice.

Construction A

- Let $\rho : \mathbb{Z}^N \mapsto \mathbb{F}_2^N$ be the reduction modulo 2 componentwise.
- Let $C \subset \mathbb{F}_2^N$ be an (N, k) linear binary code.
- Then $\rho^{-1}(C)$ is a lattice.

- Let ζ_p be a primitive pth root of unity, p a prime.
- Let $\rho : \mathbb{Z}[\zeta_p]^N \mapsto \mathbb{F}_p^N$ be the reduction componentwise modulo the prime ideal $\mathfrak{p} = (1 - \zeta_p)$.
- Then $\rho^{-1}(C)$ is a lattice, when C is an (N, k) linear code over $\mathbb{F}_p$.
- In particular, $p = 2$ yields the binary Construction A.

Construction A

- Let $\rho : \mathbb{Z}^N \mapsto \mathbb{F}_2^N$ be the reduction modulo 2 componentwise.
- Let $C \subset \mathbb{F}_2^N$ be an (N, k) linear binary code.
- Then $\rho^{-1}(C)$ is a lattice.

- Let ζ_p be a primitive pth root of unity, p a prime.
- Let $\rho : \mathbb{Z}[\zeta_p]^N \mapsto \mathbb{F}_p^N$ be the reduction componentwise modulo the prime ideal $\mathfrak{p} = (1 - \zeta_p)$.
- Then $\rho^{-1}(C)$ is a lattice, when C is an (N, k) linear code over $\mathbb{F}_p$.
- In particular, $p = 2$ yields the binary Construction A.

What about a Construction A from division algebras?

Ingredients

$$
\begin{array}{cc}
A & \Lambda \supset \mathfrak{p}\Lambda \\
| & \\
K & \mathcal{O}_K \supset \mathfrak{p}\mathcal{O}_K \\
\langle\sigma\rangle \,| & \\
F & \mathcal{O}_F \supset \mathfrak{p} \\
| & \\
\mathbb{Q} & \mathbb{Z} \supset p
\end{array}
$$

Ingredients

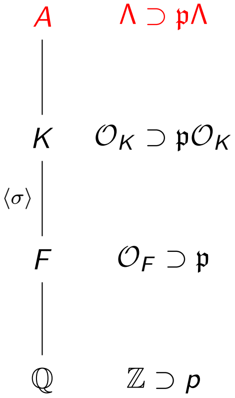
$\mathcal{A}$	$\Lambda \supset \mathfrak{p}\Lambda$
K	$\mathcal{O}_K \supset \mathfrak{p}\mathcal{O}_K$
$\langle\sigma\rangle$	
F	$\mathcal{O}_F \supset \mathfrak{p}$
$\mathbb{Q}$	$\mathbb{Z} \supset p$

- Let K/F be a cyclic number field extension of degree n, and rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Consider the cyclic division algebra

$$\mathcal{A} = K \oplus Ke \oplus \cdots Ke^{n-1}$$

where $e^n = u \in \mathcal{O}_F$, and $ek = \sigma(k)e$ for $k \in K$.

Ingredients



- Let K/F be a cyclic number field extension of degree n, and rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Consider the cyclic division algebra

$$\mathcal{A} = K \oplus Ke \oplus \cdots Ke^{n-1}$$

where $e^n = u \in \mathcal{O}_F$, and $ek = \sigma(k)e$ for $k \in K$.

- Let Λ be its natural order

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}.$$

Ingredients

A — $\Lambda \supset \mathfrak{p}\Lambda$

K — $\mathcal{O}_K \supset \mathfrak{p}\mathcal{O}_K$

$\langle\sigma\rangle$

F — $\mathcal{O}_F \supset \mathfrak{p}$

$\mathbb{Q}$ — $\mathbb{Z} \supset p$

- Let K/F be a cyclic number field extension of degree n, and rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Consider the cyclic division algebra

$$\mathcal{A} = K \oplus Ke \oplus \cdots Ke^{n-1}$$

where $e^n = u \in \mathcal{O}_F$, and $ek = \sigma(k)e$ for $k \in K$.

- Let Λ be its natural order

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}.$$

- Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ so that $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ.

Skew-polynomial Rings

- Given a ring S with a group $\langle \sigma \rangle$ acting on it, the skew-polynomial ring $S[x; \sigma]$ is the set of polynomials $s_0 + s_1 x + \ldots + s_n x^n$, $s_i \in S$ for $i = 0, \ldots, n$, with $xs = \sigma(s)x$ for all $s \in S$.

Skew-polynomial Rings

- Given a ring S with a group $\langle\sigma\rangle$ acting on it, the skew-polynomial ring $S[x;\sigma]$ is the set of polynomials $s_0 + s_1 x + \ldots + s_n x^n$, $s_i \in S$ for $i = 0, \ldots, n$, with $xs = \sigma(s)x$ for all $s \in S$.
- **Lemma.** There is an $\mathbb{F}_{p^f}$-algebra isomorphism between $\Lambda/\mathfrak{p}\Lambda$ and the quotient of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]$ by the two-sided ideal generated by $x^n - u$.

Quotients

$\Lambda \supset \mathfrak{p}\Lambda$ $\quad$ $\Lambda/\mathfrak{p}\Lambda$

$\mathcal{O}_K \supset \mathfrak{p}$ $\quad$ $\mathfrak{p}\mathcal{O}_K$

$\langle\sigma\rangle$

$\mathcal{O}_F$ $\quad$ $\mathcal{O}_F \supset \mathfrak{p}$

$\mathbb{Z} \supset p$ $\quad$ $\mathbb{Z}/p\mathbb{Z}$

Quotients

$\Lambda \supset \mathfrak{p}\Lambda$ $\quad$ $\Lambda/\mathfrak{p}\Lambda$

$\mathcal{O}_K \supset \mathfrak{p}$ $\quad$ $\mathfrak{p}\mathcal{O}_K$

$\langle\sigma\rangle$

$\mathcal{O}_F$ $\quad$ $\mathcal{O}_F \supset \mathfrak{p}$

$\mathbb{Z} \supset p$ $\quad$ $\mathbb{Z}/p\mathbb{Z}$

- There is an $\mathbb{F}_{p^f}$-algebra isomorphism

$$\psi : \Lambda/\mathfrak{p}\Lambda \cong (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u).$$

- If $\mathfrak{p}$ is inert, $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is a finite field

Codes over Finite Fields

$\Lambda/\mathfrak{p}\Lambda$ $\quad\mathbb{F}_q^n$

$\mathcal{O}_K/\mathfrak{p}$ $\quad\mathbb{F}_{p^f}^N$

$\mathbb{Z}/p\mathbb{Z}$ $\quad\mathbb{F}_p^N$

Codes over Finite Fields

$\Lambda/\mathfrak{p}\Lambda$	$\mathbb{F}_q^n$
$\mathcal{O}_K/\mathfrak{p}$	$\mathbb{F}_{p^f}^N$
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{F}_p^N$

- Let $\mathcal{I}$ be a left ideal of Λ, $\mathcal{I} \cap \mathcal{O}_F \supset \mathfrak{p}$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is an ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\psi(\mathcal{I}/\mathfrak{p}\Lambda)$ a left ideal of $\mathbb{F}_q[x;\sigma]/(x^n - u)$.

Codes over Finite Fields

$\Lambda/\mathfrak{p}\Lambda$	$\mathbb{F}_q^n$
$\mathcal{O}_K/\mathfrak{p}$	$\mathbb{F}_{p^f}^N$
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{F}_p^N$

- Let $\mathcal{I}$ be a left ideal of Λ, $\mathcal{I} \cap \mathcal{O}_F \supset \mathfrak{p}$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is an ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\psi(\mathcal{I}/\mathfrak{p}\Lambda)$ a left ideal of $\mathbb{F}_q[x;\sigma]/(x^n - u)$.
- Let $f \in \mathbb{F}_q[x;\sigma]$ be a polynomial of degree n. If (f) is a two-sided ideal of $\mathbb{F}_q[x;\sigma]$, then a *σ-code* consists of codewords $a = (a_0, a_1, \ldots, a_{n-1})$, where $a(x)$ are left multiples of a right divisor g of f.

Codes over Finite Fields

$\Lambda/\mathfrak{p}\Lambda$	$\mathbb{F}_q^n$
$\mathcal{O}_K/\mathfrak{p}$	$\mathbb{F}_{p^f}^N$
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{F}_p^N$

- Let $\mathcal{I}$ be a left ideal of Λ, $\mathcal{I} \cap \mathcal{O}_F \supset \mathfrak{p}$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is an ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\psi(\mathcal{I}/\mathfrak{p}\Lambda)$ a left ideal of $\mathbb{F}_q[x;\sigma]/(x^n - u)$.
- Let $f \in \mathbb{F}_q[x;\sigma]$ be a polynomial of degree n. If (f) is a two-sided ideal of $\mathbb{F}_q[x;\sigma]$, then a *σ-code* consists of codewords $a = (a_0, a_1, \ldots, a_{n-1})$, where $a(x)$ are left multiples of a right divisor g of f.
- Using $\psi : \Lambda/\mathfrak{p}\Lambda \cong \mathbb{F}_q[x;\sigma]/(x^n - u)$, for every left ideal $\mathcal{I}$ of Λ, we get a σ-code $C = \psi(\mathcal{I}/\mathfrak{p}\Lambda)$ over $\mathbb{F}_q$.

[D. Boucher and F. Ulmer, Coding with skew polynomial rings]

Codes over Finite Rings

$\Lambda/\mathfrak{p}\Lambda \quad (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$

$\mathcal{O}_K/\mathfrak{p} \quad (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^N$

$\mathbb{Z}/p\mathbb{Z} \qquad \mathbb{F}_p^N$

Codes over Finite Rings

$\Lambda/\mathfrak{p}\Lambda$ $\quad (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$

$\mathcal{O}_K/\mathfrak{p}$ $\quad (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^N$

$\mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{F}_p^N$

- Let $g(x)$ be a right divisor of $x^n - u$. The ideal $(g(x))/(x^n - u)$ is an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module, isomorphic to a submodule of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$. It forms a *$\sigma$-constacyclic code* of length n and dimension $k = n - deg g(x)$, consisting of codewords $a = (a_0, a_1, \ldots, a_{n-1})$, where $a(x)$ are left multiples of $g(x)$.

Codes over Finite Rings

$\Lambda/\mathfrak{p}\Lambda$ $\quad (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$

$\mathcal{O}_K/\mathfrak{p}$ $\quad (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^N$

$\mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{F}_p^N$

- Let $g(x)$ be a right divisor of $x^n - u$. The ideal $(g(x))/(x^n - u)$ is an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module, isomorphic to a submodule of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$. It forms a *$\sigma$-constacyclic code* of length n and dimension $k = n - degg(x)$, consisting of codewords $a = (a_0, a_1, \ldots, a_{n-1})$, where $a(x)$ are left multiples of $g(x)$.
- A parity check polynomial is computed.

Codes over Finite Rings

$\Lambda/\mathfrak{p}\Lambda$ $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$

$\mathcal{O}_K/\mathfrak{p}$ $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^N$

$\mathbb{Z}/p\mathbb{Z}$ $\mathbb{F}_p^N$

- Let $g(x)$ be a right divisor of $x^n - u$. The ideal $(g(x))/(x^n - u)$ is an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-module, isomorphic to a submodule of $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$. It forms a *$\sigma$-constacyclic code* of length n and dimension $k = n - deg g(x)$, consisting of codewords $a = (a_0, a_1, \ldots, a_{n-1})$, where $a(x)$ are left multiples of $g(x)$.
- A parity check polynomial is computed.
- A dual code is defined.

[Ducoat-O., On Skew Polynomial Codes and Lattices from Quotients of Cyclic Division Algebras]

Lattices

$\Lambda/\mathfrak{p}\Lambda \, (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n \supset C$

$$\begin{array}{cc} \mathcal{O}_K/\mathfrak{p} & \mathbb{F}_p^N \supset C \\ | & \\ \mathbb{Z}/p\mathbb{Z} & \mathbb{F}_p^N \supset C \end{array}$$

Lattices

$\Lambda/\mathfrak{p}\Lambda\,(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n \supset C$

$\mathcal{O}_K/\mathfrak{p}$ $\quad \mathbb{F}_p^N \supset C$

$\mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{F}_p^N \supset C$

- Set the map :

$$\rho : \Lambda \to \psi(\Lambda/\mathfrak{p}\Lambda) = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u),$$

compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ.

Lattices

$\Lambda/\mathfrak{p}\Lambda \, (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n \supset C$

$\mathcal{O}_K/\mathfrak{p} \quad \mathbb{F}_p^N \supset C$

$\mathbb{Z}/p\mathbb{Z} \quad \mathbb{F}_p^N \supset C$

- Set the map :

$$\rho : \Lambda \to \psi(\Lambda/\mathfrak{p}\Lambda) = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u),$$

compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ.

- Set

$$L = \rho^{-1}(C) = \mathcal{I}.$$

Lattices

$\Lambda/\mathfrak{p}\Lambda\,(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n \supset C$

$\mathcal{O}_K/\mathfrak{p}$ $\quad \mathbb{F}_p^N \supset C$

$\mathbb{Z}/p\mathbb{Z}$ $\quad \mathbb{F}_p^N \supset C$

- Set the map :

$$\rho : \Lambda \to \psi(\Lambda/\mathfrak{p}\Lambda) = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(x^n - u),$$

  compositum of the canonical projection $\Lambda \to \Lambda/\mathfrak{p}\Lambda$ with ψ.
- Set

$$L = \rho^{-1}(C) = \mathcal{I}.$$

- Then L is a lattice, that is a $\mathbb{Z}$-module of rank $n^2[F:\mathbb{Q}]$.

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.
- Set $p = 3$, inert in $\mathbb{Q}(i)$, and $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$.

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.
- Set $p = 3$, inert in $\mathbb{Q}(i)$, and $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$.
- Let $\mathfrak{Q}$ be the quaternion division algebra

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e, \;\; e^2 = -1.$$

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.
- Set $p = 3$, inert in $\mathbb{Q}(i)$, and $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$.
- Let $\mathfrak{Q}$ be the quaternion division algebra

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e, \;\; e^2 = -1.$$

- Set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ and $\mathcal{I} = (1 + i + e)\Lambda$.

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.
- Set $p = 3$, inert in $\mathbb{Q}(i)$, and $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$.
- Let $\mathfrak{Q}$ be the quaternion division algebra

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e, \ e^2 = -1.$$

- Set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ and $\mathcal{I} = (1 + i + e)\Lambda$.
- Let $\alpha \in \mathbb{F}_9$ over $\mathbb{F}_3$ satisfy $\alpha^2 + 1 = 0$.

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.
- Set $p = 3$, inert in $\mathbb{Q}(i)$, and $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$.
- Let $\mathfrak{Q}$ be the quaternion division algebra

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e,\ \ e^2 = -1.$$

- Set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ and $\mathcal{I} = (1 + i + e)\Lambda$.
- Let $\alpha \in \mathbb{F}_9$ over $\mathbb{F}_3$ satisfy $\alpha^2 + 1 = 0$.
- We have

$$\psi((1 + i + e)\mathrm{mod} 3) = 1 + \alpha + x,$$

  which is a right divisor of $x^2 + 1$ in $\mathbb{F}_9[x;\sigma]$. Therefore, the left ideal $(x + 1 + \alpha)\mathbb{F}_9[x;\sigma]/(x^2 + 1)$ is a central σ-code.

Example (I)

- Let $K = \mathbb{Q}(i)$ and $F = \mathbb{Q}$. Then $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$.
- Set $p = 3$, inert in $\mathbb{Q}(i)$, and $\mathbb{Z}[i]/3\mathbb{Z}[i] \simeq \mathbb{F}_9$.
- Let $\mathfrak{Q}$ be the quaternion division algebra

$$\mathfrak{Q} = \mathbb{Q}(i) \oplus \mathbb{Q}(i)e, \ \ e^2 = -1.$$

- Set $\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$ and $\mathcal{I} = (1 + i + e)\Lambda$.
- Let $\alpha \in \mathbb{F}_9$ over $\mathbb{F}_3$ satisfy $\alpha^2 + 1 = 0$.
- We have

$$\psi((1 + i + e)\mathrm{mod}3) = 1 + \alpha + x,$$

  which is a right divisor of $x^2 + 1$ in $\mathbb{F}_9[x;\sigma]$. Therefore, the left ideal $(x + 1 + \alpha)\mathbb{F}_9[x;\sigma]/(x^2 + 1)$ is a central σ-code.
- Taking the pre-image by ψ, it corresponds to the left-ideal $\mathcal{I}/3\Lambda$, with $\mathcal{I} = \Lambda(1 + i + e)$.

Example (II)

- For $q = a + be$ in $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e \subset \mathfrak{Q}$, $a, b \in \mathbb{Z}[i]$

$$M(q) = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$$

where $\bar{\cdot}$ is the non-trivial Galois automorphism of $\mathbb{Q}(i)/\mathbb{Q}$.

Example (II)

- For $q = a + be$ in $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e \subset \mathfrak{Q}$, $a, b \in \mathbb{Z}[i]$

$$M(q) = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$$

where $\bar{\cdot}$ is the non-trivial Galois automorphism of $\mathbb{Q}(i)/\mathbb{Q}$.

- $M(q)$ used as codeword for space-time coding.

Example (II)

- For $q = a + be$ in $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e \subset \mathfrak{Q}$, $a, b \in \mathbb{Z}[i]$

$$M(q) = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$$

  where $\bar{\cdot}$ is the non-trivial Galois automorphism of $\mathbb{Q}(i)/\mathbb{Q}$.
- $M(q)$ used as codeword for space-time coding.
- Let $t = (a + be)(1 + i + e)$ be an element of $\mathcal{I} = \Lambda(1 + i + e)$. Then

$$M(t) = \begin{bmatrix} a(1+i) - b & -(\bar{a} + \bar{b}(1+i)) \\ a + b(1-i) & \bar{a}(1-i) - \bar{b} \end{bmatrix}.$$

Example (II)

- For $q = a + be$ in $\mathbb{Z}[i] \oplus \mathbb{Z}[i]e \subset \mathfrak{O}$, $a, b \in \mathbb{Z}[i]$

$$M(q) = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$$

  where $\bar{\cdot}$ is the non-trivial Galois automorphism of $\mathbb{Q}(i)/\mathbb{Q}$.
- $M(q)$ used as codeword for space-time coding.
- Let $t = (a + be)(1 + i + e)$ be an element of $\mathcal{I} = \Lambda(1 + i + e)$. Then

$$M(t) = \begin{bmatrix} a(1+i) - b & -(\bar{a} + \bar{b}(1+i)) \\ a + b(1-i) & \bar{a}(1-i) - \bar{b} \end{bmatrix}.$$

- Then $\mathcal{I} = \rho^{-1}(C)$ is a real lattice of rank 4 embedded in $\mathbb{R}^8$.

Coset Encoding

- Let $v = (v_1, \ldots, v_n)$ be an information vector to be mapped to a lattice point in L.

Coset Encoding

- Let $v = (v_1, \dots, v_n)$ be an information vector to be mapped to a lattice point in L.
- The lattice $L = \rho^{-1}(C) = \mathcal{I}\Lambda$ is a union of cosets of $\mathfrak{p}\Lambda$, each codeword in C is a coset representative.

Coset Encoding

- Let $v = (v_1, \ldots, v_n)$ be an information vector to be mapped to a lattice point in L.
- The lattice $L = \rho^{-1}(C) = \mathcal{I}\Lambda$ is a union of cosets of $\mathfrak{p}\Lambda$, each codeword in C is a coset representative.
- Coset encoding: $v_1, \ldots, v_k$ are encoded using the code C, and the rest of the information coefficients are mapped to a point in the lattice $\mathfrak{p}\Lambda$.

Coset Encoding

- Let $v = (v_1, \ldots, v_n)$ be an information vector to be mapped to a lattice point in L.
- The lattice $L = \rho^{-1}(C) = \mathcal{I}\Lambda$ is a union of cosets of $\mathfrak{p}\Lambda$, each codeword in C is a coset representative.
- Coset encoding: $v_1, \ldots, v_k$ are encoded using the code C, and the rest of the information coefficients are mapped to a point in the lattice $\mathfrak{p}\Lambda$.
- Coset encoding is necessary for wiretap codes: information symbols are mapped to a codeword in C, while random symbols are picked uniformly at random in the lattice $\mathfrak{p}\Lambda$ to confuse the eavesdropper.

Coset Encoding

- Let $v = (v_1, \dots, v_n)$ be an information vector to be mapped to a lattice point in L.
- The lattice $L = \rho^{-1}(C) = \mathcal{I}\Lambda$ is a union of cosets of $\mathfrak{p}\Lambda$, each codeword in C is a coset representative.
- Coset encoding: $v_1, \dots, v_k$ are encoded using the code C, and the rest of the information coefficients are mapped to a point in the lattice $\mathfrak{p}\Lambda$.
- Coset encoding is necessary for wiretap codes: information symbols are mapped to a codeword in C, while random symbols are picked uniformly at random in the lattice $\mathfrak{p}\Lambda$ to confuse the eavesdropper.
- The lattice $L = \rho^{-1}(C) = \mathcal{I}$ thus enables coset encoding for wiretap space-time codes.

Summary

- Cyclic division algebras are useful for space-time coding. Some applications require to understand quotients of cyclic division algebras.
- The view point of skew-polynomial rings.
- Construction A of lattices from codes over skew-polynomial rings.
- Further work:
    1. Study the lattice properties inherited from codes.
    2. Study the space-time codes obtained.
    3. Study constacyclic codes over $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[x;\sigma]/(f(x))$, and duality with respect to a Hermitian inner product.

Construction A

The non-commutative case

Non-associative Algebras

Non-associative Quaternions Algebras: Definition

- Take F a field of characteristic not 2, and K a quadratic extension of F, with non-trivial Galois automorphism σ. Take $\gamma \in K \setminus F$.

Non-associative Quaternions Algebras: Definition

- Take F a field of characteristic not 2, and K a quadratic extension of F, with non-trivial Galois automorphism σ. Take $\gamma \in K \setminus F$.
- Define an algebra structure on the F-vector space $K \times K$ via the multiplication

$$(u, v)(u', v') := (uu' + \gamma v' \sigma(v), \sigma(u)v' + u'v), \; u, u', v'v' \in K.$$

Non-associative Quaternions Algebras: Definition

- Take F a field of characteristic not 2, and K a quadratic extension of F, with non-trivial Galois automorphism σ. Take $\gamma \in K \backslash F$.
- Define an algebra structure on the F-vector space $K \times K$ via the multiplication

$$(u, v)(u', v') := (uu' + \gamma v'\sigma(v), \sigma(u)v' + u'v), \; u, u', v'v' \in K.$$

- Similar to associative quaternions, but for $\gamma \in K \backslash F$, which makes the multiplication not associative anymore.

Non-associative Quaternions Algebras: Definition

- Take F a field of characteristic not 2, and K a quadratic extension of F, with non-trivial Galois automorphism σ.Take $\gamma \in K \backslash F$.
- Define an algebra structure on the F-vector space $K \times K$ via the multiplication

$$(u, v)(u', v') := (uu' + \gamma v'\sigma(v), \sigma(u)v' + u'v), \ u, u', v'v' \in K.$$

- Similar to associative quaternions, but for $\gamma \in K \backslash F$, which makes the multiplication not associative anymore.
- The algebra A is called a *non-associative quaternion algebra* over F. It is a division algebra.

Non-associative Quaternions Algebras: Coding

- In the associative case, codewords are obtained by left regular representation over a maximal subfield K. How to obtain it for A a non-associative F-algebra?

Non-associative Quaternions Algebras: Coding

- In the associative case, codewords are obtained by left regular representation over a maximal subfield K. How to obtain it for A a non-associative F-algebra?
- Let K be a subfield of A. For A to be a right K-vector space, it is sufficient to have $K \subset \mathcal{N}_r(A)$ or $K \subset \mathcal{N}_m(A)$:

$$\mathcal{N}_r(A) = \{x \in A | [A, A, x] = 0\},\ [x, y, z] = (xy)z - x(yz).$$

Non-associative Quaternions Algebras: Coding

- In the associative case, codewords are obtained by left regular representation over a maximal subfield K. How to obtain it for A a non-associative F-algebra?
- Let K be a subfield of A. For A to be a right K-vector space, it is sufficient to have $K \subset \mathcal{N}_r(A)$ or $K \subset \mathcal{N}_m(A)$:

$$\mathcal{N}_r(A) = \{x \in A | [A, A, x] = 0\}, \ [x, y, z] = (xy)z - x(yz).$$

- That the left multiplication λ_a is a linear endomorphism of the right K-vector space A is equivalent to have $K \subset \mathcal{N}_l(A)$.

Non-associative Quaternions Algebras: Coding

- In the associative case, codewords are obtained by left regular representation over a maximal subfield K. How to obtain it for A a non-associative F-algebra?
- Let K be a subfield of A. For A to be a right K-vector space, it is sufficient to have $K \subset \mathcal{N}_r(A)$ or $K \subset \mathcal{N}_m(A)$:

$$\mathcal{N}_r(A) = \{x \in A | [A, A, x] = 0\}, \ [x, y, z] = (xy)z - x(yz).$$

- That the left multiplication λ_a is a linear endomorphism of the right K-vector space A is equivalent to have $K \subset \mathcal{N}_l(A)$.
- Take $K \subset \mathcal{N}_r(A) \cap \mathcal{N}_l(A)$ or $K \subset \mathcal{N}_m(A) \cap \mathcal{N}_l(A)$, which is maximal with respect to inclusion. Consider A as a right K-vector space. We get an embedding

$$\lambda : A \to \mathrm{Mat}_r(K), \ a \mapsto \lambda_a$$

of vector spaces, $r = \dim_K(A)$.

An Example of Non-associative codebook

- Take $K = F(\sqrt{a}) = F(i)$, $\gamma \in K \backslash F$, and A a nonassocative quaternion divison algebras. Set $j = (0, 1)$. Then A has F-basis $\{1, i, j, ji\}$ such that $i^2 = a$, $j^2 = b$ and $xj = j\sigma(x)$ for all $x \in K$.

An Example of Non-associative codebook

- Take $K = F(\sqrt{a}) = F(i)$, $\gamma \in K \backslash F$, and A a nonassocative quaternion divison algebras. Set $j = (0, 1)$. Then A has F-basis $\{1, i, j, ji\}$ such that $i^2 = a$, $j^2 = b$ and $xj = j\sigma(x)$ for all $x \in K$.
- Consider the K-basis $\{1, j\}$ of A. We have an embedding $\lambda : A \to \mathrm{Mat}_2(K)$ which sends $x \in A$ to the matrix of λ_x in the basis $\{1, j\}$.

An Example of Non-associative codebook

- Take $K = F(\sqrt{a}) = F(i)$, $\gamma \in K \backslash F$, and A a nonassocative quaternion divison algebras. Set $j = (0, 1)$. Then A has F-basis $\{1, i, j, ji\}$ such that $i^2 = a$, $j^2 = b$ and $xj = j\sigma(x)$ for all $x \in K$.
- Consider the K-basis $\{1, j\}$ of A. We have an embedding $\lambda : A \to \mathrm{Mat}_2(K)$ which sends $x \in A$ to the matrix of λ_x in the basis $\{1, j\}$.
- This gives the codebook

$$\left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}, \ x_0, x_1 \in K \right\}.$$

[S. Pumplün, T. Unger, "Space-Time Block Codes from Nonassociative Division Algebras."]

Take Home Message (I)

1. *Space-time coding* = Families of square complex matrices, to be transmitted over multiple antenna channels.

Take Home Message (I)

1. *Space-time coding* = Families of square complex matrices, to be transmitted over multiple antenna channels.
2. Good space-time codes = *codes with full diversity*, can be obtained as multiplication matrices coming from cyclic division algebras.

Take Home Message (I)

1. *Space-time coding*= Families of square complex matrices, to be transmitted over multiple antenna channels.
2. Good space-time codes = *codes with full diversity*, can be obtained as multiplication matrices coming from cyclic division algebras.
3. *Codes with high minimum determinant* are obtained by restricting matrix coefficients to rings of integers of number fields.

Take Home Message (I)

1. *Space-time coding*= Families of square complex matrices, to be transmitted over multiple antenna channels.
2. Good space-time codes = *codes with full diversity*, can be obtained as multiplication matrices coming from cyclic division algebras.
3. *Codes with high minimum determinant* are obtained by restricting matrix coefficients to rings of integers of number fields.
4. Recent constructions using *cyclic*, *crossed-products*, *non-associative* algebras.

Take Home Message (II)

1. *Concatenated Space-time coding* using quotients of space-time codes. Connections with codes over finite fields/rings. Joint design?

Take Home Message (II)

1. *Concatenated Space-time coding* using quotients of space-time codes. Connections with codes over finite fields/rings. Joint design?
2. *Construction A* for space-time codes.

Open Questions

Open Questions

1. Space-time block code modulation: characterization of quotients, weights and codes.
2. Construction A: lattices, space-time codes, constacyclic codes.

Thank you for your attention!