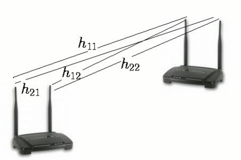
Space-Time Codes from Quotients of Division Algebras

Frédérique Oggier
joint work with B. A. Sethuraman and J. Ducoat

Division of Mathematical Sciences
Nanyang Technological University, Singapore

NCRA IV, Lens

Space-Time Coding: Model



$$\mathbf{Y} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \underbrace{\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}}_{space-time \quad codeword \quad \mathbf{X}} + \mathbf{W}$$

Space-Time Coding: Code Design

- We need a family $\mathcal{C}$ of complex matrices of $n \times n$ matrices such that

$$\det(\mathbf{X} - \mathbf{X}') \neq 0, \ \mathbf{X} \neq \mathbf{X}' \in \mathcal{C}.$$

Space-Time Coding: Code Design

- We need a family $\mathcal{C}$ of complex matrices of $n \times n$ matrices such that
$$\det(\mathbf{X} - \mathbf{X}') \neq 0, \ \ \mathbf{X} \neq \mathbf{X}' \in \mathcal{C}.$$

- *Central simple division algebras* have been used to design space-time codes, in particular cyclic division algebras and crossed products, over number fields.

Cyclic Division Algebras and Natural Order

- Let K/F be a number field extension of degree n with cyclic Galois group $\langle \sigma \rangle$, and respective rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$.
- Consider the cyclic F-algebra A defined by

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

where $e^n = u \in F$, and $ek = \sigma(k)e$ for $k \in K$.

- We assume that u^i, $i = 0, \ldots, n-1$, are not norms in K/F so that the algebra is division, and that $u \in \mathcal{O}_F$.
- Then

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

is an $\mathcal{O}_F$-order of A, which is typically not maximal.

Quotients of Cyclic Division Algebras

The questions are:

- Determine the structure of $\Lambda/\mathcal{J}$ when $\Lambda = \oplus_{i=0}^{n-1}\mathcal{O}_K e^i$ and $\mathcal{J}$ is a two-sided ideal of Λ.
- Construct codes over $\Lambda/\mathcal{J}$ and relate them to the original space-time code.

The Structure of $\Lambda/\mathcal{J}$

- **Lemma.** Let $\mathcal{J}$ be a non zero two-sided ideal of Λ. Then $\mathcal{J} \cap \mathcal{O}_F \neq 0$.
- The intersection $\mathcal{I} = \mathcal{J} \cap \mathcal{O}_F$ is a nonzero ideal of $\mathcal{O}_F$.
- An ideal $\mathcal{I} \neq 0$ of $\mathcal{O}_F$ lies in the center of Λ, and generates $\mathcal{I}\Lambda$.
- We have $\mathcal{J} \supseteq \mathcal{I}$ if and only if $\mathcal{J} \supseteq \mathcal{I}\Lambda$. There is then a one-to-one correspondence between ideals of Λ that contain $\mathcal{I}\Lambda$ and ideals of the quotient $\Lambda/\mathcal{I}\Lambda$ (the ideal $\mathcal{J} \supseteq \mathcal{I}\Lambda$ of Λ corresponds to the ideal $\mathcal{J}/\mathcal{I}\Lambda$ of $\Lambda/\mathcal{I}\Lambda$).
- To determine all quotient rings $\Lambda/\mathcal{J}$, it is enough to determine the ideal structure of $\Lambda/\mathcal{I}\Lambda$ for $\mathcal{I}$ a nonzero ideal of $\mathcal{O}_F$.

[O.-Sethuraman, Quotients of Orders in Cyclic Algebras and Space-Time Codes]

The Structure of $\Lambda/\mathcal{I}\Lambda$

- We have
$$\Lambda/\mathcal{I}\Lambda \cong \oplus_{i=0}^{n-1}(\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)e^i.$$
- **Lemma.**
$$\Lambda/\mathcal{I}\Lambda \cong \mathcal{R}_1 \times \cdots \times \mathcal{R}_t$$
where $\mathcal{R}_i$ is the ring $\oplus_{j=0}^{n-1}(\mathcal{O}_K/\mathfrak{p}_i^{s_i}\mathcal{O}_K)e^j$ is subject to $e(k+\mathfrak{p}_i^{s_i}\mathcal{O}_K) = (\sigma(k)+\mathfrak{p}_i^{s_i}\mathcal{O}_K)e$ and $e^n = u + \mathfrak{p}_i^{s_i}$.
- Characterization for the inertial case ($\mathcal{I} = \mathfrak{p}$ and $\mathcal{I} = q^s,\ s > 1,\ g = e = 1,\ f = n$) and the split case ($\mathcal{I} = \mathfrak{p}$ and $\mathcal{I} = q^s,\ s > 1,\ g > 1,\ e = 1,\ f = n/g$) , for $u \in \mathfrak{p}$ and $u \notin \mathfrak{p}$.
- For example, when $\mathcal{I} = \mathfrak{p}$ and $u \notin \mathfrak{p}$, $\Lambda/\mathcal{I}\Lambda \cong Mat_n(\mathcal{O}_F/\mathfrak{p})$.

Quotients of Cyclic Division Algebras

The questions are:

- Determine the structure of $\Lambda/\mathcal{J}$ when $\Lambda = \oplus_{i=0}^{n-1}\mathcal{O}_K e^i$ and $\mathcal{J}$ is a two-sided ideal of Λ.
  Characterization partially answered (the ramified case is still open).
- Construct codes over $\Lambda/\mathcal{J}$ and relate them to the original space-time code.

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 $x^n - u$.

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

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

Ingredients

	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

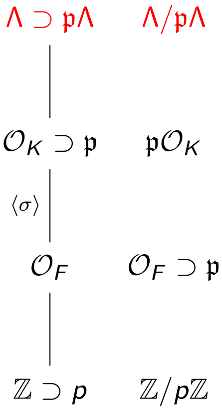
$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}.$$

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

Quotients

$\Lambda \supset \mathfrak{p}\Lambda$	$\Lambda/\mathfrak{p}\Lambda$
$\mathcal{O}_K \supset \mathfrak{p}$	$\mathfrak{p}\mathcal{O}_K$
$\langle\sigma\rangle$	
$\mathcal{O}_F$	$\mathcal{O}_F \supset \mathfrak{p}$
$\mathbb{Z} \supset p$	$\mathbb{Z}/p\mathbb{Z}$

Quotients



- 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 $\mathbb{F}_q[x;\sigma]/(x^n - u)$.
- 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 $a = (a_0, a_1, \dots, a_{n-1})$, 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

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

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

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

- 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 $k = n - degg(x)$, 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.
- A dual code is defined.

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

Lattices

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

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

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

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 $\mathcal{O}_K = \mathbb{Z}[i]$.
- 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 $\mathbb{Q}(i)/\mathbb{Q}$.
- $M(q)$ 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.
- 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.
- The lattice $L = \rho^{-1}(C) = \mathcal{I}$ thus enables coset encoding for wiretap space-time codes.

Thank You

- Cyclic division algebras are useful for space-time coding. Some applications require to understand quotients of cyclic division algebras.
- Characterization of $\Lambda/\mathcal{J}$ (apart for the ramified case).
- 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.