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

$n \times n$ MIMO slow fading channel

$$\underbrace{\mathbf{Y}}_{n \times nL} = \underbrace{\mathbf{H}}_{n \times n} \mathbf{X} + \underbrace{\mathbf{Z}}_{n \times nL}$$

- nL = frame length.
- $\mathbf{X} = [X_1, \ldots, X_L] \in \mathbb{C}^{n \times nL}$.

Code design criteria

Design

$$\mathbf{X} = [X_1, \ldots, X_L] \in \mathbb{C}^{n \times nL}$$

such that

1. X_i are fully diverse, $i = 1, \ldots, L$.
2. the minimum determinant

$$\begin{aligned} \Delta_{min} &= \min_{\mathbf{0} \neq \mathbf{X}} \det(\mathbf{X}\mathbf{X}^*) \\ &= \min_{\mathbf{0} \neq \mathbf{X}} \det(\sum_{i=1}^{L} X_i X_i^*) \\ &\geq \min_{\mathbf{0} \neq \mathbf{X}} (\sum_{i=1}^{L} |\det(X_i)|)^2 \end{aligned}$$

is maximized.

Concatenated codes

1. Choose X_i, $i = 1, \dots, L$ *independently*.
2. Use a *concatenated code*:
   - *inner code* for diversity
   - *outer code* for coding gain

Orders

- Given a cyclic algebra $\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L$, then $\Lambda = \mathcal{O}_L \oplus e\mathcal{O}_L \oplus \ldots \oplus e^{n-1}\mathcal{O}_L$ is an $\mathcal{O}_K$-order.

Orders

- Given a cyclic algebra $\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L$, then $\Lambda = \mathcal{O}_L \oplus e\mathcal{O}_L \oplus \ldots \oplus e^{n-1}\mathcal{O}_L$ is an $\mathcal{O}_K$-order.
- Then Λ is a free module over $\mathcal{O}_K$, with basis $\{b_i\}$, $i = 1, \ldots, n^2$:
$$\Lambda \simeq \oplus_{i=1}^{n^2} b_i \mathcal{O}_K.$$

Orders

- Given a cyclic algebra $\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L$, then $\Lambda = \mathcal{O}_L \oplus e\mathcal{O}_L \oplus \ldots \oplus e^{n-1}\mathcal{O}_L$ is an $\mathcal{O}_K$-order.
- Then Λ is a free module over $\mathcal{O}_K$, with basis $\{b_i\}$, $i = 1, \ldots, n^2$:
$$\Lambda \simeq \oplus_{i=1}^{n^2} b_i \mathcal{O}_K.$$
- If $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank n with basis $\{\beta_k\}$, $k = 1, \ldots, n$:
$$\Lambda \simeq \oplus_{j=1}^{n} e^j \oplus_{k=1}^{n} \beta_k \mathcal{O}_K.$$
Thus $\{b_i\} = \{e^j \beta_k\}$.

Quotients of Orders

- Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, then $\mathfrak{a}\Lambda$ is two-sided and

$$\Lambda/\mathfrak{a}\Lambda \simeq \oplus_{i=1}^{n^2} b_i\mathcal{O}_K/b_i\mathfrak{a}$$

  is a free module over $\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ with basis $\pi(b_i)$ where $\pi : \Lambda \to \Lambda/\mathfrak{a}\Lambda$.

Coset codes for $n = 2, 3, 4$

For $\mathcal{A}$ over L/K, with

$$\begin{aligned} L/K &= \mathbb{Q}(i, \sqrt{5}), \quad \gamma = i \\ L/K &= \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}), \quad \gamma = \zeta_3 \\ L/K &= \mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1}), \quad \gamma = i \end{aligned}$$

we have

$$\begin{aligned} \Lambda/\mathfrak{a}\Lambda &\simeq \mathcal{M}_n(\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K) \\ &\simeq \begin{cases} \mathcal{M}_2(\mathbb{F}_2) & \text{for } n = 2 \\ \mathcal{M}_3(\mathbb{F}_4) & \text{for } n = 3 \\ \mathcal{M}_4(\mathbb{F}_2) & \text{for } n = 4 \end{cases} \end{aligned}$$

Linking $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$.
- We have

$$\mathcal{M}_2(\mathbb{F}_2) \simeq \mathbb{F}_2(\omega) + \mathbb{F}_2(\omega)j \simeq \mathbb{F}_4 \times \mathbb{F}_4$$

where $j^2 = 1$ and $j\omega = \omega^2 j$, given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto j, \ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \mapsto w.$$

Linking $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$.
- We have

$$\mathcal{M}_2(\mathbb{F}_2) \simeq \mathbb{F}_2(\omega) + \mathbb{F}_2(\omega)j \simeq \mathbb{F}_4 \times \mathbb{F}_4$$

where $j^2 = 1$ and $j\omega = \omega^2 j$, given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mapsto j, \ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \mapsto w.$$

- This means:

$$\phi : (a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \mapsto M_{a,b} \in \mathcal{M}_2(\mathbb{F}_2).$$

Cyclic algebras over finite fields

- Cyclic algebra $\mathcal{A} = (\mathbb{F}_{2^n}/\mathbb{F}_2, \sigma, 1)$, with

$$\mathcal{A} \simeq \mathbb{F}_{2^n} \oplus \ldots \mathbb{F}_{2^n} e \oplus \mathbb{F}_{2^n} e^{n-1}.$$

- We have $\mathcal{A} \simeq \mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_{2^n})$.
- The isomorphism $j : \mathcal{A} \to \mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_{2^n})$ is explicitly given by $j(a)$, which is the multiplication by a for all a in $\mathbb{F}_{2^n}$, and $j(e) = \sigma$.
- Induces an isomorphism of $\mathbb{F}_2$-left vector space

$$\phi : \underbrace{\mathbb{F}_{2^n} \times \ldots \times \mathbb{F}_{2^n}}_{n} \to \mathcal{M}_n(\mathbb{F}_2).$$

An isometry between $\mathcal{M}_2(\mathbb{F}_2)$ and $\mathbb{F}_4$

- $\phi : (a, b) \in \mathbb{F}_4 \times \mathbb{F}_4 \mapsto M_{a,b} \in \mathcal{M}_2(\mathbb{F}_2)$ maps

  Hamming weight $1 \mapsto$ invertible.

- Define a weight on the matrices

$$w(M_{a,b}) = \begin{cases} 0 & M_{a,b} = 0 \\ 1 & M_{a,b} \text{invertible} \\ 2 & 0 \neq M_{a,b} \text{non-invertible} \end{cases} .$$

- ϕ is an isometry:

$$w(M_{a,b}) = w(\phi((a, b))) = w_H((a, b))$$

where w_H=Hamming weight.

Higher dimensions

- ϕ can be extended to m-tuples

$$\phi: \quad (\mathbb{F}_{2^n} \times \ldots \times \mathbb{F}_{2^n})^m \quad \to \mathcal{M}_n(\mathbb{F}_2)^m$$

so that if $\pi(\mathcal{C})$ is a code of length m over $\mathcal{M}_n(\mathbb{F}_2)$, then $\phi^{-1}(\pi(\mathcal{C}))$ is a code of length $2m$ over $\mathbb{F}_{2^n}$.

Higher dimensions

- ϕ can be extended to m-tuples

$$\phi : \quad (\mathbb{F}_{2^n} \times \ldots \times \mathbb{F}_{2^n})^m \quad \rightarrow \mathcal{M}_n(\mathbb{F}_2)^m$$

so that if $\pi(\mathcal{C})$ is a code of length m over $\mathcal{M}_n(\mathbb{F}_2)$, then $\phi^{-1}(\pi(\mathcal{C}))$ is a code of length $2m$ over $\mathbb{F}_{2^n}$.

- Open Questions: Variations of Bachoc weight, best weight?

[O., Sole, Belfiore, "Codes over Matrix Rings for Space-Time Coded Modulations"]

Coset codes (non-prime ideals)

- For $\mathcal{G} = \alpha(\mathbb{Z}[i,\theta] \oplus e\mathbb{Z}[i,\theta])$, $e^2 = i$, we have

$$\mathcal{G}/(1+i)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2)$$

and

$$\Delta_{min} \geq \min_{\mathbf{0}\neq\mathbf{X}}(\sum_{i=1}^{L} |\det(X_i)|)^2 \geq \min\left(|1+i|^4\delta, d_{min}^2\delta\right),$$

$\delta=$ minimum determinant of $\mathcal{G}$, d_{min}=minimum distance.

Coset codes (non-prime ideals)

- For $\mathcal{G} = \alpha(\mathbb{Z}[i,\theta] \oplus e\mathbb{Z}[i,\theta])$, $e^2 = i$, we have

$$\mathcal{G}/(1+i)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2)$$

and

$$\Delta_{min} \geq \min_{\mathbf{0}\neq\mathbf{X}} (\sum_{i=1}^{L} |\det(X_i)|)^2 \geq \min\left(|1+i|^4\delta, d_{min}^2\delta\right),$$

$\delta=$ minimum determinant of $\mathcal{G}$, d_{min}=minimum distance.

- To increase the lower bound, what about replacing $(1+i)$ by 2?

$\mathcal{M}_2(\mathbb{F}_2[i])$

- We have

$$\mathcal{G}/(2)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2[i]).$$

$\mathcal{M}_2(\mathbb{F}_2[i])$

- We have
$$\mathcal{G}/(2)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2[i]).$$

- We have
$$\mathcal{M}_2(\mathbb{F}_2[i]) \simeq \mathbb{F}_2(\omega)[i] + \mathbb{F}_2(\omega)[i]j \simeq \mathbb{F}_4[i] \times \mathbb{F}_4[i]$$
where $j^2 = 1$ and $j\omega = \omega^2 j$.

$\mathcal{M}_2(\mathbb{F}_2[i])$

- We have

$$\mathcal{G}/(2)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2[i]).$$

- We have

$$\mathcal{M}_2(\mathbb{F}_2[i]) \simeq \mathbb{F}_2(\omega)[i] + \mathbb{F}_2(\omega)[i]j \simeq \mathbb{F}_4[i] \times \mathbb{F}_4[i]$$

where $j^2 = 1$ and $j\omega = \omega^2 j$.

- This means:

$$\phi : \mathbb{F}_4[i] \times \mathbb{F}_4[i] \mapsto \mathcal{M}_2(\mathbb{F}_2[i]).$$

$\mathbb{F}_4[i])$

- $\mathbb{F}_4[i]$ has 16 elements, 4 of them non-invertible $(a(1+i)$, $a \in \mathbb{F}_4)$.

$\mathbb{F}_4[i])$

- $\mathbb{F}_4[i]$ has 16 elements, 4 of them non-invertible ($a(1+i)$, $a \in \mathbb{F}_4$).
- If $a + b\omega$ is not invertible and $c + d\omega$ is (or vice-versa), then

$$\psi((a+b\omega, c+d\omega)) = \begin{bmatrix} a+d & b+c \\ b+c+d & a+b+d \end{bmatrix}$$

is invertible.

$\mathbb{F}_4[i])$

- $\mathbb{F}_4[i]$ has 16 elements, 4 of them non-invertible ($a(1+i)$, $a \in \mathbb{F}_4$).
- If $a + b\omega$ is not invertible and $c + d\omega$ is (or vice-versa), then

$$\psi((a+b\omega, c+d\omega)) = \begin{bmatrix} a+d & b+c \\ b+c+d & a+b+d \end{bmatrix}$$

is invertible.
- Open Questions: Variations of Bachoc weight, best weight?

Summary

- To design concatenated space-time codes, we looked at quotients of space-time codes.
- We started with good space-time codes, then looked at the obtained quotients, and tried to design proper weights (still quite open...).
- What about considering a joint design?

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 $\mathcal{O}_F$.

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 $k \in K$.

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 $u \in \mathcal{O}_F$.

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 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 $\mathcal{O}_F$.

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 $\mathcal{I}\Lambda$.

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 $\Lambda/\mathcal{I}\Lambda$).

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

$$\Lambda/\mathcal{I}\Lambda \cong \oplus_{i=0}^{n-1}(\mathcal{O}_K/\mathcal{I}\mathcal{O}_K)e^i.$$

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 $e^n = u + \mathfrak{p}_i^{s_i}$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (I)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (I)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.
- Then
$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1} \bar{K} e^j$$
and $e^n = u + \mathfrak{q}$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (I)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.
- Then
$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1} \bar{K} e^j$$
and $e^n = u + \mathfrak{q}$.
- If $u \notin \mathfrak{q}$, then
$$\Lambda/\mathcal{I}\Lambda \simeq (\bar{K}/\bar{F}, \bar{\sigma}, u + \mathfrak{q}) \simeq \mathcal{M}_n(\bar{F}).$$

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (I)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.
- Then

$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1} \bar{K} e^j$$

  and $e^n = u + \mathfrak{q}$.
- If $u \notin \mathfrak{q}$, then

$$\Lambda/\mathcal{I}\Lambda \simeq (\bar{K}/\bar{F}, \bar{\sigma}, u + \mathfrak{q}) \simeq \mathcal{M}_n(\bar{F}).$$

- For $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, i)$, $\Lambda/(1+i)\Lambda \simeq \mathcal{M}_2(\mathbb{F}_2)$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (II)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.
- Then

$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1} \bar{K} e^j$$

and $e^n = u + \mathfrak{q}$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (II)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.
- Then

$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1} \bar{K} e^j$$

  and $e^n = u + \mathfrak{q}$.
- If $u \in \mathfrak{q}$, then

$$\Lambda/\mathcal{I}\Lambda \simeq (\bar{K}/\bar{F}, \bar{\sigma}, 0) \simeq \bar{K}[x, \bar{\sigma}]/\langle x^n \rangle.$$

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (II)

- Inertial case: $\mathcal{I} = \mathfrak{q}$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime. Then $\bar{K} = \mathcal{O}_K/\mathfrak{q}\mathcal{O}_K$ and $\bar{F} = \mathcal{O}_F/\mathfrak{q}$ are finite fields and $\bar{K}/\bar{F}$ is a cyclic extension of degree n.
- Then
$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1} \bar{K} e^j$$
and $e^n = u + \mathfrak{q}$.
- If $u \in \mathfrak{q}$, then
$$\Lambda/\mathcal{I}\Lambda \simeq (\bar{K}/\bar{F}, \bar{\sigma}, 0) \simeq \bar{K}[x, \bar{\sigma}]/\langle x^n \rangle.$$

- For $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, i+1)$, $\Lambda/(1+i)\Lambda \simeq \mathbb{F}_4[x, \bar{\sigma}]/\langle x^2 \rangle$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (III)

- Inertial case: $\mathcal{I} = \mathfrak{q}^s$, $s > 1$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (III)

- Inertial case: $\mathcal{I} = \mathfrak{q}^s$, $s > 1$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime.
- Then

$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1}(\mathcal{O}_K/\mathfrak{q}^s)e^j$$

and $e^n = u + \mathfrak{q}^s$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (III)

- Inertial case: $\mathcal{I} = \mathfrak{q}^s$, $s > 1$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime.
- Then
$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1}(\mathcal{O}_K/\mathfrak{q}^s)e^j$$
and $e^n = u + \mathfrak{q}^s$.
- If $u \notin \mathfrak{q}^s$, then
$$\Lambda/\mathcal{I}\Lambda \simeq \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s).$$

The Structure of $\Lambda/\mathcal{I}\Lambda$: inertial case (III)

- Inertial case: $\mathcal{I} = \mathfrak{q}^s$, $s > 1$, $g = e = 1$, $f = n$ and $q\mathcal{O}_K$ is a prime.
- Then

$$\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1}(\mathcal{O}_K/\mathfrak{q}^s)e^j$$

  and $e^n = u + \mathfrak{q}^s$.
- If $u \notin \mathfrak{q}^s$, then

$$\Lambda/\mathcal{I}\Lambda \simeq \mathcal{M}_n(\mathcal{O}_F/\mathfrak{q}^s).$$

- For $\mathcal{A} = (\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i), \sigma, i)$, $\Lambda/(1+i)^2\Lambda \simeq \mathcal{M}_2(\mathbb{F}_2[i])$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: split case

- Split case: $\mathcal{I} = q$, $g > 1$, $e = 1$, $f = n/g$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: split case

- Split case: $\mathcal{I} = q$, $g > 1$, $e = 1$, $f = n/g$.
- Suppose $\bar{u} \neq 0 \in \bar{F}$. Then $\Lambda/\mathcal{I}\Lambda \simeq \mathcal{M}_n(\bar{F})$.

The Structure of $\Lambda/\mathcal{I}\Lambda$: split case

- Split case: $\mathcal{I} = q$, $g > 1$, $e = 1$, $f = n/g$.
- Suppose $\bar{u} \neq 0 \in \bar{F}$. Then $\Lambda/\mathcal{I}\Lambda \simeq \mathcal{M}_n(\bar{F})$.
- Suppose $\bar{u} = 0 \in \bar{F}$. Then $\Lambda/\mathcal{I}\Lambda \simeq \oplus_{j=0}^{n-1}(\bar{K}^{(1)} \times \ldots \times \bar{K}^{(g)})e^j$.

Quotients of Cyclic Division Algebras

Open questions:

- 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.

Construction A (Commutative)

- 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 (Commutative)

- 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 (Commutative)

- 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.

Before discussing division algebras, let us look at the commutative case.

Construction A (I)

- Take $N = 4$ copies of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$:

$$\mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \times \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \times \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \times \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}]$$

- Take the quotient modulo $p = 2$ componentwise.
- What is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]/2\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$?

Construction A (I)

- Take $N = 4$ copies of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$:

$$\mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \times \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \times \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \times \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}]$$

- Take the quotient modulo $p = 2$ componentwise.
- What is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]/2\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$?
- It is $\mathbb{F}_4 = \{a + bw,\ a, b \in \mathbb{F}_2\}$ where $w^2 + w + 1 = 0$.

Construction A (II)

- Take $N = 4$ copies of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and reduce them modulo $p = 2$ componentwise:

$$\rho : \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}]^4 \to \mathbb{F}_4^4.$$

- Take a linear code C of length 4 inside $\mathbb{F}_4^4$, say

$$\begin{bmatrix} 1 & 0 & w^2 & w \\ 0 & 1 & w & w^2 \end{bmatrix}$$

- Then $\rho^{-1}(C)$ is a lattice.

Construction A (III)

- A generator matrix for $\rho^{-1}(C)$ is given by

$$M_C = \begin{bmatrix} I_k \otimes M & A\tilde{\otimes}M \\ \mathbf{0}_{nN-nk,nk} & I_{N-k} \otimes pM \end{bmatrix}$$

where

$$(I_k, A \mod p) = \begin{bmatrix} 1 & 0 & w^2 & w \\ 0 & 1 & w & w^2 \end{bmatrix},$$

$$A\tilde{\otimes}M = [\sigma_1(A_1) \otimes M_1, \ldots, \sigma_n(A_1) \otimes M_n, \ldots]$$

and

$$M = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}.$$

Construction A: this Example

- Using $N = 4$, $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $p = 2$, and C given by

$$\begin{bmatrix} 1 & 0 & w^2 & w \\ 0 & 1 & w & w^2 \end{bmatrix}$$

  over $\mathbb{F}_4$ gives a lattice of dimension 8, minimum 4, which is 5-modular.
- This is the lattice $Q_8(1)$.

Construction A: some Background

- The case $\mathbb{Z}$ is $p = 2$ is well known, this is the standard binary Construction A proposed by Forney.
- The case $\mathbb{Z}[\zeta_p]$ is known, proposed by Ebeling.
- Many many variations using different ideals, rings etc
- Recent constructions use number fields, to combine Construction A and algebraic lattices.

Construction A: Parameters and Flexibility

- Choose n the degree of the number field, and N the length of the code.
- Use ideals or orders.
- Choose different ideals, which gives different finite structures where to code.
- Introduce a twisting (or scaling) parameter.

Construction A: What For?

- Construction of modular lattices, with large minimum, or other properties.
- Coding applications (encoding - decoding).
- Wiretap coding (secrecy gain).
- Physical network coding.

Some Results

No.	Dim	d	μ_{Λ_c}	ks	$\chi^W_{\Lambda_c}$
1	8	3	2	8	1.2077
2	8	5	2	8	1.0020
3	8	5	4	120	1.2970
4	8	6	3	16	1.1753
5	8	7	2	8	0.8838
6	8	7	3	16	1.1048
7	8	11	3	8	1.0015
8	8	14	2	8	0.5303
9	8	14	3	8	0.9216
10	8	15	3	8	0.8869
11	8	15	4	8	1.0840
12	8	23	3	8	0.6847
13	8	23	5	16	1.0396
14	8	23	5	8	1.1394

Conclusions

- Constructions of lattice from number fields.
- Combined with Construction A.
- Useful for different coding applications: encoding, modularity, wiretap coding, physical network coding.
- Generalizes to the non-commutative case (to be seen next!)

Thank you for your attention!