Algebraic reduction for low-complexity lattice decoding

LAURA LUZZI

Laboratoire ETIS (ENSEA - Université Cergy-Pontoise - CNRS)

LATTICE CODING AND CRYPTO MEETING
IMPERIAL COLLEGE LONDON - SEPTEMBER 24, 2018

Motivation

- algebraic number theory can be used to design lattices with extra multiplicative structure

Motivation

- algebraic number theory can be used to design lattices with extra multiplicative structure
  - from number fields through the canonical embedding
  - from division algebras through the left regular representation

Motivation

- algebraic number theory can be used to design lattices with extra multiplicative structure
  - from number fields through the canonical embedding
  - from division algebras through the left regular representation
- **Question:** can you exploit this extra structure to improve lattice reduction?

Motivation

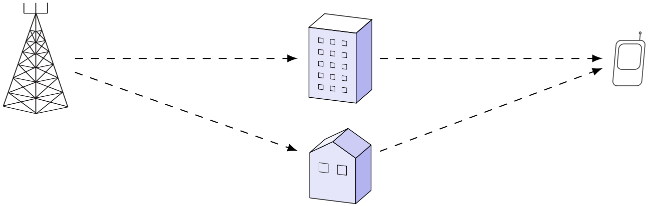
- algebraic number theory can be used to design lattices with extra multiplicative structure
  - from number fields through the canonical embedding
  - from division algebras through the left regular representation
- **Question:** can you exploit this extra structure to improve lattice reduction?
  - in coding theory: for decoding
  - in lattice-based cryptography: for attacks

Outline

Coding for wireless channels

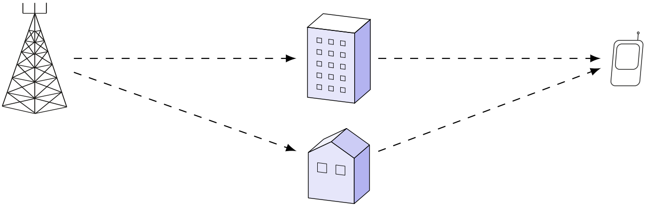
- algebraic number theory is an effective tool to design codes that are full-rate, full-diversity and information-lossless
- in order to increase data rates, both the number of antennas and the size of the signal set can be increased
- this entails a high decoding complexity which is a challenge for practical implementation

Rayleigh fading channels



- fading channel: the signal is scattered by many obstacles and propagates through multiple paths

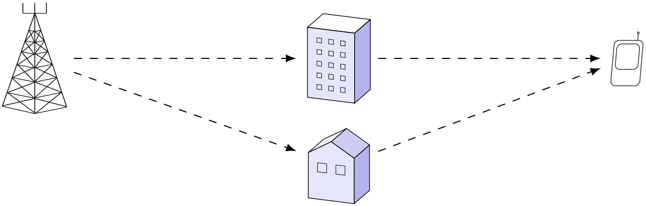
Rayleigh fading channels



- fading channel: the signal is scattered by many obstacles and propagates through multiple paths
- when the number of paths is large, fading and noise can be modelled as Gaussian random variables $h \sim \mathcal{N}_{\mathbb{C}}(0,1)$, $w \sim \mathcal{N}_{\mathbb{C}}(0,\sigma^2)$:

$$\underset{\text{received signal}}{y} = \underset{\text{channel}}{h} \; \underset{\text{codeword}}{x} + \underset{\text{noise}}{w}$$

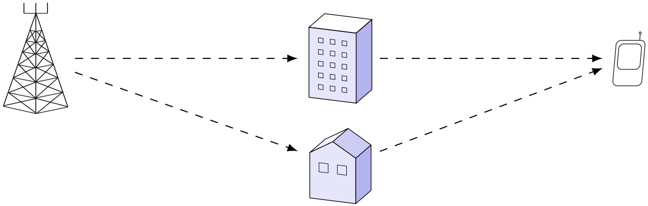
Rayleigh fading channels



- fading channel: the signal is scattered by many obstacles and propagates through multiple paths
- when the number of paths is large, fading and noise can be modelled as Gaussian random variables $h \sim \mathcal{N}_{\mathbb{C}}(0, 1)$, $w \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$:

$$\underset{\text{received signal}}{y} = \underset{\text{channel}}{h} \; \underset{\text{codeword}}{x} + \underset{\text{noise}}{w}$$

Rayleigh fading channels

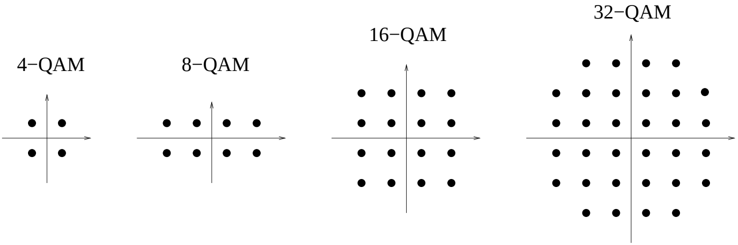


- fading channel: the signal is scattered by many obstacles and propagates through multiple paths
- when the number of paths is large, fading and noise can be modelled as Gaussian random variables $h \sim \mathcal{N}_{\mathbb{C}}(0,1)$, $w \sim \mathcal{N}_{\mathbb{C}}(0,\sigma^2)$:

$$\underbrace{y}_{\text{received signal}} = \underbrace{h}_{\text{channel}} \; \underbrace{x}_{\text{codeword}} + \underbrace{w}_{\text{noise}}$$

- open loop: channel is known at the receiver, but not at the transmitter

Digital modulation



- quadrature-amplitude modulation: a binary information vector is used to modulate an analog waveform
- the set of waveforms $s \in \mathbb{C}$ is a finite subset (constellation) in a lattice
- example: with 16-QAM modulation, each symbol carries 4 data bits

Outline

1. Coding for wireless communications
   - Single antenna systems
   - MIMO systems
2. Decoding
3. Algebraic reduction
   - Single antenna systems
   - MIMO systems

Single antenna systems: code design criteria

Received signal over n time slots:

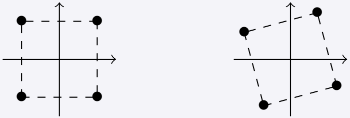
$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} h_1 & & & \\ & h_2 & & \\ & & \ddots & \\ & & & h_n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

$$\mathbf{y} = \mathbf{H} \quad \mathbf{x} + \mathbf{w}$$

Diversity order and product distance

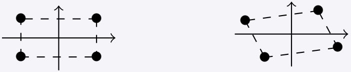
To minimize the error probability, one should maximize the diversity order L, i.e. the minimum number of distinct components between any two constellation points, and the product distance $d_p(\mathbf{x}, \mathbf{x}') = \prod_{\substack{i=1,\ldots,n \\ x_i \neq x_i'}} |x_i - x_i'|$

before fading



$L = 1$ $\qquad$ $L = 2$

after fading



Lattice codes from number fields

- K field extension of degree n of $\mathbb{Q}(i)$, $\sigma_1, \ldots, \sigma_n$ embeddings $K \to \mathbb{C}$ that fix $\mathbb{Q}(i)$
- $\mathcal{O}_K$ ring of integers of K, $\{\theta_1, \ldots, \theta_n\}$ basis of $\mathcal{O}_K$ over $\mathbb{Z}[i]$.
- (relative) **canonical embedding** $\phi : \mathcal{O}_K \to \mathbb{C}^n$
$$x \mapsto \mathbf{x} = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x))^t$$
- $x = s_1\theta_1 + \ldots + s_n\theta_n \in \mathcal{O}_K, \quad \mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{Z}[i]^n$
$$\Rightarrow \mathbf{x} = \psi(x) = s_1\psi(\theta_1) + \ldots + s_n\psi(\theta_n) = \Phi\mathbf{s} \quad \text{lattice point}$$
$\Lambda = \psi(\mathcal{O}_K)$ ideal lattice

Full diversity property

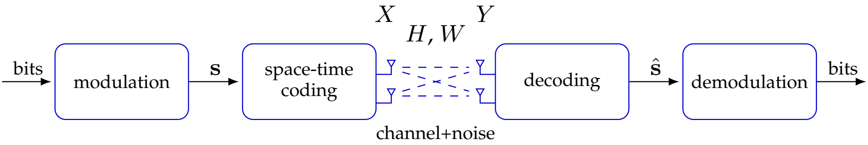
$$\forall \mathbf{x} \in \Lambda \setminus \{0\}, \quad \prod_{i=1}^{n} |x_i|^2 = \prod_{i=1}^{n} |\sigma_i(x)|^2 = N_{K/\mathbb{Q}}(x) \geq 1$$

- constructions of $\mathbb{Z}[i]^n$ from ideal lattices [Bayer-Fluckiger *et al.* 2006]
$\Rightarrow \quad \Phi$ unitary

Outline

1. Coding for wireless communications
   - Single antenna systems
   - MIMO systems
2. Decoding
3. Algebraic reduction
   - Single antenna systems
   - MIMO systems

Multiple antenna systems: space-time coding



$$\underset{\text{received signal}}{Y_{n\times t}} = \underset{\text{channel}}{H_{n\times m}} \; \underset{\text{codeword}}{X_{m\times t}} + \underset{\text{noise}}{W_{n\times t}}$$

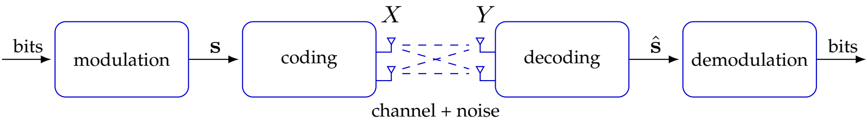
- m transmit antennas, n receive antennas, t frame length
- introduce a dependency between the spatial (antenna) and temporal domain: codewords are represented by matrices or space-time blocks
- H, W random with i.i.d. complex Gaussian entries
- the matrix element $x_{ij} \in \mathbb{C}$ represents the signal sent by antenna i at time j

MIMO techniques in communication standards

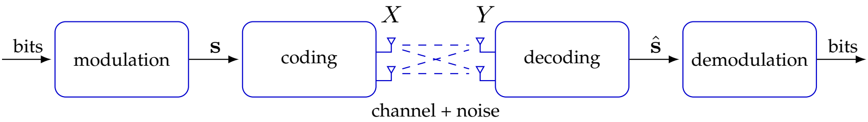
- HSPA+ (3G UMTS standard): 2×2 MIMO for mobile phones, since 2010
- LTE (4G): 2×2 and 4×4 MIMO (2600 MHz and 800 MHz frequency bands), since 2014
- WiFi: routers and laptops have 2 or 3 antennas

- 5G: hundreds of antennas at the base station (massive MIMO)

Rate-reliability trade-off

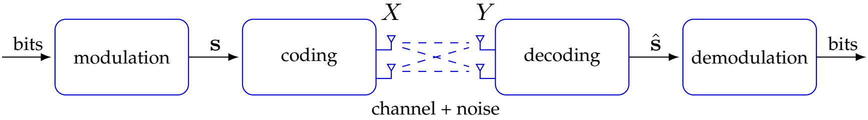


Rate-reliability trade-off



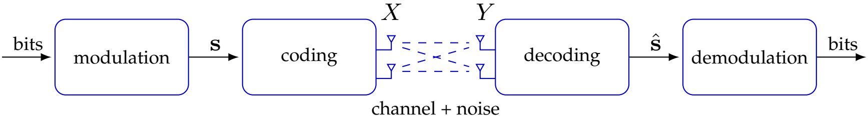
- multiplexing gain:
  - send independent data on each antenna
  - improve the rate

Rate-reliability trade-off



- multiplexing gain:
  - send independent data on each antenna
  - improve the rate
- diversity gain:
  - send multiple copies of the same data through independent paths
  - improve the reliability

Rate-reliability trade-off



- multiplexing gain:
  - send independent data on each antenna
  - improve the rate
- diversity gain:
  - send multiple copies of the same data through independent paths
  - improve the reliability
- can you do both things at the same time?

  $\Rightarrow$ diversity - multiplexing gain trade-off (DMT) [Zheng and Tse 2003]

Design criteria for space-time codes

Union bound estimate of the error probability [Tarokh *et al* 1998]

For a linear code, the difference of two codewords is still a codeword:

$$P_e \leq \sum_{X \in \mathcal{C} \setminus \{0\}} \frac{1}{(\det(I + \mathrm{SNR}\, X X^\dagger))^n}$$

$\Rightarrow$ At high signal-to noise ratio (SNR), $P_e \leq \displaystyle\sum_{X \in \mathcal{C} \setminus \{0\}} \frac{1}{\mathrm{SNR}^{nm} (\det(X X^\dagger))^n}$

Design criteria for space-time codes

Union bound estimate of the error probability [Tarokh *et al* 1998]

For a linear code, the difference of two codewords is still a codeword:

$$P_e \leq \sum_{X \in \mathcal{C} \setminus \{0\}} \frac{1}{(\det(I + \mathrm{SNR}\, XX^\dagger))^n}$$

$\Rightarrow$ At high signal-to noise ratio (SNR), $P_e \leq \sum_{X \in \mathcal{C} \setminus \{0\}} \frac{1}{\mathrm{SNR}^{nm}(\det(XX^\dagger))^n}$

- rank criterion: each nonzero codeword should be full-rank
- determinant criterion: maximize $\inf_{X \in \mathcal{C} \setminus \{0\}} \det(XX^\dagger)$

Design criteria for space-time codes

Union bound estimate of the error probability [Tarokh *et al* 1998]

For a linear code, the difference of two codewords is still a codeword:

$$P_e \leq \sum_{X \in \mathcal{C} \setminus \{0\}} \frac{1}{(\det(I + \mathrm{SNR}\, XX^\dagger))^n}$$

$\Rightarrow$ At high signal-to noise ratio (SNR), $P_e \leq \sum_{X \in \mathcal{C} \setminus \{0\}} \frac{1}{\mathrm{SNR}^{nm} (\det(XX^\dagger))^n}$

- rank criterion: each nonzero codeword should be full-rank
- determinant criterion: maximize $\inf_{X \in \mathcal{C} \setminus \{0\}} \det(XX^\dagger)$

$\Rightarrow$ the multiplicative structure of the code plays a role

- codes with non-vanishing determinant for any signal set achieve the DMT [Elia *et al.* 2006]

Space-time codes from cyclic division algebras

- F number field of degree k

Space-time codes from cyclic division algebras

- F number field of degree k
- K/F cyclic Galois extension of degree n, $\quad \mathrm{Gal}(K/F) = <\sigma>$

Space-time codes from cyclic division algebras

- F number field of degree k
- K/F cyclic Galois extension of degree n, $\quad \mathrm{Gal}(K/F) =< \sigma >$

Cyclic algebra

$$\mathcal{A} = (K/F, \sigma, \gamma) = K \oplus eK \oplus \cdots \oplus e^{n-1}K$$

where $e \in \mathcal{A}$ satisfies the following properties:

- $xe = e\sigma(x) \;\; \forall x \in K$,
- $e^n = \gamma \in F^*$

Space-time codes from cyclic division algebras

- F number field of degree k
- K/F cyclic Galois extension of degree n, $\quad \mathrm{Gal}(K/F) =< \sigma >$

Cyclic algebra

$$\mathcal{A} = (K/F, \sigma, \gamma) = K \oplus eK \oplus \cdots \oplus e^{n-1}K$$

where $e \in \mathcal{A}$ satisfies the following properties:

- $xe = e\sigma(x) \;\; \forall x \in K$,
- $e^n = \gamma \in F^*$

- $\mathcal{A}$ is a division algebra if every nonzero element is invertible

Space-time codes from cyclic division algebras

Left regular representation $\psi : \mathcal{A} \to M_n(K) \subset M_n(\mathbb{C})$

$a = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1} \in \mathcal{A}$

$$\psi(a) = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}$$

Space-time codes from cyclic division algebras

Left regular representation $\psi : \mathcal{A} \to M_n(K) \subset M_n(\mathbb{C})$

$a = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1} \in \mathcal{A}$

$$\psi(a) = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}$$

Obtain a matrix lattice $\Lambda \subset M_n(\mathbb{C})$ from a discrete subset of $\mathcal{A}$:

Space-time codes from cyclic division algebras

Left regular representation $\psi : \mathcal{A} \to M_n(K) \subset M_n(\mathbb{C})$

$a = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1} \in \mathcal{A}$

$$\psi(a) = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}$$

Obtain a matrix lattice $\Lambda \subset M_n(\mathbb{C})$ from a discrete subset of $\mathcal{A}$:

- a subring $\mathcal{O} \subset \mathcal{A}$ containing the identity is an order if it is a $\mathcal{O}_F$-module and generates $\mathcal{A}$ as a linear space over $\mathbb{Q}$

Space-time codes from cyclic division algebras

Left regular representation $\psi: \mathcal{A} \to M_n(K) \subset M_n(\mathbb{C})$

$a = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1} \in \mathcal{A}$

$$\psi(a) = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}$$

Obtain a matrix lattice $\Lambda \subset M_n(\mathbb{C})$ from a discrete subset of $\mathcal{A}$:

- a subring $\mathcal{O} \subset \mathcal{A}$ containing the identity is an order if it is a $\mathcal{O}_F$-module and generates $\mathcal{A}$ as a linear space over $\mathbb{Q}$
- $\Lambda = \psi(\mathcal{O})$ is a matrix lattice in $M_n(\mathbb{C})$

Non-vanishing determinant property

- the determinant of the regular representation of an element is its reduced norm:

$$\det(\psi(a)) = N_{\mathcal{A}/F}(a) \neq 0 \quad \text{if} \quad a \neq 0$$

Non-vanishing determinant property

- the determinant of the regular representation of an element is its reduced norm:

$$\det(\psi(a)) = N_{\mathcal{A}/F}(a) \neq 0 \quad \text{if} \quad a \neq 0$$

- problem: the minimum determinant of the code $\mathcal{C}$ might vanish when $|\mathcal{C}| \to \infty$

Non-vanishing determinant property

- the determinant of the regular representation of an element is its reduced norm:

$$\det(\psi(a)) = N_{\mathcal{A}/F}(a) \neq 0 \quad \text{if} \quad a \neq 0$$

- problem: the minimum determinant of the code $\mathcal{C}$ might vanish when $|\mathcal{C}| \to \infty$

Construction of NVD codes [Oggier *et al.* 2006], [Elia *et al.* 2006]

- if $a \in \Lambda$, $N_{\mathcal{A}/F}(a) \in \mathcal{O}_F$
- $F = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$ $\Rightarrow$ the ring of integers $\mathcal{O}_F$ is discrete
- $\mathcal{C} \subset \psi(\mathcal{O}) \Rightarrow \inf_{X \in \mathcal{C} \setminus \{0\}} |\det X| \geq 1$

Examples

Alamouti code [Alamouti 1998]

- 2 transmit and 1 receive antenna, used in WiFi and 4G standards
- $\mathcal{A}$ is the algebra of Hamilton quaternions

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} s_1 & -\bar{s}_2 \\ s_2 & \bar{s}_1 \end{pmatrix}, \quad s_1, s_2 \in \mathbb{Z}[i]$$

Examples

Alamouti code [Alamouti 1998]

- 2 transmit and 1 receive antenna, used in WiFi and 4G standards
- $\mathcal{A}$ is the algebra of Hamilton quaternions

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} s_1 & -\bar{s}_2 \\ s_2 & \bar{s}_1 \end{pmatrix}, \quad s_1, s_2 \in \mathbb{Z}[i]$$

Golden Code [Belfiore *et al* 2005]

- 2×2 MIMO, optional profile in WiMAX standard
- $\mathcal{A} = (\mathbb{Q}(i,\theta)/\mathbb{Q}(i), \sigma, i)$, $\quad \theta$ golden number, $\alpha = 1 + i\sigma(\theta)$

$$X = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(s_1 + s_2\theta) & \alpha(s_3 + s_4\theta) \\ \sigma(\alpha)i(s_3 + s_4\sigma(\theta)) & \sigma(\alpha)(s_1 + s_2\sigma(\theta)) \end{pmatrix}, \; s_1, s_2, s_3, s_4 \in \mathbb{Z}[i]$$

Outline

Lattice point representation

Example: the Golden Code

$$X = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(s_1 + s_2\theta) & \alpha(s_3 + s_4\theta) \\ \bar{\alpha}i(s_3 + s_4\bar{\theta}) & \bar{\alpha}(s_1 + s_2\bar{\theta}) \end{pmatrix}$$

$$\mathbf{x} = v(X) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \alpha\theta & 0 & 0 \\ 0 & 0 & \bar{\alpha}i & \bar{\alpha}\bar{\theta}i \\ 0 & 0 & \alpha & \alpha\theta \\ \bar{\alpha} & \bar{\alpha}\bar{\theta} & 0 & 0 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} = \Phi\mathbf{s}$$

Vectorized system

$$\mathbf{y} = H_l\Phi\mathbf{s} + \mathbf{w}$$

- H_l linear map corresponding to multiplication by H
- Φ (unitary) generator matrix
- s information vector

Lattice point representation

Example: the Golden Code

$$X = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(s_1 + s_2\theta) & \alpha(s_3 + s_4\theta) \\ \bar{\alpha} i(s_3 + s_4\bar{\theta}) & \bar{\alpha}(s_1 + s_2\bar{\theta}) \end{pmatrix}$$

$$\mathbf{x} = v(X) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \alpha\theta & 0 & 0 \\ 0 & 0 & \bar{\alpha} i & \bar{\alpha}\bar{\theta} i \\ 0 & 0 & \alpha & \alpha\theta \\ \bar{\alpha} & \bar{\alpha}\bar{\theta} & 0 & 0 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} = \Phi\mathbf{s}$$

Vectorized system

$$\mathbf{y} = H_l \Phi \mathbf{s} + \mathbf{w}$$

- H_l linear map corresponding to multiplication by H
- Φ (unitary) generator matrix
- $\mathbf{s}$ information vector

Maximum likelihood (ML) decoding

Solve the closest vector problem (CVP) in the lattice generated by H_l:

$$\hat{\mathbf{x}} = \operatorname*{argmin}_{\mathbf{x}' \in v(\mathcal{C})} \left\| \mathbf{y} - H_l \mathbf{x}' \right\|^2$$

How hard are lattice problems in wireless communications?

- for general lattices, SVP and CVP are NP-hard [Ajtai 1998, Goldreich 1999]
- in lattice-based cryptography, average-case hardness is needed rather than worst-case hardness
- Ajtai discovered a connection between worst-case and average-case complexity of lattice problems

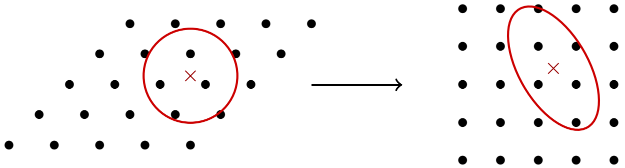
Different notions of random lattices

- in mathematics: use the invariant measure on the space of lattices $\mathrm{SL}_n(\mathbb{R})/\,\mathrm{SL}_n(\mathbb{Z})$ derived from the Haar measure on $\mathrm{SL}_n(\mathbb{R})$
- in cryptography: generator matrix is uniform mod q
- in communications: generator matrix has Gaussian entries

Decoding MIMO lattices

- ML decoders
  - Sphere Decoder, Schnorr-Euchner algorithm...
  - optimal performance but exponential complexity
- Suboptimal decoders
  - zero forcing (ZF), successive interference cancellation (SIC)...
  - polynomial complexity, but poor performance
  - can be improved by preprocessing techniques

Sphere-decoding algorithm (Finkhe-Pohst)



- enumerate all the lattice points inside a sphere centered in the received signal
- when a lattice point is found, the radius of the sphere can be updated
- apply a change of basis which maps the lattice into $\mathbb{Z}^N$: the sphere becomes an ellipsoid

Complexity of sphere decoding

J. Jalden, B. Ottersten, “On the Complexity of Sphere Decoding in Digital Communications”, *IEEE Transactions on Signal Processing* vol 53 n.4, 2005

- [Jaldén and Ottersten 2005]: the average complexity of the sphere decoding algorithm at *fixed SNR* is exponential and scales like $L^{\gamma N}$, where $\gamma \in (0, 1]$ depends on the SNR
- various techniques to reduce the complexity of sphere decoding: pruning of the decision tree, pre-processing, design of special fast-decodable codes...
- is it possible to achieve good performance with polynomial complexity?

Channel preprocessing

Example: ZF decoding

$$\mathbf{y} = H\mathbf{x} + \mathbf{w}$$
$$\hat{\mathbf{x}}_{\mathrm{ZF}} = \left\lfloor H^{-1}\mathbf{y} \right\rceil = \left\lfloor \mathbf{x} + H^{-1}\mathbf{w} \right\rceil$$

- if H is orthogonal, ZF decoding is optimal
- if H is ill-conditioned, the noise $H^{-1}\mathbf{w}$ is amplified

Channel preprocessing

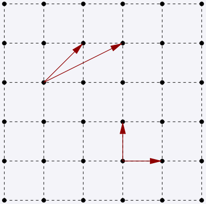
Example: ZF decoding

$$\mathbf{y} = H\mathbf{x} + \mathbf{w}$$
$$\hat{\mathbf{x}}_{\text{ZF}} = \lfloor H^{-1}\mathbf{y} \rceil = \lfloor \mathbf{x} + H^{-1}\mathbf{w} \rceil$$

- if H is orthogonal, ZF decoding is optimal
- if H is ill-conditioned, the noise $H^{-1}\mathbf{w}$ is amplified

- **Solution:** channel preprocessing by lattice reduction improves the performance of suboptimal decoders

Preprocessing using LLL reduction

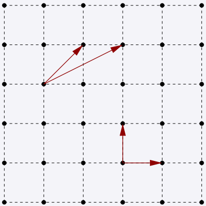


- find a better lattice basis

$$H_{\text{red}} = HT,$$

T unimodular

Preprocessing using LLL reduction



- find a better lattice basis

$$H_{\text{red}} = HT,$$

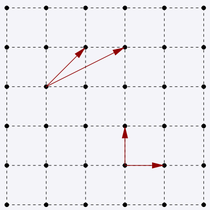
T unimodular

LLL-ZF decoder

= LLL + Babai rounding

- compute the pseudo-inverse $H_{\text{red}}^{\dagger}$
- $\hat{\mathbf{x}}_{\text{LLL}-\text{ZF}} = T\left(\left\lfloor H_{\text{red}}^{\dagger}\mathbf{y}\right\rceil\right)$

Preprocessing using LLL reduction



- find a better lattice basis

$$H_{\text{red}} = HT,$$

T unimodular

LLL-ZF decoder

= LLL + Babai rounding

- compute the pseudo-inverse $H_{\text{red}}^{\dagger}$
- $\hat{\mathbf{x}}_{\text{LLL}-\text{ZF}} = T\left(\left\lfloor H_{\text{red}}^{\dagger}\mathbf{y}\right\rceil\right)$

LLL-SIC decoder

= LLL + Babai nearest plane

- QR decomposition of H_{red}
- $\tilde{\mathbf{y}} = Q^H\mathbf{y} = R\mathbf{x} + Q^H\mathbf{w}$
- recursively compute $\tilde{x}_N = \left\lfloor \frac{\tilde{y}_N}{r_{NN}} \right\rceil$,
  $\tilde{x}_i = \left\lfloor \frac{\tilde{y}_i - \sum_{j=i+1}^{N} r_{ij}\tilde{x}_j}{r_{ii}} \right\rceil, \quad i = N-1, \ldots, 1$
- $\hat{\mathbf{x}}_{\text{LLL}-\text{SIC}} = T\tilde{\mathbf{x}}$

Preprocessing using LLL reduction

Complexity

- average number of iterations in the LLL algorithm for Rayleigh fading matrices $\sim O\left(N^2 \log N\right)$ [Jalden *et al.* 2008]
- the worst-case number of iterations is unbounded
- each iteration requires $O(N^2)$ operations, which can be reduced to $O(N)$ for LLL-SIC [Ling, Howgrave-Graham 2007]
- the average complexity of LLL-SIC is bounded by $O(N^3 \log N)$

Preprocessing using LLL reduction

Complexity

- average number of iterations in the LLL algorithm for Rayleigh fading matrices $\sim O\left(N^2 \log N\right)$ [Jalden *et al.* 2008]
- the worst-case number of iterations is unbounded
- each iteration requires $O(N^2)$ operations, which can be reduced to $O(N)$ for LLL-SIC [Ling, Howgrave-Graham 2007]
- the average complexity of LLL-SIC is bounded by $O(N^3 \log N)$

- improved decoding techniques based on LLL:
  - decoding by embedding [Luzzi, Rekaya, Belfiore 2010], [Luzzi, Stehlé, Ling 2013]
  - decoding by sampling [Liu, Ling, Stehlé 2011], [Wang, Liu, Ling 2013]

Algebraic reduction

- up to now, algebraic tools have been used for coding but not for decoding

Algebraic reduction

- up to now, algebraic tools have been used for coding but not for decoding
- algebraic reduction is a right preprocessing method that exploits the multiplicative structure of the code

Algebraic reduction

- up to now, algebraic tools have been used for coding but not for decoding
- algebraic reduction is a right preprocessing method that exploits the multiplicative structure of the code
- **main idea: absorb part of the channel into the code**

Algebraic reduction

- up to now, algebraic tools have been used for coding but not for decoding
- algebraic reduction is a right preprocessing method that exploits the multiplicative structure of the code
- **main idea: absorb part of the channel into the code**
- approximate the channel matrix with a unit of the code

Outline

Outline

1. Coding for wireless communications
   - Single antenna systems
   - MIMO systems
2. Decoding
3. Algebraic reduction
   - Single antenna systems
   - MIMO systems

Algebraic reduction for fast fading channels

G. Rekaya, J.-C. Belfiore, E. Viterbo, "A very efficient lattice reduction tool on fast fading channels", ISITA 2004

- Single antenna case:

$$\mathbf{y} = H\mathbf{x} + \mathbf{w},$$

$\mathbf{x} = \psi(x) \in \Lambda = \psi(\mathcal{O}_K)$ ideal lattice

$$x = s_1\theta_1 + \ldots + s_n\theta_n \in \mathcal{O}_K$$

Algebraic reduction for fast fading channels

G. Rekaya, J.-C. Belfiore, E. Viterbo, "A very efficient lattice reduction tool on fast fading channels", ISITA 2004

- Single antenna case:

$$\mathbf{y} = H\mathbf{x} + \mathbf{w},$$

$\mathbf{x} = \psi(x) \in \Lambda = \psi(\mathcal{O}_K)$ ideal lattice

$$x = s_1\theta_1 + \ldots + s_n\theta_n \in \mathcal{O}_K$$

- Normalization of the received signal:

$$\mathbf{y}' = \frac{\mathbf{y}}{\sqrt[n]{\det(H)}} = H_1\mathbf{x} + \mathbf{w}', \quad \det(H_1) = 1$$

Algebraic reduction for fast fading channels

G. Rekaya, J.-C. Belfiore, E. Viterbo, "A very efficient lattice reduction tool on fast fading channels", ISITA 2004

- Single antenna case:

$$\mathbf{y} = H\mathbf{x} + \mathbf{w},$$

$\mathbf{x} = \psi(x) \in \Lambda = \psi(\mathcal{O}_K)$ ideal lattice

$$x = s_1\theta_1 + \ldots + s_n\theta_n \in \mathcal{O}_K$$

- Normalization of the received signal:

$$\mathbf{y}' = \frac{\mathbf{y}}{\sqrt[n]{\det(H)}} = H_1\mathbf{x} + \mathbf{w}', \quad \det(H_1) = 1$$

Principle

Approximate $H_1 = \mathrm{diag}(h'_1, \ldots, h'_n)$ with $U_l = \mathrm{diag}(\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u))$, where u is a unit of $\mathcal{O}_K$

The group of units $\mathcal{O}_K^*$

Dirichlet's unit theorem

K algebraic number field with r_1 real $\mathbb{Q}$-embeddings and $2r_2$ complex $\mathbb{Q}$-embeddings, $r = r_1 + r_2 - 1$.
$\exists u_1, \ldots, u_r$ fundamental units such that every $u \in \mathcal{O}_K^*$ can be written as

$$u = \zeta u_1^{e_1} \cdots u_r^{e_r},$$

where $\zeta \in \mathcal{R}$, the cyclic group of roots of unity in $\mathcal{O}_K$.

The group of units $\mathcal{O}_K^*$

Dirichlet's unit theorem

K algebraic number field with r_1 real $\mathbb{Q}$-embeddings and $2r_2$ complex $\mathbb{Q}$-embeddings, $r = r_1 + r_2 - 1$.
$\exists u_1, \ldots, u_r$ fundamental units such that every $u \in \mathcal{O}_K^*$ can be written as

$$u = \zeta u_1^{e_1} \cdots u_r^{e_r},$$

where $\zeta \in \mathcal{R}$, the cyclic group of roots of unity in $\mathcal{O}_K$.

The logarithmic lattice

Focus on the totally complex case: $r_1 = 0$, $r_2 = n$. Consider $f : \mathcal{O}_K^* \to \mathbb{R}^n$

$$u \mapsto f(u) = (\log|\sigma_1(u)|, \ldots, \log|\sigma_n(u)|)$$

Then $f(\mathcal{O}_K^*)$ is an $(n-1)$-dimensional lattice in $\mathbb{R}^n$:

$$\prod_{i=1}^n |\sigma_i(x)|^2 = N_{K/\mathbb{Q}}(x) = 1 \quad \Rightarrow \quad \sum_{i=1}^n \log|\sigma_i(x)| = 0$$

- the volume of the logarithmic lattice depends on the regulator of the number field

Algebraic reduction for fast fading channels

Approximate $H_1 = \mathrm{diag}(h'_1, \ldots, h'_n)$ with $U_l = \mathrm{diag}(\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u))$, where u is a unit of $\mathcal{O}_K$:

$$H_1 = EU_l, \quad E = \mathrm{diag}(e_1, \ldots, e_n) \text{ approximation error}$$

Algebraic reduction for fast fading channels

Approximate $H_1 = \mathrm{diag}(h'_1, \ldots, h'_n)$ with $U_l = \mathrm{diag}(\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u))$, where u is a unit of $\mathcal{O}_K$:

$$H_1 = EU_l, \quad E = \mathrm{diag}(e_1, \ldots, e_n) \text{ approximation error}$$

Units and unimodular transformations

u unit of $\mathcal{O}_K \quad \Leftrightarrow \quad U_l \Phi = \Phi T_u$ with T_u **unimodular** (with entries in $\mathbb{Z}[i]$).

Proof: $ux \in \mathcal{O}_K \;\Rightarrow\; ux = \sum_i s'_i \theta_i$

$$U_l \psi(x) = \psi(ux) = \Phi \mathbf{s}' = U_l \Phi \mathbf{s}$$
$$\Rightarrow \; \mathbf{s}' = \underbrace{\Phi^{-1} U_l \Phi}_{T_u} \mathbf{s}, \quad T_u \text{ unimodular}$$

Algebraic reduction for fast fading channels

Approximate $H_1 = \text{diag}(h'_1, \ldots, h'_n)$ with $U_l = \text{diag}(\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u))$, where u is a unit of $\mathcal{O}_K$:

$$H_1 = EU_l, \quad E = \text{diag}(e_1, \ldots, e_n) \text{ approximation error}$$

Units and unimodular transformations

u unit of $\mathcal{O}_K \quad \Leftrightarrow \quad U_l\Phi = \Phi T_u$ with T_u **unimodular** (with entries in $\mathbb{Z}[i]$).

Proof: $ux \in \mathcal{O}_K \;\Rightarrow\; ux = \sum_i s'_i \theta_i$

$$U_l\psi(x) = \psi(ux) = \Phi \mathbf{s}' = U_l \Phi \mathbf{s}$$

$$\Rightarrow \mathbf{s}' = \underbrace{\Phi^{-1} U_l \Phi}_{T_u} \mathbf{s}, \quad T_u \text{ unimodular}$$

- Received signal:

$$\mathbf{y}' = EU_l\Phi\mathbf{s} + \mathbf{w}' = E\Phi T_u \mathbf{s} + \mathbf{w}' = E\Phi\mathbf{s}' + \mathbf{w}', \qquad \mathbf{s}' \in \mathbb{Z}[i]^n$$

Algebraic reduction for fast fading channels

- apply a suboptimal decoder (i.e. ZF):

$$\hat{\mathbf{s}}' = \left\lfloor \Phi^{-1} E^{-1} \mathbf{y}' \right\rceil = \left\lfloor \mathbf{s}' + \underbrace{\Phi^{-1}}_{\text{unitary}} E^{-1} \mathbf{w}' \right\rceil$$

Algebraic reduction for fast fading channels

- apply a suboptimal decoder (i.e. ZF):

$$\hat{\mathbf{s}}' = \lfloor \Phi^{-1} E^{-1} \mathbf{y}' \rceil = \left\lfloor \mathbf{s}' + \underbrace{\Phi^{-1}}_{\text{unitary}} E^{-1} \mathbf{w}' \right\rceil$$

- the i-th component of the equivalent noise is $(E^{-1}\mathbf{w}')_i = \frac{\sigma_i(u)}{h'_i} w'_i$
- to minimize noise variance, $\left|\frac{\sigma_i(u)}{h'_i}\right|$ should be small $\quad \forall i = 1, \ldots, n$

  $\Rightarrow \quad |\log|\sigma_i(u)| - \log|h'_i||$ should be small

Algebraic reduction for fast fading channels

- apply a suboptimal decoder (i.e. ZF):

$$\hat{\mathbf{s}}' = \lfloor \Phi^{-1} E^{-1} \mathbf{y}' \rceil = \left\lfloor \mathbf{s}' + \underbrace{\Phi^{-1}}_{\text{unitary}} E^{-1} \mathbf{w}' \right\rceil$$

- the i-th component of the equivalent noise is $(E^{-1}\mathbf{w}')_i = \frac{\sigma_i(u)}{h_i'} w_i'$
- to minimize noise variance, $\left|\frac{\sigma_i(u)}{h_i'}\right|$ should be small $\forall i = 1, \ldots, n$
  $\Rightarrow$ $|\log|\sigma_i(u)| - \log|h_i'||$ should be small

How to find u?

find the closest point to $(\log|h_1'|, \ldots, \log|h_n'|)$ in the logarithmic lattice.

Algebraic reduction for fast fading channels

- apply a suboptimal decoder (i.e. ZF):

$$\hat{\mathbf{s}}' = \lfloor \Phi^{-1} E^{-1} \mathbf{y}' \rceil = \Big\lfloor \mathbf{s}' + \underbrace{\Phi^{-1}}_{\text{unitary}} E^{-1} \mathbf{w}' \Big\rceil$$

- the i-th component of the equivalent noise is $(E^{-1}\mathbf{w}')_i = \frac{\sigma_i(u)}{h_i'} w_i'$
- to minimize noise variance, $\left|\frac{\sigma_i(u)}{h_i'}\right|$ should be small $\forall i = 1, \ldots, n$
  $\Rightarrow$ $\left|\log|\sigma_i(u)| - \log|h_i'|\right|$ should be small

How to find u?

find the closest point to $(\log|h_1'|, \ldots, \log|h_n'|)$ in the logarithmic lattice.

- **advantage:** the logarithmic lattice is fixed once and for all and doesn't depend on the channel

Algebraic reduction for fast fading channels

- algebraic reduction + ZF achieves the optimal diversity order
- it outperforms LLL + ZF in high dimension

Algebraic reduction for fast fading channels

- algebraic reduction + ZF achieves the optimal diversity order
- it outperforms LLL + ZF in high dimension

Recent results

- used in [Campello, Ling, Belfiore 2017] to show that mod-p lattices achieve constant gap to compound capacity for n-antenna systems with reduced complexity

Algebraic reduction for fast fading channels

- algebraic reduction + ZF achieves the optimal diversity order
- it outperforms LLL + ZF in high dimension

Recent results

- used in [Campello, Ling, Belfiore 2017] to show that mod-p lattices achieve constant gap to compound capacity for n-antenna systems with reduced complexity

- the performance depends on the covering radius r_{cov} of the logarithmic lattice
- no known general bounds for r_{cov}
- bounds for r_{cov} in cyclotomic fields of prime power index [Cramer, Ducas, Peikert, Reigev 2016]

Outline

Algebraic reduction for MIMO systems

L. Luzzi, G. Rekaya - Ben Othman, J.-C. Belfiore, "Algebraic reduction for the Golden Code", *Adv. Math. Commun.* 2012

- Multiple antenna case:
$$Y = HX + W$$
  - $\mathcal{A} = (K/\mathbb{Q}(i), \sigma, \gamma)$ division algebra, $[K : \mathbb{Q}(i)] = n$
  - $X \in \psi(\mathcal{O}\alpha)$, $\mathcal{O}$ maximal order of $\mathcal{A}$

Algebraic reduction for MIMO systems

L. Luzzi, G. Rekaya - Ben Othman, J.-C. Belfiore, "Algebraic reduction for the Golden Code", *Adv. Math. Commun.* 2012

- Multiple antenna case:
$$Y = HX + W$$
  - $\mathcal{A} = (K/\mathbb{Q}(i), \sigma, \gamma)$ division algebra, $[K : \mathbb{Q}(i)] = n$
  - $X \in \psi(\mathcal{O}\alpha)$, $\quad \mathcal{O}$ maximal order of $\mathcal{A}$
- Normalization of the received signal: $Y' = \frac{Y}{\sqrt{\det(H)}}$
$$Y' = H_1 X + W', \quad \det(H_1) = 1$$

Algebraic reduction for MIMO systems

L. Luzzi, G. Rekaya - Ben Othman, J.-C. Belfiore, "Algebraic reduction for the Golden Code", *Adv. Math. Commun.* 2012

- Multiple antenna case:

$$Y = HX + W$$

  - $\mathcal{A} = (K/\mathbb{Q}(i), \sigma, \gamma)$ division algebra, $[K : \mathbb{Q}(i)] = n$
  - $X \in \psi(\mathcal{O}\alpha), \quad \mathcal{O}$ maximal order of $\mathcal{A}$

- Normalization of the received signal: $Y' = \frac{Y}{\sqrt{\det(H)}}$

$$Y' = H_1 X + W', \quad \det(H_1) = 1$$

- **Idea:** approximate H_1 with a unit $U \in \mathcal{O}^1$

Algebraic reduction for MIMO systems

$$H_1 = EU, \qquad E \quad \text{approximation error}$$

Algebraic reduction for MIMO systems

$$H_1 = EU, \qquad E \quad \text{approximation error}$$

- in vectorized form:

$$\mathbf{y}' = E_l U_l \Phi \mathbf{s} + \mathbf{w}'$$

  - A_l linear map corresponding to left multiplication by A
  - Φ generator matrix of the code lattice
  - $\mathbf{s} \in \mathbb{Z}[i]^N$ vector of QAM information signals, $N = n^2$

Algebraic reduction for MIMO systems

$$H_1 = EU, \qquad E \quad \text{approximation error}$$

- in vectorized form:

$$\mathbf{y}' = E_l U_l \Phi \mathbf{s} + \mathbf{w}'$$

  - A_l linear map corresponding to left multiplication by A
  - Φ generator matrix of the code lattice
  - $\mathbf{s} \in \mathbb{Z}[i]^N$ vector of QAM information signals, $N = n^2$

U **unit** $\quad \Leftrightarrow \quad U_l \Phi = \Phi T$ **with** T **unimodular**

$$\mathbf{y}' = E_l \Phi T \mathbf{s} + \mathbf{w}' = E_l \Phi \mathbf{s}' + \mathbf{w}' \qquad \mathbf{s}' \in \mathbb{Z}[i]^N$$

Algebraic reduction for MIMO systems

$$\mathbf{y}' = E_l \Phi \mathbf{s}' + \mathbf{w}' \qquad \mathbf{s}' \in \mathbb{Z}[i]^N$$

Algebraic reduction for MIMO systems

$$\mathbf{y}' = E_l \Phi \mathbf{s}' + \mathbf{w}' \qquad \mathbf{s}' \in \mathbb{Z}[i]^N$$

- Apply ZF detection:

$$\hat{\mathbf{s}}' = \left\lfloor \Phi^{-1} E^{-1} \mathbf{y}' \right\rceil = \left\lfloor \mathbf{s}' + \Phi^{-1} E_l^{-1} \mathbf{w}' \right\rceil$$

Algebraic reduction for MIMO systems

$$\mathbf{y}' = E_l \Phi \mathbf{s}' + \mathbf{w}' \qquad \mathbf{s}' \in \mathbb{Z}[i]^N$$

- Apply ZF detection:

$$\hat{\mathbf{s}}' = \left\lfloor \Phi^{-1} E^{-1} \mathbf{y}' \right\rceil = \left\lfloor \mathbf{s}' + \Phi^{-1} E_l^{-1} \mathbf{w}' \right\rceil$$

- the variance of the i-th noise component is bounded by

$$\sigma_i^2 \leq \frac{N\sigma^2}{|\det(H)|^{\frac{2}{n}}} \left\| \Phi^{-1} \right\|_F^2 \left\| E^{-1} \right\|^2 \quad \forall i = 1, \ldots, N$$

Algebraic reduction for MIMO systems

$$\mathbf{y}' = E_l \Phi \mathbf{s}' + \mathbf{w}' \qquad \mathbf{s}' \in \mathbb{Z}[i]^N$$

- Apply ZF detection:

$$\hat{\mathbf{s}}' = \left\lfloor \Phi^{-1} E^{-1} \mathbf{y}' \right\rceil = \left\lfloor \mathbf{s}' + \Phi^{-1} E_l^{-1} \mathbf{w}' \right\rceil$$

- the variance of the i-th noise component is bounded by

$$\sigma_i^2 \leq \frac{N\sigma^2}{|\det(H)|^{\frac{2}{n}}} \left\|\Phi^{-1}\right\|_F^2 \left\|E^{-1}\right\|^2 \quad \forall i = 1, \ldots, N$$

How to choose U?

$\Rightarrow$ Choose U that minimizes $\left\|E^{-1}\right\|_F = \left\|U H_1^{-1}\right\|_F$

Quaternion case

- $\mathcal{O}^1$ is a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{C})$

Quaternion case

- $\mathcal{O}^1$ is a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{C})$

$$H_1 \in \mathrm{SL}_2(\mathbb{C}) \quad \longrightarrow \quad \text{find } U \in \Gamma \text{ s.t. } \left\|E\right\|_F = \left\|H_1 U^{-1}\right\|_F \text{ is small}$$

Quaternion case

- $\mathcal{O}^1$ is a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{C})$

$H_1 \in \mathrm{SL}_2(\mathbb{C}) \quad \longrightarrow \quad$ find $U \in \Gamma$ s.t. $\|E\|_F = \left\|H_1 U^{-1}\right\|_F$ is small

Action of $\mathrm{SL}_2(\mathbb{C})$ on hyperbolic 3-space

$$\mathbb{H}^3 = \{(z, r) \mid z \in \mathbb{C},\ r \in \mathbb{R}^+\}$$

with the hyperbolic distance ρ such that $\boxed{\cosh \rho(P, P') = 1 + \frac{d(P,P')}{2rr'}}$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$J = (0, 0, 1) \quad \mapsto \quad A(J) = \left(\frac{\mathrm{Re}(b\bar{d} + a\bar{c})}{|c|^2 + |d|^2}, \frac{\mathrm{Im}(b\bar{d} + a\bar{c})}{|c|^2 + |d|^2}, \frac{1}{|c|^2 + |d|^2} \right)$$

Quaternion case

- $\mathcal{O}^1$ is a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{C})$

$$H_1 \in \mathrm{SL}_2(\mathbb{C}) \quad \longrightarrow \quad \text{find } U \in \Gamma \text{ s.t. } \|E\|_F = \left\|H_1 U^{-1}\right\|_F \text{ is small}$$

Action of $\mathrm{SL}_2(\mathbb{C})$ on hyperbolic 3-space

$$\mathbb{H}^3 = \{(z,r) \mid z \in \mathbb{C},\ r \in \mathbb{R}^+\}$$

with the hyperbolic distance ρ such that $\boxed{\cosh \rho(P,P') = 1 + \frac{d(P,P')}{2rr'}}$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$J = (0,0,1) \quad \mapsto \quad A(J) = \left(\frac{\mathrm{Re}(b\bar{d} + a\bar{c})}{|c|^2 + |d|^2}, \frac{\mathrm{Im}(b\bar{d} + a\bar{c})}{|c|^2 + |d|^2}, \frac{1}{|c|^2 + |d|^2} \right)$$

- Relation to Frobenius norm: $\|A\|_F^2 = 2 \cosh \rho(J, A(J))$

Quaternion case

- $\mathcal{O}^1$ is a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{C})$

$$H_1 \in \mathrm{SL}_2(\mathbb{C}) \quad \longrightarrow \quad \text{find } U \in \Gamma \text{ s.t. } \|E\|_F = \left\|H_1 U^{-1}\right\|_F \text{ is small}$$

Action of $\mathrm{SL}_2(\mathbb{C})$ on hyperbolic 3-space

$$\mathbb{H}^3 = \{(z, r) \mid z \in \mathbb{C},\ r \in \mathbb{R}^+\}$$

with the hyperbolic distance ρ such that $\boxed{\cosh \rho(P, P') = 1 + \frac{d(P,P')}{2rr'}}$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$J = (0, 0, 1) \quad \mapsto \quad A(J) = \left(\frac{\mathrm{Re}(b\bar{d} + a\bar{c})}{|c|^2 + |d|^2}, \frac{\mathrm{Im}(b\bar{d} + a\bar{c})}{|c|^2 + |d|^2}, \frac{1}{|c|^2 + |d|^2} \right)$$

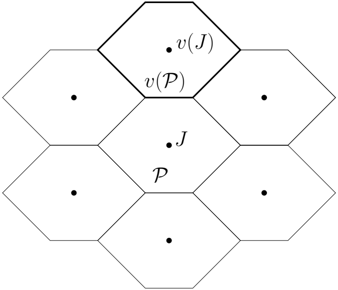
- Relation to Frobenius norm: $\|A\|_F^2 = 2 \cosh \rho(J, A(J))$

$$\left\|H_1 U^{-1}\right\|_F \textbf{ is small} \quad \Leftrightarrow \quad U^{-1}(J) \textbf{ is close to } H_1^{-1}(J)$$

Fundamental domain and generators of the group

Poincaré's polyhedron theorem

- the fundamental domain $\mathcal{P}$ for the action of Γ on $\mathbb{H}^3$ is a compact hyperbolic polyhedron
- the copies $v(\mathcal{P})$, $v \in \Gamma$ are isometric and form a tiling of $\mathbb{H}^3$
- there is a correspondence between a set of generators of the group and the set of side-pairings which map a face of $\mathcal{P}$ into another face



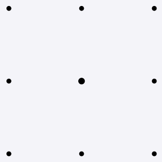
Tamagawa volume formula

$$\mathrm{Vol}(\mathcal{P}) = \frac{\zeta_F(2)}{4\pi^2} |D_F|^{\frac{3}{2}} \prod_{p|\delta_{\mathcal{O}}} (N_p - 1)$$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

- the area enclosed by **bisectors** is a **fundamental domain** for the action



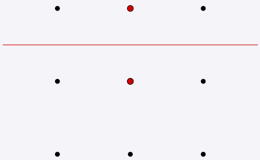
- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

Action of Γ on $\mathbb{H}^3$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

- the area enclosed by **bisectors** is a **fundamental domain** for the action



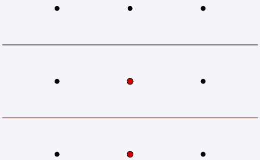
- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

Action of Γ on $\mathbb{H}^3$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

- the area enclosed by **bisectors** is a **fundamental domain** for the action



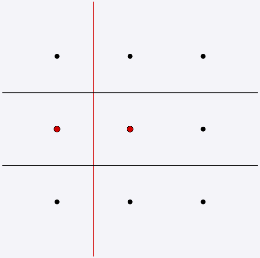
- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

Action of Γ on $\mathbb{H}^3$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

- the area enclosed by **bisectors** is a **fundamental domain** for the action



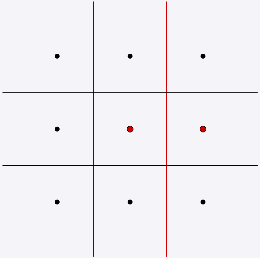
- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

Action of Γ on $\mathbb{H}^3$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

- the area enclosed by **bisectors** is a **fundamental domain** for the action



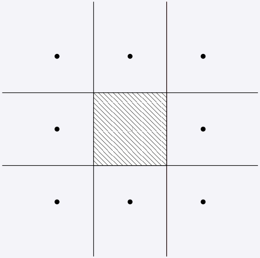
- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

Action of Γ on $\mathbb{H}^3$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

- the area enclosed by **bisectors** is a **fundamental domain** for the action



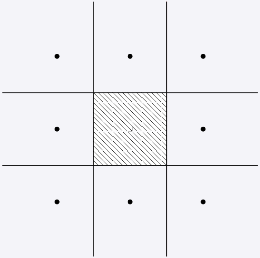
- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

Action of Γ on $\mathbb{H}^3$

Discrete subgroups and fundamental domains

Example: action of $\mathbb{Z}^2$ on $\mathbb{R}^2$

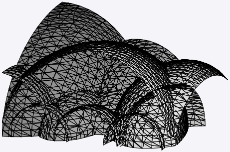
- the area enclosed by **bisectors** is a **fundamental domain** for the action



- the images of the fundamental domain form a **tiling** of $\mathbb{R}^2$

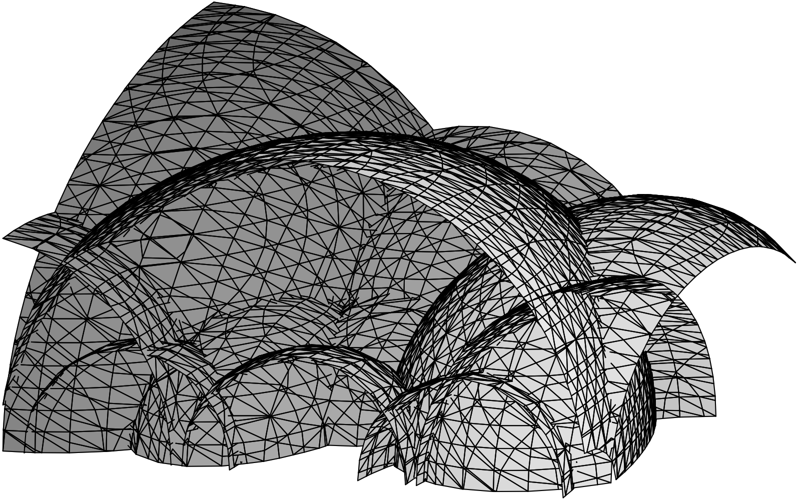
Action of Γ on $\mathbb{H}^3$

- the bisectors are Euclidean spheres



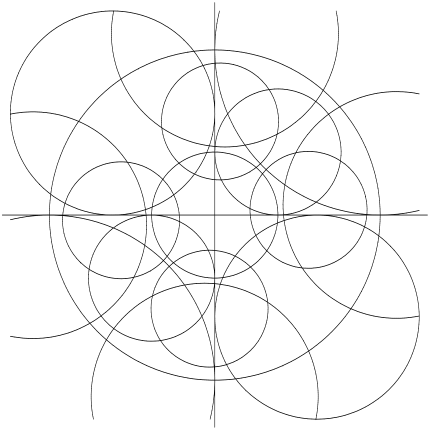
- the fundamental domain is a **hyperbolic polyhedron**
- the images of the fundamental domain form a tiling of $\mathbb{H}^3$

Intersecting bisectors: the Golden Code



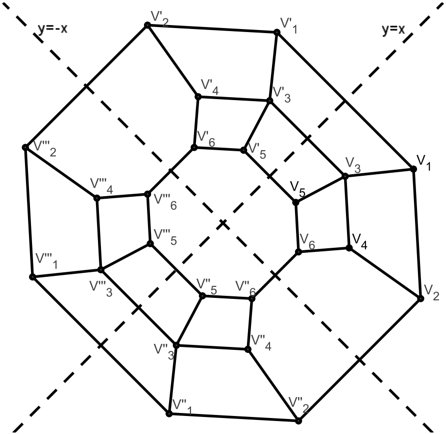
Intersecting bisectors: the Golden Code

Projection on the plane $\{r = 0\}$



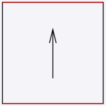
The fundamental polyhedron

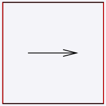
Projection on the plane $\{r = 0\}$



Finding the generators

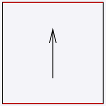
- The **generators** of the group correspond to the **side-pairings** of the fundamental polyhedron

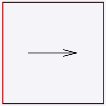




Finding the generators

- The **generators** of the group correspond to the **side-pairings** of the fundamental polyhedron





Golden Code: 8 generators for the unit group

$$U_1 = \begin{pmatrix} i\theta & 0 \\ 0 & i\bar{\theta} \end{pmatrix} \qquad U_5 = \begin{pmatrix} 1+i & 1+i\bar{\theta} \\ i(1+i\theta) & 1+i \end{pmatrix}$$

$$U_2 = \begin{pmatrix} i & 1+i \\ i-1 & i \end{pmatrix} \qquad U_6 = \begin{pmatrix} 1+i & 1+i\theta \\ i(1+i\bar{\theta}) & 1+i \end{pmatrix}$$

$$U_3 = \begin{pmatrix} \theta & 1+i \\ i-1 & \bar{\theta} \end{pmatrix} \qquad U_7 = \begin{pmatrix} 1-i & \bar{\theta}+i \\ i(\theta+i) & 1-i \end{pmatrix}$$

$$U_4 = \begin{pmatrix} \theta & -1-i \\ -i+1 & \bar{\theta} \end{pmatrix} \qquad U_8 = \begin{pmatrix} 1-i & \theta+i \\ i(\bar{\theta}+i) & 1-i \end{pmatrix}$$

- actually this is not a minimal set: 6 units are enough

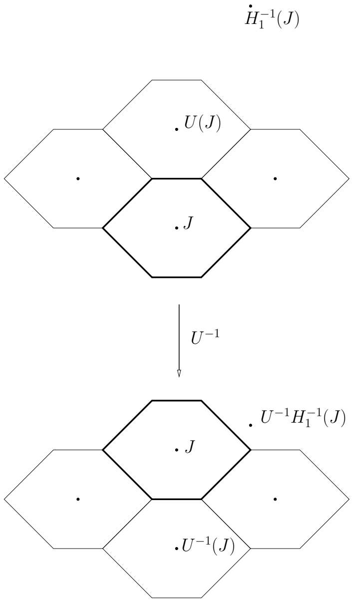
The approximation algorithm

- the polyhedra adjacent to the fundamental polyhedron $\mathcal{P}$ are of the form $U(\mathcal{P})$, with U a generator

Unit search algorithm

1) find the generator U such that $U(J)$ is closest to $H_1^{-1}(J)$
2) every U is an isometry $\Rightarrow$ apply U^{-1}

- Repeat steps 1-2 until J is the closest point to $H_1^{-1}(J)$



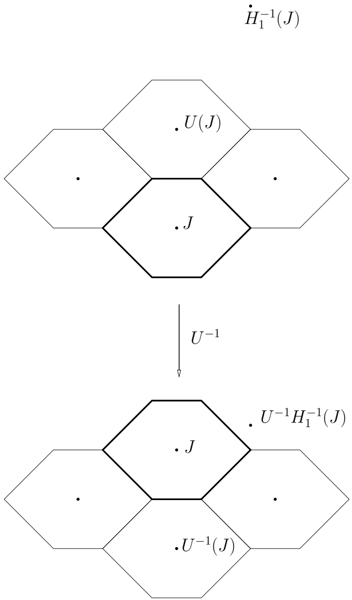
- the polyhedra adjacent to the fundamental polyhedron $\mathcal{P}$ are of the form $U(\mathcal{P})$, with U a generator

Unit search algorithm

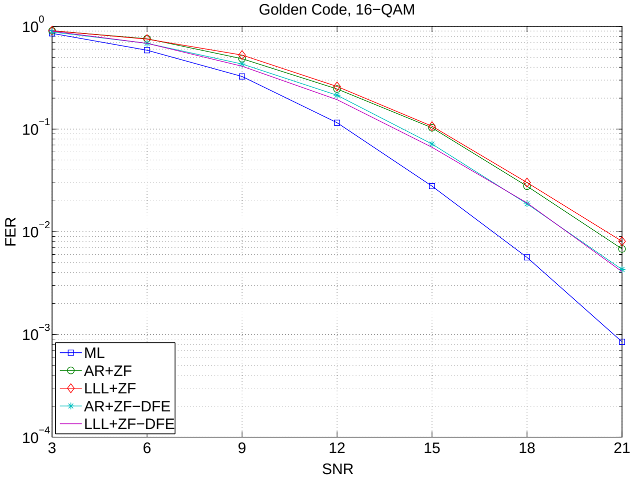
1) find the generator U such that $U(J)$ is closest to $H_1^{-1}(J)$
2) every U is an isometry $\Rightarrow$ apply U^{-1}

- Repeat steps 1-2 until J is the closest point to $H_1^{-1}(J)$

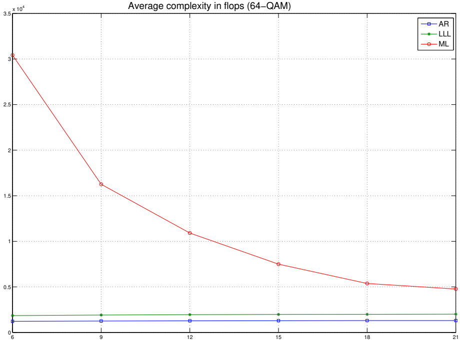
- this algorithm is suboptimal - does not solve the word problem for groups!



Performance of algebraic reduction



Complexity of algebraic reduction



- the average number of iterations in the AR algorithm is only 1.923
- with high probability, $H_1^{-1}(J)$ is already contained in $\mathcal{P}$ or one of the neighboring polyhedra
- advantage: if fading is slow, AR requires only a slight adjustment of the previous approximation

Generalization to other codes (quaternion algebras)

- general algorithm to find generators of the unit group [Swan 1971, Corrales *et al.* 2004, Page 2015]

Generalization to other codes (quaternion algebras)

- general algorithm to find generators of the unit group [Swan 1971, Corrales *et al.* 2004, Page 2015]

Design codes that are optimal for algebraic reduction

- the quality of the approximation depends on the diameter of the fundamental polyhedron (not directly related to volume!)
- the speed of the approximation depends on the number of generators of the unit group

Generalization to other codes (quaternion algebras)

- general algorithm to find generators of the unit group [Swan 1971, Corrales *et al.* 2004, Page 2015]

Design codes that are optimal for algebraic reduction

- the quality of the approximation depends on the diameter of the fundamental polyhedron (not directly related to volume!)
- the speed of the approximation depends on the number of generators of the unit group

- the unit group can be very complex in general
- for the “Golden +” code algebra [Vehkalahti *et al.* 2009] it seems to have hundreds of generators
- quaternion algebras over $\mathbb{Q}(\zeta_3)$ with 3 generators [Alves-Belfiore 2012] and over $\mathbb{Q}(\sqrt{-7})$ with small Tamagawa volume [Alves-Belfiore 2015]

Higher-dimensional division algebras

- algebraic reduction still applies for higher-dimensional algebras and achieves the receive diversity

Higher-dimensional division algebras

- algebraic reduction still applies for higher-dimensional algebras and achieves the receive diversity
- in general, $\mathcal{O}^1$ is a cocompact discrete subgroup of $\mathrm{SL}_n(\mathbb{C})$

Higher-dimensional division algebras

- algebraic reduction still applies for higher-dimensional algebras and achieves the receive diversity
- in general, $\mathcal{O}^1$ is a cocompact discrete subgroup of $\mathrm{SL}_n(\mathbb{C})$
- however, finding the generators of the unit group is a difficult open problem in computational algebra

Higher-dimensional division algebras

- algebraic reduction still applies for higher-dimensional algebras and achieves the receive diversity
- in general, $\mathcal{O}^1$ is a cocompact discrete subgroup of $\mathrm{SL}_n(\mathbb{C})$
- however, finding the generators of the unit group is a difficult open problem in computational algebra
- the choice of a group action and a relevant metric is not straightforward

Higher-dimensional division algebras

- algebraic reduction still applies for higher-dimensional algebras and achieves the receive diversity
- in general, $\mathcal{O}^1$ is a cocompact discrete subgroup of $\mathrm{SL}_n(\mathbb{C})$
- however, finding the generators of the unit group is a difficult open problem in computational algebra
- the choice of a group action and a relevant metric is not straightforward
- some recent results in [Braun *et al.* 2015]

Higher-dimensional division algebras

- algebraic reduction still applies for higher-dimensional algebras and achieves the receive diversity
- in general, $\mathcal{O}^1$ is a cocompact discrete subgroup of $\mathrm{SL}_n(\mathbb{C})$
- however, finding the generators of the unit group is a difficult open problem in computational algebra
- the choice of a group action and a relevant metric is not straightforward
- some recent results in [Braun *et al.* 2015]

Related work

- the growth rate of units of bounded norm characterizes DMT and error performance of division algebra codes [Vehkalahti, Lu, Luzzi 2013], [Luzzi, Vehkalahti 2018]

Thank you for your attention!!