Number-Theoretic Fast-Decodable Space–Time Codes for Multiuser Communications

Camilla Hollanti
with Amaro Barreal and Nadya Markin
Credit for slides: Amaro

Aalto University
Department of Mathematics and Systems Analysis
Finland

York 2016

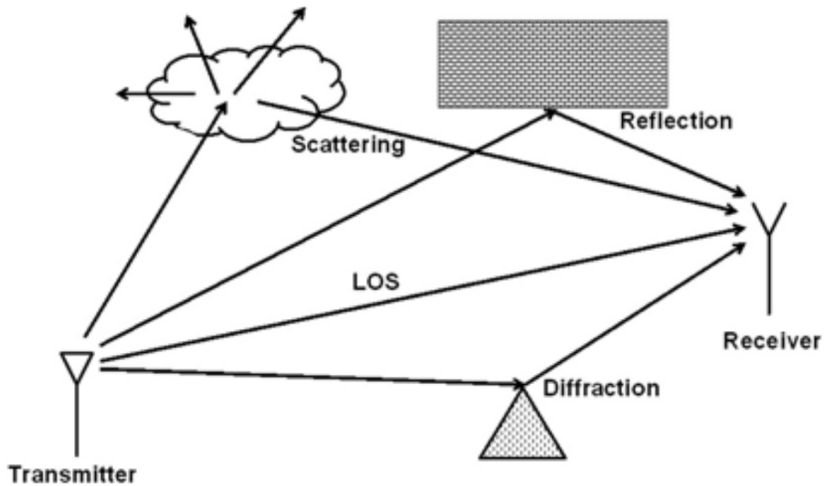
Overview

Aalto University
School of Science

1. **Space–Time Coding**
   - Space–Time Codes from Cyclic Division Algebras
   - On Fast-Decodability
   - Iterative Code Construction
2. **Amplify-and-Forward Relaying**
3. **Explicit Constructions**
   - Code Construction for SIMO-NAF
   - Code Construction for MIMO-NAF
4. **Further Applications and Conclusions**

Need for diversity

Aalto University
School of Science



Waves transmitted over a wireless channel suffer from environmental effects and fading. Combat those effects through *diversity*!

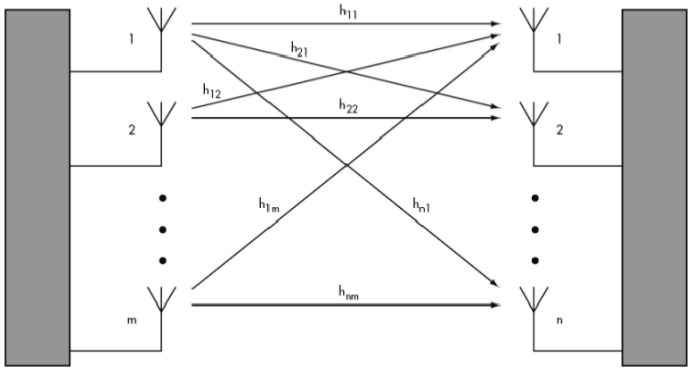
- *Spatial diversity:* Multiple antennas at the transmitter and/or receiver.
- *Temporal diversity:* Use different time slots for transmission.

$\Rightarrow$ space–time codes.

MIMO channel model

Aalto University
School of Science

Consider an $n_s \times n_d$-antenna system:



$$\Leftrightarrow \quad H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n_s} \\ h_{21} & h_{22} & \cdots & h_{2n_s} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n_d1} & h_{n_d2} & \cdots & h_{n_dn_s} \end{bmatrix}$$

Transmission using T time slots can be modeled as

$$Y = HX + N.$$

- The channel matrix $H \in \mathrm{Mat}(n_d \times n_s, \mathbb{C})$ models Rayleigh fading.
- $X \in \mathrm{Mat}(n_s \times T, \mathbb{C})$ is a codeword matrix.
- $N \in \mathrm{Mat}(n_d \times T, \mathbb{C})$ a noise matrix, whose entries are complex Gaussian with zero mean.

We will focus on square codes, $n_s = T$.

F. Oggier, J-C. Belfiore, and E. Viterbo. "Cyclic division algebras: a tool for space-time coding". In: *Foundations and trends in communications and information theory* 4.1 (2007), pp. 1–95

Algebraic setup

Aalto University
School of Science

- L/K degree n cyclic Galois extension of number fields with respective ring of integers $\mathcal{O}_K$ and $\mathcal{O}_L$.
- Cyclic Galois group $\Gamma(L/K) = \langle\sigma\rangle$.
- Choose an $\mathcal{O}_K$-basis $\{\omega_0, \ldots, \omega_{n-1}\}$ of $\mathcal{O}_L$ (assume K is a PID).
- Fix $\gamma \in K^\times$ such that $\gamma^i \notin \mathrm{Nm}_{L/K}(L^\times)$, $i = 1, \ldots, n-1$.

The triple

$$\mathcal{C} = (L/K, \sigma, \gamma) \cong \bigoplus_{i=0}^{n-1} u^i L$$

is a *cyclic division algebra* (CDA) of degree n, and multiplication is determined by the relations

$$u^n = \gamma, \quad lu = u\sigma(l) \text{ for all } l \in L.$$

$$\begin{array}{ccc} \mathcal{C} & & \mathcal{C} \\ {\scriptstyle n}\,| & & |\,\{u^i\}_{i=0}^{n-1} \\ L & & \mathcal{O}_L \\ {\scriptstyle n}\,| & & |\,\{\omega_i\}_{i=0}^{n-1} \\ K & & \mathcal{O}_K \\ {\scriptstyle m}\,| & & \\ \mathbb{Q} & & \end{array}$$

The left-regular representation

Aalto University
School of Science

We need to identify elements $x = \sum_{j=0}^{n} u^j x_j \in \mathcal{C}$ with matrices.

The (transposed) *left-regular representation* (LRR) $\lambda : \mathcal{C} \to \mathrm{Mat}(n, \mathbb{C})$ is an injective algebra homomorphism, given by

$$\lambda(x) = \begin{bmatrix} x_0 & x_1 & \cdots & x_{n-2} & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \cdots & \sigma(x_{n-3}) & \sigma(x_{n-2}) \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma\sigma^{n-2}(x_2) & \gamma\sigma^{n-2}(x_3) & \cdots & \sigma^{n-2}(x_0) & \sigma^{n-2}(x_1) \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) & \sigma^{n-1}(x_0) \end{bmatrix}.$$

Write $x_j = \sum_{i=0}^{n-1} \omega_i x_{ji} \in \mathcal{O}_L$, where $x_{ji} \in \mathcal{O}_K$. If we further expand using a $\mathbb{Z}$-basis, we see that $\lambda(x)$ carries mn^2 independent integers (e.g., PAM symbols).

Space–time codes and their properties

Aalto University
School of Science

Definition

A *space–time* (ST) code constructed from a CDA $\mathcal{C}$ is a subset

$$\mathcal{X} \underset{\text{finite}}{\subset} \mathrm{Im}(\lambda(\mathcal{C})) = \{\lambda(x) | \, x \in \mathcal{C}\}.$$

Often, a *shaping element* $\alpha \in L^\times$ is introduced to restrict the entries to an ideal $(\alpha) \subset \mathcal{O}_L$ and improve the performance of the code, which can have many desirable properties, such as

- Full-rank codeword matrices (cf. diversity gain),
- Non-vanishing determinants (cf. coding gain),
- Balanced energy among transmitters (cf. PAPR),
- Optimal DMT,
- *Fast-decodability*, etc.

Equivalent representation

We can give a more explicit presentation of a ST code in terms of its generating matrices as follows.

Definition

Let $\{B_i\}_{i=1}^{k}$ be a set of fixed $n_s \times T$ complex *weight matrices*. A *linear space–time block code* of rank k is a set of the form

$$\mathcal{X} = \left\{ \sum_{i=1}^{k} s_i B_i \middle| s_i \in S \cap \mathbb{Z} \right\},$$

where $S \subset \mathbb{Z}$ is the finite *signaling alphabet* in use.

Remark

This definition agrees with the previous one by setting $n_s = T = n$ and choosing the set of weight matrices $\{B_i\}$ to be a basis of $\mathcal{C}$ over $\mathbb{Q}$.

Full-diversity codes with NVD

Aalto University
School of Science

Motivation for the use of division algebras in space–time coding:

Lemma

Let $\mathcal{D}$ be a division algebra and K a field. If $\phi : \mathcal{D} \to \mathrm{Mat}(n, K)$ is a ring homomorphism and $\mathcal{X} \subseteq \phi(\mathcal{D})$ is any finite subset, then $\mathrm{rank}(X - X') = n$ *for any distinct* $X, X' \in \mathcal{X}$.

λ is a ring homomorphism, and we defined $\mathcal{X} \subset \mathrm{Im}(\lambda(\mathcal{C}))$ to be finite.

Lemma

Let $\mathcal{X}$ be a space–time code coming from an order $\mathcal{O}$ of a CDA $\mathcal{C} = (L/K, \sigma, \gamma)$ with center $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-m})$, $m \in \mathbb{Z}_{>1}$ squarefree. Then $\mathcal{X}$ has the non-vanishing determinant property.

Example: the Golden code

Aalto University
School of Science

Fix $n = 2$. The algebraic setup for the Golden code is as follows:

- $L/K = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$.
- Ring of integers $\mathcal{O}_K = \mathbb{Z}[i]$, $\mathcal{O}_L = \mathcal{O}_K[\omega]$, where $\omega = \frac{1+\sqrt{5}}{2}$.
- Cyclic Galois group $\Gamma(L/K) = \langle \sigma : \sqrt{5} \mapsto -\sqrt{5} \rangle$.
- Our CDA is the triple $\mathcal{C}_G = (L/K, \sigma, i) \cong L \oplus uL$, with $u^2 = i$.
- Choose the shaping element $\alpha = 1 + i - i\omega$.

Restricting the entries to $\mathcal{O}_L$, the Golden code is a finite subset

$$\mathcal{X}_G \subset \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha & \\ & \sigma(\alpha) \end{bmatrix} \begin{bmatrix} x_0 & x_1 \\ i\sigma(x_1) & \sigma(x_0) \end{bmatrix} \middle| \, x_i \in \mathcal{O}_L \right\}$$

$$= \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha & \\ & \sigma(\alpha) \end{bmatrix} \begin{bmatrix} x_{00} + \omega x_{01} & x_{10} + \omega x_{11} \\ i(x_{10} + \sigma(\omega) x_{11}) & x_{00} + \sigma(\omega) x_{01} \end{bmatrix} \middle| \, x_{ij} \in \mathcal{O}_K \right\}.$$

A slight modification

Aalto University
School of Science

We will mostly consider field extensions L/K of degree 2. To have balanced energy and good decodability, we slightly modify the matrix representation of the elements in $\mathcal{C} = (L/K, \sigma, \gamma)$.

Instead of representing $x = c + \sqrt{\gamma}d \in \mathcal{O} \subset \mathcal{C}$ using the representation $\lambda(x)$ over the maximal subfield K, we define

$$\tilde{\lambda} : x \mapsto \begin{bmatrix} c & -\sqrt{-\gamma}\sigma(d) \\ \sqrt{-\gamma}d & \sigma(c) \end{bmatrix}.$$

This function is commonly used, and maintains the original determinant.

G. Berhuy, N. Markin, and B. A. Sethuraman. "Bounds on Fast Decodability of Space-Time Block Codes, Skew-Hermitian Matrices, and Azumaya Algebras". In: *IEEE Trans. Inf. Theory* 61.4 (2015), pp. 1959–1970

E. Biglieri, Y. Hong, and E. Viterbo. "On fast-decodable space-time block codes". In: *IEEE Trans. Inf. Theory* 55.2 (2009), pp. 524–530

Complexity of ML-decoding

Aalto University
School of Science

Given a space–time code $\mathcal{X}$, *Maximum-Likelihood* (ML) decoding amounts to finding the codeword $X \in \mathcal{X}$ that minimizes

$$\delta(X) := ||Y - HX||_F^2.$$

By defining the real-valued matrix $B := \begin{bmatrix} \text{vec}(HB_1) & \dots & \text{vec}(HB_k) \end{bmatrix}$, we can reduce the decoding problem to read

$$\begin{aligned} \arg\min_{X \in \mathcal{X}} \left\{ ||Y - HX||_F^2 \right\} &\rightsquigarrow \arg\min_{s \in S^k} \left\{ || \,\text{vec}(Y) - Bs||_E^2 \right\} \\ (B = QR) \ &\rightsquigarrow \arg\min_{s \in S^k} \left\{ ||Q^\dagger \,\text{vec}(Y) - Rs||_E^2 \right\}. \end{aligned}$$

Definition

The *ML decoding complexity* of a rank-k ST code $\mathcal{X}$ is upper bounded by the worst-case (ML) complexity $|S|^k$ corresponding to an exhaustive search. A ST code $\mathcal{X}$ is said to be *fast-decodable* if its worst-case ML decoding complexity is of the form $|S|^{k'}$ for $k' < k - 1$.

Hurwitz-Radon quadratic form

Aalto University
School of Science

Introducing the R-matrix in the decoding process permits to directly read out the decoding complexity of a given code.

Definition

The *Hurwitz-Radon Quadratic Form* (HRQF) is the map

$$\mathcal{Q} : \mathcal{X} \to \mathbb{R}; \qquad X \mapsto \sum_{1 \leq i \leq j \leq k} s_i s_j m_{ij},$$

where $m_{ij} := ||B_i B_j^\dagger + B_j B_i^\dagger||_F^2$ and $s_i \in S$.

- Define the matrix $M = (m_{ij})$. Then $m_{ij} = 0$ if and only if $B_i B_j^\dagger + B_j B_i^\dagger = \mathbf{0}$, that is, if B_i and B_j are *mutually orthogonal*.
- Premultiplication of the weight matrices by H does not affect the zero structure of M, whereas it does affect that of R.
- Yet, the zero structure of the R and M matrices are conveniently related to each other.

Hurwitz-Radon quadratic form

Aalto University
School of Science

Introducing the R-matrix in the decoding process permits to directly read out the decoding complexity of a given code.

Definition

T

Breaking News!

Recently, the criteria for fast-decodability have been revisited:

A. Mejri, M. Kshiba, and G. Rekaya. "Reduced-Complexity ML Decodable STBCs: Revisited Design Criteria". In: *IEEE ISWCS*. 2015, pp. 666–670.

The authors show that the HRQF method does not capture all possible fast-decodable code families, and propose a relaxed criterion on the mutual orthogonality condition.

w

ıe

- Yet, the zero structure of the R and M matrices are conveniently related to each other.

(Conditional) g-group decodability

Aalto University
School of Science

Definition

A rank-k ST code $\mathcal{X}$ is *conditionally g-group decodable* if there exists a partition of $\{1,\dots,k\}$ into $g+1 \geq 3$ disjoint subsets $\Gamma_1,\dots,\Gamma_g,\Gamma^{\mathcal{X}}$, such that $B_iB_j^\dagger + B_jB_i^\dagger = 0$ for $i \in \Gamma_p$, $j \in \Gamma_q$, $1 \leq p < q \leq g$.
$\mathcal{X}$ is *g-group decodable* if $|\Gamma^{\mathcal{X}}| = 0$.

The R-matrices related to these families of codes are of the form

$$R_{\text{cond}} = \begin{bmatrix} D_1 & & & G_1 \\ & \ddots & & \vdots \\ & & D_g & G_g \\ & & & G \end{bmatrix} \quad \text{resp.} \quad R = \begin{bmatrix} D_1 & & \\ & \ddots & \\ & & D_g \end{bmatrix},$$

where $D_i \in \text{Mat}(|\Gamma_i|,\mathbb{R})$, $G \in \text{Mat}(|\Gamma^{\mathcal{X}}|,\mathbb{R})$ upper triangular.

Lemma

The ML-decoding complexity of $\mathcal{X}$ is $|S|^{|\Gamma^{\mathcal{X}}|+\max\limits_{1\leq i\leq g}|\Gamma_i|}$.

N. Markin and F. Oggier. "Iterated space-time code constructions from cyclic algebras". In: *IEEE Trans. Inf. Theory* 59.9 (2013), pp. 5966–5979

Iterative codes from CDAs

Let $\mathcal{C} = (L/K, \sigma, \gamma)$ be a CDA or degree n. Fix $\theta = \zeta\theta' \in \mathcal{C}$, $\tau \in \mathrm{Aut}_{\mathbb{Q}}(K)$. For $X = \lambda(x)$, $Y = \lambda(y)$ (LRR), define the following function:

$$\alpha_{\tau,\theta} : \mathcal{C} \times \mathcal{C} \to \mathrm{Mat}(2n, K)$$
$$(x, y) \mapsto \begin{bmatrix} X & \zeta\sqrt{\theta'}\tau(Y) \\ \sqrt{\theta'}Y & \tau(X) \end{bmatrix}.$$

If the matrices $\{B_i\}_{i=1}^{k}$ define a ST code $\mathcal{X}$, the iterated ST code $\mathcal{X}_{\mathrm{it}}$ is double the rank and defined by the matrices

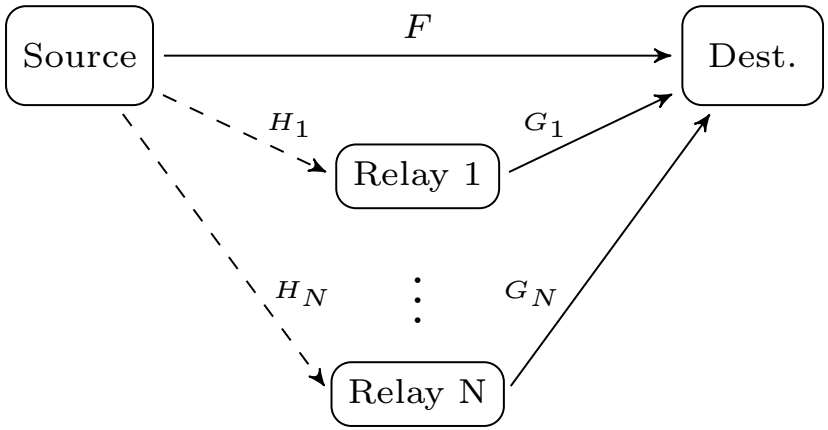
$$\{\alpha_{\tau,\theta}(B_i, 0), \alpha_{\tau,\theta}(0, B_i)\}.$$

The importance of this construction is that by making certain assumptions, we can guarantee that the code $\mathcal{X}_{\mathrm{it}}$ will inherit desirable properties from $\mathcal{X}$, such as *fast-decodability*.

S. Yang and J-C. Belfiore. "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel". In: *IEEE Trans. Inf. Theory* 53.2 (2007), pp. 647–663

N-relay MIMO NAF channel

Aalto University
School of Science



n_s antennas at the source.
$n_r \leq n_s$ antennas at each relay.
n_d antennas at the destination.

We impose the *half-duplex* constraint, i.e., a relay cannot receive and transmit at the same time.

From the destination's point of view this can be viewed as a virtual single-user MIMO channel

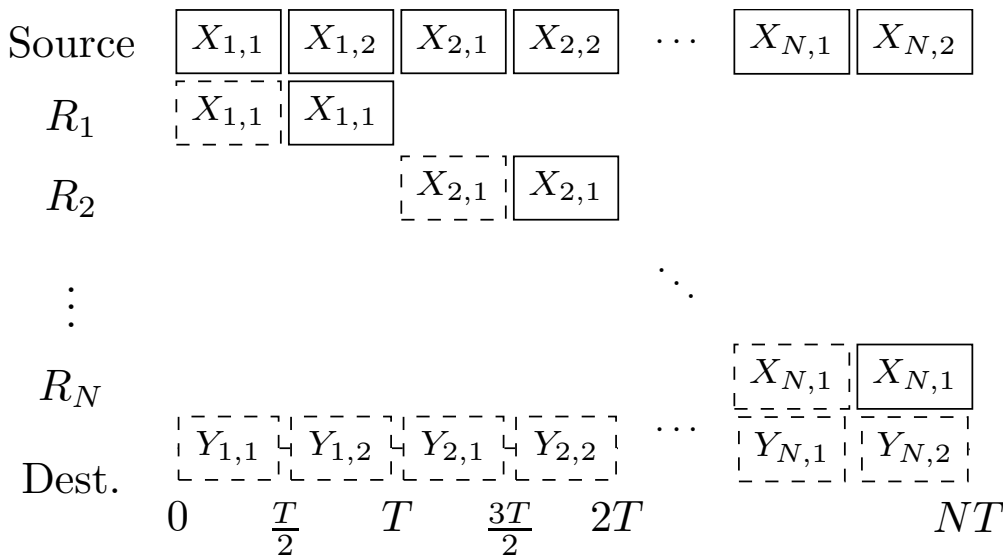
$$Y_{n_d \times n} = H_{n_d \times n} X_{n \times n} + V_{n_d \times n},$$

where $n = 2Nn_s$ and H has a special structure.

Frame model

Aalto University
School of Science

- N consecutive cooperation frames define a *superframe*.
- The relays take turns to cooperate with the transmitter in their respective cooperation frame.
- All channels remain static for the entire superframe.



Transmitted and received signals are represented by solid and dashed boxes, respectively.

Codeword structure

Aalto University
School of Science

The overall (equivalent) codewords are of the form

$$X = \operatorname{diag}\left\{\Xi_i\right\}_{i=1}^{N} = \begin{bmatrix} \Xi_1 & & \\ & \ddots & \\ & & \Xi_N \end{bmatrix},$$

where $\Xi_i \in \mathrm{Mat}(2n_s, \mathbb{C})$.

It would be desirable to construct block-diagonal codes which have

- "full" rate $2n_d$ (real) symbols per channel use (rspcu), i.e., the number of independent real information symbols (e.g., PAM) per codeword equals $4n_d n_s N$,
- full rank $2n_s N$,
- non-vanishing determinants,
- fast(er) decoding.

A. Barreal, C. Hollanti, and N. Markin. "Fast-Decodable Space–Time Codes for the N-Relay and Multiple-Access MIMO Channel". In: *IEEE Trans. Wireless Commun.* 15.3 (2016), pp. 1754–1767

The map that does the trick

Aalto University
School of Science

Definition

Consider an N-relay NAF channel. Given a ST code $\mathcal{X} \subset \mathrm{Mat}(2n_s, \mathbb{C})$ and a suitable function η of order N (*i.e.*, $\eta^N(X) = X$), define the function

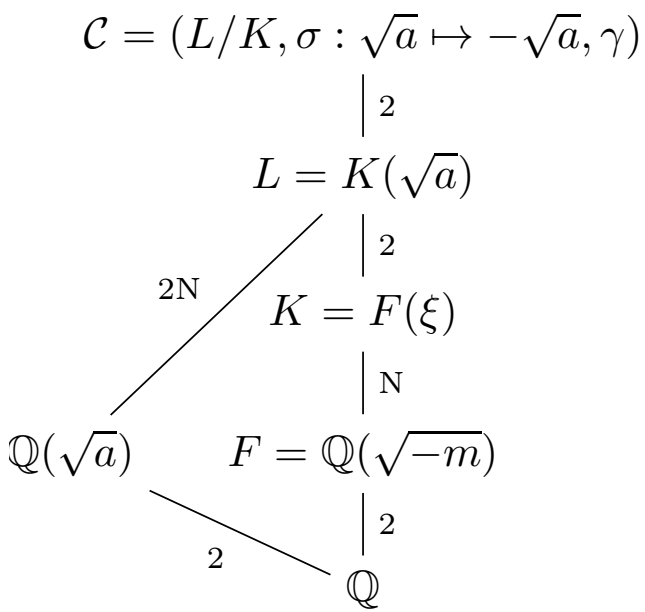
$$\Psi_{\eta,N} : \mathcal{X} \to \mathrm{Mat}(nN, \mathbb{C})$$

$$X \mapsto \mathrm{diag}\left\{\eta^i(X)\right\}_{i=0}^{N-1} = \begin{bmatrix} X & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \eta(X) & \cdots & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \cdots & & \eta^{N-1}(X) \end{bmatrix}.$$

Algebraic framework – SIMO

Aalto University
School of Science

Assume $n_s = n_r = 1$, and $n_d \geq 2$, and consider the tower



We assume $m \in \mathbb{Z}_{\geq 1}$ and $a \in \mathbb{Z} \setminus \{0\}$, both square-free.

Infinite family for SIMO

Aalto University
School of Science

Theorem

Consider the algebraic setup from above with $a < 0$, $\gamma < 0$. Fix a generator $\langle \eta \rangle = \Gamma(K/F)$ and define the set

$$\mathcal{X} = \{\Psi_{\eta,N}(X)\}_{X \in \tilde{\lambda}(\mathcal{O})} = \left\{ \operatorname{diag}\left\{\eta^i(X)\right\}_{i=0}^{N-1} \middle| \, X \in \tilde{\lambda}(\mathcal{O}) \right\}.$$

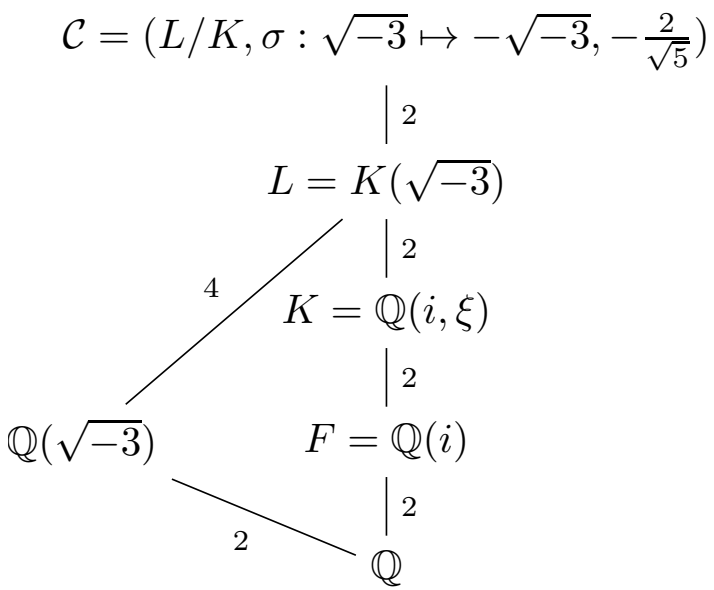
The code $\mathcal{X}$ is of rank $8N$, rate $R = 4$ rspcu and has the NVD property. It is full-rate if $n_d = 2$. Moreover, $\mathcal{X}$ is conditionally 4-group decodable, and its decoding complexity (up to a constant) can be reduced from $|S|^{8N}$ to $|S|^{5N}$, where S is the real constellation used, resulting in a complexity order reduction of 37.5%.

Moreover, full-rate codes constructed using this method will achieve the optimal DMT of the channel.

A two-relay example code

Aalto University
School of Science

Consider $N = 2$ relays and the following tower of extensions.



- For $\xi = \sqrt{5}$, the algebra $\mathcal{C}$ is division.
- Let $\langle \eta \rangle = \Gamma(K/F)$.
- $X \in \tilde{\lambda}(\mathcal{O}_L)$ is of the form

$$X = \begin{bmatrix} c & -\sqrt{-\gamma}\sigma(d) \\ \sqrt{-\gamma}d & \sigma(c) \end{bmatrix}$$

Define the 2-relay code

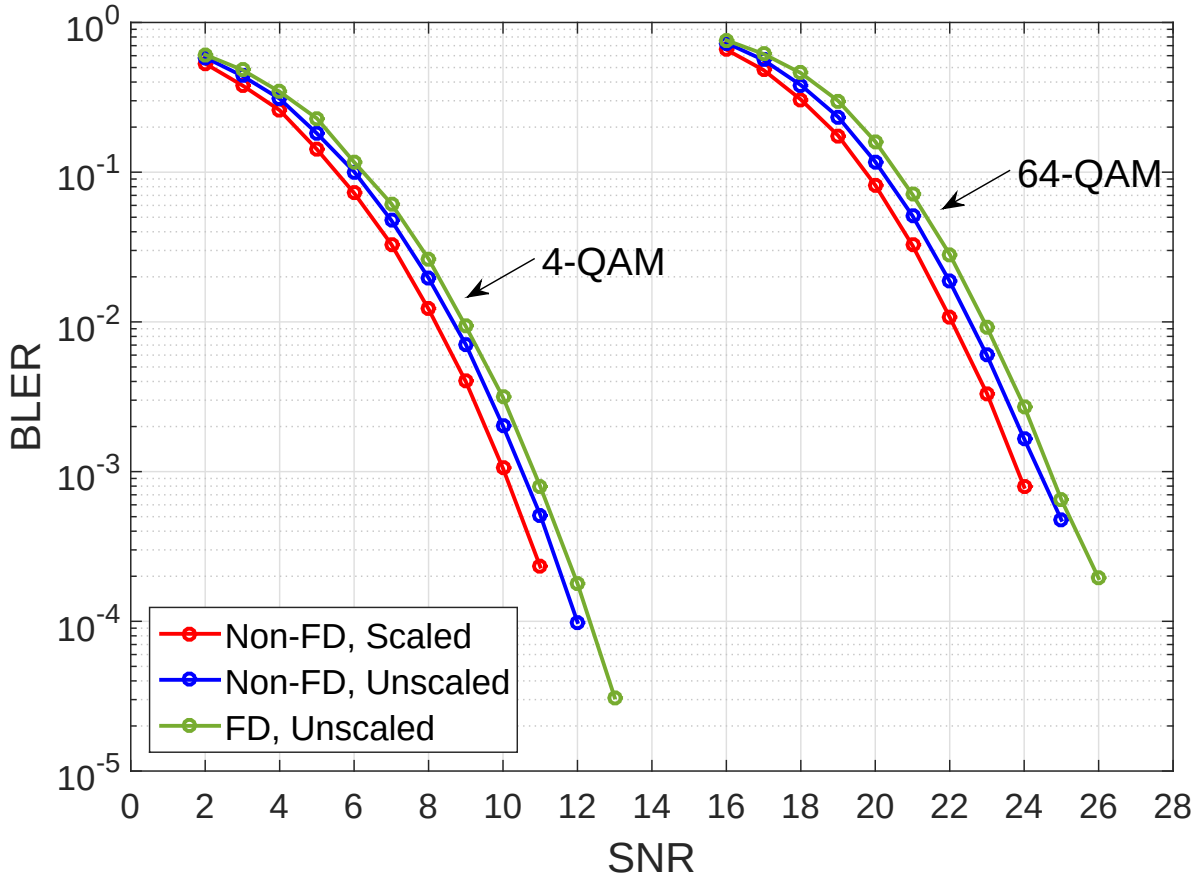
$$\mathcal{X} = \left\{ \Psi_{\eta,2}(X) \middle| \, X \in \tilde{\lambda}(\mathcal{O}_L) \right\} = \left\{ \begin{bmatrix} X & \\ & \eta(X) \end{bmatrix} \middle| \, X \in \tilde{\lambda}(\mathcal{O}_L) \right\}.$$

This is a fully diverse NVD code of rank 16. It is conditionally 4-group decodable, and its decoding compexity is $|S|^{10}$ in contrast to $|S|^{16}$.

What about performance?

Aalto University
School of Science

We compare the performance of the example code with the optimal code proposed in [Yang]) – a lifted version of the Golden code – and further an unshaped version of the same. ($n_s = n_r = 1$, $n_d = 4$)

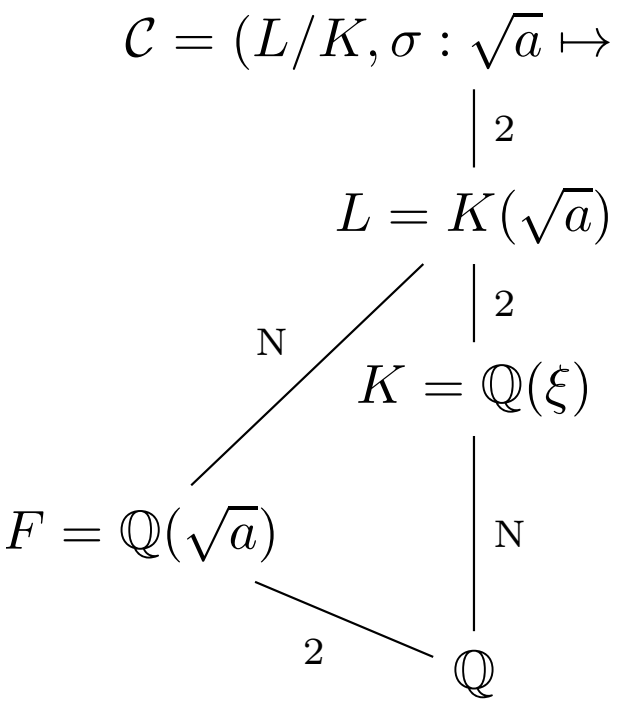


S. Yang and J-C. Belfiore. "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel". In: *IEEE Trans. Inf. Theory* 53.2 (2007), pp. 647–663

Algebraic framework – MIMO

Aalto University
School of Science

Assume $n_s = 2$, $n_d \geq 1$ and $N = (p-1)/2$ relays ($p \geq 5$ prime) equipped with $n_r \leq 2$ antennas.



- $K = \mathbb{Q}(\xi) = \mathbb{Q}^+(\zeta_p) \subset \mathbb{Q}(\zeta_p)$ maximal real subfield of the p^{th} cyclotomic field. ($\xi = \zeta_p + \zeta_p^{-1}$)
- $a \in \mathbb{Z} \backslash \{0\}$ is square-free.
- $\langle \sigma \rangle = \Gamma(L/K)$ and $\langle \eta \rangle = \Gamma(L/F)$.

Infinite family for MIMO

Aalto University
School of Science

Theorem

Consider the algebraic setup from above, and choose $a \in \mathbb{Z}_{<0}$ *such that* $\mathfrak{p} = a\mathcal{O}_K$ *is a prime ideal. Fix further* $\gamma < 0$ *and* $\theta \in \mathcal{O}_K \cap \mathbb{R}^\times = \mathbb{Z}[\xi] \cap \mathbb{R}^\times$ *such that*

- γ *and* θ *are both nonsquare* $\bmod \mathfrak{p}$,
- *the quadratic form* $\langle \gamma, -\theta \rangle_L$ *is anisotropic,*

and further let $\tau = \sigma$. *For* $\mathcal{O} \subset \mathcal{C}$ *an order, the distributed ST code*

$$\mathcal{X} = \left\{ \Psi_{\eta,N}(\alpha_{\tau,\theta}(X,Y)) = \operatorname{diag}\left\{\eta^i(\alpha_{\tau,\theta}(X,Y))\right\}_{i=0}^{N-1} \middle| \, X, Y \in \tilde{\lambda}(\mathcal{O}) \right\}$$

is a full-diversity ST code of rank $8N$, *rate* $R = 2$ *rspcu, exhibits the NVD property and is FD. Its decoding complexity is* $|S|^{k'}$, *where*

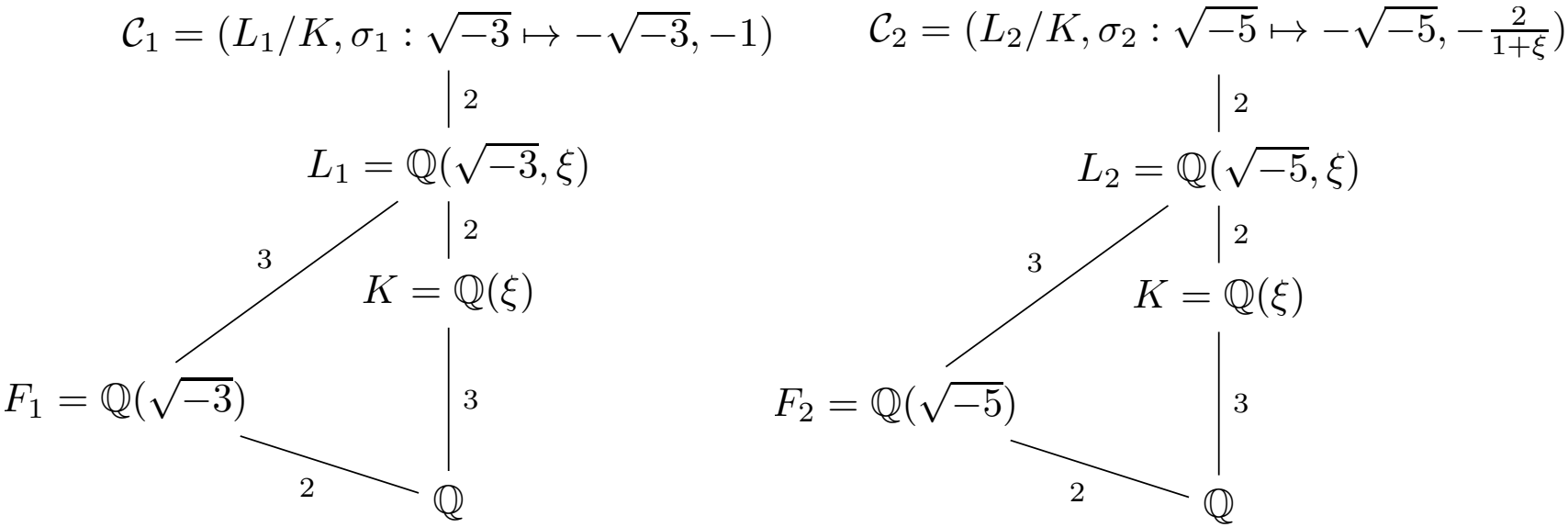
$$k' = \begin{cases} 4N & \text{if } a \equiv 1 \bmod 4, \\ 2N & \text{if } a \not\equiv 1 \bmod 4, \end{cases}$$

resulting in a reduction in complexity of 50% *and* 75%, *respectively.*

Two 3-relay example codes

Aalto University
School of Science

Consider $N = 3$ relays and the following towers of extensions.



- Both algebras are division for $\xi = \zeta_7 + \zeta_7^{-1}$.
- For $i = 1, 2$, set $\tau_i = \sigma_i$ and $\langle \eta_i : \xi \mapsto \xi^2 - 2 \rangle = \Gamma\left(L_i/F_i\right)$. ($\eta_1 \neq \eta_2$, since they have distinct fixed fields.)
- Let $\mathcal{O}_i \subset \mathcal{C}_i$, and set $\omega_1 = \frac{1+\sqrt{-3}}{2}$, $\omega_2 = \sqrt{-5}$.

Codeword structure

The original codes (before iteration an diagonalization) consist of codewords of the form

$$X_i = \tilde{\lambda}(x_i) = \begin{bmatrix} x_{1,i}+x_{2,i}\omega_i & -\sqrt{-\gamma_i}(x_{3,i}+x_{4,i}\sigma_i(\omega_i)) \\ \sqrt{-\gamma_i}(x_{3,i}+x_{4,i}\omega_i) & x_{1,i}+x_{2,i}\sigma_i(\omega_i) \end{bmatrix},$$

respectively.

Using these codes as building blocks, the overall 3-relay codes can be constructed as

$$\mathcal{X}_i = \left\{ \Psi_{\eta_i,3}(\alpha_{\tau_i,\theta_i}(X,Y)) = \mathrm{diag}\left\{ \eta_i^j(\alpha_{\tau_i,\theta_i}(X,Y)) \right\}_{j=0}^{2} \middle| \, X,Y \in \tilde{\lambda}(\mathcal{O}_i) \right\}$$

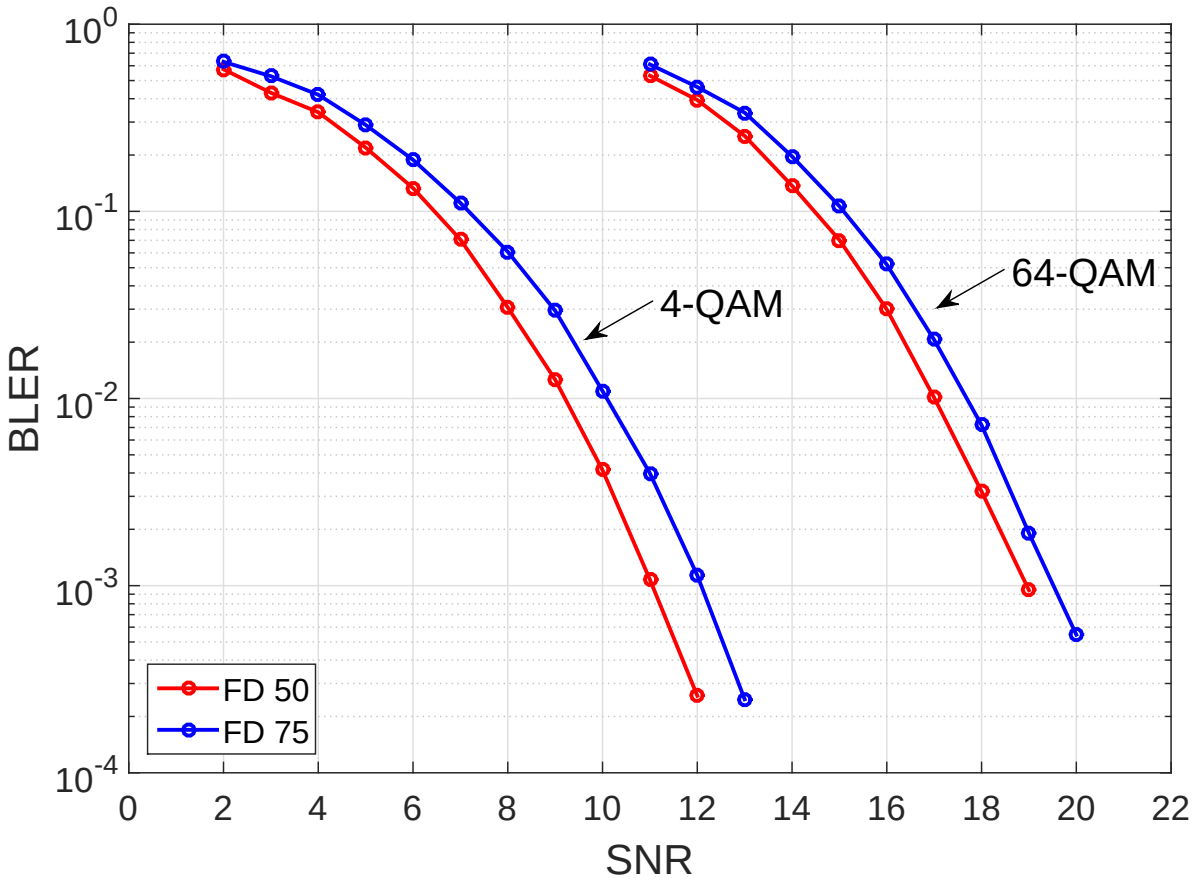
The code $\mathcal{X}_1$ is 2-group decodable and enjoys a reduction in decoding complexity of 50%, from $|S|^{24}$ to $|S|^{12}$.

The complexity of the 4-group decodable code $\mathcal{X}_2$ is reduced by 75% to $|S|^6$.

Comparing the performance

Aalto University
School of Science

No (ST) codes can be found in the literature for $N \geq 3$ relays. Thus, we compare the two example codes. $(n_s = 2, n_d = 6)$.



A two-user 2 Tx MIMO-MAC example I

Aalto University
School of Science

The previous constructions can also yield fast-decodable codes for a K-user MIMO-MAC.

- $K = 2$ with $n_s = 2$ and a single destination with $n_d = 4$.
- Both transmitters carve their ST codes from the algebra $\mathcal{C} = \left(\mathbb{Q}(\sqrt{-2}, \sqrt{-3}, i)/\mathbb{Q}(\sqrt{-2}, i), \sigma : \sqrt{-3} \mapsto -\sqrt{-3}, -\frac{2}{\sqrt{5}}\right)$.
- Let $\langle \tau : i \mapsto -i \rangle = \Gamma(\mathbb{Q}(\sqrt{-2}, i)/\mathbb{Q}(\sqrt{-2}))$.
- Codewords (for each transmitter) are of the form $U_k = [\, X_k \ \tau(X_k) \,]$, where for $x_k \in \mathcal{O} \subset \mathcal{C}$ and $\theta = \frac{1+\sqrt{-3}}{2}$,

$$X_k = \tilde{\lambda}(x_k) = \begin{bmatrix} x_{k,1}+x_{k,2}\theta & -\sqrt{-\gamma}(x_{k,3}+x_{k,4}\sigma(\theta)) \\ \sqrt{-\gamma}(x_{k,3}+x_{k,4}\theta) & x_{k,1}+x_{k,2}\sigma(\theta) \end{bmatrix}.$$

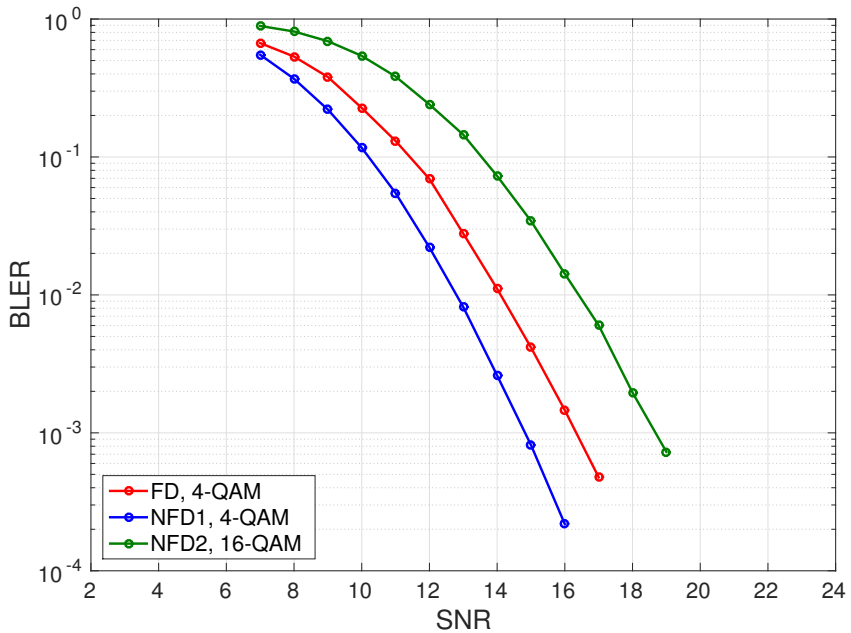
A two-user 2 Tx MIMO-MAC example II

Aalto University
School of Science

The overall transmitted codewords are of the form

$$X = \begin{bmatrix} X_1 & \tau(X_1) \\ X_2 & \tau(X_2) \end{bmatrix}.$$

This code has the *conditional* NVD property, and its reduction in decoding complexity is 50%, from $|S|^{32}$ to $|S|^{16}$.



The two codes chosen from comparison were adapted to match the data rate, and can be found in [Lu].

H. f. Lu et al. "New space–time code constructions for two-user multiple access channels". In: *IEEE J. Sel. Top. Signal Process.* 3.6 (2009), pp. 939–957

Conclusions and future research

Aalto University
School of Science

- Constructions of fast-decodable space–time codes for the N-relay NAF amplify-and-forward channel.
- Full-diversity and NVD.
- SIMO: 37% reduction in decoding complexity order.
  Achieves the DMT of the channel.
- MIMO: up to 75% reduction in decoding complexity order.
- Constructions can be adapted to the N-user MIMO-MAC, resulting in fast-decodable codes with CNVD for that setting.

- In future, xtensions to $n_s > 2$, which means dealing with higher-degree algebras.
- Maybe the new relaxed conditions on fast-decodability facilitate new constructions.
- More accurate complexity comparison by counting floating point operations.

Conclusions and future research

Aalto University
School of Science

- Constructions of fast-decodable space–time codes for the N-relay NAF amplify-and-forward channel.
- Full-diversity and NVD.
- SIMO: 37% reduction in decoding complexity order.
  Achieves the DMT of the channel.
- MIMO: up to 75% reduction in decoding complexity order.
- Constructions can be adapted to the N-user MIMO-MAC, resulting in fast-decodable codes with CNVD for that setting.

- In future, xtensions to $n_s > 2$, which means dealing with higher-degree algebras.
- Maybe the new relaxed conditions on fast-decodability facilitate new constructions.
- More accurate complexity comparison by counting floating point operations.

Kiitos!