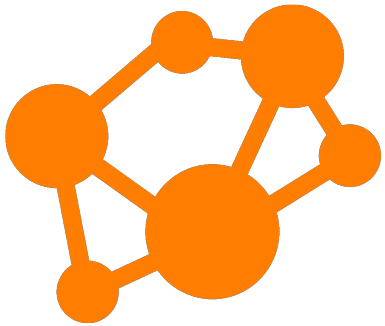

unine
Université de Neuchâtel

Submodule codes and matrix codes for physical-layer network coding

Anestis Alvertos Tzogias (joint w/ E. Gorla)
Université de Neuchâtel

OpeRa 2026 - Bordeaux

February 2026

Acknowledgement

Funded by the European Union

Among us

One of these is not like the others...

$$\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_{2^2}, \mathbb{F}_5, \mathbb{Z}/8\mathbb{Z}$$

Among us

One of these is not like the others...

$$\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_{2^2}, \mathbb{F}_5, \mathbb{Z}/8\mathbb{Z}$$

Finite fields farming aura

Finite rings losing aura

Background

- 2008: Silva, Kschischang, Kötter[1] introduced **subspace codes** for AMMC matrix channel in random network coding.

[1] D. Silva, F. Kschischang, R. Kötter, *A Rank-Metric Approach to Error Control in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54 (2008), no. 9, pp. 3951-3967.

[2] E. Gorla, A. Ravagnani, *An algebraic framework for end-to-end physical-layer network coding*, IEEE Transactions on Information Theory, vol. 64 (2018), no. 6, pp. 4480-4495.

Background

- 2008: Silva, Kschischang, Kötter[1] introduced **subspace codes** for AMMC matrix channel in random network coding.
- No algebraic structure $\rightarrow$ use **rank-metric codes** as proxy.

[1] D. Silva, F. Kschischang, R. Kötter, *A Rank-Metric Approach to Error Control in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54 (2008), no. 9, pp. 3951-3967.

[2] E. Gorla, A. Ravagnani, *An algebraic framework for end-to-end physical-layer network coding*, IEEE Transactions on Information Theory, vol. 64 (2018), no. 6, pp. 4480-4495.

Background

- 2008: Silva, Kschischang, Kötter[1] introduced **subspace codes** for AMMC matrix channel in random network coding.
- No algebraic structure $\rightarrow$ use **rank-metric codes** as proxy.
- 2018: Gorla, Ravagnani[2] introduced **submodule codes** over finite **principal ideal rings (PIRs)** for end-to-end physical layer network coding based on nested complex lattices ("compute-and-forward", algebraic realisation by Feng, Silva, Kschischang)

[1] D. Silva, F. Kschischang, R. Kötter, *A Rank-Metric Approach to Error Control in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54 (2008), no. 9, pp. 3951-3967.

[2] E. Gorla, A. Ravagnani, *An algebraic framework for end-to-end physical-layer network coding*, IEEE Transactions on Information Theory, vol. 64 (2018), no. 6, pp. 4480-4495.

Background

- 2008: Silva, Kschischang, Kötter[1] introduced **subspace codes** for AMMC matrix channel in random network coding.
- No algebraic structure $\rightarrow$ use **rank-metric codes** as proxy.
- 2018: Gorla, Ravagnani[2] introduced **submodule codes** over finite **principal ideal rings (PIRs)** for end-to-end physical layer network coding based on nested complex lattices ("compute-and-forward", algebraic realisation by Feng, Silva, Kschischang)
- This project: find a proxy for submodule codes.

---

[1] D. Silva, F. Kschischang, R. Kötter, *A Rank-Metric Approach to Error Control in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54 (2008), no. 9, pp. 3951-3967.

[2] E. Gorla, A. Ravagnani, *An algebraic framework for end-to-end physical-layer network coding*, IEEE Transactions on Information Theory, vol. 64 (2018), no. 6, pp. 4480-4495.

Algebraic preliminaries

- Codes of row modules of $m \times n$ matrices over a finite PIR R (e.g. $\mathbb{Z}/n\mathbb{Z}$), and for submodules $M, N \subseteq R^n$, the **submodule distance** is

$$d_S(M, N) = \lambda_R(M/M \cap N) + \lambda_R(N/M \cap N),$$

  where $\lambda_R(M)$ is the **length** of M as an R-module, i.e. the # of inclusions in a composition series of M.

Algebraic preliminaries

- Codes of row modules of $m \times n$ matrices over a finite PIR R (e.g. $\mathbb{Z}/n\mathbb{Z}$), and for submodules $M, N \subseteq R^n$, the **submodule distance** is

$$d_S(M, N) = \lambda_R(M/M \cap N) + \lambda_R(N/M \cap N),$$

  where $\lambda_R(M)$ is the **length** of M as an R-module, i.e. the # of inclusions in a composition series of M.
- E.g.: $\mathbb{Z}/8\mathbb{Z}$ has length 3 as a module over itself: $(0) \subset (4) \subset (2) \subset (1)$.
- $\langle (1,0), (0,4) \rangle$ has length 4 over $\mathbb{Z}/8\mathbb{Z}$.

Algebraic preliminaries

- Codes of row modules of $m \times n$ matrices over a finite PIR R (e.g. $\mathbb{Z}/n\mathbb{Z}$), and for submodules $M, N \subseteq R^n$, the **submodule distance** is

$$d_S(M, N) = \lambda_R(M/M \cap N) + \lambda_R(N/M \cap N),$$

  where $\lambda_R(M)$ is the **length** of M as an R-module, i.e. the # of inclusions in a composition series of M.
- E.g.: $\mathbb{Z}/8\mathbb{Z}$ has length 3 as a module over itself: $(0) \subset (4) \subset (2) \subset (1)$.
- $\langle (1,0), (0,4) \rangle$ has length 4 over $\mathbb{Z}/8\mathbb{Z}$.
- We defined **length-metric codes**: submodules $\mathcal{C} \subseteq \mathrm{Mat}_{m \times n}(R)$, with the metric

$$d(A, A') = \lambda_R(\mathrm{rowsp}(A - A')).$$

The Singleton bound and MLD codes

- Observe: If R is a field, we recover the theory of rank-metric codes.

The Singleton bound and MLD codes

- Observe: If R is a field, we recover the theory of rank-metric codes.

Theorem (Singleton bound for length-metric codes)

Let R be a finite PIR and $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(R)$ a length-metric code of minimum distance d. Then

$$\lambda_R(\mathcal{C}) \leq \max\{m,n\}(\min\{m,n\} - d + 1)\lambda_R(R).$$

*$\mathcal{C}$ is an **MLD** code if it meets this bound with equality.*

The Singleton bound and MLD codes

- Observe: If R is a field, we recover the theory of rank-metric codes.

Theorem (Singleton bound for length-metric codes)

Let R be a finite PIR and $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(R)$ a length-metric code of minimum distance d. Then

$$\lambda_R(\mathcal{C}) \leq \max\{m,n\}(\min\{m,n\} - d + 1)\lambda_R(R).$$

*$\mathcal{C}$ is an **MLD** code if it meets this bound with equality.*

- Use properties of finite PIRs and of the length to reduce to **finite chain ring** case (i.e. R has only 1 maximal ideal (ϖ), e.g. $\mathbb{Z}/p^n\mathbb{Z}$).

The Singleton bound and MLD codes

- Observe: If R is a field, we recover the theory of rank-metric codes.

Theorem (Singleton bound for length-metric codes)

Let R be a finite PIR and $\mathcal{C} \subseteq \mathrm{Mat}_{m\times n}(R)$ a length-metric code of minimum distance d. Then

$$\lambda_R(\mathcal{C}) \leq \max\{m,n\}(\min\{m,n\} - d + 1)\lambda_R(R).$$

*$\mathcal{C}$ is an **MLD** code if it meets this bound with equality.*

- Use properties of finite PIRs and of the length to reduce to **finite chain ring** case (i.e. R has only 1 maximal ideal (ϖ), e.g. $\mathbb{Z}/p^n\mathbb{Z}$).
- **Question**: Do there exist MLD codes? What do they look like?

The Singleton bound and MLD codes

- **Observation**: When R is local, it "contains" its residue field $R/(\varpi) \implies$ A code $\mathcal{C}$ over R "contains" a rank-metric code $\mathcal{D}$ over a finite field $\mathbb{F}_q$!

The Singleton bound and MLD codes

- **Observation**: When R is local, it "contains" its residue field $R/(\varpi) \implies$ A code $\mathcal{C}$ over R "contains" a rank-metric code $\mathcal{D}$ over a finite field $\mathbb{F}_q$!

Theorem

Every MRD code $\mathcal{D}$ over $\mathbb{F}_q$ gives rise to an MLD code over any finite local PIR R that has residue field $\mathbb{F}_q$.

The Singleton bound and MLD codes

- **Observation**: When R is local, it "contains" its residue field $R/(\varpi) \implies$ A code $\mathcal{C}$ over R "contains" a rank-metric code $\mathcal{D}$ over a finite field $\mathbb{F}_q$!

Theorem

Every MRD code $\mathcal{D}$ over $\mathbb{F}_q$ gives rise to an MLD code over any finite local PIR R that has residue field $\mathbb{F}_q$.

Remark

Not every code $\mathcal{C}$ over R that "contains" an MRD code is an MLD code.

Equivalence of length-metric codes

Definition

An R- **linear isometry** ϕ of $\mathrm{Mat}_{n\times n}(R)$ is an R-module homomorphism $\mathrm{Mat}_{n\times n}(R) \to \mathrm{Mat}_{n\times n}(R)$ such that $\lambda(\phi(M)) = \lambda(M)$ for every $M \in \mathrm{Mat}_{n\times n}(R)$. $\mathcal{C}, \mathcal{D} \subseteq \mathrm{Mat}_{n\times n}(R)$ are **equivalent** if there is an isometry $\phi : \mathrm{Mat}_{n\times n}(R) \to \mathrm{Mat}_{n\times n}(R)$ with $\phi(\mathcal{C}) = \mathcal{D}$.

Theorem (Hua, Wan)

Let $\phi : \mathrm{Mat}_{m\times n}(\mathbb{F}_q) \to \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ be an $\mathbb{F}_q$-linear isometry of rank-metric codes. Then there exist $P \in \mathrm{GL}_m(\mathbb{F}_q), Q \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\phi(A) = PAQ$, for every $A \in \mathrm{Mat}_{m\times n}(\mathbb{F}_q)$ (up to transposition if $m = n$).

- **Question**: What does code equivalence look like in the length metric?

Equivalence of length-metric codes

Theorem (McDonald)

Let R be a local ring, $\phi : \mathrm{Mat}_{m\times n}(R) \to \mathrm{Mat}_{m\times n}(R)$ be an R-module hom. mapping rank 1 matrices to rank 1 matrices. Then there exist $P \in \mathrm{GL}_m(R), Q \in \mathrm{GL}_n(R)$ such that $\phi(A) = PAQ$, $\forall A \in \mathrm{Mat}_{m\times n}(R)$ (up to transposition if $m = n$).

Equivalence of length-metric codes

Theorem (McDonald)

Let R be a local ring, $\phi : \mathrm{Mat}_{m\times n}(R) \to \mathrm{Mat}_{m\times n}(R)$ be an R-module hom. mapping rank 1 matrices to rank 1 matrices. Then there exist $P \in \mathrm{GL}_m(R), Q \in \mathrm{GL}_n(R)$ such that $\phi(A) = PAQ$, $\forall A \in \mathrm{Mat}_{m\times n}(R)$ (up to transposition if $m = n$).

Lemma

Let R be a finite chain ring. Then R- linear isometries map rank 1 matrices to rank 1 matrices.

Equivalence of length-metric codes

Theorem (McDonald)

Let R be a local ring, $\phi : \mathrm{Mat}_{m\times n}(R) \to \mathrm{Mat}_{m\times n}(R)$ be an R-module hom. mapping rank 1 matrices to rank 1 matrices. Then there exist $P \in \mathrm{GL}_m(R), Q \in \mathrm{GL}_n(R)$ such that $\phi(A) = PAQ$, $\forall A \in \mathrm{Mat}_{m\times n}(R)$ (up to transposition if $m = n$).

Lemma

Let R be a finite chain ring. Then R- linear isometries map rank 1 matrices to rank 1 matrices.

Theorem

Let R be a finite PIR, let $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\ell$ a length-metric code over R and $\phi : \mathrm{Mat}_{m\times n}(R) \to \mathrm{Mat}_{m\times n}(R)$ be an isometry. Then there exist $P \in \mathrm{GL}_m(R), Q \in \mathrm{GL}_n(R)$ s.t. $\phi(A) = P\psi(A)Q$ for all $A \in \mathrm{Mat}_{m\times n}(R)$, where ψ is either the identity or may transpose some factors if $m = n$.

Thank you for OpeRa!