On the hardness of code equivalence problem in rank metric

A. Couvreur, T. Debris–Alazard, P. Gaborit

Lfant seminar, Bordeaux, January 12, 2021

1. Introduction

2. In Hamming metric

3. In rank metric
   - The code equivalence problem for $\mathbb{F}_{q^m}$–linear codes
   - The general case

1. Introduction
2. In Hamming metric
3. In rank metric
   - The code equivalence problem for $\mathbb{F}_{q^m}$–linear codes
   - The general case

The problem

Problem 1

Let V_1, V_2 be metric spaces, decide whether they are isometric.

The metric may be:

The problem

Problem 1

Let V_1, V_2 be metric spaces, decide whether they are isometric.

The metric may be:

- Euclidean metric (lattice isometry/similitude problem);

The problem

Problem 1

Let V_1, V_2 be metric spaces, decide whether they are isometric.

The metric may be:

- Euclidean metric (lattice isometry/similitude problem);
- Hamming metric (code permutation/monomial equivalence problem);

The problem

Problem 1

Let V_1, V_2 be metric spaces, decide whether they are isometric.

The metric may be:

- Euclidean metric (lattice isometry/similitude problem);
- Hamming metric (code permutation/monomial equivalence problem);
- **Today's purpose** rank metric.

Code equivalence problems in Hamming metric

Problem 2 (Permutation Equivalence of Codes (PEC))

Let $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$ *be two codes. Decide whether there exists* $\boldsymbol{P} \in \mathfrak{S}_n$ *such that*

$$\mathscr{C}_1 = \mathscr{C}_2 \cdot \boldsymbol{P}.$$

Problem 3 (Monomial Equivalence of Codes (MEC))

Let $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$ *be two codes. Decide whether there exists* $\boldsymbol{P} \in \mathfrak{S}_n$ *and* $\boldsymbol{D} \in Diag(n)$ *such that*

$$\mathscr{C}_1 = \mathscr{C}_2 \cdot \boldsymbol{D} \cdot \boldsymbol{P}.$$

Previous works on equivalence in Hamming metric

- **Theoretical results**
  - Code equivalence is harder than graph isomorphism (Petrank, Roth, 1997);
  - Code equivalence is **not** $\mathcal{NP}$–hard (unless polynomial time hierarchy collapses)
  - If $\mathscr{C} \cap \mathscr{C}^{\perp} = \{0\}$ then code equivalence is as hard as graph isomorphism (Bardet, Otmani, Saeed 2019)

Previous works on equivalence in Hamming metric

- **Theoretical results**
  - Code equivalence is harder than graph isomorphism (Petrank, Roth, 1997);
  - Code equivalence is **not** $\mathcal{NP}$–hard (unless polynomial time hierarchy collapses)
  - If $\mathscr{C} \cap \mathscr{C}^\perp = \{0\}$ then code equivalence is as hard as graph isomorphism (Bardet, Otmani, Saeed 2019)
- **Algorithms**
  - Leon (1982);
  - Sendrier (2000) solves equivalence in $O(2^{\dim \mathscr{C} \cap \mathscr{C}^\perp} n^\omega)$;
  - Feulner (2009), techniques from symmetric cryptography;
  - Saeed (2017), Gröbner bases.

1. Introduction

2. In Hamming metric

3. In rank metric
   - The code equivalence problem for $\mathbb{F}_{q^m}$–linear codes
   - The general case

Matrix codes

The space of $m \times n$ matrices with entries in $\mathbb{F}_q$ is denoted by $\mathcal{M}_{m,n}(\mathbb{F}_q)$.

Definition 1

A matrix code is a subspace $\mathscr{C}^{mat}$ of $\mathcal{M}_{m,n}(\mathbb{F}_q)$ endowed with the rank metric *:*

$$d_R(\boldsymbol{A}, \boldsymbol{B}) = Rk\,(\boldsymbol{A} - \boldsymbol{B}).$$

Vector codes

- Fix an $\mathbb{F}_q$–basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$. Then, to any subspace $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ corresponds a matrix code

$$\mathscr{C}^{\mathrm{mat}} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q).$$

- Conversely, let a be a primitive element of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $C(a)$ the matrix representing the $\mathbb{F}_q$–linear map $x \mapsto ax$ in a basis $\mathcal{B}$. A matrix code $\mathscr{C}^{\mathrm{mat}}$ such that

$$C(a) \cdot \mathscr{C}^{\mathrm{mat}} \subseteq \mathscr{C}^{\mathrm{mat}}$$

comes from a vector code.

Stabilizer algebras

Definition 2

Let $\mathscr{C} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$ be a matrix code. The left *(resp.* right*)* stabilizer algebra *of $\mathscr{C}$ is defined as*

$$\mathrm{Stab}_L(\mathscr{C}) \overset{def}{=} \{\boldsymbol{P} \in \mathcal{M}_m(\mathbb{F}_q) \mid \boldsymbol{P} \cdot \mathscr{C} \subseteq \mathscr{C}\}$$

$$\text{resp.} \quad \mathrm{Stab}_R(\mathscr{C}) \overset{def}{=} \{\boldsymbol{Q} \in \mathcal{M}_n(\mathbb{F}_q) \mid \mathscr{C} \cdot \boldsymbol{Q} \subseteq \mathscr{C}\}$$

Lemma 1

A matrix code $\mathscr{C} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$ whose left stabilizer algebra contains a representation of $\mathbb{F}_{q^m}$ is $\mathbb{F}_{q^m}$–linear.

Rank–preserving linear maps

Theorem 1

The group of linear automorphisms $\phi : \mathcal{M}_{m,n}(\mathbb{F}_q) \to \mathcal{M}_{m,n(\mathbb{F}_q)}$ *preserving the ranks is spanned by the maps:*

- $\boldsymbol{X} \mapsto \boldsymbol{A} \cdot \boldsymbol{X}$ *for some* $\boldsymbol{A} \in \mathrm{GL}_m(\mathbb{F}_q)$*;*
- $\boldsymbol{X} \mapsto \boldsymbol{X} \cdot \boldsymbol{B}$ *for some* $\boldsymbol{B} \in \mathrm{GL}_n(\mathbb{F}_q)$*;*
- *(only for* $m = n$*):* $\boldsymbol{X} \mapsto \boldsymbol{X}^T$*.*

Equivalence problem in rank metric

Problem 4 (Rank Equivalence of Matrix Codes (REMC))

Given $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$, *decide wheter there exists* $\boldsymbol{P} \in \mathsf{GL}_m(\mathbb{F}_q)$ *and* $\boldsymbol{Q} \in \mathsf{GL}_n(\mathbb{F}_q)$ *such that*

$$\mathscr{C}_1^{mat} = \boldsymbol{P} \cdot \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}.$$

Our contribution

Theorem 2 (C., Debris–Alazard, Gaborit, 2020)

For $\mathbb{F}_{q^m}$–linear codes $\mathscr{C}_1^{vec}, \mathscr{C}_2^{vec} \subseteq \mathbb{F}_{q^m}^n$, the equivalence problem in rank metric is in $\mathcal{P}$ if $q = (mn)^{O(1)}$. Else it is in $\mathcal{ZPP}$.

Theorem 3 (C., Debris–Alazard, Gaborit, 2020)

For general matrix spaces, the equivalence problem in rank metric is harder than the equivalence problem in Hamming metric.

Statement

If the vector structure is known:

Problem 5 (Rank Equivalence of Vector Codes (REVC))

Given $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_{q^m}^n$, decide whether there exists $\boldsymbol{P} \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathscr{C}_1 = \mathscr{C}_2 \cdot \boldsymbol{P}$$

If not:

Problem 6 (Rank Equivalence of Hidden Vector Codes (REHVC))

Given $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$ constructed from $\mathbb{F}_{q^m}$–linear codes with possibly distinct bases. Decide whether there exists $\boldsymbol{P} \in \mathrm{GL}_m(\mathbb{F}_q)$ and $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathscr{C}_1^{mat} = \boldsymbol{P} \cdot \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}.$$

Reducing to another problem

Even when the vector structure is hidden, $\boldsymbol{P}$ may be recovered separately by computing the left stabilizer algebras which are conjugated under $\boldsymbol{P}$. Hence we are reduced to:

Problem 7 (Right equivalence)

Given matrix codes $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$, *decide whether there exists* $\boldsymbol{P} \in \mathrm{GL}_n(\mathbb{F}_q)$ *such that*

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{P}.$$

Reducing to another problem

Even when the vector structure is hidden, $\boldsymbol{P}$ may be recovered separately by computing the left stabilizer algebras which are conjugated under $\boldsymbol{P}$. Hence we are reduced to:

Problem 7 (Right equivalence)

Given matrix codes $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$*, decide whether there exists* $\boldsymbol{P} \in \mathrm{GL}_n(\mathbb{F}_q)$ *such that*

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{P}.$$

Fact

Finding the space of $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ *such that* $\mathscr{C}_2^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_1^{mat}$ *boils down to solve a linear system.*

Reducing to another problem

Even when the vector structure is hidden, $\boldsymbol{P}$ may be recovered separately by computing the left stabilizer algebras which are conjugated under $\boldsymbol{P}$. Hence we are reduced to:

Problem 7 (Right equivalence)

Given matrix codes $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$, *decide whether there exists* $\boldsymbol{P} \in \mathrm{GL}_n(\mathbb{F}_q)$ *such that*

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{P}.$$

Fact

Finding the space of $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ *such that* $\mathscr{C}_2^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_1^{mat}$ *boils down to solve a linear system.*

But, what if the space of solutions contains singular matrices? How to decide whether there is a nonsingular one in it?

Considering the right stabilizer algebras

Theorem 4

Let $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ *such that* $\mathrm{Stab}_R(\mathscr{C}_1^{mat})$ *is a division algebra. If there exists* $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ *such that*

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}$$

then any $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ *such that* $\mathscr{C}_1^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{mat}$ *is nonsingular.*

Considering the right stabilizer algebras

Theorem 4

Let $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\mathrm{Stab}_R(\mathscr{C}_1^{mat})$ is a division algebra. If there exists $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}$$

then any $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ such that $\mathscr{C}_1^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{mat}$ is nonsingular.

Proof.

Suppose that $\exists \boldsymbol{P}$ singular such that $\mathscr{C}_1^{\mathrm{mat}} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{\mathrm{mat}}$. Then

$$\mathscr{C}_1^{\mathrm{mat}} \cdot \boldsymbol{P} \cdot \boldsymbol{Q} \subseteq \mathscr{C}_2^{\mathrm{mat}} \cdot \boldsymbol{Q} = \mathscr{C}_1^{\mathrm{mat}}$$

Hence $\boldsymbol{PQ} \in \mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}})$ and is singular: a contradiction. $\square$

Considering the right stabilizer algebras

Theorem 4

Let $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\mathrm{Stab}_R(\mathscr{C}_1^{mat})$ is a division algebra. If there exists $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}$$

then any $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ such that $\mathscr{C}_1^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{mat}$ is nonsingular.

Consequence. In this situation, the problem is easy to solve:

Considering the right stabilizer algebras

Theorem 4

Let $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\mathrm{Stab}_R(\mathscr{C}_1^{mat})$ is a division algebra. If there exists $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}$$

then any $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ such that $\mathscr{C}_1^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{mat}$ is nonsingular.

Consequence. In this situation, the problem is easy to solve:

1. Compute the space of $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ such that $\mathscr{C}_1^{\mathrm{mat}} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{\mathrm{mat}}$;

Considering the right stabilizer algebras

Theorem 4

Let $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ such that $\mathrm{Stab}_R(\mathscr{C}_1^{mat})$ is a division algebra. If there exists $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathscr{C}_1^{mat} = \mathscr{C}_2^{mat} \cdot \boldsymbol{Q}$$

then any $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ such that $\mathscr{C}_1^{mat} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{mat}$ is nonsingular.

Consequence. In this situation, the problem is easy to solve:

1. Compute the space of $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q)$ such that $\mathscr{C}_1^{\mathrm{mat}} \cdot \boldsymbol{P} \subseteq \mathscr{C}_2^{\mathrm{mat}}$;
2. Pick a nonzero element $\boldsymbol{P}$ in the solution space:
   - if $\boldsymbol{P}$ is singular, then the codes are **not** right equivalent;
   - else they are right equivalent and $\boldsymbol{P}$ realizes the equivalence.

About finite dimensional algebras

A subalgebra $\mathcal{A} \subseteq \mathcal{M}_n(\mathbb{F}_q)$ is

- **simple** if it has no nontrivial two–sided ideals. Artin Wedderburn theory $\Rightarrow$ any simple algebra over $\mathbb{F}_q$ are isomorphic to $\mathcal{M}_r(\mathbb{F}_{q^\ell})$ for some r, ℓ.
- **semi-simple** if it is isomorphic to a cartesian product of simple algebras.

Definition 3 (Jacobson radical)

The radical of an algebra $\mathcal{A}$ is defined as

$$\mathrm{Rad}(\mathcal{A}) \stackrel{def}{=} \{\boldsymbol{N} \in \mathcal{A} \mid \forall \boldsymbol{M} \in \mathcal{A},\ \boldsymbol{MN} \text{ is nilpotent}\}$$

Theorem 5

$\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ *is semi–simple.*

A picture

About finite dimensional algebras – algorithms

- Friedl, Rónyai 1985: the Jacobson radical and the Artin Wedderburn decomposition can be computed in polynomial time. Their algorithm rests on two tools:
  - linear algebra;
  - factorisation of univariate polynomials (this is the why of $\mathcal{P}$ v.s. $\mathcal{ZPP}$).
- Rónyai 1990. Given a simple algebra the isomorphism with $\mathcal{M}_r(\mathbb{F}_{q^\ell})$ can be explicitly computed.

Framework for solving right equivalence

Input. Two matrix codes $\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$.

Framework for solving right equivalence

Input. Two matrix codes $\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$.

- Compute their right stabilizer algebras;

Framework for solving right equivalence

Input. Two matrix codes $\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$.

- Compute their right stabilizer algebras;
- If they are local (i.e. $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ is a field), then, take any element of $Cond(\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}}) \setminus \mathrm{Rad}(\mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}}))$ and check whether it is singular.

Framework for solving right equivalence

Input. Two matrix codes $\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$.

- Compute their right stabilizer algebras;
- If they are local (i.e. $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ is a field), then, take any element of $Cond(\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}}) \setminus \mathrm{Rad}(\mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}}))$ and check whether it is singular.
- Compute the Artin–Wedderburn decomposition of $\mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}})/\mathrm{Rad}(\mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}}))$, deduce a decomposition of

$$1 = e_1 + \cdots + e_r$$

as a sum of minimal orthogonal idempotents; lift idempotents (effective Wedderburn Malcev) and compare the codes

$$\mathscr{C}_1^{\mathrm{mat}} e_1, \ldots, \mathscr{C}_1^{\mathrm{mat}} e_r$$

with the corresponding codes from $\mathscr{C}_2^{\mathrm{mat}}$.

A picture

A picture

The general problem

Theorem 6

The general rank equivalence of matrix codes (REMC) problem is harder than the Hamming metric monomial equivalence problem.

Sketch of proof of the reduction

Let $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_{q^m}$ with generator matrices $\boldsymbol{G}_1, \boldsymbol{G}_2$.

$$\boldsymbol{G}_1 = \left(\begin{array}{c|c|c|c} \boldsymbol{c}_1^\top & \boldsymbol{c}_2^\top & \cdots & \boldsymbol{c}_n^\top \end{array} \right), \quad \boldsymbol{G}_2 = \left(\begin{array}{c|c|c|c} \boldsymbol{d}_1^\top & \boldsymbol{d}_2^\top & \cdots & \boldsymbol{d}_n^\top \end{array} \right)$$

Sketch of proof of the reduction

$$\boldsymbol{G}_1 = \left(\begin{array}{c|c|c|c} \boldsymbol{c}_1^\top & \boldsymbol{c}_2^\top & \cdots & \boldsymbol{c}_n^\top \end{array} \right), \quad \boldsymbol{G}_2 = \left(\begin{array}{c|c|c|c} \boldsymbol{d}_1^\top & \boldsymbol{d}_2^\top & \cdots & \boldsymbol{d}_n^\top \end{array} \right)$$

We look for $S \in \mathrm{GL}_k(\mathbb{F}_q)$ and $\boldsymbol{P} \in (\mathbb{F}_q^\times)^n \ltimes \mathfrak{S}_n$ such that

$$\boldsymbol{G}_1 = \boldsymbol{S}\boldsymbol{G}_2\boldsymbol{P}.$$

Sketch of proof of the reduction

$$\boldsymbol{G}_1 = \left(\begin{array}{c|c|c|c} \boldsymbol{c}_1^\top & \boldsymbol{c}_2^\top & \cdots & \boldsymbol{c}_n^\top \end{array} \right), \quad \boldsymbol{G}_2 = \left(\begin{array}{c|c|c|c} \boldsymbol{d}_1^\top & \boldsymbol{d}_2^\top & \cdots & \boldsymbol{d}_n^\top \end{array} \right)$$

We look for $S \in \mathsf{GL}_k(\mathbb{F}_q)$ and $\boldsymbol{P} \in (\mathbb{F}_q^\times)^n \ltimes \mathfrak{S}_n$ such that

$$\boldsymbol{G}_1 = \boldsymbol{S}\boldsymbol{G}_2\boldsymbol{P}.$$

Define

$$\mathscr{C}_1^{\mathrm{mat}} \stackrel{\mathsf{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\left\{\boldsymbol{c}_i^\top \cdot \boldsymbol{c}_i\right\}, \quad \mathscr{C}_2^{\mathrm{mat}} \stackrel{\mathsf{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\left\{\boldsymbol{d}_i^\top \cdot \boldsymbol{d}_i\right\}$$

Sketch of proof of the reduction

$$\boldsymbol{G}_1 = \left(\begin{array}{c|c|c|c} \boldsymbol{c}_1^\top & \boldsymbol{c}_2^\top & \cdots & \boldsymbol{c}_n^\top \end{array} \right), \quad \boldsymbol{G}_2 = \left(\begin{array}{c|c|c|c} \boldsymbol{d}_1^\top & \boldsymbol{d}_2^\top & \cdots & \boldsymbol{d}_n^\top \end{array} \right)$$

We look for $S \in \mathrm{GL}_k(\mathbb{F}_q)$ and $\boldsymbol{P} \in (\mathbb{F}_q^\times)^n \ltimes \mathfrak{S}_n$ such that

$$\boldsymbol{G}_1 = \boldsymbol{S}\boldsymbol{G}_2\boldsymbol{P}.$$

Define

$$\mathscr{C}_1^{\mathrm{mat}} \stackrel{\mathrm{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\left\{\boldsymbol{c}_i^\top \cdot \boldsymbol{c}_i\right\}, \quad \mathscr{C}_2^{\mathrm{mat}} \stackrel{\mathrm{def}}{=} \mathrm{Span}_{\mathbb{F}_q}\left\{\boldsymbol{d}_i^\top \cdot \boldsymbol{d}_i\right\}$$

Fact

These matrix spaces are independent from $\boldsymbol{P}$! In addition:

$$\mathscr{C}_1^{mat} = \boldsymbol{S}\mathscr{C}_2^{mat}\boldsymbol{S}^\top.$$

Last observation

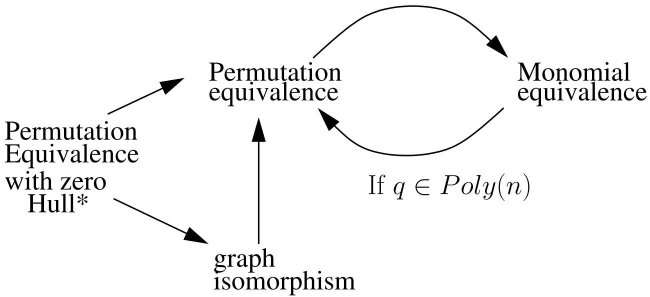
Remark

It might be possible that $\mathscr{C}_1^{mat}$ and $\mathscr{C}_2^{mat}$ are equivalent while $\mathscr{C}_1, \mathscr{C}_2$ are **not** *monomially equivalent. To address this issue, we consider slightly more complicated matrix codes:*

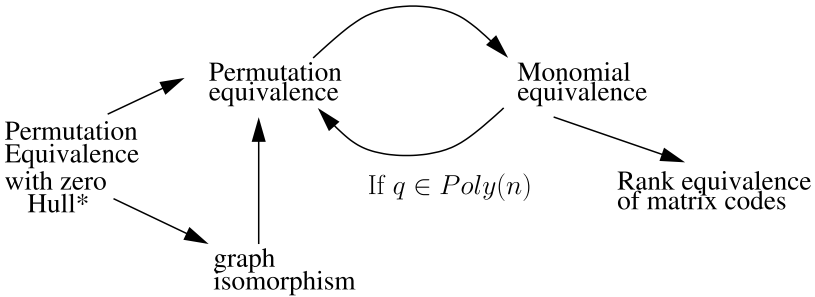
$$\mathscr{C}_1^{mat} \stackrel{def}{=} \mathrm{Span}\left\{ \begin{pmatrix} \boldsymbol{c}_i^\top \cdot \boldsymbol{c}_i \\ \hline \boldsymbol{M}_i \end{pmatrix} \right\},$$

where $\boldsymbol{M}_i \in \mathcal{M}_k(\mathbb{F}_q)$ is zero but at the i–th row which is all-one.

A picture


Permutation equivalence
Monomial equivalence
Permutation Equivalence with zero Hull*
If $q \in Poly(n)$
graph isomorphism

A picture


Permutation
equivalence
Monomial
equivalence
Permutation
Equivalence
with zero
Hull*
If $q \in Poly(n)$
Rank equivalence
of matrix codes
graph
isomorphism

Conclusion

- In Hamming metric

Conclusion

- In Hamming metric
    - permutation equivalence is "most of the times" easy to solve;

Conclusion

- In Hamming metric
  - permutation equivalence is “most of the times” easy to solve;
  - monomimal equivalence is hard to solve.

Conclusion

- In Hamming metric
  - permutation equivalence is "most of the times" easy to solve;
  - monomimal equivalence is hard to solve.
- In rank metric
  - Equivalence of $\mathbb{F}_{q^m}$–linear codes would be easy even when hiding the $\mathbb{F}_{q^m}$–linear structure

Conclusion

- In Hamming metric
  - permutation equivalence is "most of the times" easy to solve;
  - monomimal equivalence is hard to solve.
- In rank metric
  - Equivalence of $\mathbb{F}_{q^m}$–linear codes would be easy even when hiding the $\mathbb{F}_{q^m}$–linear structure
  - Equivalence of non structured matrix codes is at least as hard (in the worst case) to monomial equivalence in Hamming metric.

Thank you for your attention!