On the hardness of the code equivalence problem in rank metric

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

December 2, 2020

1. In Hamming metric
2. In rank metric
3. Equivalence of $\mathbb{F}_{q^m}$–linear codes is easy
4. General equivalence is hard

Isometries in Hamming metric

Definition 1

The group of linear Hamming isometries, is the group of linear maps $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$, $d_H(\phi(\boldsymbol{x}), \phi(\boldsymbol{y})) = d_H(\boldsymbol{x}, \boldsymbol{y})$.

Theorem 1

The group of linear isometries is the subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ spanned by

- *permutation matrices;*
- *nonsingular diagonal matrices.*

$$\mathsf{Isom}_{\mathrm{Hamming}}(\mathbb{F}_q^n) = (\mathbb{F}_q^\times)^n \ltimes \mathfrak{S}_n.$$

Code equivalence problems

Problem 1 (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 2 (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*

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

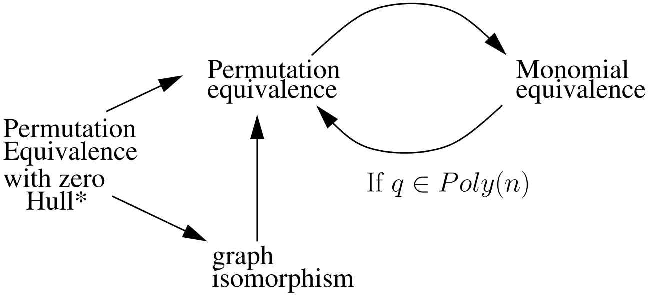
Theoretical hardness of code equivalence problems

Theorem 2 (Petrank, Roth, 1997)

Code equivalence problems are **not** *NP–Complete... unless the polynomial–time hierarchy collapses.*

Last overview

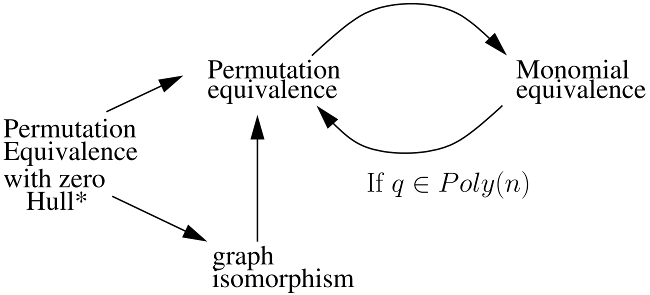
Notation $A \to B$ means "if I can solve B, then I can solve A".



* Bardet, Otmani, Saeed 2019.

Last overview

Notation $A \to B$ means "if I can solve B, then I can solve A".



In practice,

- Permutation equivalence is most of the times easy to solve;
- Monomial equivalence is hard over $\mathbb{F}_q$ as soon as $q \geqslant 5$.

* Bardet, Otmani, Saeed 2019.

Practical hardness

Best known algorithm Sendrier's *Support Splitting Algorithm*.

- **Permutation equivalence problem**
  - Heuristic complexity in $O(n^3 + 2^{\dim \mathscr{C} \cap \mathscr{C}^\perp} n^2 \log n)$.
  - Efficient since $\mathscr{C} \cap \mathscr{C}^\perp$ is typically small.
  - Nightmare for self–dual codes or codes like Reed–Muller codes.
- **Monomial equivalence problem**
  - still works when $q = 3, 4$;
  - No practical algorithm when $q \geqslant 5$.

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 2

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 3

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*

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

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

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 3

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 3 (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* $\boldsymbol{P} \in \mathrm{GL}_m(\mathbb{F}_q)$ *and* $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$ *such that*

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

Equivalence problems in rank metric (vector codes)

Problem 4 (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*

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

One could also consider:

Problem 5 (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*

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

Our results

Theorem 4

Equivalence problems of $\mathbb{F}_{q^m}$–linear codes are in $\mathcal{P}$ is q is polynomial in mn and in $\mathcal{ZPP}$ in the general case.

Theorem 5

The equivalence problem of matrix codes (REMC) is at least as hard as the monomial equivalence problem in Hamming metric: MEC reduces in polynomial time to REMC.

Right equivalence of matrix codes

REVC is solved if one can solve the following problem:

Problem 6 (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*

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

Definition 4

The conductor *of* $\mathscr{C}_1^{mat}$ *into* $\mathscr{C}_2^{mat}$ *is defined as:*

$$\mathrm{Cond}(\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}) \stackrel{def}{=} \{\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q) \mid \mathscr{C}_1^{mat}\boldsymbol{P} \subseteq \mathscr{C}_2^{mat}\}$$

Computing $\mathrm{Cond}(\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}})$ boils down to solve a linear system.

Right equivalence of matrix codes

REVC is solved if one can solve the following problem:

Problem 6 (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*

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

Definition 4

The conductor *of* $\mathscr{C}_1^{mat}$ *into* $\mathscr{C}_2^{mat}$ *is defined as:*

$$\mathrm{Cond}(\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}) \stackrel{def}{=} \{\boldsymbol{P} \in \mathcal{M}_n(\mathbb{F}_q) \mid \mathscr{C}_1^{mat}\boldsymbol{P} \subseteq \mathscr{C}_2^{mat}\}$$

Computing $\mathrm{Cond}(\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}})$ boils down to solve a linear system.
But, what if this space contains singular matrices? How to decide whether there is a nonsingular one in it?

The worst cases correspond to non trivial stabilizer algebras

Proposition 1

Let $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}$ be two codes such that $\mathscr{C}_1^{mat}\boldsymbol{Q} = \mathscr{C}_2^{mat}$ for some $\boldsymbol{Q} \in \mathrm{GL}_n(\mathbb{F}_q)$. If $\dim \mathrm{Cond}(\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}) > 1$, then $\mathrm{Stab}_R(\mathscr{C}_1^{mat})$ is non trivial.

Proof.

Take $\boldsymbol{M} \in \mathrm{Cond}(\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}}) \setminus \{\lambda \boldsymbol{Q} \mid \lambda \in \mathbb{F}_q\}$, then

$$\boldsymbol{M}\boldsymbol{Q}^{-1} \in \mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}}).$$

□

An easy case

Theorem 6

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.*

An easy case

Theorem 6

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. □

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 5 (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 7

$\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ *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 $\mathrm{C}\mathit{ond}(\mathscr{C}_1^{\mathrm{mat}}, \mathscr{C}_2^{\mathrm{mat}}) \setminus \mathrm{Rad}(\mathrm{Stab}_R(\mathscr{C}_1^{\mathrm{mat}}))$ 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

Back to $\mathbb{F}_{q^m}$–linear codes

The following problem is easy.

Problem (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*

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

What about this one?

Problem (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*

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

Recovering the hidden $\mathbb{F}_{q^m}$–linear structure

Fact

The left stabilizer algebras of $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}$ both contain a representation of $\mathbb{F}_{q^m}$.

If $\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}}) \simeq \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \simeq \mathbb{F}_{q^m}$, then we have to find

$$\boldsymbol{P} \in \mathsf{GL}_n(\mathbb{F}_q) \quad \text{such that} \quad \boldsymbol{P}^{-1}\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})\boldsymbol{P} = \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \tag{1}$$

Recovering the hidden $\mathbb{F}_{q^m}$–linear structure

Fact

The left stabilizer algebras of $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}$ both contain a representation of $\mathbb{F}_{q^m}$.

If $\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}}) \simeq \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \simeq \mathbb{F}_{q^m}$, then we have to find

$$\boldsymbol{P} \in \mathsf{GL}_n(\mathbb{F}_q) \quad \text{such that} \quad \boldsymbol{P}^{-1}\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})\boldsymbol{P} = \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \qquad (1)$$

Algorithm:

- find $\boldsymbol{A} \in \mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})$ (resp. $\boldsymbol{B} \in \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}})$) generating the algebra;

Recovering the hidden $\mathbb{F}_{q^m}$–linear structure

Fact

The left stabilizer algebras of $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}$ both contain a representation of $\mathbb{F}_{q^m}$.

If $\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}}) \simeq \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \simeq \mathbb{F}_{q^m}$, then we have to find

$$\boldsymbol{P} \in \mathsf{GL}_n(\mathbb{F}_q) \quad \text{such that} \quad \boldsymbol{P}^{-1}\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})\boldsymbol{P} = \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \qquad (1)$$

Algorithm:

- find $\boldsymbol{A} \in \mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})$ (resp. $\boldsymbol{B} \in \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}})$) generating the algebra;
- Compute the roots of $\chi_{\boldsymbol{B}}$ in $\mathbb{F}_q[X]/(\chi_{\boldsymbol{A}})$ and get $f \in \mathbb{F}_q[X]$ such that $f(\boldsymbol{A})$ is similar to $\boldsymbol{B}$.

Recovering the hidden $\mathbb{F}_{q^m}$–linear structure

Fact

The left stabilizer algebras of $\mathscr{C}_1^{mat}, \mathscr{C}_2^{mat}$ both contain a representation of $\mathbb{F}_{q^m}$.

If $\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}}) \simeq \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \simeq \mathbb{F}_{q^m}$, then we have to find

$$\boldsymbol{P} \in \mathsf{GL}_n(\mathbb{F}_q) \quad \text{such that} \quad \boldsymbol{P}^{-1}\mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})\boldsymbol{P} = \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}) \tag{1}$$

Algorithm:

- find $\boldsymbol{A} \in \mathsf{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})$ (resp. $\boldsymbol{B} \in \mathsf{Stab}_L(\mathscr{C}_2^{\mathrm{mat}})$) generating the algebra;
- Compute the roots of $\chi_{\boldsymbol{B}}$ in $\mathbb{F}_q[X]/(\chi_{\boldsymbol{A}})$ and get $f \in \mathbb{F}_q[X]$ such that $f(\boldsymbol{A})$ is similar to $\boldsymbol{B}$.
- Compute $\boldsymbol{P} \in \mathsf{GL}_n(\mathbb{F}_q)$ such that $\boldsymbol{P}^{-1}(\boldsymbol{A})\boldsymbol{P} = \boldsymbol{B}$, it satisfies (1).

What is the stabilizer algebra is larger?

Proposition 2

Let $\mathcal{A} \subseteq \mathcal{M}_m(\mathbb{F}_q)$ strictly containing a representation of $\mathbb{F}_{q^m}$. Then there exists $a|m$ such that $\mathcal{A}$ is isomorphic to $\mathcal{M}_{m/a}(\mathbb{F}_{q^a})$. In particular, if m is prime, then $\mathcal{A} = \mathcal{M}_m(\mathbb{F}_q)$.

Sketch of proof.

One proves that such an algebra is simple and that its centre is a subfield of $\mathbb{F}_{q^m}$. Over finite fields, central simple algebras are either fields or matrix algebras. □

What is the stabilizer algebra is larger?

Proposition 2

Let $\mathcal{A} \subseteq \mathcal{M}_m(\mathbb{F}_q)$ strictly containing a representation of $\mathbb{F}_{q^m}$. Then there exists $a|m$ such that $\mathcal{A}$ is isomorphic to $\mathcal{M}_{m/a}(\mathbb{F}_{q^a})$. In particular, if m is prime, then $\mathcal{A} = \mathcal{M}_m(\mathbb{F}_q)$.

Sketch of proof.

One proves that such an algebra is simple and that its centre is a subfield of $\mathbb{F}_{q^m}$. Over finite fields, central simple algebras are either fields or matrix algebras. □

Fact 1

In this situation, the conjugation problem is solvable

Solving the problem with hidden $\mathbb{F}_{q^m}$–linear structure

1. Compute $\boldsymbol{P} \in \mathrm{GL}_m(\mathbb{F}_q)$ such that

$$\boldsymbol{P}^{-1}\mathrm{Stab}_L(\mathscr{C}_1^{\mathrm{mat}})\boldsymbol{P} = \mathrm{Stab}_L(\mathscr{C}_2^{\mathrm{mat}}).$$

2. Search for $\boldsymbol{Q}$ such that

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

Here $\boldsymbol{P}$ is already known! Hence, hiding the $\mathbb{F}_{q^m}$–linear structure does not increase the hardness.

Remark

Actually, what precedes is true up to a Frobenius action, which make the situation slightly more complicated.

1. In Hamming metric
2. In rank metric
3. Equivalence of $\mathbb{F}_{q^m}$–linear codes is easy
4. General equivalence is hard

The general problem

Theorem 8

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 $\boldsymbol{S} \in \mathrm{GL}_k(\mathbb{F}_q)$ 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 $\boldsymbol{S} \in \mathrm{GL}_k(\mathbb{F}_q)$ 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

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

Sketch of proof of the reduction

$$G_1 = \left(c_1^\top \,\middle|\, c_2^\top \,\middle|\, \cdots \,\middle|\, c_n^\top \right), \quad G_2 = \left(d_1^\top \,\middle|\, d_2^\top \,\middle|\, \cdots \,\middle|\, d_n^\top \right)$$

We look for $\boldsymbol{S} \in \mathrm{GL}_k(\mathbb{F}_q)$ 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

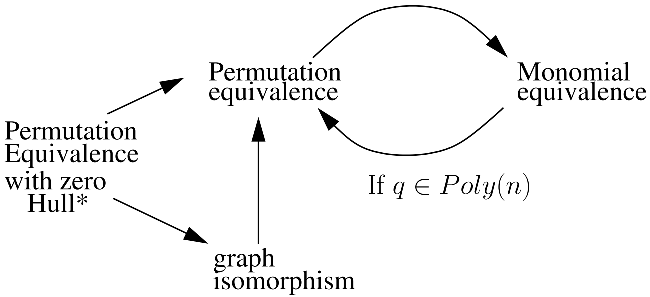
Remark

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:*

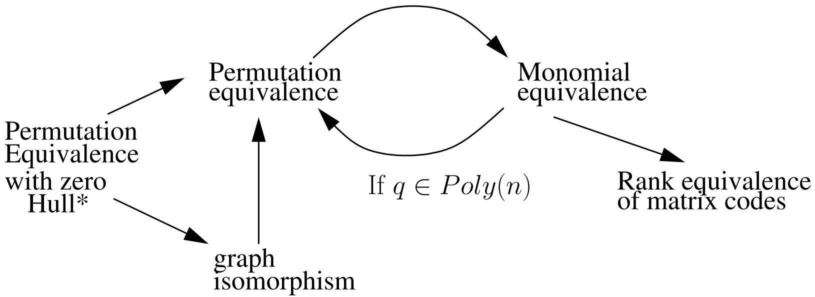
$$\mathscr{C}_1^{mat} \stackrel{def}{=} \mathrm{Span}\left\{ \begin{pmatrix} \boldsymbol{c}_i^\top \cdot \boldsymbol{c}_i \\ \boldsymbol{M}_i \end{pmatrix} \right\},$$

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
  - Left/right equivalence is easy to solve in the worst case.

Conclusion

- In Hamming metric
  - permutation equivalence is "most of the times" easy to solve;
  - monomimal equivalence is hard to solve.
- In rank metric
  - Left/right equivalence is easy to solve in the worst case.
  - Equivalence of $\mathbb{F}_{q^m}$–linear codes is also easy in the worst case, 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
  - Left/right equivalence is easy to solve in the worst case.
  - Equivalence of $\mathbb{F}_{q^m}$–linear codes is also easy in the worst case, 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.

Conclusion

- In Hamming metric
  - permutation equivalence is "most of the times" easy to solve;
  - monomimal equivalence is hard to solve.
- In rank metric
  - Left/right equivalence is easy to solve in the worst case.
  - Equivalence of $\mathbb{F}_{q^m}$–linear codes is also easy in the worst case, 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.
- **Open questions**
  - What about characteristic zero?
  - Is it possible to use the reduction to get a new algorithm to decide monomial equivalence in Hamming metric?