Permutation Code Equivalence Problem

Magali Bardet   Ayoub Otmani   Mohamed Saeed-Taha

University of Rouen Normandie – LITIS

Terminology and Notation

- $\mathbb{F}$ finite field
- $\mathbf{G}_U$ generator matrix and $\mathbf{H}_U$ parity check matrix of $U \subset \mathbb{F}^n$
- $\mathcal{H}(U) \triangleq U \cap U^{\perp}$ (**Hull**)

Code Isomorphism (Decision)

Given two **linear** *codes $A \subsetneq \mathbb{F}^n$ and $B \subsetneq \mathbb{F}^n$, is there an* **isometry** *of $\mathbb{F}^n$ that sends A in B ?*

Open Questions

- Theoretical complexity
- Algorithm design
- Practical difficulty

Motivations

- Classification of codes
- Security of some cryptographic primitives (McEliece cryptosystem and alike)

Isometries of the Hamming Space $\mathbb{F}^n$

- **Permutations** $\sigma \in \mathfrak{S}_n$

$$(u_1, \ldots, u_n) \mapsto (u_{\sigma^{-1}(1)}, \ldots, u_{\sigma^{-1}(n)})$$

- **Monomial (diagonal) transformations**

$$(u_1, \ldots, u_n) \mapsto (\lambda_1 u_1, \ldots, \lambda_n u_n) \quad \text{with} \quad \forall i, \quad \lambda_i \neq 0$$

- **Frobenius action** $\zeta(x) = x^p$ when $\mathbb{F} = \mathbb{F}_{p^m}$

$$(u_1, \ldots, u_n) \mapsto (\zeta^i(u_1), \ldots, \zeta^i(u_n))$$

Permutation Code Equivalence (PCE)

Given two **linear** *codes $A \subsetneq \mathbb{F}^n$ and $B \subsetneq \mathbb{F}^n$, is there a* **permutation** *of $\mathbb{F}^n$ that sends A in B ?*

What is known about PCE?

- **Theoretical complexity** (Petrank-Roth '97)
  - PCE is **not** NP-Complete
  - Graph Isomorphism (GI) **is easier than** PCE
- **Algorithm design**
  - Leon's algorithm (Magma). Low weight enumeration
    $\rightsquigarrow$ Exponential in the dimension
  - Sendrier's algorithm. Weight enumerator of $U \cap U^{\perp}$
    $\rightsquigarrow$ Exponential in the dimension of $U \cap U^{\perp}$
  - Quadratic system (Saeed-Taha)
- **Practical difficulty**
  - PCE is **easy** for **random** linear codes (Sendrier's algorithm)
  - In general, **unknown?**

Codes with trivial hulls

- $\mathcal{H}(U)^{\perp} = \left(U \cap U^{\perp}\right)^{\perp} = U + U^{\perp}$

$$\rightsquigarrow \mathbf{H}_{\mathcal{H}(U)} = \begin{bmatrix} \mathbf{G}_U \\ \mathbf{H}_U \end{bmatrix}$$

- $\mathcal{H}(U) = \{\mathbf{0}\}$ if and only if $\mathbb{F}^N = U \oplus U^{\perp}$

$$\forall v \in \mathbb{F}^N, \quad \mathbf{v} = \mathbf{v}_U + \mathbf{v}_{U^{\perp}} \quad \text{with} \quad \begin{cases} \mathbf{v}_U \in U \\ \mathbf{v}_{U^{\perp}} \in U^{\perp} \end{cases}$$

Proposition

$\mathcal{H}(U) = \{\mathbf{0}\}$ *if and only if* $\mathbf{H}_{\mathcal{H}(U)}$ *is* **invertible**

Codes with trivial hulls

Proposition

$\mathcal{H}(U) = \{\mathbf{0}\}$ *if and only if* $\mathbf{G}_U\mathbf{G}_U^T$ *and* $\mathbf{H}_U\mathbf{H}_U^T$ *are invertible and*

$$\mathbf{H}_{\mathcal{H}(U)}^{-1} = \left[\mathbf{G}_U^T\left(\mathbf{G}_U\mathbf{G}_U^T\right)^{-1} \quad \mathbf{H}_U^T\left(\mathbf{H}_U\mathbf{H}_U^T\right)^{-1}\right]$$

Codes with trivial hulls

Assume $\mathcal{H}(U) = \{\mathbf{0}\}$

$$\begin{cases} \mathbf{\Sigma}_U & \triangleq & \mathbf{G}_U^T\left(\mathbf{G}_U\mathbf{G}_U^T\right)^{-1}\mathbf{G}_U \\ \\ \mathbf{\Sigma}_{U^\perp} & \triangleq & \mathbf{H}_U^T\left(\mathbf{H}_U\mathbf{H}_U^T\right)^{-1}\mathbf{H}_U \end{cases}$$

Proposition

$$\forall \mathbf{v} \in \mathbb{F}^N, \quad \mathbf{v}_U \triangleq \mathbf{v}\,\mathbf{\Sigma}_U \qquad \textit{and} \qquad \mathbf{v}_{U^\perp} \triangleq \mathbf{v}\,\mathbf{\Sigma}_{U^\perp}.$$

Codes with trivial hulls

When $U \cap U^{\perp} = \{\mathbf{0}\}$

1. $\mathbf{\Sigma}_U$ generates U ($\mathbf{\Sigma}_U^{\perp}$ generates $U^{\perp}$)
2. $\mathbf{\Sigma}_U^T = \mathbf{\Sigma}_U$
3. $\mathbf{\Sigma}_U^2 = \mathbf{\Sigma}_U$
4. $\mathbf{\Sigma}_U \mathbf{\Sigma}_{U^{\perp}} = \mathbf{0}$ and $\mathbf{\Sigma}_{U^{\perp}} \mathbf{\Sigma}_U = \mathbf{0}$
5. $\mathbf{\Sigma}_U + \mathbf{\Sigma}_{U^{\perp}} = \mathbf{I}_N$

A New Invariant

Proposition

$\mathbf{\Sigma}_U$ and $\mathbf{\Sigma}_{U^\perp}$ are **invariants** *of U and $U^\perp$*

Proof.

Assume that $\mathbf{D} = \mathbf{SG}$ where $\mathbf{S}$ is an invertible matrix

$$\begin{aligned}
\mathbf{D}^T\left(\mathbf{D}\mathbf{D}^T\right)^{-1}\mathbf{D} &= (\mathbf{SG})^T\left(\mathbf{SG}(\mathbf{SG})^T\right)^{-1}\mathbf{SG} \\
&= \mathbf{G}^T(\mathbf{S}^{-1}\mathbf{S})^T\left(\mathbf{G}\mathbf{G}^T\right)^{-1}(\mathbf{S}^{-1}\mathbf{S})\mathbf{G} \\
&= \mathbf{G}^T\left(\mathbf{G}\mathbf{G}^T\right)^{-1}\mathbf{G}
\end{aligned}$$

□

Graph Associated to a Code

- Assume that U has a trivial hull
- Then let us interpret $\mathbf{\Sigma}_U$ as the **adjacency** matrix of **weighted graph**
- The graph $\mathcal{G}(U)$ associated to U is the graph defined by $\mathbf{\Sigma}_U$

Codes with trivial hull

- For any permutation $\mathbf{X}$

$$\begin{aligned}\mathbf{I}_N = \mathbf{X}^T\mathbf{X} &= \mathbf{X}^T\left(\boldsymbol{\Sigma}_U + \boldsymbol{\Sigma}_{U^\perp}\right)\mathbf{X} \\ &= \mathbf{X}^T\boldsymbol{\Sigma}_U\mathbf{X} + \mathbf{X}^T\boldsymbol{\Sigma}_{U^\perp}\mathbf{X}\end{aligned}$$

- In particular if $B = A\mathbf{X}$ then

$$\boldsymbol{\Sigma}_B \triangleq \mathbf{X}^T\boldsymbol{\Sigma}_A\mathbf{X} \quad \text{and} \quad \boldsymbol{\Sigma}_{B^\perp} \triangleq \mathbf{X}^T\boldsymbol{\Sigma}_A^\perp\mathbf{X}$$

Codes with trivial hulls

Theorem

Assume that A and B have **trivial** *hulls.*

Then A and B are **permutation equivalent** *if and only if both*

- $\mathcal{G}(A)$ *and* $\mathcal{G}(B)$ *are* **isomorphic** *($\mathbf{\Sigma}_B = \mathbf{X}^T \mathbf{\Sigma}_A \mathbf{X}$)*
- $\mathcal{G}(A^\perp)$ *and* $\mathcal{G}(B^\perp)$ *are* **isomorphic** *($\mathbf{\Sigma}_{B^\perp} = \mathbf{X}^T \mathbf{\Sigma}_A^\perp \mathbf{X}$)*

Codes with Non-Trivial Hull

Definition (Shortened code)

$$\mathbf{u} \in \mathcal{S}_{\mathcal{I}}(U) \text{ if and only if } (\mathbf{u} \in U \text{ and } \forall i \in \mathcal{I}, \;\; u_i = 0)$$

Proposition

$\mathcal{S}_{\mathcal{I}}(U)$ has a trivial hull when $\mathcal{I}$ is an information set for $\mathcal{H}(U)$

Codes with Non-Trivial Hulls

Proposition

- $B = A\mathbf{X}$
- $\mathcal{I} \subset [1, n]$
- $\mathcal{J} \triangleq \mathbf{X}(\mathcal{I})$

Then $\mathcal{S}_{\mathcal{J}}(B)$ *and* $\mathcal{S}_{\mathcal{I}}(A)$ *are permutation equivalent with*

$$\mathcal{S}_{\mathcal{J}}(B) = \mathcal{S}_{\mathcal{I}}(A)\,\mathbf{X}$$

PCE for Codes with Non-Trivial Hulls

Theorem

PCE can be solved in $O\left(hn^{\omega+h+1}\mathsf{GI}(n)\right)$ *time where*

- $h =$ *Dimension of the hull*
- $\omega =$ *Exponent of matrix multiplication* $(2 \leqslant \omega < 3)$.
- $\mathsf{GI}(n) =$ *Time complexity for testing if two weighted graphs with* n *vertices are isomorphic*

Conclusion and Open Questions

- PCE **is not harder than** GI for codes with **trivial hulls**
- Generalizing the reduction to codes with **non trivial hulls**
- Treating the **diagonal** equivalence