A New Approach for Solving the Permutation Code Equivalence Problem

JNCF 2018

Magali Bardet, Ayoub Otmani, Mohamed Saeed-Taha

Laboratoire LITIS - Université de Rouen
University of Khartoum, Sudan

22 janvier 2018

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.
- Matrice génératrice $G_{\mathscr{C}} \in \mathscr{M}_{k,n}(\mathbb{F})$.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.
- Matrice génératrice $G_{\mathscr{C}} \in \mathscr{M}_{k,n}(\mathbb{F})$.
- Matrice de parité $H_{\mathscr{C}} \in \mathscr{M}_{n-k,n}(\mathbb{F})$.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.
- Matrice génératrice $G_{\mathscr{C}} \in \mathscr{M}_{k,n}(\mathbb{F})$.
- Matrice de parité $H_{\mathscr{C}} \in \mathscr{M}_{n-k,n}(\mathbb{F})$.
- Relations $G_{\mathscr{C}} \cdot H_{\mathscr{C}}^T = \mathbf{0}_{k,n-k}$.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.
- Matrice génératrice $G_{\mathscr{C}} \in \mathscr{M}_{k,n}(\mathbb{F})$.
- Matrice de parité $H_{\mathscr{C}} \in \mathscr{M}_{n-k,n}(\mathbb{F})$.
- Relations $G_{\mathscr{C}} \cdot H_{\mathscr{C}}^T = \mathbf{0}_{k,n-k}$.
- $H_{\mathscr{C}}$ est la matrice génératrice du code dual $\mathscr{C}^\perp = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{x} \cdot G_{\mathscr{C}}^T = \mathbf{0}_{1,k}\}$.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.
- Matrice génératrice $G_{\mathscr{C}} \in \mathscr{M}_{k,n}(\mathbb{F})$.
- Matrice de parité $H_{\mathscr{C}} \in \mathscr{M}_{n-k,n}(\mathbb{F})$.
- Relations $G_{\mathscr{C}} \cdot H_{\mathscr{C}}^T = \mathbf{0}_{k,n-k}$.
- $H_{\mathscr{C}}$ est la matrice génératrice du code dual $\mathscr{C}^\perp = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{x} \cdot G_{\mathscr{C}}^T = \mathbf{0}_{1,k}\}$.
- Le *hull* de $\mathscr{C}$ est $\mathscr{H}(\mathscr{C}) = \mathscr{C} \cap \mathscr{C}^\perp$, matrice génératrice $\begin{bmatrix} G_{\mathscr{C}} \\ H_{\mathscr{C}} \end{bmatrix}$.

Notations

- $\mathbb{F}$ est un corps, $\mathbb{F}_q$ le corps fini à q éléments.
- Un *code linéaire* $\mathscr{C}[n,k]$ est un sev de $\mathbb{F}^n$ de dimension k.
- Matrice génératrice $G_{\mathscr{C}} \in \mathscr{M}_{k,n}(\mathbb{F})$.
- Matrice de parité $H_{\mathscr{C}} \in \mathscr{M}_{n-k,n}(\mathbb{F})$.
- Relations $G_{\mathscr{C}} \cdot H_{\mathscr{C}}^T = \mathbf{0}_{k,n-k}$.
- $H_{\mathscr{C}}$ est la matrice génératrice du code dual $\mathscr{C}^\perp = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{x} \cdot G_{\mathscr{C}}^T = \mathbf{0}_{1,k}\}$.
- Le *hull* de $\mathscr{C}$ est $\mathscr{H}(\mathscr{C}) = \mathscr{C} \cap \mathscr{C}^\perp$, matrice génératrice $\begin{bmatrix} G_{\mathscr{C}} \\ H_{\mathscr{C}} \end{bmatrix}$.
- Distance de Hamming : nombre de coordonnées $\neq$.

Équivalence linéaire de codes

Codes linéairement équivalents

Deux codes $\mathscr{A}$ et $\mathscr{B}$ sont linéairements équivalents s'il existe un isomorphisme $\psi : \mathscr{A} \to \mathscr{B}$ préservant la distance de Hamming, noté $\mathscr{B} = \mathscr{A}^{\psi}$.

Équivalence linéaire de codes

Codes linéairement équivalents

Deux codes $\mathscr{A}$ et $\mathscr{B}$ sont linéairements équivalents s'il existe un isomorphisme $\psi : \mathscr{A} \to \mathscr{B}$ préservant la distance de Hamming, noté $\mathscr{B} = \mathscr{A}^{\psi}$.

Équivalence linéaire ou diagonale, MacWilliams 61

Deux codes $\mathscr{A}$ et $\mathscr{B}$ sont linéairements équivalents s'il existe une matrice de permutation P et une matrice diagonale D telles que

$$G_A \cdot P \cdot D$$

est une matrice génératrice de $\mathscr{B}$ si G_A est une matrice génératrice de $\mathscr{B}$.

Équivalence linéaire de codes

Codes linéairement équivalents

Deux codes $\mathscr{A}$ et $\mathscr{B}$ sont linéairements équivalents s'il existe un isomorphisme $\psi : \mathscr{A} \to \mathscr{B}$ préservant la distance de Hamming, noté $\mathscr{B} = \mathscr{A}^{\psi}$.

Équivalence linéaire ou diagonale, MacWilliams 61

Deux codes $\mathscr{A}$ et $\mathscr{B}$ sont linéairements équivalents s'il existe une matrice de permutation P et une matrice diagonale D telles que

$$G_A \cdot P \cdot D$$

est une matrice génératrice de $\mathscr{B}$ si G_A est une matrice génératrice de $\mathscr{B}$.

Groupe d'automorphisme linéaire

$Aut(\mathscr{C}) = \{\psi : \mathscr{C} = \mathscr{C}^{\psi}\}$.

Équivalence de codes par permutations

Permutational Code Equivalence Problem

Un code linéaire $\mathscr{A}$ est équivalent par permutation à un code $\mathscr{B}$ s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\mathscr{B} = \mathscr{A}^{\sigma}$.

Équivalence de codes par permutations

Permutational Code Equivalence Problem

Un code linéaire $\mathscr{A}$ est équivalent par permutation à un code $\mathscr{B}$ s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\mathscr{B} = \mathscr{A}^\sigma$.

Groupe des permutations

Le groupe des permutations d'un code $\mathscr{A}$ est $\Pi(\mathscr{A}) = \{\sigma \in \mathfrak{S}_n : \mathscr{A}^\sigma = \mathscr{A}\}$.

Équivalence de codes par permutations

Permutational Code Equivalence Problem

Un code linéaire $\mathscr{A}$ est équivalent par permutation à un code $\mathscr{B}$ s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\mathscr{B} = \mathscr{A}^\sigma$.

Groupe des permutations

Le groupe des permutations d'un code $\mathscr{A}$ est $\Pi(\mathscr{A}) = \{\sigma \in \mathfrak{S}_n : \mathscr{A}^\sigma = \mathscr{A}\}$.

Cas binaire $\mathbb{F} = \mathbb{F}_2$

Les isométries sont les permutations.

Équivalence de codes par permutations

Permutational Code Equivalence Problem

Un code linéaire $\mathscr{A}$ est équivalent par permutation à un code $\mathscr{B}$ s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\mathscr{B} = \mathscr{A}^\sigma$.

Groupe des permutations

Le groupe des permutations d'un code $\mathscr{A}$ est $\Pi(\mathscr{A}) = \{\sigma \in \mathfrak{S}_n : \mathscr{A}^\sigma = \mathscr{A}\}$.

Cas binaire $\mathbb{F} = \mathbb{F}_2$

Les isométries sont les permutations.

Applications

- Cryptographie (cryptosystèmes de type McEliece par ex.),
- Classification des codes (mêmes paramètres).

Problèmes décisionnels

PEP (Permutation Equivalence Problem)

Problème de décision de l'équivalence de codes par permutation.

DEP (Diagonal Equivalence Problem)

Problème de décision de l'équivalence linéaire de code.

Problèmes décisionnels

PEP (Permutation Equivalence Problem)

Problème de décision de l'équivalence de codes par permutation.

DEP (Diagonal Equivalence Problem)

Problème de décision de l'équivalence linéaire de code.

Deux graphes $\mathscr{G} = ([1,n], E_{\mathscr{G}})$ et $\mathscr{H} = ([1,n], E_{\mathscr{H}})$ sont isomorphes s'il existe une permutation σ des sommets tq $(i,j) \in E_{\mathscr{G}} \iff (\sigma(i), \sigma(j)) \in E_{\mathscr{H}}$.

GI (Graph Isomorphism)

Problème de décision de l'équivalence de graphes.

Historique

Autour de PEP / DEP / GI

- Leon 82 : algorithme de calcul de $Aut(\mathscr{C})$, en cherchant les mots de petit poids.
- Petrank and Roth 97 : réduction de GI à PEP en temps polynomial, et PEP n'est pas NP-complet si P$\neq$NP.
- Support Splitting Algorithm (SSA) de Sendrier 99 : résout PEP pour des codes de petit hull et groupe de permutation trivial. Complexité heuristique en $O(n^3 + q^h n^2 \log n)$.
- Sendrier Simos 2013 : réduction de DEP à PEP via la clôture d'un code, de paramètres $[n(q-1), k]$, hull de dimension $\tilde{h} = h$ si $q = 3$ et k si $q \geq 4$.
- Babai, arXiv 2017 : la complexité de GI est quasi-polynomiale en le nombre de sommets, $\exp(\log(n)^{O(1)})$.

Modélisation algébrique de PEP

$\mathscr{A}, \mathscr{B}$ deux codes de paramètres $[n, k]$, et

- h la dimension des hulls,
- $G_{\mathscr{A}}, G_{\mathscr{B}}$ des matrices génératrices,
- $H_{\mathscr{A}}, H_{\mathscr{B}}$ des matrices de parité.

$\mathscr{A}$ et $\mathscr{B}$ sont équivalents par permutation ssi $\exists$ une matrice de permutation P vérifiant l'une des conditions :

1. $G_{\mathscr{A}} \cdot P$ est une matrice génératrice de $\mathscr{B}$.

Modélisation algébrique de PEP

$\mathscr{A}, \mathscr{B}$ deux codes de paramètres $[n, k]$, et

- h la dimension des hulls,
- $G_{\mathscr{A}}, G_{\mathscr{B}}$ des matrices génératrices,
- $H_{\mathscr{A}}, H_{\mathscr{B}}$ des matrices de parité.

$\mathscr{A}$ et $\mathscr{B}$ sont équivalents par permutation ssi $\exists$ une matrice de permutation P vérifiant l'une des conditions :

1. $G_{\mathscr{A}} \cdot P$ est une matrice génératrice de $\mathscr{B}$.
2. $\exists$ une matrice inversible S telles que $G_{\mathscr{B}} = S \cdot G_{\mathscr{A}} \cdot P$.

Modélisation algébrique de PEP

$\mathscr{A}, \mathscr{B}$ deux codes de paramètres $[n, k]$, et

- h la dimension des hulls,
- $G_{\mathscr{A}}, G_{\mathscr{B}}$ des matrices génératrices,
- $H_{\mathscr{A}}, H_{\mathscr{B}}$ des matrices de parité.

$\mathscr{A}$ et $\mathscr{B}$ sont équivalents par permutation ssi $\exists$ une matrice de permutation P vérifiant l'une des conditions :

1. $G_{\mathscr{A}} \cdot P$ est une matrice génératrice de $\mathscr{B}$.
2. $\exists$ une matrice inversible S telles que $G_{\mathscr{B}} = S \cdot G_{\mathscr{A}} \cdot P$.
3. $$G_{\mathscr{A}} \cdot P \cdot {H_{\mathscr{B}}}^T = \mathbf{0}_{k,n-k}.$$

Modélisation algébrique de PEP

$\mathscr{A}, \mathscr{B}$ deux codes de paramètres $[n, k]$, et

- h la dimension des hulls,
- $G_{\mathscr{A}}, G_{\mathscr{B}}$ des matrices génératrices,
- $H_{\mathscr{A}}, H_{\mathscr{B}}$ des matrices de parité.

$\mathscr{A}$ et $\mathscr{B}$ sont équivalents par permutation ssi $\exists$ une matrice de permutation P vérifiant l'une des conditions :

1. $G_{\mathscr{A}} \cdot P$ est une matrice génératrice de $\mathscr{B}$.
2. $\exists$ une matrice inversible S telles que $G_{\mathscr{B}} = S \cdot G_{\mathscr{A}} \cdot P$.
3. $$G_{\mathscr{A}} \cdot P \cdot {H_{\mathscr{B}}}^T = \mathbf{0}_{k,n-k}.$$
4. $$H_{\mathscr{A}} \cdot P \cdot {G_{\mathscr{B}}}^T = \mathbf{0}_{n-k,k}.$$

Caractérisation algébrique de PEP - système réduit

Proposition

$$\mathfrak{S}_{min} : \begin{cases} G_{\mathscr{A}} \cdot X \cdot H_{\mathscr{B}}^T &= \mathbf{0}_{k,n-k} \\ X \cdot \mathbb{1}_n^T &= \mathbb{1}_n^T \\ x_{i,j} x_{i',j} &= 0, \qquad 1 \leq i \neq i', j \leq n \end{cases}$$

Théorème

Les permutations solutions du PEP entre les codes $\mathscr{A}$ et $\mathscr{B}$ sont exactement les solutions de $\mathfrak{S}_{min}$ et $\langle \mathfrak{S}_{min} \rangle$ est radical (il contient ${x_{i,j}}^2 - x_{i,j}$ pour tout $x_{i,j}$).

Mais...

Équations linéaires

$$\mathfrak{E} : \begin{cases} G_{\mathscr{A}} \cdot X \cdot H_{\mathscr{B}}^T &= \mathbf{0}_{k,n-k} \\ H_{\mathscr{A}} \cdot X \cdot G_{\mathscr{B}}^T &= \mathbf{0}_{n-k,k} \end{cases}$$

$$\mathfrak{L} : \begin{cases} \mathbb{1}_n^T \cdot X &= \mathbb{1}_n^T \\ X \cdot \mathbb{1}_n &= \mathbb{1}_n \end{cases}$$

Alors $\mathfrak{E} \cup \mathfrak{L} \subset \langle \mathfrak{S}_{min} \rangle$ et $\mathtt{rank}(\mathfrak{E}) = 2k(n-k) - h^2$, $\mathtt{rank}(\mathfrak{L}) = 2n - 1$.

Mais...

Équations linéaires

$$\mathfrak{E} : \begin{cases} G_{\mathscr{A}} \cdot X \cdot H_{\mathscr{B}}^T &= \mathbf{0}_{k,n-k} \\ H_{\mathscr{A}} \cdot X \cdot G_{\mathscr{B}}^T &= \mathbf{0}_{n-k,k} \end{cases}$$

$$\mathfrak{L} : \begin{cases} \mathbb{1}_n^T \cdot X &= \mathbb{1}_n^T \\ X \cdot \mathbb{1}_n &= \mathbb{1}_n \end{cases}$$

Alors $\mathfrak{E} \cup \mathfrak{L} \subset \langle \mathfrak{S}_{min} \rangle$ et $\mathtt{rank}(\mathfrak{E}) = 2k(n-k) - h^2$, $\mathtt{rank}(\mathfrak{L}) = 2n-1$.

Proposition

$\mathtt{rank}(\mathfrak{E} \cup \mathfrak{L}) \leq 2k(n-k) - h^2 + 2n - 1$ (borne atteinte).
Pour $h = 0$,

$$\mathtt{rank}(\mathfrak{E} \cup \mathfrak{L}) \leq \begin{cases} 2k(n-k)+2k-1 & \text{if } \mathbb{1}_n \in \mathscr{C} \\ 2k(n-k)+2(n-k)-1 & \text{if } \mathbb{1}_n \in \mathscr{C}^\perp \\ 2k(n-k)+2n-2 & \text{if } \mathbb{1}_n \notin \mathscr{C}, \mathbb{1}_n \notin \mathscr{C}^\perp. \end{cases}$$

Caractérisation algébrique de PEP

Inconnues : $X = (x_{i,j})_{1 \leq i,j \leq n}$, $\mathbb{1}_n = (1, \ldots, 1) \in \mathbb{F}^n$.

$$
\mathfrak{S} : \begin{cases}
G_{\mathscr{A}} \cdot X \cdot H_{\mathscr{B}}^T &= \mathbf{0}_{k,n-k} & \\
H_{\mathscr{A}} \cdot X \cdot G_{\mathscr{B}}^T &= \mathbf{0}_{n-k,k} & \\
\mathbb{1}_n \cdot X &= \mathbb{1}_n & \\
X \cdot \mathbb{1}_n^T &= \mathbb{1}_n^T & \\
x_{i,j} x_{i',j} &= 0, & 1 \leq i \neq i', j \leq n \\
x_{i,j} x_{i,j'} &= 0, & 1 \leq i, j \neq j' \leq n \\
{x_{i,j}}^2 - x_{i,j} &= 0, & 1 \leq i \neq j \leq n
\end{cases}
$$

Caractérisation algébrique de PEP

Inconnues : $X = (x_{i,j})_{1 \leq i,j \leq n}$, $\mathbb{1}_n = (1, \ldots, 1) \in \mathbb{F}^n$.

$$\mathfrak{S} : \begin{cases} G_{\mathscr{A}} \cdot X \cdot H_{\mathscr{B}}^T &= \mathbf{0}_{k,n-k} \\ H_{\mathscr{A}} \cdot X \cdot G_{\mathscr{B}}^T &= \mathbf{0}_{n-k,k} \\ \mathbb{1}_n \cdot X &= \mathbb{1}_n \\ X \cdot \mathbb{1}_n^T &= \mathbb{1}_n^T \\ x_{i,j} x_{i',j} &= 0, \quad 1 \leq i \neq i', j \leq n \\ x_{i,j} x_{i,j'} &= 0, \quad 1 \leq i, j \neq j' \leq n \\ {x_{i,j}}^2 - x_{i,j} &= 0, \quad 1 \leq i \neq j \leq n \end{cases}$$

Caractéristiques, $R = k/n$

n^2 variables, de l'ordre de $2R(1-R)n^2$ équations linéaires et n^3 quadratiques.

Caractérisation algébrique de PEP

Inconnues : $X = (x_{i,j})_{1 \leq i,j \leq n}$, $\mathbb{1}_n = (1, \ldots, 1) \in \mathbb{F}^n$.

$$\mathfrak{S} : \begin{cases} G_{\mathscr{A}} \cdot X \cdot H_{\mathscr{B}}^T &= \mathbf{0}_{k,n-k} \\ H_{\mathscr{A}} \cdot X \cdot G_{\mathscr{B}}^T &= \mathbf{0}_{n-k,k} \\ \mathbb{1}_n \cdot X &= \mathbb{1}_n \\ X \cdot \mathbb{1}_n^T &= \mathbb{1}_n^T \\ x_{i,j} x_{i',j} &= 0, \quad 1 \leq i \neq i', j \leq n \\ x_{i,j} x_{i,j'} &= 0, \quad 1 \leq i, j \neq j' \leq n \\ {x_{i,j}}^2 - x_{i,j} &= 0, \quad 1 \leq i \neq j \leq n \end{cases}$$

Caractéristiques, $R = k/n$

n^2 variables, de l'ordre de $2R(1-R)n^2$ équations linéaires et n^3 quadratiques.

Calculs de bases de Gröbner : on peut calculer modulo l'idéal $I = \langle \{x_{i,j} x_{i',j}\}_{1 \leq i \neq i', j \leq n}, \{x_{i,j} x_{i,j'}\}_{1 \leq i, j \neq j' \leq n}, \{{x_{i,j}}^2 - x_{i,j}\}_{1 \leq i \neq j \leq n} \rangle$.

Cas particulier du hull trivial

Rappels sur le hull d'un code

- $\mathscr{H}(\mathscr{C}) = \mathscr{C} \cap \mathscr{C}^{\perp}$ et $\mathscr{H}(\mathscr{C})^{\perp} = \mathscr{C} + \mathscr{C}^{\perp}$.

Cas particulier du hull trivial

Rappels sur le hull d'un code

- $\mathscr{H}(\mathscr{C}) = \mathscr{C} \cap \mathscr{C}^{\perp}$ et $\mathscr{H}(\mathscr{C})^{\perp} = \mathscr{C} + \mathscr{C}^{\perp}$.
- $H_{\mathscr{H}(\mathscr{C})} = \begin{bmatrix} G_{\mathscr{C}} \\ H_{\mathscr{C}} \end{bmatrix}$.

Cas particulier du hull trivial

Rappels sur le hull d'un code

- $\mathscr{H}(\mathscr{C}) = \mathscr{C} \cap \mathscr{C}^{\perp}$ et $\mathscr{H}(\mathscr{C})^{\perp} = \mathscr{C} + \mathscr{C}^{\perp}$.
- $H_{\mathscr{H}(\mathscr{C})} = \begin{bmatrix} G_{\mathscr{C}} \\ H_{\mathscr{C}} \end{bmatrix}$.
- $\mathscr{H}(\mathscr{C}) = \{0\}$ ssi $H_{\mathscr{H}(\mathscr{C})}$ est inversible, et

$$H^{-1}_{\mathscr{H}(\mathscr{C})} = \begin{bmatrix} G_{\mathscr{C}}^T \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T \right)^{-1} & H_{\mathscr{C}}^T \left(H_{\mathscr{C}} \cdot H_{\mathscr{C}}^T \right)^{-1} \end{bmatrix}$$

Cas particulier du hull trivial

Rappels sur le hull d'un code

- $\mathscr{H}(\mathscr{C}) = \mathscr{C} \cap \mathscr{C}^{\perp}$ et $\mathscr{H}(\mathscr{C})^{\perp} = \mathscr{C} + \mathscr{C}^{\perp}$.
- $H_{\mathscr{H}(\mathscr{C})} = \begin{bmatrix} G_{\mathscr{C}} \\ H_{\mathscr{C}} \end{bmatrix}$.
- $\mathscr{H}(\mathscr{C}) = \{0\}$ ssi $H_{\mathscr{H}(\mathscr{C})}$ est inversible, et

$$H^{-1}_{\mathscr{H}(\mathscr{C})} = \begin{bmatrix} G_{\mathscr{C}}^T \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T \right)^{-1} & H_{\mathscr{C}}^T \left(H_{\mathscr{C}} \cdot H_{\mathscr{C}}^T \right)^{-1} \end{bmatrix}$$

- Si $\mathscr{H}(\mathscr{C}) = \{0\}$,
  $I_n = G_{\mathscr{C}}^T \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T \right)^{-1} \cdot G_{\mathscr{C}} + H_{\mathscr{C}}^T \left(H_{\mathscr{C}} \cdot H_{\mathscr{C}}^T \right)^{-1} \cdot H_{\mathscr{C}} = \Sigma_{\mathscr{C}} + \Sigma_{\mathscr{C}^{\perp}}$
  et pour tout $v \in \mathbb{F}^n$,

$$v = v_{\mathscr{C}} + v_{\mathscr{C}^{\perp}}$$

  où $v_{\mathscr{C}} = v \cdot \Sigma_{\mathscr{C}} \in \mathscr{C}$ et $v_{\mathscr{C}^{\perp}} = v \cdot \Sigma_{\mathscr{C}^{\perp}} \in \mathscr{C}^{\perp}$.

Modélisation algébrique quand $h = 0$

Proposition

Si $\mathscr{H}(\mathscr{A}) = \mathscr{H}(\mathscr{B}) = \{0\}$, alors

$$\begin{aligned} \mathbb{1}_n &= \mathbb{1}_{\mathscr{A}} + \mathbb{1}_{\mathscr{A}^\perp} \in \mathscr{A} + \mathscr{A}^\perp \\ \mathbb{1}_n &= \mathbb{1}_{\mathscr{B}} + \mathbb{1}_{\mathscr{B}^\perp} \in \mathscr{B} + \mathscr{B}^\perp \end{aligned}$$

donc $\{\mathbb{1}_{\mathscr{A}} \cdot X - \mathbb{1}_{\mathscr{B}}, \mathbb{1}_{\mathscr{A}^\perp} \cdot X - \mathbb{1}_{\mathscr{B}^\perp}\} \in \langle \mathfrak{S} \rangle$.

Modélisation algébrique quand $h = 0$

Proposition

Si $\mathscr{H}(\mathscr{A}) = \mathscr{H}(\mathscr{B}) = \{0\}$, alors

$$\begin{aligned} \mathbb{1}_n &= \mathbb{1}_{\mathscr{A}} + \mathbb{1}_{\mathscr{A}^\perp} \in \mathscr{A} + \mathscr{A}^\perp \\ \mathbb{1}_n &= \mathbb{1}_{\mathscr{B}} + \mathbb{1}_{\mathscr{B}^\perp} \in \mathscr{B} + \mathscr{B}^\perp \end{aligned}$$

donc $\{\mathbb{1}_{\mathscr{A}} \cdot X - \mathbb{1}_{\mathscr{B}}, \mathbb{1}_{\mathscr{A}^\perp} \cdot X - \mathbb{1}_{\mathscr{B}^\perp}\} \in \langle \mathfrak{S} \rangle$.

Preuve

Pour toute permutation P entre $\mathscr{A}$ et $\mathscr{B}$, $\mathbb{1}_n \cdot P = \mathbb{1}_n$ donc

$$\begin{aligned} \mathbb{1}_{\mathscr{A}} \cdot P &= \mathbb{1}_{\mathscr{B}} \\ \mathbb{1}_{\mathscr{A}^\perp} \cdot P &= \mathbb{1}_{\mathscr{B}^\perp} \end{aligned}$$

et $\langle \mathfrak{S} \rangle$ est radical.

Équations de blocs

$\mathscr{H}(\mathscr{A}) = \{0\}$

La $j$ème équation de $\mathbb{1}_{\mathscr{A}} \cdot X - \mathbb{1}_{\mathscr{B}}$ ne dépend que de n variables $x_{i,j}$, $1 \leq i \leq n$.

Équations de blocs

$\mathscr{H}(\mathscr{A}) = \{0\}$

La $j$ème équation de $\mathbb{1}_{\mathscr{A}} \cdot X - \mathbb{1}_{\mathscr{B}}$ ne dépend que de n variables $x_{i,j}$, $1 \leq i \leq n$.

Si $\mathbb{1}_{\mathscr{A}} = (a_i)_{1 \leq i \leq n}$ et $\mathbb{1}_{\mathscr{B}} = (b_i)_{1 \leq i \leq n}$,

Le sous-système de $\mathfrak{S}$,
$$\begin{cases} \sum_{i=1}^{n} a_i x_{i,j} - b_j & \\ \sum_{i=1}^{n} x_{i,j} - 1 & \\ x_{i,j} x_{i',j} & 1 \leq i \neq i' \leq n \\ {x_{i,j}}^2 - x_{i,j}, & 1 \leq i \leq n \end{cases}$$
admet comme base de Gröbner
$$\begin{cases} \sum_{i \notin I_j}^{n} x_{i,j} - 1, & \\ x_{i,j}, & i \in I_j \\ x_{i,j} x_{i',j}, & 1 \leq i \neq i' \leq n, i, i' \notin I_j \\ {x_{i,j}}^2 - x_{i,j}, & i \notin I_j \end{cases} \quad \text{avec } I_j = \{i : a_i \neq b_j\}.$$

Caractérisation algébrique de PEP quand $h = 0$

Proposition

Lorsque $h = 0$, on peut ajouter à $\mathfrak{S}$ les équations

$$\{x_{i,j} = 0, (i,j) \in J\}$$

où $J = \{(i,j) : a_i \neq b_j\}$ avec $a = \mathbb{1}_n \cdot \Sigma_{\mathscr{A}}$ et $b = \mathbb{1}_n \cdot \Sigma_{\mathscr{B}}$.
$(\Sigma_{\mathscr{C}} = G_{\mathscr{C}}^T \cdot \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T\right)^{-1} G_{\mathscr{C}}.)$

Caractérisation algébrique de PEP quand $h = 0$

Proposition

Lorsque $h = 0$, on peut ajouter à $\mathfrak{S}$ les équations

$$\{x_{i,j} = 0, (i,j) \in J\}$$

où $J = \{(i,j) : a_i \neq b_j\}$ avec $a = \mathbb{1}_n \cdot \Sigma_{\mathscr{A}}$ et $b = \mathbb{1}_n \cdot \Sigma_{\mathscr{B}}$.
$(\Sigma_{\mathscr{C}} = G_{\mathscr{C}}^T \cdot \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T\right)^{-1} G_{\mathscr{C}}.)$

Remarque

Si $\mathbb{1}_n \in \mathscr{A}$ ou $\mathbb{1}_n \in \mathscr{A}^{\perp}$, alors $a = b = \mathbb{1}_n$ et $J = \emptyset$.

Caractérisation algébrique de PEP quand $h = 0$

Proposition

Lorsque $h = 0$, on peut ajouter à $\mathfrak{S}$ les équations

$$\{x_{i,j} = 0, (i,j) \in J\}$$

où $J = \{(i,j) : a_i \neq b_j\}$ avec $a = \mathbb{1}_n \cdot \Sigma_{\mathscr{A}}$ et $b = \mathbb{1}_n \cdot \Sigma_{\mathscr{B}}$.
$(\Sigma_{\mathscr{C}} = G_{\mathscr{C}}^T \cdot \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T\right)^{-1} G_{\mathscr{C}}.)$

Remarque

Si $\mathbb{1}_n \in \mathscr{A}$ ou $\mathbb{1}_n \in \mathscr{A}^{\perp}$, alors $a = b = \mathbb{1}_n$ et $J = \emptyset$.

Proposition

Si $\mathscr{A}$ et $\mathscr{B}$ sont des codes aléatoires, J est de taille $O(n^2\left(1 - \frac{1}{q}\right))$.

PEP pour des codes aléatoires avec hull trivial

Si

- $\mathscr{H}(\mathscr{A}) = \mathscr{H}(\mathscr{B}) = \{0\}$,
- $\mathbb{1}_n \notin \mathscr{A}$ et $\mathbb{1}_n \notin \mathscr{A}^{\perp}$, (idem pour $\mathscr{B}$),
- $\mathbb{1}_{\mathscr{A}}$ et $\mathbb{1}_{\mathscr{B}}$ sont uniformément distribués,
- $\langle \mathfrak{S} \rangle$ a un petit nombre de solutions,
- $2R(1-R) \geq \frac{1}{q}$ où $R = \frac{k}{n}$,

Alors PEP peut être résolu en temps polynomial $O\left(n^{2\omega}\right)$ où ω est l'exposant de l'algèbre linéaire.

Linéarisation par blocs

Autres équations de blocs

- Il peut exister d'autres équations de blocs que celles provenant de $\mathbb{1}_{\mathscr{A}} X = \mathbb{1}_{\mathscr{B}}$.
- On les trouve par mise sous forme échelon du système linéaire.
- Toute équation $\sum_{i=1}^{n} a_i x_{i,j} - b$ équivaut à $\{\sum_{i \notin J} x_{i,j} - 1, \{x_{i,j}\}_{i \in J}\}$ où $J = \{i : a_i \neq b\}$.
- Complexité au pire $O(n^{1+2\omega})$ pour toutes les trouver, chacune annule $|J|$ variables.

PEP sur $\mathbb{F}_2$ et GI

Définition

La matrice d'adjacence d'un graphe $\mathscr{G}$ non orienté est une matrice binaire symétrique $\mathbf{A}^{\mathscr{G}} = (a_{i,j})_{1 \leq i,j \leq n}$ telle que

$$a_{i,j} = 1 \text{ si } (i,j) \in E_{\mathscr{G}} \text{ et } 0 \text{ sinon.}$$

Théorème

Le problème PEP pour deux codes $\mathscr{A}, \mathscr{B}$ de hull trivial sur $\mathbb{F}_2$ et de longueur n se réduit au problème GI entre deux graphes avec n sommets et de matrices d'adjacence $\Sigma_{\mathscr{A}}$ et $\Sigma_{\mathscr{B}}$.
$(\Sigma_{\mathscr{C}} = G_{\mathscr{C}}^T \cdot \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T\right)^{-1} G_{\mathscr{C}}.)$

PEP sur $\mathbb{F}_2$ et GI

Définition

La matrice d'adjacence d'un graphe $\mathscr{G}$ non orienté est une matrice binaire symétrique $\mathbf{A}^{\mathscr{G}} = (a_{i,j})_{1 \leq i,j \leq n}$ telle que

$$a_{i,j} = 1 \text{ si } (i,j) \in E_{\mathscr{G}} \text{ et } 0 \text{ sinon.}$$

Théorème

Le problème PEP pour deux codes $\mathscr{A}, \mathscr{B}$ de hull trivial sur $\mathbb{F}_2$ et de longueur n se réduit au problème GI entre deux graphes avec n sommets et de matrices d'adjacence $\Sigma_{\mathscr{A}}$ et $\Sigma_{\mathscr{B}}$.
$(\Sigma_{\mathscr{C}} = G_{\mathscr{C}}^T \cdot \left(G_{\mathscr{C}} \cdot G_{\mathscr{C}}^T\right)^{-1} G_{\mathscr{C}}.)$

Babai, arXiv 2017

La complexité en temps de GI est quasi-polynomiale en le nombre de sommets, $\exp(\log(n)^{O(1)})$.

PEP sur des extensions de corps

On suppose que $\mathbb{F} = \mathbb{F}_{p^m}$ où p premier et $m \geq 1$.
On note $\zeta_p : \mathbb{F} \to \mathbb{F}$ défini par $\zeta_p(x) = x^p$ le morphisme de Frobenius.

Proposition

Si $\sum_{i,j} \alpha_{i,j} x_{i,j} - b \in \langle \mathfrak{S} \rangle$, alors

$$\sum_{i,j} \alpha_{i,j}^{p^u} x_{i,j} - b^{p^u} \in \langle \mathfrak{S} \rangle.$$

Conclusion

- Modélisation algébrique de PEP.
- Un calcul de bases de Gröbner donne les solutions.
  Comprendre la complexité du calcul modulo
  $\{x_{i,j}x_{i',j}\}_{1\leq i\neq i',j\leq n}, \{x_{i,j}x_{i,j'}\}_{1\leq i,j\neq j'\leq n}, \{{x_{i,j}}^2 - x_{i,j}\}_{1\leq i\neq j\leq n}$?
- Modélisation particulière si hulls triviaux et extensions de corps (plus d'équations linéaires).
- Méthode efficace de résolution partielle par blocs du système algébrique pour réduire le nombre de variables.
- La seule partie linéaire + résolution par blocs du système permet de résoudre dans certains cas.
- On résout pour $n \simeq 30$ dans le cas général, jusqu'à $n \simeq 500$ dans les cas particuliers.
- Une réduction polynomiale de $\mathrm{PEP}_{h=0}$ à GI.