“ $C^{\langle 2 \rangle}$ ”

Hugues Randriambololona

École nationale supérieure des télécommunications,
LTCI CNRS UMR 5141,
Institut Mines-Télécom,
Université Paris-Saclay,
Télécom ParisTech,
etc.

Journées C2
La Londe-les-Maures, 2015-10-07

Partie 1
Généralités

Code linéaire : c'est un sous-espace vectoriel d'un certain $(\mathbb{F}_q)^n$.
Paramètres $[n, k, d, d^\perp, \dots]_q$: longueur, dimension, distance minimale, distance duale, ..., taille de l'alphabet.

Code linéaire : c'est un sous-espace vectoriel d'un certain $(\mathbb{F}_q)^n$.
Paramètres $[n, k, d, d^\perp, \dots]_q$: longueur, dimension, distance minimale, distance duale, ..., taille de l'alphabet.

On munit $(\mathbb{F}_q)^n$ d'une structure de $\mathbb{F}_q$-algèbre au moyen de la multiplication coordonnée par coordonnée : $\mathbf{c} = (c_1, \dots, c_n), \mathbf{c}' = (c'_1, \dots, c'_n) \in (\mathbb{F}_q)^n$

$$\mathbf{c} * \mathbf{c}' = (c_1 c'_1, \dots, c_n c'_n) \in (\mathbb{F}_q)^n.$$

Code linéaire : c'est un sous-espace vectoriel d'un certain $(\mathbb{F}_q)^n$.
Paramètres $[n, k, d, d^\perp, \dots]_q$: longueur, dimension, distance minimale, distance duale, ..., taille de l'alphabet.

On munit $(\mathbb{F}_q)^n$ d'une structure de $\mathbb{F}_q$-algèbre au moyen de la multiplication coordonnée par coordonnée : $\mathbf{c} = (c_1, \dots, c_n), \mathbf{c}' = (c'_1, \dots, c'_n) \in (\mathbb{F}_q)^n$

$$\mathbf{c} * \mathbf{c}' = (c_1 c'_1, \dots, c_n c'_n) \in (\mathbb{F}_q)^n.$$

Définition

Pour $C, C' \subseteq (\mathbb{F}_q)^n$ on pose

$$C * C' = \langle \mathbf{c} * \mathbf{c}' \rangle_{\mathbf{c} \in C, \mathbf{c}' \in C'} \subseteq (\mathbb{F}_q)^n$$

le sous-espace engendré.

Code linéaire : c'est un sous-espace vectoriel d'un certain $(\mathbb{F}_q)^n$.
Paramètres $[n, k, d, d^\perp, \dots]_q$: longueur, dimension, distance minimale, distance duale, ..., taille de l'alphabet.

On munit $(\mathbb{F}_q)^n$ d'une structure de $\mathbb{F}_q$-algèbre au moyen de la multiplication coordonnée par coordonnée : $\mathbf{c} = (c_1, \dots, c_n), \mathbf{c}' = (c'_1, \dots, c'_n) \in (\mathbb{F}_q)^n$

$$\mathbf{c} * \mathbf{c}' = (c_1 c'_1, \dots, c_n c'_n) \in (\mathbb{F}_q)^n.$$

Définition

Pour $C, C' \subseteq (\mathbb{F}_q)^n$ on pose

$$C * C' = \langle \mathbf{c} * \mathbf{c}' \rangle_{\mathbf{c} \in C, \mathbf{c}' \in C'} \subseteq (\mathbb{F}_q)^n$$

le sous-espace engendré.

$\rightarrow$ $(+, *, \subseteq)$ munit le treillis des sous-espaces de $(\mathbb{F}_q)^n$ d'une structure de semi-anneau ordonné, de neutre $\{\mathbf{0}\}$ et unité $\mathbb{1} = \langle \mathbf{1}_{[n]} \rangle$; attention : ne pas confondre $+, *$ avec $\oplus, \otimes$ qui changent la longueur !

$\rightarrow$ notion de carré $C^{\langle 2 \rangle} = C * C$, de puissances $C^{\langle s \rangle}$ pour $s \geq 0$.

Exemple : soient $C, C' \subseteq (\mathbb{F}_2)^7$ engendrés par les lignes de

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad \mathbf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix},$$

i.e. $C = \{(0000000), (1001111), (0111100), (1110011)\}$,
et $C' = \{(0000000), (1001111), (0110011), (1111100)\}$.
Alors $C * C'$ est engendré par

$$\widetilde{\mathbf{G}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Exemple : soient $C, C' \subseteq (\mathbb{F}_2)^7$ engendrés par les lignes de

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad \mathbf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix},$$

i.e. $C = \{(0000000), (1001111), (0111100), (1110011)\}$,
et $C' = \{(0000000), (1001111), (0110011), (1111100)\}$.
Alors $C * C'$ est engendré par

$$\widetilde{\mathbf{G}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

On note que $(1000000) \in C * C'$ donc

$$\mathrm{d}_{\min}(C * C') = 1$$

alors que

$$\|\mathbf{c} * \mathbf{c}'\| \geq 2$$

pour tous $\mathbf{c} \in C, \mathbf{c}' \in C'$ non nuls.

Autre point de vue : soient $\mathbf{p}_1, \ldots, \mathbf{p}_n \in (\mathbb{F}_q)^k$ les colonnes de la matrice génératrice $\mathbf{G}$ de C.

Autre point de vue : soient $\mathbf{p}_1, \ldots, \mathbf{p}_n \in (\mathbb{F}_q)^k$ les colonnes de la matrice génératrice $\mathbf{G}$ de C.

Ainsi C se voit comme un code d'évaluation de formes linéaires

$$\begin{array}{rccc} ev_1 : & \mathbb{F}_q[X_1, \ldots, X_k]_1 & \longrightarrow & (\mathbb{F}_q)^n \\ & L & \mapsto & (L(\mathbf{p}_1), \ldots, L(\mathbf{p}_n)) \end{array}$$

Autre point de vue : soient $\mathbf{p}_1, \ldots, \mathbf{p}_n \in (\mathbb{F}_q)^k$ les colonnes de la matrice génératrice $\mathbf{G}$ de C.

Ainsi C se voit comme un code d'évaluation de formes linéaires

$$\begin{array}{rccc} ev_1 : & \mathbb{F}_q[X_1, \ldots, X_k]_1 & \longrightarrow & (\mathbb{F}_q)^n \\ & L & \mapsto & (L(\mathbf{p}_1), \ldots, L(\mathbf{p}_n)) \end{array}$$

et alors $C^{\langle s \rangle}$ s'obtient de même avec les polynômes homogènes

$$\begin{array}{rccc} ev_s : & \mathbb{F}_q[X_1, \ldots, X_k]_s & \longrightarrow & (\mathbb{F}_q)^n \\ & P & \mapsto & (P(\mathbf{p}_1), \ldots, P(\mathbf{p}_n)). \end{array}$$

Autre point de vue : soient $\mathbf{p}_1, \ldots, \mathbf{p}_n \in (\mathbb{F}_q)^k$ les colonnes de la matrice génératrice $\mathbf{G}$ de C.

Ainsi C se voit comme un code d'évaluation de formes linéaires

$$\begin{array}{rccc} ev_1 : & \mathbb{F}_q[X_1, \ldots, X_k]_1 & \longrightarrow & (\mathbb{F}_q)^n \\ & L & \mapsto & (L(\mathbf{p}_1), \ldots, L(\mathbf{p}_n)) \end{array}$$

et alors $C^{\langle s \rangle}$ s'obtient de même avec les polynômes homogènes

$$\begin{array}{rccc} ev_s : & \mathbb{F}_q[X_1, \ldots, X_k]_s & \longrightarrow & (\mathbb{F}_q)^n \\ & P & \mapsto & (P(\mathbf{p}_1), \ldots, P(\mathbf{p}_n)). \end{array}$$

(Pour $C * C'$, description analogue avec les applications bilinéaires.)

Autre point de vue : soient $\mathbf{p}_1, \ldots, \mathbf{p}_n \in (\mathbb{F}_q)^k$ les colonnes de la matrice génératrice $\mathbf{G}$ de C.

Ainsi C se voit comme un code d'évaluation de formes linéaires

$$\begin{array}{rccc} ev_1 : & \mathbb{F}_q[X_1, \ldots, X_k]_1 & \longrightarrow & (\mathbb{F}_q)^n \\ & L & \mapsto & (L(\mathbf{p}_1), \ldots, L(\mathbf{p}_n)) \end{array}$$

et alors $C^{\langle s \rangle}$ s'obtient de même avec les polynômes homogènes

$$\begin{array}{rccc} ev_s : & \mathbb{F}_q[X_1, \ldots, X_k]_s & \longrightarrow & (\mathbb{F}_q)^n \\ & P & \mapsto & (P(\mathbf{p}_1), \ldots, P(\mathbf{p}_n)). \end{array}$$

(Pour $C * C'$, description analogue avec les applications bilinéaires.)

Exemples de codes d'évaluation "natifs" :

- Reed-Solomon, $RS(n,k) * RS(n,k') = RS(n, k+k'-1)$ pour $k + k' \leq n + 1$
- idem pour les Reed-Muller, les codes géométriques...

On suppose $\mathrm{d}^{\perp}(C) \geq 3$, i.e. C de support plein et "sans colonne répétée".
Dictionnaire :

$$
\begin{array}{rcl}
C & \longleftrightarrow & \Pi_C = \{\overline{\mathbf{p}}_1, \ldots, \overline{\mathbf{p}}_n\} \subseteq \mathbb{P}^{k-1} \\
C^{\langle s \rangle} & \longleftrightarrow & \Pi_{C^{\langle s \rangle}} = v_s(\Pi_C) \subseteq \mathbb{P}^{\binom{k+s-1}{s}-1} \text{ image par Veronese} \\
C^{\langle \cdot \rangle} = \bigoplus_{s \geq 0} C^{\langle s \rangle} & = & \text{anneau de coordonnées homogènes de } \Pi_C \\
\ker(S^{\cdot}C \twoheadrightarrow C^{\langle \cdot \rangle}) & = & \text{idéal homogène de } \Pi_C \\
\dim(C^{\langle \cdot \rangle}) & = & \text{fonction de Hilbert de } \Pi_C.
\end{array}
$$

On suppose $\mathrm{d}^{\perp}(C) \geq 3$, i.e. C de support plein et "sans colonne répétée".
Dictionnaire :

$$
\begin{aligned}
C &\longleftrightarrow \Pi_C = \{\overline{\mathbf{p}}_1, \ldots, \overline{\mathbf{p}}_n\} \subseteq \mathbb{P}^{k-1} \\
C^{\langle s \rangle} &\longleftrightarrow \Pi_{C^{\langle s \rangle}} = v_s(\Pi_C) \subseteq \mathbb{P}^{\binom{k+s-1}{s}-1} \text{ image par Veronese} \\
C^{\langle \cdot \rangle} = \bigoplus_{s \geq 0} C^{\langle s \rangle} &= \text{anneau de coordonnées homogènes de } \Pi_C \\
\ker(S^{\cdot}C \twoheadrightarrow C^{\langle \cdot \rangle}) &= \text{idéal homogène de } \Pi_C \\
\dim(C^{\langle \cdot \rangle}) &= \text{fonction de Hilbert de } \Pi_C.
\end{aligned}
$$

Proposition

$$\dim(C^{\langle s+1 \rangle}) \geq \dim(C^{\langle s \rangle}),$$

$$\mathrm{d}_{\min}(C^{\langle s+1 \rangle}) \leq \mathrm{d}_{\min}(C^{\langle s \rangle}), \qquad \mathrm{d}^{\perp}(C^{\langle s+1 \rangle}) \geq \mathrm{d}^{\perp}(C^{\langle s \rangle}).$$

On suppose $\mathrm{d}^\perp(C) \geq 3$, i.e. C de support plein et "sans colonne répétée".
Dictionnaire :

$$\begin{aligned} C &\longleftrightarrow \Pi_C = \{\overline{\mathbf{p}}_1, \ldots, \overline{\mathbf{p}}_n\} \subseteq \mathbb{P}^{k-1} \\ C^{\langle s \rangle} &\longleftrightarrow \Pi_{C^{\langle s \rangle}} = v_s(\Pi_C) \subseteq \mathbb{P}^{\binom{k+s-1}{s}-1} \text{ image par Veronese} \\ C^{\langle \cdot \rangle} = \bigoplus_{s \geq 0} C^{\langle s \rangle} &= \text{anneau de coordonnées homogènes de } \Pi_C \\ \ker(S^{\cdot}C \twoheadrightarrow C^{\langle \cdot \rangle}) &= \text{idéal homogène de } \Pi_C \\ \dim(C^{\langle \cdot \rangle}) &= \text{fonction de Hilbert de } \Pi_C. \end{aligned}$$

Proposition

$$\dim(C^{\langle s+1 \rangle}) \geq \dim(C^{\langle s \rangle}),$$
$$\mathrm{d}_{\min}(C^{\langle s+1 \rangle}) \leq \mathrm{d}_{\min}(C^{\langle s \rangle}), \qquad \mathrm{d}^\perp(C^{\langle s+1 \rangle}) \geq \mathrm{d}^\perp(C^{\langle s \rangle}).$$

Ainsi $\dim(C^{\langle s \rangle})$ se stabilise pour s assez grand, en l'occurence à partir de $s = r(C) = r(\Pi_C)$ régularité de Castelnuovo-Mumford de Π_C.

Proposition

$$\dim(C^{\langle s \rangle}) = \dim(C^{\langle s+1 \rangle}) \iff s \geq r(C) \iff C^{\langle s \rangle} = (\mathbb{F}_q)^n.$$

Une question ouverte : automorphismes des puissances d'un code.

$$\begin{aligned}\mathrm{Aut}((\mathbb{F}_q)^n) &= \text{ matrices “monomiales”, ou permutations généralisées} \\ &= \mathfrak{S}_n \ltimes (\mathbb{F}_q^\times)^n \text{ produit semi-direct}\end{aligned}$$

- agit à droite sur $(\mathbb{F}_q)^n$ par $(\sigma, \mathbf{a}) : \mathbf{x} \mapsto \mathbf{x}^\sigma * \mathbf{a}$
- loi de composition : $(\sigma, \mathbf{a})(\tau, \mathbf{b}) = (\sigma\tau, \mathbf{a}^\tau * \mathbf{b})$
- s.e. (scindée) $\quad 1 \longrightarrow (\mathbb{F}_q^\times)^n \longrightarrow \mathrm{Aut}((\mathbb{F}_q)^n) \xrightarrow{\pi} \mathfrak{S}_n \longrightarrow 1.$

Une question ouverte : automorphismes des puissances d'un code.

$$\begin{aligned}\mathrm{Aut}((\mathbb{F}_q)^n) &= \text{ matrices “monomiales”, ou permutations généralisées} \\ &= \mathfrak{S}_n \ltimes (\mathbb{F}_q^\times)^n \text{ produit semi-direct}\end{aligned}$$

- agit à droite sur $(\mathbb{F}_q)^n$ par $(\sigma, \mathbf{a})\colon \mathbf{x} \mapsto \mathbf{x}^\sigma * \mathbf{a}$
- loi de composition : $(\sigma, \mathbf{a})(\tau, \mathbf{b}) = (\sigma\tau, \mathbf{a}^\tau * \mathbf{b})$
- s.e. (scindée) $\quad 1 \longrightarrow (\mathbb{F}_q^\times)^n \longrightarrow \mathrm{Aut}((\mathbb{F}_q)^n) \xrightarrow{\pi} \mathfrak{S}_n \longrightarrow 1.$

Définition

Pour deux sous-groupes H, H' de $\mathrm{Aut}((\mathbb{F}_q)^n)$, on écrit

$$H \ \widehat{\subseteq} \ H'$$

si

$$\pi(H) \subseteq \pi(H') \quad \text{et} \quad H \cap (\mathbb{F}_q^\times)^n \subseteq H' \cap (\mathbb{F}_q^\times)^n.$$

Remarque : et alors, $|H|$ divise $|H'|$.

Pour $C \subseteq (\mathbb{F}_q)^n$,

$$\mathrm{Aut}(C) = \{(\sigma, \mathbf{a}) \in \mathrm{Aut}((\mathbb{F}_q)^n)\,;\; C^\sigma * \mathbf{a} = C\}.$$

Proposition

Pour $t \geq 1$ on a $\mathrm{Aut}(C) \,\widehat{\subseteq}\, \mathrm{Aut}(C^{\langle t \rangle})$.

D'où plus généralement $\mathrm{Aut}(C^{\langle s \rangle}) \,\widehat{\subseteq}\, \mathrm{Aut}(C^{\langle t \rangle})$ si $s|t$.
Par ailleurs pour $s \geq r(C)$ on a $\mathrm{Aut}(C^{\langle s \rangle}) = \mathrm{Aut}((\mathbb{F}_q)^n)$ maximal.

Pour $C \subseteq (\mathbb{F}_q)^n$,

$$\mathrm{Aut}(C) = \{(\sigma, \mathbf{a}) \in \mathrm{Aut}((\mathbb{F}_q)^n)\,;\; C^\sigma * \mathbf{a} = C\}.$$

Proposition

Pour $t \geq 1$ on a $\mathrm{Aut}(C) \,\widehat{\subseteq}\, \mathrm{Aut}(C^{\langle t \rangle})$.

D'où plus généralement $\mathrm{Aut}(C^{\langle s \rangle}) \,\widehat{\subseteq}\, \mathrm{Aut}(C^{\langle t \rangle})$ si $s|t$.
Par ailleurs pour $s \geq r(C)$ on a $\mathrm{Aut}(C^{\langle s \rangle}) = \mathrm{Aut}((\mathbb{F}_q)^n)$ maximal.
Ceci suggère :

Les $\mathrm{Aut}(C^{\langle s \rangle})$ "croissent"-ils avec s ?
Par exemple, peut-on "comparer" $\mathrm{Aut}(C^{\langle 2 \rangle})$ et $\mathrm{Aut}(C^{\langle 3 \rangle})$?

Pour $C \subseteq (\mathbb{F}_q)^n$,

$$\mathrm{Aut}(C) = \{(\sigma, \mathbf{a}) \in \mathrm{Aut}((\mathbb{F}_q)^n)\,;\; C^\sigma * \mathbf{a} = C\}.$$

Proposition

Pour $t \geq 1$ on a $\mathrm{Aut}(C) \,\widehat{\subseteq}\, \mathrm{Aut}(C^{\langle t \rangle})$.

D'où plus généralement $\mathrm{Aut}(C^{\langle s \rangle}) \,\widehat{\subseteq}\, \mathrm{Aut}(C^{\langle t \rangle})$ si $s|t$.
Par ailleurs pour $s \geq r(C)$ on a $\mathrm{Aut}(C^{\langle s \rangle}) = \mathrm{Aut}((\mathbb{F}_q)^n)$ maximal.
Ceci suggère :

Les $\mathrm{Aut}(C^{\langle s \rangle})$ "croissent"-ils avec s ?
Par exemple, peut-on "comparer" $\mathrm{Aut}(C^{\langle 2 \rangle})$ et $\mathrm{Aut}(C^{\langle 3 \rangle})$?

Variante géométrique :

$$\Pi \subseteq \mathbb{P}^{k-1} \quad \rightarrow \quad \Gamma(\Pi) = \{g \in \mathrm{PGL}_k\,;\; g(\Pi) = \Pi\}.$$

Si $v_s : \mathbb{P}^{k-1} \to \mathbb{P}^{\binom{k+s-1}{s}-1}$ Veronese, les $\Gamma(v_s(\Pi))$ "croissent"-ils avec s ?
Peut-on "comparer" $\Gamma(v_2(\Pi))$ et $\Gamma(v_3(\Pi))$?

Étude des produits de codes motivée par de nombreuses applications (récentes ou moins récentes) :

- algorithmes bilinéaires & systèmes de partage de secret arithmétiques
- cryptanalyse de systèmes à la McEliece
- décodage algébrique (error-correcting pairs, power decoding...)
- construction de réseaux euclidiens (via $\mathbf{x} \underset{\mathbb{Z}}{+} \mathbf{y} = (\mathbf{x} \underset{\mathbb{F}_2}{+} \mathbf{y}) + 2 \cdot (\mathbf{x} * \mathbf{y})$...), raccourcissement de codes quantiques, transfert inconscient...

Étude des produits de codes motivée par de nombreuses applications (récentes ou moins récentes) :

- algorithmes bilinéaires & systèmes de partage de secret arithmétiques
- cryptanalyse de systèmes à la McEliece
- décodage algébrique (error-correcting pairs, power decoding...)
- construction de réseaux euclidiens (via $\mathbf{x} \underset{\mathbb{Z}}{+} \mathbf{y} = (\mathbf{x} \underset{\mathbb{F}_2}{+} \mathbf{y}) + 2 \cdot (\mathbf{x} * \mathbf{y})$...), raccourcissement de codes quantiques, transfert inconscient...

Souvent la difficulté provient de l'étape de passage au sous-espace engendré dans la définition du produit de codes. Celle-ci n'est pas gratuite mais bien dictée par les applications.
Situation typique : $C = (A * B)^{\perp}$, alors

$$\mathrm{d}^{\perp}(C) = \mathrm{d}_{\min}(A * B)$$

peut être inférieure au $\min\|\mathbf{a} * \mathbf{b}\|$.

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Exemple : multiplication de deux polynômes de degré 1

$$(u + vX)(u' + v'X) =$$

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Exemple : multiplication de deux polynômes de degré 1 avec 4 $\cdot$

$$(u + vX)(u' + v'X) = u \cdot u' + (u \cdot v' + u' \cdot v)X + v \cdot v' X^2$$

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Exemple : multiplication de deux polynômes de degré 1 avec 3 $\cdot$

$$(u+vX)(u'+v'X) = u\cdot u'(1-X) + (u+v)\cdot(u'+v')X + v\cdot v'(X^2-X).$$

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Exemple : multiplication de deux polynômes de degré 1 avec 3 $\cdot$

$$(u+vX)(u'+v'X) = u\cdot u'(1-X) + (u+v)\cdot(u'+v')X + v\cdot v'(X^2-X).$$

Interprétation : évaluation puis interpolation en $0, 1, \infty$.

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Exemple : multiplication de deux polynômes de degré 1 avec 3 $\cdot$

$$(u+vX)(u'+v'X) = u\cdot u'(1-X) + (u+v)\cdot(u'+v')X + v\cdot v'(X^2-X).$$

Interprétation : évaluation puis interpolation en $0, 1, \infty$.

Application : multiplication dans $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ avec 3 $\cdot$ dans $\mathbb{F}_q$

$$(u+v\alpha)(u'+v'\alpha) = u\cdot u'(1-\alpha) + (u+v)\cdot(u'+v')\alpha + v\cdot v'(\alpha^2-\alpha).$$

Algorithmes bilinéaires :

- Strassen, multiplication rapide de matrices
- Karatsuba, multiplication rapide de polynômes, ou d'entiers.

Exemple : multiplication de deux polynômes de degré 1 avec 3 $\cdot$

$$(u+vX)(u'+v'X) = u\cdot u'(1-X) + (u+v)\cdot(u'+v')X + v\cdot v'(X^2-X).$$

Interprétation : évaluation puis interpolation en $0, 1, \infty$.

Application : multiplication dans $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ avec 3 $\cdot$ dans $\mathbb{F}_q$

$$(u+v\alpha)(u'+v'\alpha) = u\cdot u'(1-\alpha) + (u+v)\cdot(u'+v')\alpha + v\cdot v'(\alpha^2-\alpha).$$

Généralisation (Chudnovsky-Chudnovsky) : évaluation-interpolation sur des courbes de genre supérieur, permet de multiplier dans $\mathbb{F}_{q^k}$ avec un nombre n de $\cdot$ dans $\mathbb{F}_q$ qui reste linéaire en k.

En termes de codes, on a deux applications $\mathbb{F}_q$-linéaires φ, θ avec

$$\begin{array}{ccc} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \xrightarrow{\times} & \mathbb{F}_{q^k} \\ {\scriptstyle \varphi\times\varphi}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

i.e. $zz' = \theta(\varphi(z) * \varphi(z'))$ pour tous $z, z' \in \mathbb{F}_{q^k}$
$\iff$ "diagonalisation" sur $\mathbb{F}_q$ du tenseur de multiplication dans $\mathbb{F}_{q^k}$.

Exemple : $k=2$, $n=3$, $\quad \varphi : z=u+v\alpha \mapsto \varphi(z)=(u,\, u+v,\, v)$,
$$\varphi(z) * \varphi(z') = (u\cdot u',\ (u+v)\cdot(u'+v'),\ v\cdot v').$$

En termes de codes, on a deux applications $\mathbb{F}_q$-linéaires φ, θ avec

$$\begin{array}{ccc} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \xrightarrow{\times} & \mathbb{F}_{q^k} \\ {\scriptstyle \varphi\times\varphi}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

i.e. $zz' = \theta(\varphi(z) * \varphi(z'))$ pour tous $z, z' \in \mathbb{F}_{q^k}$
$\iff$ "diagonalisation" sur $\mathbb{F}_q$ du tenseur de multiplication dans $\mathbb{F}_{q^k}$.

Exemple : $k=2$, $n=3$, $\quad \varphi : z=u+v\alpha \mapsto \varphi(z)=(u,\, u+v,\, v)$,
$$\varphi(z) * \varphi(z') = (u\cdot u',\ (u+v)\cdot(u'+v'),\ v\cdot v').$$

Note $C = \mathrm{im}(\varphi)$, ainsi $\varphi(z) * \varphi(z') \in C^{\langle 2 \rangle}$.

En termes de codes, on a deux applications $\mathbb{F}_q$-linéaires φ, θ avec

$$\begin{array}{ccc} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \xrightarrow{\times} & \mathbb{F}_{q^k} \\ {\scriptstyle \varphi\times\varphi}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

i.e. $zz' = \theta(\varphi(z) * \varphi(z'))$ pour tous $z, z' \in \mathbb{F}_{q^k}$
$\iff$ "diagonalisation" sur $\mathbb{F}_q$ du tenseur de multiplication dans $\mathbb{F}_{q^k}$.

Exemple : $k=2$, $n=3$, $\quad \varphi : z=u+v\alpha \mapsto \varphi(z)=(u,\, u+v,\, v)$,
$$\varphi(z) * \varphi(z') = (u\cdot u',\ (u+v)\cdot(u'+v'),\ v\cdot v').$$

Note $C = \mathrm{im}(\varphi)$, ainsi $\varphi(z) * \varphi(z') \in C^{\langle 2 \rangle}$.

Jeu sur les paramètres :

- du point de vue "complexité bilinéaire", k donné, minimiser n
- du point de vue "partage de secret à seuils", reconstructibilité liée à $\mathrm{d}_{\min}(C^{\langle 2 \rangle})$, résistance aux collusions liée à $\mathrm{d}^{\perp}(C)$.

Cryptosystèmes à la McEliece :

Clé secrète : $\mathbf{G}$ avec un algorithme de décodage efficace, $\mathbf{S}, \mathbf{P}$ "masques".

Clé publique : $\widetilde{\mathbf{G}} = \mathbf{SGP}$ difficile à décoder (NP-difficile si $\widetilde{\mathbf{G}}$ était vraiment aléatoire).

Cryptosystèmes à la McEliece :

Clé secrète : $\mathbf{G}$ avec un algorithme de décodage efficace, $\mathbf{S}, \mathbf{P}$ "masques".
Clé publique : $\widetilde{\mathbf{G}} = \mathbf{SGP}$ difficile à décoder (NP-difficile si $\widetilde{\mathbf{G}}$ était vraiment aléatoire).

Attaques:

- distinguer $\widetilde{\mathbf{G}}$ d'une matrice aléatoire
- retrouver sa structure algébrique cachée.

Cryptosystèmes à la McEliece :
Clé secrète : $\mathbf{G}$ avec un algorithme de décodage efficace, $\mathbf{S}, \mathbf{P}$ "masques".
Clé publique : $\widetilde{\mathbf{G}} = \mathbf{SGP}$ difficile à décoder (NP-difficile si $\widetilde{\mathbf{G}}$ était vraiment aléatoire).

Attaques:

- distinguer $\widetilde{\mathbf{G}}$ d'une matrice aléatoire
- retrouver sa structure algébrique cachée.

Heuristique : pour $k = \dim C$, $l = \dim C'$, de même longueur n,

$$\dim(C * C') \leq \min(n, kl)$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{i \in [k]}$, $C' = \langle \mathbf{c}'_j \rangle_{j \in [l]} \implies C * C' = \langle \mathbf{c}_i * \mathbf{c}'_j \rangle_{i \in [k], j \in [l]}$).
On s'attend à avoir egalité pour C, C' aléatoires.
Cas d'inégalité stricte signifie qu'il y a des relations algébriques (bilinéaires) entre C et C'.

Cryptosystèmes à la McEliece :
Clé secrète : $\mathbf{G}$ avec un algorithme de décodage efficace, $\mathbf{S}, \mathbf{P}$ "masques".
Clé publique : $\widetilde{\mathbf{G}} = \mathbf{SGP}$ difficile à décoder (NP-difficile si $\widetilde{\mathbf{G}}$ était vraiment aléatoire).

Attaques:

- distinguer $\widetilde{\mathbf{G}}$ d'une matrice aléatoire
- retrouver sa structure algébrique cachée.

Heuristique : pour $k = \dim C$, $l = \dim C'$, de même longueur n,

$$\dim(C * C') \leq \min(n, kl)$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{i \in [k]}$, $C' = \langle \mathbf{c}'_j \rangle_{j \in [l]} \implies C * C' = \langle \mathbf{c}_i * \mathbf{c}'_j \rangle_{i \in [k], j \in [l]}$).
On s'attend à avoir egalité pour C, C' aléatoires.
Cas d'inégalité stricte signifie qu'il y a des relations algébriques (bilinéaires) entre C et C'.

$\rightarrow$ Applique à $C, C' =$ sous-codes du code engendré par les lignes de $\widetilde{\mathbf{G}}$.

Partie 2
Dimensions

Une digression

Soient V un e.v. de dimension finie, et $X \subseteq V$ un sous-ensemble arbitraire.

Définition

X est dit (linéairement) en position générale si, pour tout $S \subseteq X$ fini,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

Soit : pas de relation linéaire "inattendue" entre éléments de X.

Une digression

Soient V un e.v. de dimension finie, et $X \subseteq V$ un sous-ensemble arbitraire.

Définition

X est dit (linéairement) en position générale si, pour tout $S \subseteq X$ fini,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

Soit : pas de relation linéaire "inattendue" entre éléments de X.

Exemple: $V = (\mathbb{F}_q)^k$, $X \subseteq V$, $n = |X| \geq k$, $C = [n,k]_q$-code de matrice génératrice de colonnes X. Alors : X en position générale $\iff$ C MDS.

Une digression

Soient V un e.v. de dimension finie, et $X \subseteq V$ un sous-ensemble arbitraire.

Définition

X est dit (linéairement) en position générale si, pour tout $S \subseteq X$ fini,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

Soit : pas de relation linéaire "inattendue" entre éléments de X.

Exemple: $V = (\mathbb{F}_q)^k$, $X \subseteq V$, $n = |X| \geq k$, $C = [n,k]_q$-code de matrice génératrice de colonnes X. Alors : X en position générale $\iff$ C MDS.

Variantes plus faibles ? Mesure d'erreur ?

Une digression

Soient V un e.v. de dimension finie, et $X \subseteq V$ un sous-ensemble arbitraire.

Définition

X est dit (linéairement) en position générale si, pour tout $S \subseteq X$ fini,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

Soit : pas de relation linéaire "inattendue" entre éléments de X.

Exemple: $V = (\mathbb{F}_q)^k$, $X \subseteq V$, $n = |X| \geq k$, $C = [n,k]_q$-code de matrice génératrice de colonnes X. Alors : X en position générale $\iff$ C MDS.

Variantes plus faibles ? Mesure d'erreur ?

Suppose X equipé d'une distribution de probabilités.

Estimer la "probabilité d'erreur"

$$\mathbb{P}(n) = \mathbb{P}[\dim\langle \mathbf{u}_1, \ldots, \mathbf{u}_n\rangle < \min(n, \dim V)]$$

pour $\mathbf{u}_1, \ldots, \mathbf{u}_n \in X$ aléatoires.

Une digression

Soient V un e.v. de dimension finie, et $X \subseteq V$ un sous-ensemble arbitraire.

Définition

X est dit (linéairement) en position générale si, pour tout $S \subseteq X$ fini,

$$\dim\langle S\rangle = \min(|S|, \dim V).$$

Soit : pas de relation linéaire "inattendue" entre éléments de X.

Exemple: $V = (\mathbb{F}_q)^k$, $X \subseteq V$, $n = |X| \geq k$, $C = [n,k]_q$-code de matrice génératrice de colonnes X. Alors : X en position générale $\iff$ C MDS.

Variantes plus faibles ? Mesure d'erreur ?

Suppose X equipé d'une distribution de probabilités.

Estimer la "probabilité d'erreur"

$$\mathbb{P}(n) = \mathbb{P}[\dim\langle \mathbf{u}_1, \ldots, \mathbf{u}_n\rangle < \min(n, \dim V)]$$

pour $\mathbf{u}_1, \ldots, \mathbf{u}_n \in X$ aléatoires.

Ici : $V = \mathbb{F}_q^{k\times l}$ espace de matrices, $X \subseteq V$ ensemble des matrices de rang 1.

Lien avec les produits de codes

$C = [n, k]_q$-code, $C' = [n, l]_q$-code, donnés par $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l \times n}$.
On en déduit une matrice génératrice $\widetilde{\mathbf{G}}$ pour $C * C'$ (remarque : on autorise des lignes redondantes).
Deux approches possibles.

Lien avec les produits de codes

$C = [n, k]_q$-code, $C' = [n, l]_q$-code, donnés par $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l \times n}$.
On en déduit une matrice génératrice $\widetilde{\mathbf{G}}$ pour $C * C'$ (remarque : on autorise des lignes redondantes).
Deux approches possibles.

Lignes : Comme déjà vu, $\{\mathbf{c}_i\}_{i \in [k]}$ lignes de $\mathbf{G}$, $\{\mathbf{c}'_j\}_{j \in [l]}$ lignes de $\mathbf{G}'$,
$\rightarrow \{\mathbf{c}_i * \mathbf{c}'_j\}_{i \in [k], j \in [l]}$ lignes de $\widetilde{\mathbf{G}}$.

Lien avec les produits de codes

$C = [n,k]_q$-code, $C' = [n,l]_q$-code, donnés par $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$.
On en déduit une matrice génératrice $\widetilde{\mathbf{G}}$ pour $C * C'$ (remarque : on autorise des lignes redondantes).
Deux approches possibles.

Lignes : Comme déjà vu, $\{\mathbf{c}_i\}_{i\in[k]}$ lignes de $\mathbf{G}$, $\{\mathbf{c}'_j\}_{j\in[l]}$ lignes de $\mathbf{G}'$,
$\rightarrow$ $\{\mathbf{c}_i * \mathbf{c}'_j\}_{i\in[k],j\in[l]}$ lignes de $\widetilde{\mathbf{G}}$.

Colonnes : On identifie $(\mathbb{F}_q)^{kl}$ à l'espace de matrices $\mathbb{F}_q^{k\times l}$.
Soient $\mathbf{p}_1,\ldots,\mathbf{p}_n \in (\mathbb{F}_q)^k$ colonnes de $\mathbf{G}$, $\mathbf{q}_1,\ldots,\mathbf{q}_n \in (\mathbb{F}_q)^l$ celles de $\mathbf{G}'$,

$$\longrightarrow \quad \mathbf{u}_i = \mathbf{p}_i\mathbf{q}_i^T \in \mathbb{F}_q^{k\times l} \text{ de rang } (\leq)1.$$

Alors $\mathbf{u}_1,\ldots,\mathbf{u}_n$ sont les colonnes de $\widetilde{\mathbf{G}}$.

Lien avec les produits de codes

$C = [n,k]_q$-code, $C' = [n,l]_q$-code, donnés par $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$.
On en déduit une matrice génératrice $\widetilde{\mathbf{G}}$ pour $C * C'$ (remarque : on autorise des lignes redondantes).
Deux approches possibles.

Lignes : Comme déjà vu, $\{\mathbf{c}_i\}_{i\in[k]}$ lignes de $\mathbf{G}$, $\{\mathbf{c}'_j\}_{j\in[l]}$ lignes de $\mathbf{G}'$,
$\rightarrow$ $\{\mathbf{c}_i * \mathbf{c}'_j\}_{i\in[k],j\in[l]}$ lignes de $\widetilde{\mathbf{G}}$.

Colonnes : On identifie $(\mathbb{F}_q)^{kl}$ à l'espace de matrices $\mathbb{F}_q^{k\times l}$.
Soient $\mathbf{p}_1,\dots,\mathbf{p}_n \in (\mathbb{F}_q)^k$ colonnes de $\mathbf{G}$, $\mathbf{q}_1,\dots,\mathbf{q}_n \in (\mathbb{F}_q)^l$ celles de $\mathbf{G}'$,

$$\longrightarrow \quad \mathbf{u}_i = \mathbf{p}_i\mathbf{q}_i^T \in \mathbb{F}_q^{k\times l} \text{ de rang } (\leq) 1.$$

Alors $\mathbf{u}_1,\dots,\mathbf{u}_n$ sont les colonnes de $\widetilde{\mathbf{G}}$.

Rang-lignes = rang-colonnes !

$$\dim(C * C') = \dim\langle \mathbf{u}_1,\dots,\mathbf{u}_n\rangle$$

$$\mathbb{P}(n) = \mathbb{P}[\dim\langle \mathbf{u}_1,\dots,\mathbf{u}_n\rangle < \min(n,kl)] = \mathbb{P}[\dim(C * C') < \min(n,kl)].$$

Pose $C_q = \prod_{j\geq 1}(1-q^{-j})^{-1} \leq C_2 \approx 3{,}463$, et (domaine de paramètres)

$$\mathcal{P}(\varepsilon,\kappa) = \left\{(k,l);\ 2 \leq k \leq l \leq \frac{\varepsilon q^{\kappa k}}{(q-1)k}\right\} \qquad (0<\varepsilon<1,\ \kappa>0).$$

Pose $C_q = \prod_{j\geq 1}(1-q^{-j})^{-1} \leq C_2 \approx 3{,}463$, et (domaine de paramètres)

$$\mathcal{P}(\varepsilon,\kappa) = \left\{(k,l);\ 2 \leq k \leq l \leq \frac{\varepsilon q^{\kappa k}}{(q-1)k}\right\} \qquad (0<\varepsilon<1,\ \kappa>0).$$

On suppose $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, $\mathbf{G}' \in \mathbb{F}_q^{l\times n}$ aléatoires uniformes.

Théorème $n \geq kl$

Suppose κ assez petit pour que $q^{(1-\kappa)^2} \geq 1 + \frac{q-1}{q}$ (ex : $\kappa = 0{,}23$).
Alors pour $(k,l) \in \mathcal{P}(\varepsilon,\kappa)$ et $n \geq kl$, on a

$$\mathbb{P}(n) = \mathbb{P}[\dim(C * C') < kl] \leq c'' \rho^{n-kl}$$

où $\rho = \frac{1}{q}\left(1 + \frac{q-1}{q}\right) < 1$ et $c'' = \frac{qC_q}{(q-1)^2}\left(1 + \frac{1}{1-\varepsilon}\right)$.

Théorème $n \leq kl$

Pour $(k,l) \in \mathcal{P}(\varepsilon, \frac{1}{2})$ et $n \leq kl$, on a

$$\mathbb{P}(n) = \mathbb{P}[\dim(C * C') < n] \leq \frac{qC_q}{(q-1)^2}\left(\frac{2\varepsilon}{1-\varepsilon} + q^{-(kl-n)}\right).$$

Preuve du Théorème $n \geq kl$: Borne de l'union + indépendance donnent

$$\mathbb{P}(n) \leq \sum\nolimits_H \mathbb{P}[\mathbf{u}_1, \ldots, \mathbf{u}_n \in H] = \sum\nolimits_H \mathbb{P}[\mathbf{u}_1 \in H]^n \leq c' \rho^{n-kl}$$

où $\rho = \max_H \mathbb{P}[\mathbf{u}_1 \in H]$, $c' = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^{kl}$, et H parcourt les hyperplans de $V = \mathbb{F}_q^{k \times l}$.
Conclut avec majoration de c' $\iff$ compter les formes bilinéaires de rang donné et les paires de vecteurs sur lesquels elles s'annulent.

Preuve du Théorème $n \geq kl$: Borne de l'union + indépendance donnent

$$\mathbb{P}(n) \leq \sum\nolimits_H \mathbb{P}[\mathbf{u}_1, \ldots, \mathbf{u}_n \in H] = \sum\nolimits_H \mathbb{P}[\mathbf{u}_1 \in H]^n \leq c' \rho^{n-kl}$$

où $\rho = \max_H \mathbb{P}[\mathbf{u}_1 \in H]$, $c' = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^{kl}$, et H parcourt les hyperplans de $V = \mathbb{F}_q^{k \times l}$.
Conclut avec majoration de c' $\iff$ compter les formes bilinéaires de rang donné et les paires de vecteurs sur lesquels elles s'annulent.

Preuve du Théorème $n \leq kl$: Pose $\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j$ (marche aléatoire dans $\mathbb{F}_q^{k \times l}$). Alors pour $\mathbf{z} \in (\mathbb{F}_q)^n$ donné, de poids $\mathrm{wt}(\mathbf{z}) = w$, on a

$$\mathbb{P}[\mathbf{z} \text{ relation linéaire entre } \mathbf{u}_1, \ldots, \mathbf{u}_n] \;=\; \mathbb{P}[\mathbf{s}_w = 0].$$

Et alors

$$\mathbf{s}_w = 0 \quad \iff \quad \langle \mathbf{x}_1, \ldots, \mathbf{x}_k \rangle \perp \langle \mathbf{y}_1, \ldots, \mathbf{y}_l \rangle \text{ dans } (\mathbb{F}_q)^w$$

où $\mathbf{x}_1, \ldots, \mathbf{x}_k$ et $\mathbf{y}_1, \ldots, \mathbf{y}_l$ sont les projections sur $[w]$ des lignes de $\mathbf{G}, \mathbf{G}'$...

Preuve du Théorème $n \geq kl$: Borne de l'union + indépendance donnent

$$\mathbb{P}(n) \leq \sum\nolimits_H \mathbb{P}[\mathbf{u}_1, \ldots, \mathbf{u}_n \in H] = \sum\nolimits_H \mathbb{P}[\mathbf{u}_1 \in H]^n \leq c' \rho^{n-kl}$$

où $\rho = \max_H \mathbb{P}[\mathbf{u}_1 \in H]$, $c' = \sum_H \mathbb{P}[\mathbf{u}_1 \in H]^{kl}$, et H parcourt les hyperplans de $V = \mathbb{F}_q^{k \times l}$.
Conclut avec majoration de c' $\iff$ compter les formes bilinéaires de rang donné et les paires de vecteurs sur lesquels elles s'annulent.

Preuve du Théorème $n \leq kl$: Pose $\mathbf{s}_j = \mathbf{u}_1 + \cdots + \mathbf{u}_j$ (marche aléatoire dans $\mathbb{F}_q^{k \times l}$). Alors pour $\mathbf{z} \in (\mathbb{F}_q)^n$ donné, de poids $\mathrm{wt}(\mathbf{z}) = w$, on a

$$\mathbb{P}[\mathbf{z} \text{ relation linéaire entre } \mathbf{u}_1, \ldots, \mathbf{u}_n] \;=\; \mathbb{P}[\mathbf{s}_w = 0].$$

Et alors

$$\mathbf{s}_w = 0 \quad \iff \quad \langle \mathbf{x}_1, \ldots, \mathbf{x}_k \rangle \perp \langle \mathbf{y}_1, \ldots, \mathbf{y}_l \rangle \text{ dans } (\mathbb{F}_q)^w$$

où $\mathbf{x}_1, \ldots, \mathbf{x}_k$ et $\mathbf{y}_1, \ldots, \mathbf{y}_l$ sont les projections sur $[w]$ des lignes de $\mathbf{G}, \mathbf{G}'$...

Commentaires :

- Peut-on se débarrasser des conditions $\mathcal{P}(\varepsilon, \kappa)$?
- On peut affiner le modèle probabiliste $\rightarrow$ résultats plus forts ?

Carrés et puissances supérieures

Pour tout $[n,k]_q$-code C on a

$$\dim(C^{\langle 2\rangle}) \leq \min(n, \tfrac{k(k+1)}{2})$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
On s'attend à avoir égalité pour C aléatoire.

Carrés et puissances supérieures

Pour tout $[n,k]_q$-code C on a

$$\dim(C^{\langle 2\rangle}) \leq \min(n, \tfrac{k(k+1)}{2})$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
On s'attend à avoir égalité pour C aléatoire.
Et en effet, Cascudo-Cramer-Mirandola-Zémor ont donné une majoration sur $\mathbb{P}[\dim(C^{\langle 2\rangle}) < \min(n, \frac{k(k+1)}{2})]$ similaire.

Carrés et puissances supérieures

Pour tout $[n,k]_q$-code C on a

$$\dim(C^{\langle 2\rangle}) \leq \min(n, \tfrac{k(k+1)}{2})$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
On s'attend à avoir égalité pour C aléatoire.
Et en effet, Cascudo-Cramer-Mirandola-Zémor ont donné une majoration sur $\mathbb{P}[\dim(C^{\langle 2\rangle}) < \min(n, \frac{k(k+1)}{2})]$ similaire.

De même pour tout $s \geq 2$,

$$\dim(C^{\langle s\rangle}) \leq \min(n, \tbinom{k+s-1}{s}).$$

Carrés et puissances supérieures

Pour tout $[n,k]_q$-code C on a

$$\dim(C^{\langle 2\rangle}) \leq \min(n, \tfrac{k(k+1)}{2})$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
On s'attend à avoir égalité pour C aléatoire.
Et en effet, Cascudo-Cramer-Mirandola-Zémor ont donné une majoration sur $\mathbb{P}[\dim(C^{\langle 2\rangle}) < \min(n, \frac{k(k+1)}{2})]$ similaire.

De même pour tout $s \geq 2$,

$$\dim(C^{\langle s\rangle}) \leq \min(n, \tbinom{k+s-1}{s}).$$

Piège !

Pour $s > q$, on a : $\dim(C^{\langle s\rangle}) < \binom{k+s-1}{s}$ toujours stricte.

Carrés et puissances supérieures

Pour tout $[n,k]_q$-code C on a

$$\dim(C^{\langle 2\rangle}) \leq \min(n, \tfrac{k(k+1)}{2})$$

(preuve : $C = \langle \mathbf{c}_i \rangle_{1\leq i\leq k} \implies C^{\langle 2\rangle} = \langle \mathbf{c}_i * \mathbf{c}_j \rangle_{1\leq i\leq j\leq k}$).
On s'attend à avoir égalité pour C aléatoire.
Et en effet, Cascudo-Cramer-Mirandola-Zémor ont donné une majoration sur $\mathbb{P}[\dim(C^{\langle 2\rangle}) < \min(n, \frac{k(k+1)}{2})]$ similaire.

De même pour tout $s \geq 2$,

$$\dim(C^{\langle s\rangle}) \leq \min(n, \tbinom{k+s-1}{s}).$$

Piège !

Pour $s > q$, on a : $\dim(C^{\langle s\rangle}) < \tbinom{k+s-1}{s}$ toujours stricte.

Raison : $C^s \xrightarrow{*} C^{\langle s\rangle}$ est "Frobenius-symétrique". D'où

$$\dim(C^{\langle s\rangle}) \leq \min(n, \chi_q(k,s))$$

où $\chi_q(k,s) = \dim(\mathbb{F}_q[t_1,\ldots,t_k]/(t_i^q t_j - t_i t_j^q))_s < \tbinom{k+s-1}{s}$.

À l'autre extrême

Reed-Solomon : $\dim(C * C') = \dim(C) + \dim(C') - 1$. "Moralement" ça devrait être le cas minimal. Problème : dégénérescences possibles...

À l'autre extrême

Reed-Solomon : $\dim(C * C') = \dim(C) + \dim(C') - 1$. "Moralement" ça devrait être le cas minimal. Problème : dégénérescences possibles...

Notion d'algèbre stabilisatrice : pour $C \subseteq (\mathbb{F}_q)^n$ de support plein,

$$\mathscr{A}(C) = \{\mathbf{a} \in (\mathbb{F}_q)^n \,;\, C * \mathbf{a} \subseteq C\}.$$

Propriétés :

- $\mathscr{A}(C) = \bigoplus_i \langle \mathbf{1}_{\mathrm{Supp}(C_i)} \rangle$, où C_i composantes indécomposables de C
- $\mathscr{A}(C)^\times \subseteq \mathrm{Aut}(C)$ sous-groupe distingué "diagonal"
- $\mathscr{A}(C) = (C * C^\perp)^\perp$.

À l'autre extrême

Reed-Solomon : $\dim(C * C') = \dim(C) + \dim(C') - 1$. "Moralement" ça devrait être le cas minimal. Problème : dégénérescences possibles...

Notion d'algèbre stabilisatrice : pour $C \subseteq (\mathbb{F}_q)^n$ de support plein,

$$\mathscr{A}(C) = \{\mathbf{a} \in (\mathbb{F}_q)^n \,;\, C * \mathbf{a} \subseteq C\}.$$

Propriétés :

- $\mathscr{A}(C) = \bigoplus_i \langle \mathbf{1}_{\mathrm{Supp}(C_i)} \rangle$, où C_i composantes indécomposables de C
- $\mathscr{A}(C)^\times \subseteq \mathrm{Aut}(C)$ sous-groupe distingué "diagonal"
- $\mathscr{A}(C) = (C * C^\perp)^\perp$.

Théorème (Mirandola-Zémor)

$$\dim(C * C') \geq \dim(C) + \dim(C') - \dim(\mathscr{A}(C * C'))$$

C'est l'exact analogue du théorème de Kneser en combinatoire additive : $|A + B| \geq |A| + |B| - |\mathrm{Stab}(A + B)|$. Preuve similaire, par "échange".

Partie 3
Dimension et distance

Définition

Fonctions fondamentales de la théorie des codes en blocs linéaires :

$$a_q(n,d) = \max\{k \geq 0\,;\ \exists C \subseteq (\mathbb{F}_q)^n,\ \dim(C) = k,\ \mathrm{d}_{\min}(C) \geq d\}$$

$$\alpha_q(\delta) = \limsup_{n\to\infty} \frac{a_q(n, \lfloor \delta n \rfloor)}{n}$$

Définition

Fonctions fondamentales généralisées :

$$a_q^{\langle s \rangle}(n,d) = \max\{k \geq 0\,;\ \exists C \subseteq (\mathbb{F}_q)^n,\ \dim(C) = k,\ \mathrm{d}_{\min}(C^{\langle s \rangle}) \geq d\}$$

$$\alpha_q^{\langle s \rangle}(\delta) = \limsup_{n \to \infty} \frac{a_q^{\langle s \rangle}(n, \lfloor \delta n \rfloor)}{n}$$

Définition

Fonctions fondamentales généralisées :

$$a_q^{\langle s \rangle}(n,d) = \max\{k \geq 0\,;\ \exists C \subseteq (\mathbb{F}_q)^n,\ \dim(C) = k,\ \mathrm{d}_{\min}(C^{\langle s \rangle}) \geq d\}$$

$$\alpha_q^{\langle s \rangle}(\delta) = \limsup_{n \to \infty} \frac{a_q^{\langle s \rangle}(n, \lfloor \delta n \rfloor)}{n}$$

ce qui motive aussi :

$$\tau(q) = \sup\{s \in \mathbb{N} \,|\, \alpha_q^{\langle s \rangle} \not\equiv 0\}$$

le supremum (éventuellement $+\infty$?) des s tels qu'il existe des codes *asymptotiquement bons* C_i sur $\mathbb{F}_q$ dont les puissances s-ièmes $C_i^{\langle s \rangle}$ soient aussi *asymptotiquement bonnes* :

$$\liminf_i\ \mathrm{R}(C_i) > 0 \qquad \text{et} \qquad \liminf_i\ \delta(C_i^{\langle s \rangle}) > 0.$$

Définition

Fonctions fondamentales généralisées :

$$a_q^{\langle s \rangle}(n,d) = \max\{k \geq 0\,;\ \exists C \subseteq (\mathbb{F}_q)^n,\ \dim(C) = k,\ \mathrm{d_{min}}(C^{\langle s \rangle}) \geq d\}$$

$$\alpha_q^{\langle s \rangle}(\delta) = \limsup_{n \to \infty} \frac{a_q^{\langle s \rangle}(n, \lfloor \delta n \rfloor)}{n}$$

ce qui motive aussi :

$$\tau(q) = \sup\{s \in \mathbb{N} \,|\, \alpha_q^{\langle s \rangle} \not\equiv 0\}$$

le supremum (éventuellement $+\infty$?) des s tels qu'il existe des codes *asymptotiquement bons* C_i sur $\mathbb{F}_q$ dont les puissances s-ièmes $C_i^{\langle s \rangle}$ soient aussi *asymptotiquement bonnes* :

$$\liminf_i\ \mathrm{R}(C_i) > 0 \qquad \text{et} \qquad \liminf_i\ \delta(C_i^{\langle s \rangle}) > 0.$$

Remarque :

$$t \geq s \qquad \Longrightarrow \qquad a_q^{\langle t \rangle} \leq a_q^{\langle s \rangle}.$$

Une borne sup

Théorème : "Singleton produit" *(rem : $C' = \mathbb{1} \rightarrow$ Singleton classique)*

Pour tous $C = [n, k]$-code et $C' = [n, k']$-code de supports non disjoints,

$$\mathrm{d}_{\min}(C * C') \leq \max(1,\, n - k - k' + 2).$$

Une borne sup

Théorème : "Singleton produit" *(rem : $C' = \mathbb{1} \rightarrow$ Singleton classique)*

Pour tous $C = [n, k]$-code et $C' = [n, k']$-code de supports non disjoints,

$$\mathrm{d}_{\min}(C * C') \leq \max(1,\, n - k - k' + 2).$$

Première preuve : $\dim(C * (C * C')^{\perp}) \geq \dim(C) + \mathrm{d}^{\perp}((C * C')^{\perp}) - 2$ & $C' \perp C * (C * C')^{\perp}$. $\square$

Une borne sup

Théorème : "Singleton produit" *(rem : $C' = \mathbb{1} \to$ Singleton classique)*

Pour tous $C = [n, k]$-code et $C' = [n, k']$-code de supports non disjoints,

$$\mathrm{d}_{\min}(C * C') \leq \max(1,\, n - k - k' + 2).$$

Première preuve : $\dim(C * (C * C')^{\perp}) \geq \dim(C) + \mathrm{d}^{\perp}((C * C')^{\perp}) - 2$ & $C' \perp C * (C * C')^{\perp}$. $\square$

$\to$ Amélioration par Mirandola-Zémor : cas d'égalité = essentiellement les Reed-Solomon (analogue de Vosper : cas d'égalité pour Cauchy-Kneser $|A + B| = |A| + |B| - 1$ dans $\mathbb{Z}/p\mathbb{Z}$ = suites arithmétiques).

Une borne sup

Théorème : "Singleton produit" *(rem : $C' = \mathbb{1} \to$ Singleton classique)*

Pour tous $C = [n, k]$-code et $C' = [n, k']$-code de supports non disjoints,

$$\mathrm{d}_{\min}(C * C') \leq \max(1,\, n - k - k' + 2).$$

Première preuve : $\dim(C * (C * C')^{\perp}) \geq \dim(C) + \mathrm{d}^{\perp}((C * C')^{\perp}) - 2$ & $C' \perp C * (C * C')^{\perp}$. $\square$

$\to$ Amélioration par Mirandola-Zémor : cas d'égalité = essentiellement les Reed-Solomon (analogue de Vosper : cas d'égalité pour Cauchy-Kneser $|A + B| = |A| + |B| - 1$ dans $\mathbb{Z}/p\mathbb{Z}$ = suites arithmétiques).

Seconde preuve (d'après une idée de N. Kashyap) : construction explicite d'un mot de petit poids. Résultat plus fort :

$\to$ sous forme produit

$\to$ se généralise au produit d'un nombre arbitraire de codes.

Une borne sup

Théorème : "Singleton produit" *(rem : $C' = \mathbb{1} \to$ Singleton classique)*

Pour tous $C = [n, k]$-code et $C' = [n, k']$-code de supports non disjoints,

$$\mathrm{d}_{\min}(C * C') \leq \max(1,\, n - k - k' + 2).$$

Première preuve : $\dim(C * (C * C')^{\perp}) \geq \dim(C) + \mathrm{d}^{\perp}((C * C')^{\perp}) - 2$ & $C' \perp C * (C * C')^{\perp}$. $\square$

$\to$ Amélioration par Mirandola-Zémor : cas d'égalité = essentiellement les Reed-Solomon (analogue de Vosper : cas d'égalité pour Cauchy-Kneser $|A + B| = |A| + |B| - 1$ dans $\mathbb{Z}/p\mathbb{Z}$ = suites arithmétiques).

Seconde preuve (d'après une idée de N. Kashyap) : construction explicite d'un mot de petit poids. Résultat plus fort :

$\to$ sous forme produit

$\to$ se généralise au produit d'un nombre arbitraire de codes.

Corollaire

$$\alpha_q^{\langle s \rangle}(\delta) \leq \frac{1 - \delta}{s}.$$

Borne inf (construction) pour q grand : codes géométriques

Théorème

$$\alpha_q^{\langle s \rangle}(\delta) \geq \frac{1-\delta}{s} - \frac{1}{A(q)}$$

où $A(q)$ est la *constante d'Ihara* sur le nombre de points des courbes sur $\mathbb{F}_q$.
Rappel : $A(q) \leq q^{1/2} - 1$ (Drinfeld-Vladut), avec égalité pour q carré.

Borne inf (construction) pour q grand : codes géométriques

Théorème

$$\alpha_q^{\langle s \rangle}(\delta) \geq \frac{1-\delta}{s} - \frac{1}{A(q)}$$

où $A(q)$ est la *constante d'Ihara* sur le nombre de points des courbes sur $\mathbb{F}_q$.
Rappel : $A(q) \leq q^{1/2} - 1$ (Drinfeld-Vladut), avec égalité pour q carré.

Preuve repose sur

$$C(D,G)^{\langle s \rangle} \subseteq C(sD,G)$$

auxquels on applique les estimées de Goppa : pour $g \leq \deg(D) < n$,

$$\dim(C(D,G)) = l(D) \geq \deg(D) + 1 - g$$

$$\mathrm{d}_{\min}(C(D,G)) \geq n - \deg(D).$$

Borne inf (construction) pour q grand : codes géométriques

Théorème

$$\alpha_q^{\langle s \rangle}(\delta) \geq \frac{1-\delta}{s} - \frac{1}{A(q)}$$

où $A(q)$ est la *constante d'Ihara* sur le nombre de points des courbes sur $\mathbb{F}_q$.
Rappel : $A(q) \leq q^{1/2} - 1$ (Drinfeld-Vladut), avec égalité pour q carré.

Preuve repose sur

$$C(D,G)^{\langle s \rangle} \subseteq C(sD,G)$$

auxquels on applique les estimées de Goppa : pour $g \leq \deg(D) < n$,

$$\dim(C(D,G)) = l(D) \geq \deg(D) + 1 - g$$

$$\mathrm{d}_{\min}(C(D,G)) \geq n - \deg(D).$$

Corollaire

$$\tau(q) \geq \lceil A(q) \rceil - 1$$

Borne inf pour q petit (typiquement $q = 2$) : concaténation

- $C = [n, k]$-code sur $\mathbb{F}_{q^r}$
- $\varphi : \mathbb{F}_{q^r} \hookrightarrow (\mathbb{F}_q)^m$ injective $\mathbb{F}_q$-linéaire

$\rightarrow$ code concaténé

$$\underline{\varphi}(C) = \{\underline{\varphi}(\mathbf{c}) = (\varphi(c_1), \ldots, \varphi(c_n))\,;\ \mathbf{c} = (c_1, \ldots, c_n) \in C\}$$

de paramètres $[mn, kr]$ sur $\mathbb{F}_q$ (identifier $((\mathbb{F}_q)^m)^n = (\mathbb{F}_q)^{mn}$).

Borne inf pour q petit (typiquement $q = 2$) : concaténation

- $C = [n, k]$-code sur $\mathbb{F}_{q^r}$
- $\varphi : \mathbb{F}_{q^r} \hookrightarrow (\mathbb{F}_q)^m$ injective $\mathbb{F}_q$-linéaire

$\rightarrow$ code concaténé

$$\underline{\varphi}(C) = \{\underline{\varphi}(\mathbf{c}) = (\varphi(c_1), \ldots, \varphi(c_n))\,;\ \mathbf{c} = (c_1, \ldots, c_n) \in C\}$$

de paramètres $[mn, kr]$ sur $\mathbb{F}_q$ (identifier $((\mathbb{F}_q)^m)^n = (\mathbb{F}_q)^{mn}$).

Borne inf pour q grand + concaténation (+ un peu de travail) vont donner :

Théorème

$$\alpha_2^{\langle 2\rangle}(\delta) \geq \frac{74}{39525} - \frac{9}{17}\,\delta \approx 0{,}001872 - 0{,}5294\,\delta$$

d'où

$$\tau(2) \geq 2$$

et plus généralement $\tau(q) \geq 2$ pour tout q : *il existe des codes q-aires asymptotiquement bons de carrés asymptotiquement bons*.

On part de C sur $\mathbb{F}_{q^r}$ avec contrôle sur $\mathrm{d}_{\min}(C^{\langle 2\rangle})$, on concatène avec $\varphi : \mathbb{F}_{q^r} \longrightarrow (\mathbb{F}_q)^m$, comment contrôler $\mathrm{d}_{\min}(\underline{\varphi}(C)^{\langle 2\rangle})$?

$$\begin{array}{ccc} C \times C & \xrightarrow{*,\mathbb{F}_{q^r}} & C^{\langle 2\rangle} \\ \Big\downarrow{\scriptstyle \underline{\varphi}\times\underline{\varphi}} & & \\ \underline{\varphi}(C) \times \underline{\varphi}(C) & \xrightarrow{*,\mathbb{F}_q} & \underline{\varphi}(C)^{\langle 2\rangle} \end{array}$$

On part de C sur $\mathbb{F}_{q^r}$ avec contrôle sur $\mathrm{d}_{\min}(C^{\langle 2\rangle})$, on concatène avec $\varphi : \mathbb{F}_{q^r} \longrightarrow (\mathbb{F}_q)^m$, comment contrôler $\mathrm{d}_{\min}(\underline{\varphi}(C)^{\langle 2\rangle})$?

$$\begin{array}{ccc} C \times C & \xrightarrow{*,\mathbb{F}_{q^r}} & C^{\langle 2\rangle} \\ \Big\downarrow{\scriptstyle \underline{\varphi}\times\underline{\varphi}} & & \Big\uparrow{\scriptstyle \underline{\theta}} \\ \underline{\varphi}(C) \times \underline{\varphi}(C) & \xrightarrow{*,\mathbb{F}_q} & \underline{\varphi}(C)^{\langle 2\rangle} \end{array}$$

Solution : prendre (φ, θ) définissant un algorithme bilinéaire !

$$\begin{array}{ccc} \mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \longrightarrow & \mathbb{F}_{q^r} \\ \Big\downarrow{\scriptstyle \varphi\times\varphi} & & \Big\uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^m \times (\mathbb{F}_q)^m & \longrightarrow & (\mathbb{F}_q)^m \end{array}$$

Si $\mathbf{c} \in \underline{\varphi}(C)^{\langle 2\rangle}$ de poids w, alors au plus w blocs sont non nuls
$\rightarrow \underline{\theta}(\mathbf{c}) \in C^{\langle 2\rangle}$ de poids au plus w
$\rightarrow \mathrm{d}_{\min}(\underline{\varphi}(C)^{\langle 2\rangle}) \geq \mathrm{d}_{\min}(C^{\langle 2\rangle})$. $\square$

Problème :

Problème : ... et si $\underline{\theta}(\mathbf{c}) = \mathbf{0}$!?

Problème : ... et si $\underline{\theta}(\mathbf{c}) = \mathbf{0}$!?

Comprendre $\ker(\theta)$?

Pour se simplifier la vie on prendra φ universelle (donc $m = \frac{r(r+1)}{2}$)

$\rightarrow$ comprendre $\ker(S^2_{\mathbb{F}_q}\mathbb{F}_{q^r} \twoheadrightarrow \mathbb{F}_{q^r})$?

Comprendre $\ker(\theta)$?

Pour se simplifier la vie on prendra φ universelle (donc $m = \frac{r(r+1)}{2}$)

$$\rightarrow \text{ comprendre } \ker(S^2_{\mathbb{F}_q}\mathbb{F}_{q^r} \twoheadrightarrow \mathbb{F}_{q^r}) \text{ ?}$$

Exemple de $\varphi = (\varphi_1, \ldots, \varphi_{\frac{r(r+1)}{2}}) : \mathbb{F}_{q^r} \rightarrow (\mathbb{F}_q)^{\frac{r(r+1)}{2}}$ universelle :

- soit $a_1, \ldots, a_r$ une base de $\mathbb{F}_{q^r}$ sur $\mathbb{F}_q$
- alors les $\lambda_i : x \mapsto \mathrm{Tr}(a_i x)$ forment une base de l'espace dual $(\mathbb{F}_{q^r})^\vee$
- pose $\left\{\varphi_1, \ldots, \varphi_{\frac{r(r+1)}{2}}\right\} = \{\lambda_i\}_{1\leq i\leq r} \cup \{\lambda_i + \lambda_j\}_{1\leq i<j\leq r}$
- alors les $\varphi_u^{\otimes 2} : (x, y) \mapsto \varphi_u(x)\varphi_u(y)$ forment une base de l'espace des formes $\mathbb{F}_q$-bilinéaires symétriques sur $\mathbb{F}_{q^r}$.

Comprendre $\ker(\theta)$?

Pour se simplifier la vie on prendra φ universelle (donc $m = \frac{r(r+1)}{2}$)

$$\rightarrow \text{ comprendre } \ker(S^2_{\mathbb{F}_q}\mathbb{F}_{q^r} \twoheadrightarrow \mathbb{F}_{q^r}) \text{ ?}$$

Exemple de $\varphi = (\varphi_1, \ldots, \varphi_{\frac{r(r+1)}{2}}) : \mathbb{F}_{q^r} \rightarrow (\mathbb{F}_q)^{\frac{r(r+1)}{2}}$ universelle :

- soit $a_1, \ldots, a_r$ une base de $\mathbb{F}_{q^r}$ sur $\mathbb{F}_q$
- alors les $\lambda_i : x \mapsto \mathrm{Tr}(a_i x)$ forment une base de l'espace dual $(\mathbb{F}_{q^r})^\vee$
- pose $\left\{\varphi_1, \ldots, \varphi_{\frac{r(r+1)}{2}}\right\} = \{\lambda_i\}_{1\leq i\leq r} \cup \{\lambda_i + \lambda_j\}_{1\leq i<j\leq r}$
- alors les $\varphi_u^{\otimes 2} : (x, y) \mapsto \varphi_u(x)\varphi_u(y)$ forment une base de l'espace des formes $\mathbb{F}_q$-bilinéaires symétriques sur $\mathbb{F}_{q^r}$.

Dans une base convenable, la matrice de φ (= la matrice génératrice du code interne de la concaténation) est de la forme (ici pour $r = 4$)

$$\mathbf{G}_\varphi = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

et en effet, les $\mathbf{p}_u\mathbf{p}_u^T$, pour $\mathbf{p}_u$ colonne de $\mathbf{G}_\varphi$, forment bien une base de l'espace des matrices symétriques de taille r.

Formule-clé : posant $a = a_i$ ou $a = a_i + a_j$, $\varphi_u^{\otimes 2}$ s'écrit

$$\begin{aligned}\mathrm{Tr}(ax)\,\mathrm{Tr}(ay) &= (ax+a^q x^q+\cdots+a^{q^{r-1}}x^{q^{r-1}})(ay+a^q y^q+\cdots+a^{q^{r-1}}y^{q^{r-1}}) \\ &= \mathrm{Tr}(a^2xy) + \sum_{1\le j\le \lfloor r/2\rfloor} \mathrm{Tr}(a^{1+q^j}(xy^{q^j}+x^{q^j}y))\end{aligned}$$

(les traces sont de $\mathbb{F}_{q^r}$ vers $\mathbb{F}_q$, sauf éventuellement pour r pair la dernière est de $\mathbb{F}_{q^{r/2}}$ vers $\mathbb{F}_q$).

$\rightarrow$ Pose

$$m_0(x,y) = xy$$

multiplication usuelle dans $\mathbb{F}_{q^r}$, et pour $j \ge 1$

$$m_j(x,y) = xy^{q^j} + x^{q^j}y$$

j-ième multiplication tordue (rem : polynômes bilinéarisés symétriques). Alors les traces des $m_0, \ldots, m_{\lfloor r/2\rfloor}$ vont donner une autre base de l'espace des formes $\mathbb{F}_q$-bilinéaires symétriques sur $\mathbb{F}_{q^r}$.

En conséquence : il existe une (unique) θ $\mathbb{F}_q$-linéaire inversible telle que

$$\begin{array}{ccc} \mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \xrightarrow{(m_0,m_1,\ldots,m_{r/2})} & \left(\mathbb{F}_{q^r}\right)^{\frac{r+1}{2}} \\ \Big\downarrow{\scriptstyle \varphi\times\varphi} & & \Big\uparrow{\scriptstyle \theta,\simeq} \\ \left(\mathbb{F}_q\right)^{\frac{r(r+1)}{2}} \times \left(\mathbb{F}_q\right)^{\frac{r(r+1)}{2}} & \xrightarrow{*,\mathbb{F}_q} & \left(\mathbb{F}_q\right)^{\frac{r(r+1)}{2}} \end{array}$$

En conséquence : il existe une (unique) θ $\mathbb{F}_q$-linéaire inversible telle que

$$\begin{array}{ccc}
\mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \xrightarrow{(m_0, m_1, \ldots, m_{r/2})} & (\mathbb{F}_{q^r})^{\frac{r+1}{2}} \\
\varphi \times \varphi \downarrow & & \uparrow \theta, \simeq \\
(\mathbb{F}_q)^{\frac{r(r+1)}{2}} \times (\mathbb{F}_q)^{\frac{r(r+1)}{2}} & \xrightarrow{*, \mathbb{F}_q} & (\mathbb{F}_q)^{\frac{r(r+1)}{2}}
\end{array}$$

donc

$$\begin{array}{ccc}
C \times C & \xrightarrow{(\underline{m}_0, \underline{m}_1, \ldots, \underline{m}_{r/2})} & C^{\langle 2 \rangle} \oplus C^{\langle 1+q \rangle} \oplus \cdots \oplus C^{\langle 1+q^{r/2} \rangle} \\
\underline{\varphi} \times \underline{\varphi} \downarrow & & \uparrow \underline{\theta}, \hookrightarrow \\
\underline{\varphi}(C) \times \underline{\varphi}(C) & \xrightarrow{*, \mathbb{F}_q} & \underline{\varphi}(C)^{\langle 2 \rangle}
\end{array}$$

En conséquence : il existe une (unique) θ $\mathbb{F}_q$-linéaire inversible telle que

$$\begin{array}{ccc} \mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \xrightarrow{(m_0,m_1,\ldots,m_{r/2})} & (\mathbb{F}_{q^r})^{\frac{r+1}{2}} \\ \Big\downarrow{\scriptstyle \varphi\times\varphi} & & \Big\uparrow{\scriptstyle \theta,\simeq} \\ (\mathbb{F}_q)^{\frac{r(r+1)}{2}} \times (\mathbb{F}_q)^{\frac{r(r+1)}{2}} & \xrightarrow{*,\mathbb{F}_q} & (\mathbb{F}_q)^{\frac{r(r+1)}{2}} \end{array}$$

donc

$$\begin{array}{ccc} C \times C & \xrightarrow{(\underline{m}_0,\underline{m}_1,\ldots,\underline{m}_{r/2})} & C^{\langle 2\rangle} \oplus C^{\langle 1+q\rangle} \oplus \cdots \oplus C^{\langle 1+q^{r/2}\rangle} \\ \Big\downarrow{\scriptstyle \underline{\varphi}\times\underline{\varphi}} & & \Big\uparrow{\scriptstyle \underline{\theta},\hookrightarrow} \\ \underline{\varphi}(C) \times \underline{\varphi}(C) & \xrightarrow{*,\mathbb{F}_q} & \underline{\varphi}(C)^{\langle 2\rangle} \end{array}$$

et cette fois l'injectivité de θ donne bien

$$\mathrm{d}_{\min}(\underline{\varphi}(C)^{\langle 2\rangle}) \geq \mathrm{d}_{\min}(C^{\langle 1+q^{r/2}\rangle}).$$

Bilan (disons pour $q = p$ premier) :

- on veut C sur $\mathbb{F}_{q^r}$ de puissances jusqu'à l'ordre $1 + q^{r/2}$ bonnes

Bilan (disons pour $q = p$ premier) :

- on veut C sur $\mathbb{F}_{q^r}$ de puissances jusqu'à l'ordre $1 + q^{r/2}$ bonnes
- avec les codes géométriques on sait faire jusqu'à l'ordre $\lceil A(q^r) \rceil - 1$

Bilan (disons pour $q = p$ premier) :

- on veut C sur $\mathbb{F}_{q^r}$ de puissances jusqu'à l'ordre $1 + q^{r/2}$ bonnes
- avec les codes géométriques on sait faire jusqu'à l'ordre $\lceil A(q^r) \rceil - 1$
- $A(q^r) \leq q^{r/2} - 1$ (Drinfeld-Vladut), avec égalité ssi r pair.

Bilan (disons pour $q = p$ premier) :

- on veut C sur $\mathbb{F}_{q^r}$ de puissances jusqu'à l'ordre $1 + q^{r/2}$ bonnes
- avec les codes géométriques on sait faire jusqu'à l'ordre $\lceil A(q^r) \rceil - 1$
- $A(q^r) \leq q^{r/2} - 1$ (Drinfeld-Vladut), avec égalité ssi r pair.

Bilan (disons pour $q = p$ premier) :

- on veut C sur $\mathbb{F}_{q^r}$ de puissances jusqu'à l'ordre $1 + q^{r/2}$ bonnes
- avec les codes géométriques on sait faire jusqu'à l'ordre $\lceil A(q^r) \rceil - 1$
- $A(q^r) \leq q^{r/2} - 1$ (Drinfeld-Vladut), avec égalité ssi r pair.

Issue de secours : en fait on veut les puissances jusqu'à l'ordre $1 + q^{\lfloor r/2 \rfloor}$.

Garcia-Stichtenoth-Bassa-Beleen : pour $r \to \infty$ impair,

$$(\frac{2q}{q+1} + o(1))q^{\lfloor r/2 \rfloor} \ \leq \ A(q^r) \ \leq \ q^{r/2} - 1.$$

Issue de secours : en fait on veut les puissances jusqu'à l'ordre $1 + q^{\lfloor r/2 \rfloor}$.
Garcia-Stichtenoth-Bassa-Beleen : pour $r \to \infty$ impair,

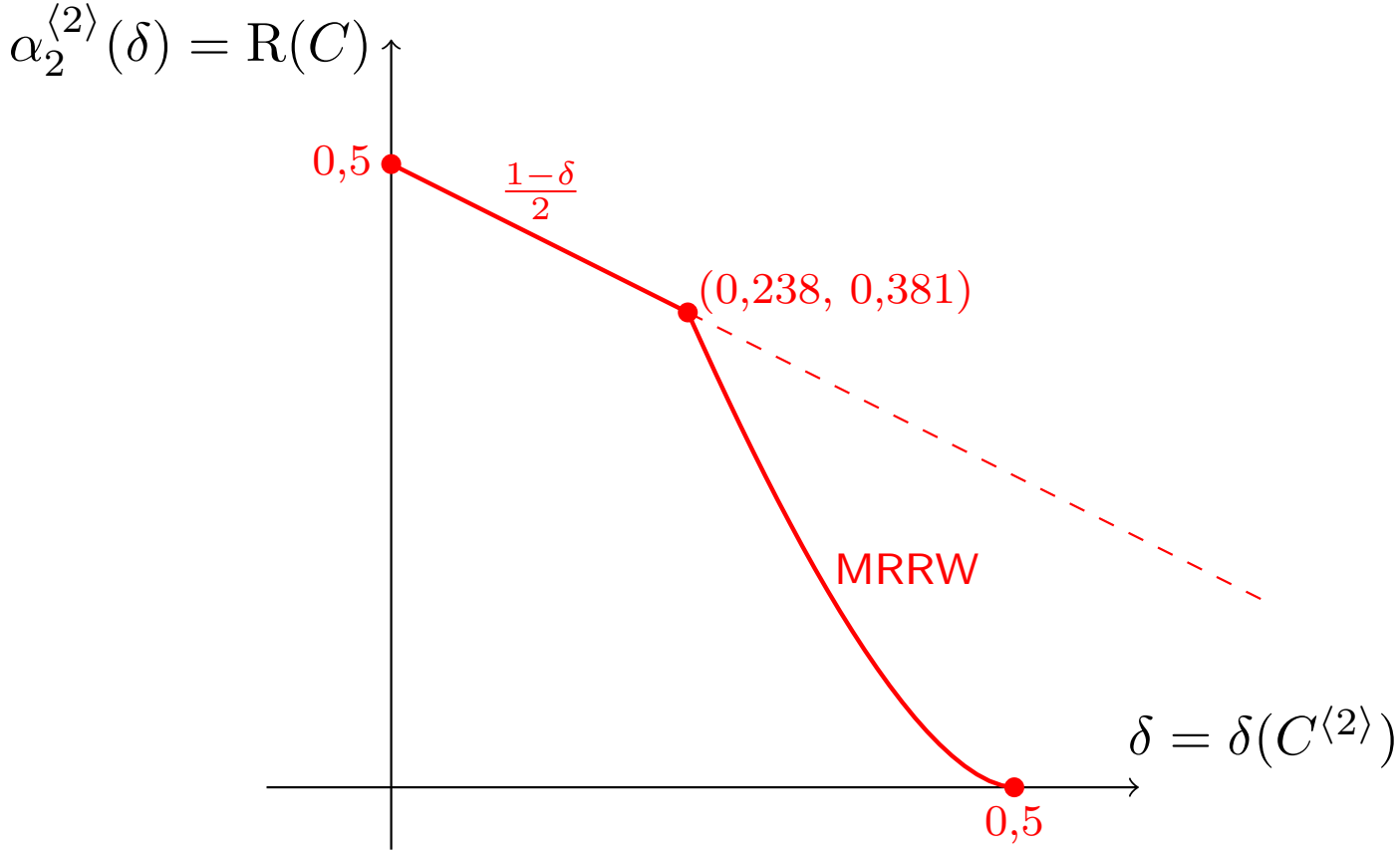
$$(\frac{2q}{q+1} + o(1))q^{\lfloor r/2 \rfloor} \ \leq \ A(q^r) \ \leq \ q^{r/2} - 1.$$

Application numérique : $q = 2, r = 9$; GSBB : $A(512) \geq 465/23 \approx 20{,}217$;
codes géométriques : $\alpha_{512}^{\langle 17 \rangle}(\delta) \geq \frac{1-\delta}{17} - \frac{1}{A(512)}$; code interne $\varphi = [45, 9]_2$
$\to \alpha_2^{\langle 2 \rangle}(\delta) \geq \frac{1}{5}\alpha_{512}^{\langle 17 \rangle}(45\delta) \geq \frac{74}{39525} - \frac{9}{17}\,\delta \ \approx \ 0{,}001872 - 0{,}5294\,\delta.$

Issue de secours : en fait on veut les puissances jusqu'à l'ordre $1 + q^{\lfloor r/2 \rfloor}$.
Garcia-Stichtenoth-Bassa-Beleen : pour $r \to \infty$ impair,

$$(\frac{2q}{q+1} + o(1))q^{\lfloor r/2 \rfloor} \ \leq \ A(q^r) \ \leq \ q^{r/2} - 1.$$

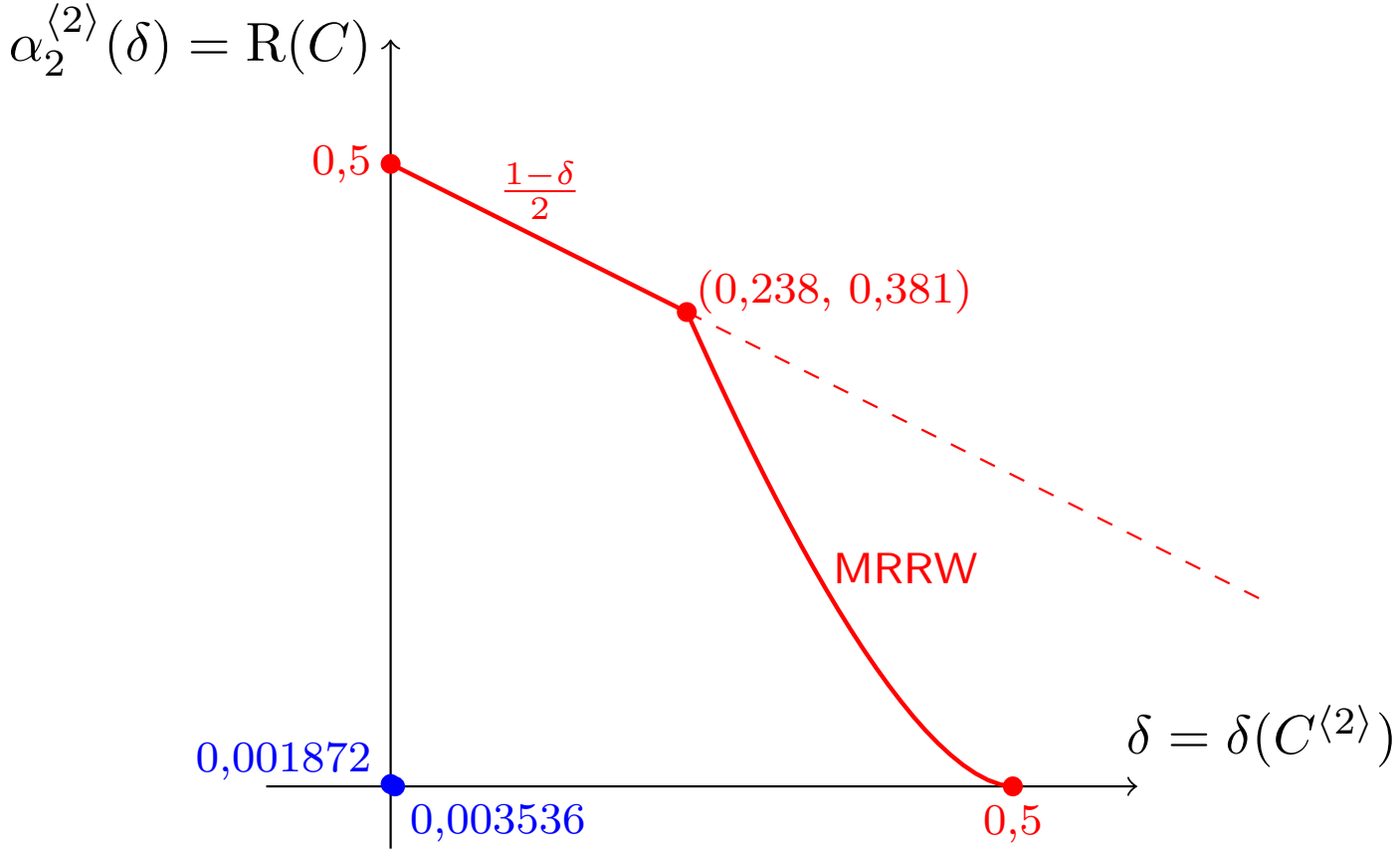
Application numérique : $q = 2, r = 9$; GSBB : $A(512) \geq 465/23 \approx 20{,}217$;
codes géométriques : $\alpha_{512}^{\langle 17 \rangle}(\delta) \geq \frac{1-\delta}{17} - \frac{1}{A(512)}$; code interne $\varphi = [45, 9]_2$
$\to \alpha_2^{\langle 2 \rangle}(\delta) \geq \frac{1}{5}\alpha_{512}^{\langle 17 \rangle}(45\delta) \geq \frac{74}{39525} - \frac{9}{17}\,\delta \ \approx \ 0{,}001872 - 0{,}5294\,\delta.$



Issue de secours : en fait on veut les puissances jusqu'à l'ordre $1 + q^{\lfloor r/2 \rfloor}$.
Garcia-Stichtenoth-Bassa-Beleen : pour $r \to \infty$ impair,

$$(\frac{2q}{q+1} + o(1))q^{\lfloor r/2 \rfloor} \ \leq \ A(q^r) \ \leq \ q^{r/2} - 1.$$

Application numérique : $q = 2, r = 9$; GSBB : $A(512) \geq 465/23 \approx 20{,}217$;
codes géométriques : $\alpha_{512}^{\langle 17 \rangle}(\delta) \geq \frac{1-\delta}{17} - \frac{1}{A(512)}$; code interne $\varphi = [45, 9]_2$
$\to \alpha_2^{\langle 2 \rangle}(\delta) \geq \frac{1}{5}\alpha_{512}^{\langle 17 \rangle}(45\delta) \geq \frac{74}{39525} - \frac{9}{17}\,\delta \ \approx \ 0{,}001872 - 0{,}5294\,\delta.$



Quelques questions ouvertes

- On sait que les codes aléatoires sont asymptotiquement bons, et même qu'ils atteignent la borne de Varshamov-Gilbert $R = 1 - H(\delta)$.

Les produits de codes aléatoires, ou les carrés de codes aléatoires, sont-ils asymptotiquement bons ?
Atteignent-ils la borne de Varshamov-Gilbert ?

Rem : si on remplace $*$ par $\otimes$, la première question a une réponse positive, la seconde négative.

Quelques questions ouvertes

- On sait que les codes aléatoires sont asymptotiquement bons, et même qu'ils atteignent la borne de Varshamov-Gilbert $R = 1 - H(\delta)$.

Les produits de codes aléatoires, ou les carrés de codes aléatoires, sont-ils asymptotiquement bons ?
Atteignent-ils la borne de Varshamov-Gilbert ?

Rem : si on remplace $*$ par $\otimes$, la première question a une réponse positive, la seconde négative.

- Passage aux puissances supérieures :

Existe-t-il des codes binaires asymptotiquement bons dont les cubes sont asymptotiquement bons ? Les puissances quatrièmes ? Jusqu'où peut-on continuer ?
Plus généralement peut-on calculer la constante $\tau(q)$ pour certains q ? Ou même juste déterminer si elle est finie ou infinie ?

Le mieux qu'on sache dire est : $\max(\lceil A(q) \rceil - 1,\, 2) \leq \tau(q) \leq +\infty$.

Quelques questions ouvertes

- On sait que les codes aléatoires sont asymptotiquement bons, et même qu'ils atteignent la borne de Varshamov-Gilbert $R = 1 - H(\delta)$.

Les produits de codes aléatoires, ou les carrés de codes aléatoires, sont-ils asymptotiquement bons ?
Atteignent-ils la borne de Varshamov-Gilbert ?

Rem : si on remplace $*$ par $\otimes$, la première question a une réponse positive, la seconde négative.

- Passage aux puissances supérieures :

Existe-t-il des codes binaires asymptotiquement bons dont les cubes sont asymptotiquement bons ? Les puissances quatrièmes ? Jusqu'où peut-on continuer ?
Plus généralement peut-on calculer la constante $\tau(q)$ pour certains q ? Ou même juste déterminer si elle est finie ou infinie ?

Le mieux qu'on sache dire est : $\max(\lceil A(q) \rceil - 1,\, 2) \leq \tau(q) \leq +\infty$.

- Avec application potentielle au partage de secret arithmétique :

Existe-t-il des codes binaires asymptotiquement bons, dont les carrés, et aussi les duaux, sont asymptotiquement bons ?

Rem : la concaténation tue la distance duale.

Normalement c'est fini
mais s'il reste encore deux minutes à meubler,
suit une dernière question-bonus.

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit
  $\to$ donner une borne uniforme sur le résultat.

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 0 = (7, 5, 3, 2, 1) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 1 = (0, 6, 4, 3, 2) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 2 = (1, 7, 5, 4, 3) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 3 = (2, 0, 6, 5, 4) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 4 = (3, 1, 7, 6, 5) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 5 = (4, 2, 0, 7, 6) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 6 = (5, 3, 1, 0, 7) > (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 7 = (6, 4, 2, 1, 0) < (6, 4, 3, 1, 0)$$

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 7 = (6, 4, 2, 1, 0) < (6, 4, 3, 1, 0)$$

J'ai une preuve "naturelle" mais un peu technique $\to$ faire plus *simple* ???

On travaille dans $E = (\mathbb{Z}/r\mathbb{Z})^s \simeq \{0, 1, \ldots, r-1\}^s$.

- Pré-ordre total : pour comparer deux s-uplets, on compare leurs plus grands éléments, en cas d'égalité on compare leurs seconds plus grands éléments, etc.
- Translation : $J = (j_1, \ldots, j_s) \in E$, $j \in \mathbb{Z}/r\mathbb{Z} \to J \boxplus j = (j_1 + j, \ldots, j_s + j)$.
- But : montrer que tout $J \in E$ admet un translaté suffisamment petit $\to$ donner une borne uniforme sur le résultat.

On pose $I_{\text{equi}} = \left(\left\lfloor \frac{(s-1)r}{s} \right\rfloor, \left\lfloor \frac{(s-2)r}{s} \right\rfloor, \ldots, \left\lfloor \frac{r}{s} \right\rfloor, 0 \right)$ (rem : minimal dans sa classe).

Lemme

Tout J admet un translaté tel que $J \boxplus j \leq I_{\text{equi}}$.

Exemple : $r = 8$, $s = 5$, $J = (7, 5, 3, 2, 1)$, $I_{\text{equi}} = (6, 4, 3, 1, 0)$

$$J \boxplus 7 = (6, 4, 2, 1, 0) < (6, 4, 3, 1, 0)$$

J'ai une preuve "naturelle" mais un peu technique $\to$ faire plus *simple* ???

Motivation : Pour étudier $\underline{\varphi}(C)^{\langle s \rangle}$ pour $s > 2$, un outil potentiellement utile est la double représentation des formes s-multilinéaires symétriques sur $\mathbb{F}_{q^r}$ au-dessus de $\mathbb{F}_q$:

- comme combinaisons de puissances tensorielles s-ièmes de formes linéaires
- comme traces de polynômes s-multilinéarisés.

Polynômes multilinéarisés : $M_J = x_1^{q^{j_1}} \cdots x_s^{q^{j_s}} : (\mathbb{F}_{q^r})^s \longrightarrow \mathbb{F}_{q^r}$, ou S_J son symétrisé...

On a intérêt à les choisir de degré aussi petit que possible.

Or la trace est invariante par Frobenius : $\mathrm{Tr}(M^{q^j}) = \mathrm{Tr}(M)$, et ce dernier agit par translation des exposants : $(M_J)^{q^j} = M_{J \boxplus j}$, $(S_J)^{q^j} = S_{J \boxplus j}$.