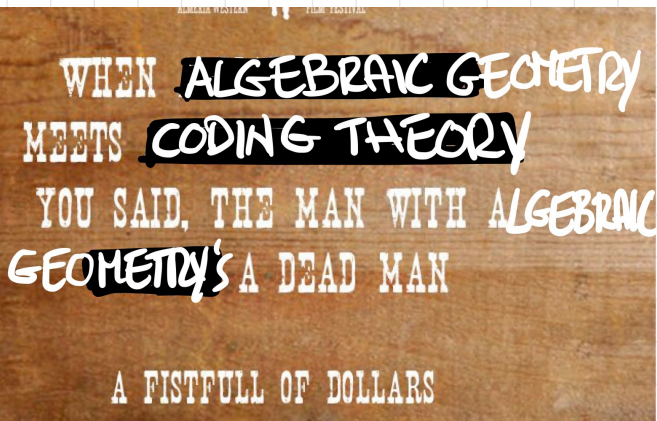


AG CODES: WHEN ALGEBRAIC GEOMETRY MEETS CODING THEORY

GT OISSILON - 18/12/2020 - Elena Berardini



JOYEUX
NOËL ☺



I - CODES LINÉAIRES

II - COURBES ALG / CORPS FINIS

III - CODES DE GOPPA

IV - UNE MOTIVATION & UNE GÉNÉRALISATION

I - CODES LINÉAIRES

A long time ago in a GT far,
far away....

Définitions Un code linéaire $\mathcal{C}$ est un $\mathbb{F}_q$ -s.e.v. de $\mathbb{F}_q^n$. Un $[[n, k, d]]$ -code linéaire est un code de :

- longueur n
- dimension k
- distance minimale d

DISTANCE MINIMALE:

$$\forall c \in \mathcal{C}, \quad w(c) := \#\{i \mid c_i \neq 0\}$$

"
($c_1, \dots, c_n$)

$$d_{\mathcal{C}} = \min_{c \in \mathcal{C} \setminus \{0\}} \{w(c)\} \in \mathbb{N}$$

Borne de Singleton: $k + d \leq n + 1$

$k + d = n + 1 \rightarrow$ MDS code !

SPOILER! $\mathcal{O}(X, D) = \text{Im}(\text{ev}(L(D)))$

$$\begin{aligned} \text{ev}: L(D) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \dots, f(P_n)) \end{aligned}$$

X - une courbe "symple"

D - un diviseur sur X

$L(D)$ - un espace vectoriel, appelé espace de Riemann-Roch

II - COURBES ALGÈBRIQUES / CORPS FINIS

Définition: Une courbe algébrique X est l'ensemble de zéros dans $\mathbb{P}_{\mathbb{F}_q}^n$ d'un système de polynômes homogènes à $n+1$ variables à coefficient dans $\mathbb{F}_q$ et irréductible sur $\mathbb{F}_q$. On notera g son genre.

→ la courbe est définie $\mathbb{F}_q$

→ la courbe est absolument irréductible

→ la courbe est projective

Définition: $X(\mathbb{F}_q)$ est l'ensemble des points rationnels sur X , c-à-d les points $P \in X$ t.q. $P = (a_0 : \dots : a_n)$ $a_i \in \mathbb{F}_q, \forall i$.

Définition: le corps des fonctions de X

$$\mathbb{F}_q(X) := \left\{ \frac{g}{h} \mid g, h \in \underbrace{\mathbb{F}_q[x_0, \dots, x_n]}_{I(X)}, \text{ homogènes, de même degré, } h \neq 0 \right\}$$

$$I(X) = \{ f \in \mathbb{F}_q[x_0, \dots, x_n] \mid f \text{ homogène et } f(P) = 0 \forall P \in X \}$$

DIVISEURS:

- Un diviseur D de X est un élément du $\mathbb{Z}$ -module libre engendré par les points de X , i.e. $D = \sum_{P \in X} n_P P$, $n_P \in \mathbb{Z}$ presque tous nuls
- $\text{Supp}(D) = \{ P \text{ t.q. } n_P \neq 0 \}$
- $\text{Div}(X)$ = ensemble des diviseurs sur X (graphe)
- $D = \sum_{P \in X} n_P P$ est EFFECTIF (POSITIF), note $D \geq 0$ si $n_P \geq 0 \forall P$.

Diviseurs principaux:

$$\forall P \in X, \quad v_P : \mathbb{F}_q(X) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

$$v_P(f) = \begin{cases} r \geq 0 & \text{si } P \text{ est un zéro de multiplicité } r \\ r < 0 & \text{si } P \text{ est un pôle de multiplicité } r \\ 0 & \text{si } P \text{ ni pôle ni zéro} \end{cases}$$

A' $f \in \mathbb{F}_q(X)$, $f \neq 0$, on associe le diviseur

$$(f) = \text{div}(f) = \sum_{P \in X} v_P(f) P = (f)_0 - (f)_\infty$$

$$= \sum_{\substack{P \text{ zéro de } f}} v_P(f) P - \sum_{\substack{P \text{ pôle de } f}} -v_P(f) P$$

- Si $D = \sum n_p P$, alors $\deg(D) = \sum_{P \in X} n_p \deg(P)$

Remarques:

- P rationnel alors $\deg(P) = 1$
- D diviseur rationnel $\Rightarrow \deg(D) = \sum n_p$
- une fonction $f \in \mathbb{F}_q(X)$ possède autant de zéros et de pôles (comptés avec multiplicité) $\Rightarrow \deg(dw(f)) = 0$

ESPACES DE NEYMAN-ROCH:

$$D \in \text{Div}(X)$$

$$L(D) = \{f \in \mathbb{F}_q(X) \mid (f) + D \geq 0\} \cup \{0\}$$

Exemple: $D = 2P - 3Q$

$P, Q \in X(\mathbb{F}_q)$. Alors

$$f \in L(D) \Leftrightarrow (f) + 2P - 3Q \geq 0$$

$$\Leftrightarrow \begin{cases} v_P(f) \geq -2 \rightarrow f \text{ peut avoir un pôle en } P, \text{ d'ordre au plus } 2 \\ v_Q(f) \geq 3 \rightarrow f \text{ a un zéro en } Q \text{ d'ordre au moins } 3 \\ f \text{ ne peut pas avoir de pôles en dehors de } P, \text{ mais peut avoir des zéros en dehors de } Q \end{cases}$$

$L(D)$ est un $\mathbb{F}_q$ -e.v. $\leftarrow$ facile

de dimension finie, noté $l(D)$ $\leftarrow$ difficile



Théorème de Riemann (1857, sur $\mathbb{C}$)

$l(D) \geq \deg(D) + 1 - g$ $\hookrightarrow$ genre de la courbe
avec égalité si $\deg(D) > 2g - 2$

Théorème de Riemann-Roch (1865, sur $\mathbb{C}$)

$$l(D) = \deg(D) + 1 - g + l(K - D)$$

$\uparrow$ diviseur canonique de la courbe

1931: R-R en tout caract. (Schmidt).

III - CODES DE GOPPA

CONSTRUCTION:

Soit X une courbe.

Soient $P_1, \dots, P_n \in X(\mathbb{F}_q)$.

$G \in \text{Div}(X)$ t.q. $\text{Supp}(G) \cap \{P_1, \dots, P_n\} = \emptyset$
et $\deg(G) = m < n$.

On considère l'application

$$\begin{aligned} \text{ev}: L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \dots, f(P_n)) \end{aligned}$$

$$\mathcal{C}(X, G) = \mathcal{I}_m(\text{ev}(L(G)))$$

$\hookrightarrow$ code linéaire associé à X et G

PARAMETRES

$$m = \deg(G)$$

le code $C(X, G)$ est un $[n, k, d]$ -code avec
 $d \geq n - m$ et $k \geq m - g + 1$.

Preuve:

I) $d \geq n - m$

II) Puisque $m < n$, on a $d > 0$ et donc l'application est injective.

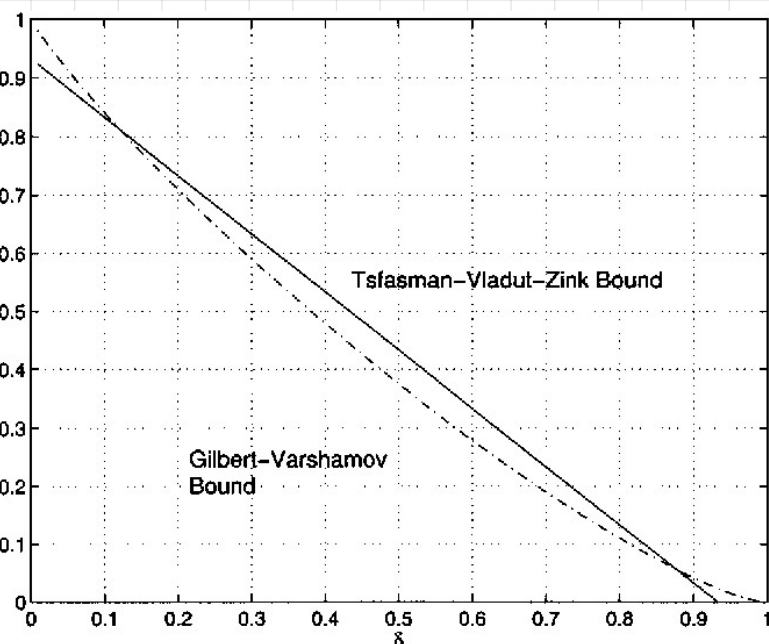
Du coup $\dim C = k = \dim_{\mathbb{F}_q} L(D) \geq m - g + 1$
d'après le th. de Riemann.

Remarque: $n + 1 - g \leq k + d \leq n + 1$ $\hookrightarrow$ Singleton

Par $g = 0 \rightarrow k + d = n + 1 \rightarrow$ codes MDS!
 $\hookrightarrow$ codes de Reed-Solomon!

IV - CONCLUSIONS

Pourquoi les codes AG?



Théorème (Tsfasman-Vladut-Zink, 1982)
Pour q un carré, $q \geq 49$, il existe une suite infinie de codes linéaires au-dessus de la borne de Gilbert-Varshamov.

Codes de Gappa généralisés

La constructeur de Gappa tient sur les unités de n'importe quelle dimension!

