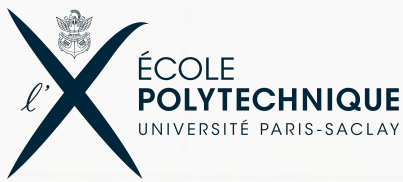
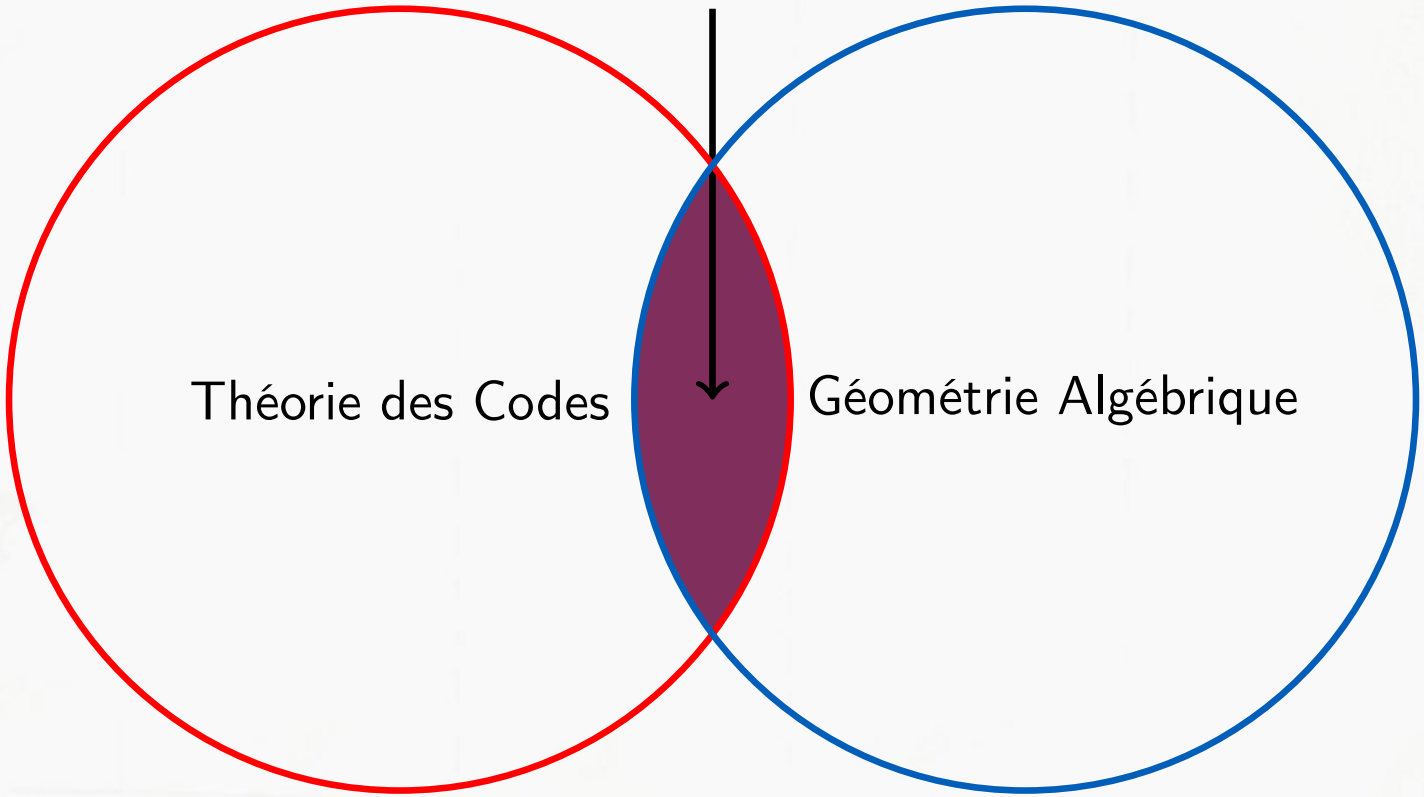
Étude théorique de codes géométriques sur des surfaces algébriques

Elena Berardini



GT équipe GRACE, LIX, l'X
17 novembre 2020

Codes Géométriques Algébriques



Dans cette exposé...

Vous trouverez :

- ✓ des outils de géométrie algébrique
- ✓ des bornes théoriques

Vous ne trouverez pas :

- × des algorithmes
- × de la complexité

Codes linéaire

Un code linéaire $\mathcal{C}$ est un $\mathbb{F}_q$-sous espace vectoriel de $\mathbb{F}_q^n$. Il est caractérisé par :

- n, la longueur de chaque mot du code ;
- k, sa dimension en tant qu'espace vectoriel ;
- $d(\mathcal{C})$, la distance minimale.

Définition

Pour $\omega(c)$ le nombre de coordonnées non nulles de c, la distance minimale du code $\mathcal{C}$ est

$$d(\mathcal{C}) := \min_{c \in \mathcal{C} \setminus \{0\}} \{\omega(c) | \, c \in \mathcal{C}\}.$$

BUT : avoir k et d les plus grands possible
Borne de Singleton : $k + d \leqslant n + 1$

Exemple

Soit $\mathbb{F}_4 = \mathbb{F}_2/(x^2 + x + 1)$, avec $\alpha^2 = \alpha + 1$.

Considérons le code linéaire $\mathcal{C}$ engendré par les vecteurs :

$$v_1 = (1, \ldots, 1),$$

$$v_2 = (0, 0, 1, 1, \alpha, \alpha, \alpha + 1, \alpha + 1),$$

$$v_3 = (0, 1, \alpha, \alpha + 1, \alpha, \alpha + 1, \alpha, \alpha + 1).$$

Notamment

$$v_1 + v_2 + v_3 = (1, 0, \alpha, \alpha + 1, 1, 0, 0, 1).$$

Les paramètres du code sont : $n = 8$

$$k = 3$$

$$d = 5$$

Codes d'Evaluation

1. Considérons une variété algébrique V définie sur le corps fini $\mathbb{F}_q$
2. Considérons une énumération $\{P_1, \ldots, P_n\}$ de ses points rationnels
3. Considérons l'espace vectoriel de fonctions $f_1, \ldots, f_k$ dans le corps de fonctions $\mathbb{F}_q(V)$ qui satisfont certaines conditions (qu'on appellera espace de Riemann-Roch)
4. On construit le code $\mathcal{C}(V)$ comme l'espace des vecteurs de la forme $(f_i(P_1), \ldots, f_i(P_n))$, pour $i = 1, \ldots, k$

Exemple (Reprise)

Soit $\mathbb{F}_4 = \mathbb{F}_2/(x^2 + x + 1)$, avec $\alpha^2 = \alpha + 1$.

Soit $E : y^2z + yz^2 = x^3$ dans $\mathbb{P}^2(\mathbb{F}_4)$.

$$E(\mathbb{F}_4) = \{(0,0),(0,1),(1,\alpha),(1,\alpha+1),(\alpha,\alpha),\\ (\alpha,\alpha+1),(\alpha+1,\alpha),(\alpha+1,\alpha+1)\} \cup P_\infty$$

On a $L(3P_\infty) = \langle 1, x/z, y/z\rangle$. Soit $S = E(\mathbb{F}_4) \setminus \{P_\infty\}$.

Le code $\mathcal{C}(E, 3P_\infty, S)$ est engendré par les vecteurs v_1, v_2, v_3:

$(1,\ldots,1),(0,0,1,1,\alpha,\alpha,\alpha+1,\alpha+1),(0,1,\alpha,\alpha+1,\alpha,\alpha+1,\alpha,\alpha+1)$

Notamment $v_1 + v_2 + v_3 = (1,0,\alpha,\alpha+1,1,0,0,1)$.

Les paramètres du code sont : $n = 8$

$k = 3$

$d = 5$

Exemple (Reprise)

Soit $\mathbb{F}_4 = \mathbb{F}_2/(x^2+x+1)$, avec $\alpha^2 = \alpha + 1$.

Soit $E : y^2z + yz^2 = x^3$ dans $\mathbb{P}^2(\mathbb{F}_4)$.

$$E(\mathbb{F}_4) = \{(0,0),(0,1),(1,\alpha),(1,\alpha+1),(\alpha,\alpha),\\ (\alpha,\alpha+1),(\alpha+1,\alpha),(\alpha+1,\alpha+1)\} \cup P_\infty$$

On a $L(3P_\infty) = \langle 1, x/z, y/z\rangle$. Soit $S = E(\mathbb{F}_4) \setminus \{P_\infty\}$.

Le code $\mathcal{C}(E, 3P_\infty, S)$ est engendré par les vecteurs v_1, v_2, v_3:

$(1,\ldots,1),(0,0,1,1,\alpha,\alpha,\alpha+1,\alpha+1),(0,1,\alpha,\alpha+1,\alpha,\alpha+1,\alpha,\alpha+1)$

Notamment $v_1 + v_2 + v_3 = (1,0,\alpha,\alpha+1,1,0,0,1)$.

Les paramètres du code sont : $n = 8$

$$k = 3 = \deg(3P_\infty)$$

$$d = 5 = n - \deg(3P_\infty)$$

Exemple (Reprise)

Soit $\mathbb{F}_4 = \mathbb{F}_2/(x^2 + x + 1)$, avec $\alpha^2 = \alpha + 1$.

Soit $E : y^2z + yz^2 = x^3$ dans $\mathbb{P}^2(\mathbb{F}_4)$.

$$E(\mathbb{F}_4) = \{(0,0),(0,1),(1,\alpha),(1,\alpha+1),(\alpha,\alpha),\\ (\alpha,\alpha+1),(\alpha+1,\alpha),(\alpha+1,\alpha+1)\} \cup P_\infty$$

On a $L(3P_\infty) = \langle 1, x/z, y/z\rangle$. Soit $S = E(\mathbb{F}_4) \setminus \{P_\infty\}$.

Le code $\mathcal{C}(E, 3P_\infty, S)$ est engendré par les vecteurs v_1, v_2, v_3:

$(1,\ldots,1),(0,0,1,1,\alpha,\alpha,\alpha+1,\alpha+1),(0,1,\alpha,\alpha+1,\alpha,\alpha+1,\alpha,\alpha+1)$

Notamment $v_1 + v_2 + v_3 = (1,0,\alpha,\alpha+1,1,0,0,1)$.

Les paramètres du code sont : $n = 8$

$$k = 3 = \deg(3P_\infty) \quad \underline{k = \deg(D) - g + 1}$$

$$d = 5 = n - \deg(3P_\infty) \quad \underline{d \geqslant n - \deg(D)}$$

Codes géométriques algébriques : long story short

1981 : Goppa introduit les codes AG sur les courbes algébriques

1982 : Tsfaman, Vlăduț et Zink utilisent les codes de Goppa pour dépasser la borne de Gilbert-Varshamov

$\sim$XX siècle : des nombreuse familles de courbes sont étudiées afin de construire des codes de Goppa optimaux

$\sim$XXI siècle : l'étude des codes AG sur les surfaces commence

...mais pourquoi les surfaces ?

Courbe de genre «petit»: $O(q)$ points rationnels
Surface avec nombres de Betti «petits»: $O(q^2)$ points rationnels

Les surfaces permettent de construire des codes de même longueur sur des corps finis de cardinal plus petit (arithmétique plus efficace)

Sommaire

I. Surfaces algébriques : notations et notions de base

X, surface projective, lisse, absolument irréductible, définie sur $\mathbb{F}_q$

$D \in \mathrm{Div}(X)$, une somme formelle de courbes sur X : $D = \sum n_i D_i$

$D \in \mathrm{Div}(X)$ est effectif si $n_i \geqslant 0$

$(f) = (f)_0 - (f)_\infty$, diviseur principal associé à $f \in \mathbb{F}_q(X)$
zeros $-$ *poles*

Equivalence linéaire : $D \sim D' \iff D - D' = (f)$

$. : \mathrm{Div}(X) \times \mathrm{Div}(X) \to \mathbb{Z}$, $(D, D') \mapsto D.D'$, le pairing d'intersection, symétrique et bilinéaire

- si C et D s'intersectent transversalement $C.D = \#(C \cap D)$
- dépend seulement des classes d'equivalence linéaire

$D \in \mathrm{Div}(X)$ est nef (strictement-nef) si $D.C \geqslant 0$ ($D.C > 0$) pour toute courbe irréductible C on X

I. Quelques outils de la théorie d'intersection

Notations : K_X, le diviseur canonique de X, H, un diviseur ample sur X

- Nakai-Moishezon : H est ample $\iff$ $H^2 > 0$ et $H.C > 0$ pour toute courbe irréductible C sur X
- Formule d'adjonction : C courbe de genre π sur X, alors

$$C.(C + K_X) = 2\pi - 2$$

Genre virtuel d'un diviseur : D diviseur sur X, alors

$$\pi_D = \frac{D^2}{2} + \frac{D.K_X}{2} + 1$$

- Corollaire du Théorème d'Indice de Hodge : soit D un diviseur sur X, alors

$$(H.D)^2 \geqslant H^2 D^2$$

I. Codes d'evaluation sur les surfaces algébriques

Soit X une surface, H un diviseur effectif et ample sur X et r un entier positif. Considérons l'espace de Riemann-Roch

$$L(rH) = \{f \in \mathbb{F}_q^*(X) \mid (f) + rH \geqslant 0\} \cup \{0\}.$$

Définition

Soit $S = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$. Le code $\mathcal{C}(X, rH, S)$ est défini comme l'image de la fonction d'évaluation

$$\begin{aligned} \mathrm{ev} : \quad L(rH) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

I. Longueur, Dimension, Distance minimale

$$n = \#S$$

$$\dim(\mathcal{C}(X, rH, S)) = \dim_{\mathbb{F}_q} L(rH)$$

utiliser le théorème de Riemann-Roch

I. Longueur, Dimension, Distance minimale

$$n = \#S$$

$$\dim(\mathcal{C}(X, rH, S)) = \dim_{\mathbb{F}_q} L(rH)$$

utiliser le théorème de Riemann-Roch

$$\boxed{d(X, rH, S) = ?}$$

I. Longueur, Dimension, Distance minimale

$$n = \#S$$

$$\dim(\mathcal{C}(X, rH, S)) = \dim_{\mathbb{F}_q} L(rH)$$

utiliser le théorème de Riemann-Roch

$$\boxed{d(X, rH, S) \geqslant ?}$$

I. Comment borner d ?

$$d(\mathcal{C}) := \min_{c \in \mathcal{C} \setminus \{0\}} \{\omega(c) \mid \omega(c) = \text{nombre de coordonnées non nulles de } c\}$$

Soit $f \in L(rH) \setminus \{0\} = \{f \in \mathbb{F}_q^*(X) \mid (f)_0 - (f)_\infty + rH \geqslant 0\}$

$$N(f) := \text{nombre de points rationnels sur } (f)_0$$

$$\#S - \omega(\mathrm{ev}(f)) \leq N(f)$$

$$d(X, rH, S) \geqslant \#S - \max_{f \in L(rH)\setminus\{0\}} N(f)$$

borne sup pour $N(f)$ $\Rightarrow$ borne inf pour la distance minimale

I. Comment borner $N(f)$?

$$N(f) := \text{nombre de points rationnels sur } (f)_0$$

où $f \in L(rH) \setminus \{0\} = \{f \in \mathbb{F}_q^*(X) \mid (f)_0 - (f)_\infty + rH \geqslant 0\}$

Considérons le diviseur effectif

$$D_f = (f)_0 - (f)_\infty + rH = \sum_{i=1}^{k} n_i D_i$$

où chaque D_i est une courbe irréductible de genre π_i et $n_i \geqslant 0$.

I. Comment borner $N(f)$?

$$N(f) := \text{nombre de points rationnels sur } (f)_0$$

où $f \in L(rH) \setminus \{0\} = \{f \in \mathbb{F}_q^*(X) \mid (f)_0 - (f)_\infty + rH \geqslant 0\}$

Considérons le diviseur effectif

$$D_f = (f)_0 - (f)_\infty + rH = \sum_{i=1}^{k} n_i D_i$$

où chaque D_i est une courbe irréductible de genre π_i et $n_i \geqslant 0$.

$$\boxed{\#(f)_0 = N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q)}$$

I. Comment borner $N(f)$?

$$N(f) := \text{nombre de points rationnels sur } (f)_0$$

où $f \in L(rH) \setminus \{0\} = \{f \in \mathbb{F}_q^*(X) \mid (f)_0 - (f)_\infty + rH \geqslant 0\}$

Considérons le diviseur effectif

$$D_f = (f)_0 - (f)_\infty + rH = \sum_{i=1}^{k} n_i D_i$$

où chaque D_i est une courbe irréductible de genre π_i et $n_i \geqslant 0$.

$$\boxed{\#(f)_0 = N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q)}$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème (Serre-Weil, 1983)

Soit C une courbe absolument irréductible lisse de genre g définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + gm.$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème (Serre-Weil, 1983)

Soit C une courbe absolument irréductible lisse de genre g définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + gm.$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème (Serre-Weil, 1983)

Soit C une courbe absolument irréductible lisse de genre g définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + gm.$$

Théorème (Aubry-Perret, 1995)

Soit C une courbe absolument irréductible de genre arithmétique π définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + \pi m.$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème (Aubry-Perret, 1995)

Soit C une courbe absolument irréductible de genre arithmétique π définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + \pi m.$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème (Aubry-Perret, 1995)

Soit C une courbe absolument irréductible de genre arithmétique π définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + \pi m.$$

Théorème (Little-Schenck, 2018)

Soit C une courbe irréductible de genre arithmétique π, non absolument irréductible, définie sur le corps fini $\mathbb{F}_q$, plongée dans une surface lisse. Alors

$$\#C(\mathbb{F}_q) \leqslant \pi + 1.$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème (Aubry-Perret, 1995)

Soit C une courbe absolument irréductible de genre arithmétique π définie sur le corps fini $\mathbb{F}_q$. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + \pi m.$$

Théorème (Little-Schenck, 2018)

Soit C une courbe irréductible de genre arithmétique π, non absolument irréductible, définie sur le corps fini $\mathbb{F}_q$, plongée dans une surface lisse. Alors

$$\#C(\mathbb{F}_q) \leqslant \pi + 1 \leqslant q + 1 + \pi m.$$

II. Points rationnels d'une courbe sur une surface

Soit $m := \lfloor 2\sqrt{q} \rfloor$.

Théorème

Soit C une courbe irréductible de genre arithmétique π définie sur le corps fini $\mathbb{F}_q$ et plongée dans une surface lisse. Alors

$$\#C(\mathbb{F}_q) \leqslant q + 1 + \pi m.$$

III. Une borne pour $N(f)$

$$N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q)$$

III. Une borne pour $N(f)$

$$N(f) \leqslant k(q+1) + m \sum_{i=1}^{k} \pi_i$$

III. Une borne pour $N(f)$

$$N(f) \leqslant k(q+1) + m\sum_{i=1}^{k} \pi_i$$

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2}rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (1) :

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (1) :

$rH.H = D_f.H$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (1) :

$rH.H = D_f.H = \sum_{i=1}^{k} n_i D_i.H$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (1) :

$rH.H = D_f.H = \sum_{i=1}^{k} n_i D_i.H \geqslant \sum_{i=1}^{k} D_i.H$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (1) :

$rH.H = D_f.H = \sum_{i=1}^{k} n_i D_i.H \geqslant \sum_{i=1}^{k} D_i.H \geqslant k.$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (2) :

Corollaire du Théorème de l'Indice de Hodge : $D_i^2 \leqslant \frac{(D_i.H)^2}{H^2}$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (2) :

Corollaire du Théorème de l'Indice de Hodge : $D_i^2 \leqslant \frac{(D_i.H)^2}{H^2}$

Formule d'adjonction : $\pi_i \leqslant \frac{(D_i.H)^2}{2H^2} + \frac{D_i.K_X}{2} + 1$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

Idée de la preuve (2) :

Corollaire du Théorème de l'Indice de Hodge : $D_i^2 \leqslant \frac{(D_i.H)^2}{H^2}$

Formule d'adjonction : $\pi_i \leqslant \frac{(D_i.H)^2}{2H^2} + \frac{D_i.K_X}{2} + 1$

$$\sum_{i=1}^{k} \pi_i \leqslant \frac{r^2 H^2}{2} + \frac{1}{2} \sum_{i=1}^{k} D_i.K_X + k$$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

$$N(f) \leqslant k(q+1) + m \sum_{i=1}^{k} \pi_i$$

III. Être (nef) ou ne pas être (nef)

Lemme

Soit H un diviseur ample sur X, $r > 0$ un entier. Alors :

1. $k \leqslant rH^2$,
2. $\sum_{i=1}^{k} \pi_i \leqslant \begin{cases} \pi_{rH} - 1 + k \text{ si } K_X \text{ est nef,} \\ \pi_{rH} - 1 - \frac{1}{2} rH.K_X + \frac{k}{2} \text{ si } -K_X \text{ est strict-nef.} \end{cases}$

$$N(f) \leqslant k(q+1) + m \sum_{i=1}^{k} \pi_i$$

$$d(X, rH, S) \geqslant \#S - \max_{f \in L(rH) \setminus \{0\}} N(f).$$

III. Borne pour la distance minimale

Théorème 1 (Aubry, B., Herbaut, Perret)

Soit

$$d^*(X, rH, S) := \#S - rH^2(q + 1 + m) - m(\pi_{rH} - 1).$$

La distance minimale du code $\mathcal{C}(X, rH, S)$ satisfait :

1. *Si K_X est nef, alors*

$$d(X, rH, S) \geqslant d^*(X, rH, S).$$

2. *Si $-K_X$ est strictement nef, alors*

$$d(X, rH, S) \geqslant d^*(X, rH, S) + mr(\pi_H - 1).$$

III. Surfaces sans courbes irréductibles de petit genre

Lemme

Soit H un diviseur ample sur X. Supposons que X ne contient pas des courbes de genre plus petit ou égal à un entier positif ℓ. Alors :

1. $k \leqslant \frac{\pi_{rH}-1}{\ell}$.
2. $\sum_{i=1}^{k} \pi_i \leqslant \pi_{rH} - 1 + k$.

III. Surfaces sans courbes irréductibles de petit genre

Lemme

Soit H un diviseur ample sur X. Supposons que X ne contient pas des courbes de genre plus petit ou égal à un entier positif ℓ. Alors :

1. $k \leqslant \frac{\pi_{rH}-1}{\ell}$. *Mieux que la borne précédente si ℓ est «grand»!*
2. $\sum_{i=1}^{k} \pi_i \leqslant \pi_{rH} - 1 + k$.

III. Surfaces sans courbes irréductibles de petit genre

Lemme

Soit H un diviseur ample sur X. Supposons que X ne contient pas des courbes de genre plus petit ou égal à un entier positif ℓ. Alors :

1. $k \leqslant \frac{\pi_{rH}-1}{\ell}$. *Mieux que la borne précédente si ℓ est «grand»!*
2. $\sum_{i=1}^{k} \pi_i \leqslant \pi_{rH} - 1 + k$. *Même borne du cas K_X nef !*

III. Surfaces sans courbes irréductibles de petit genre

Lemme

Soit H un diviseur ample sur X. Supposons que X ne contient pas des courbes de genre plus petit ou égal à un entier positif ℓ. Alors :

1. $k \leqslant \frac{\pi_{rH}-1}{\ell}$.
2. $\sum_{i=1}^{k} \pi_i \leqslant \pi_{rH} - 1 + k$.

Théorème 2 (Aubry, B., Herbaut, Perret, 2020)

Supposons que X ne contient pas des courbes de genre plus petit ou égal à un entier positif ℓ. Alors la distance minimale du code $\mathcal{C}(X, rH, S)$ satisfait :

$$d(X, rH, S) \geqslant d^*(X, rH, S) + \left(rH^2 - \frac{\pi_{rH} - 1}{\ell} \right) (q + 1 + m).$$

IV. Surfaces fibrées

Définition

Une fibration $f : X \to B$ est un morphisme surjectif f d'une surface projective lisse X sur une courbe lisse absolument irréductible B.

Nous écrivons π_0 pour le genre arithmétique de la fibre générique.

- $\pi_0 = 0 \to$ surfaces reglées ;
- $\pi_0 = 1 \to$ surfaces elliptiques ;
- $\pi_0 \geqslant 2 \to$ surfaces de type général.

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

$$N(f) \leqslant \sum_{i=1}^{k} \#D_i(\mathbb{F}_q)$$

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

$$N(f) \leqslant \sum_{i=1}^{h} \#H_i(\mathbb{F}_q) + \sum_{i=1}^{v} \#F_i(\mathbb{F}_q).$$

h: #courbes horizontales

v: #courbes fibrales

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

$$N(f) \leqslant \sum_{i=1}^{h} \#H_i(\mathbb{F}_q) + \sum_{i=1}^{v} \#F_i(\mathbb{F}_q).$$

Théorème (Aubry-Perret, 2004)

Soit $f : H_i \to B$ un morphisme surjective plat entre la courbe irréductible H_i de genre aritmétique π_{H_i} et la courbe lisse absolument irréductible B de genre g_B, définies sur le corps fini $\mathbb{F}_q$. Soit $\bar{r}_{H_i}$ le nombre de composants absolument irréductibles de H_i. Alors

$$\#H_i(\mathbb{F}_q) \leqslant \#B(\mathbb{F}_q) + (\bar{r}_{H_i} - 1)q + m(\pi_{H_i} - g_B)$$

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

$$N(f) \leqslant \sum_{i=1}^{h} \#H_i(\mathbb{F}_q) + \sum_{i=1}^{v} \#F_i(\mathbb{F}_q).$$

h: #courbes horizontales $\rightarrow \#H_i(\mathbb{F}_q) \leqslant \#B(\mathbb{F}_q) + (\bar{r}_i - 1)q + m(\pi_{H_i} - g_B)$

v: #courbes fibrales

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

$$N(f) \leqslant \sum_{i=1}^{h} \#H_i(\mathbb{F}_q) + \sum_{i=1}^{v} \#F_i(\mathbb{F}_q).$$

h: #courbes horizontales $\rightarrow \#H_i(\mathbb{F}_q) \leqslant \#B(\mathbb{F}_q) + (\bar{r}_i - 1)q + m(\pi_{H_i} - g_B)$

v: #courbes fibrales $\rightarrow \#F_i(\mathbb{F}_q) \leqslant q + 1 + m\pi_{F_i}$

IV. La géométrie des surfaces fibrées

Tout diviseur sur X s'écrit de façon unique comme la somme de courbes horizontales (envoyées sur B par f) et courbes fibrales (envoyées sur un point de B par f).

On étudie le code $\mathcal{C}(X, rH, S)$, pour H un diviseur ample

$$N(f) \leqslant \sum_{i=1}^{h} \#H_i(\mathbb{F}_q) + \sum_{i=1}^{v} \#F_i(\mathbb{F}_q).$$

h: $\#\text{courbes horizontales} \to \#H_i(\mathbb{F}_q) \leqslant \#B(\mathbb{F}_q) + (\bar{r}_i - 1)q + m(\pi_{H_i} - g_B)$

v: $\#\text{courbes fibrales} \to \#F_i(\mathbb{F}_q) \leqslant q + 1 + m\pi_{F_i}$

$$N(f) \leqslant h(\#B(\mathbb{F}_q) - (q + 1 + mg_B)) + q\sum_{i=1}^{k} \bar{r}_i + m\sum_{i=1}^{k} \pi_i + k.$$

IV. Surfaces fibrées avec diviseur canonique nef

Théorème 3 (Aubry, B., Herbaut, Perret, 2020)

La distance minimale du code $\mathcal{C}(X, rH, S)$ satisfait

$$d(X, rH, S) \geqslant d^*(X, rH, S) + \delta(B),$$

où $\delta(B) := q + 1 + g_B m - \#B(\mathbb{F}_q) \geqslant 0$.

En comparant avec

$$d(X, rH, S) \geqslant d^*(X, rH, S),$$

la nouvelle borne est toujours meilleure et est d'autant plus meilleure que le défaut de la courbe $\delta(B)$ augmente !

IV. La géométrie des surfaces abéliennes

Soit X une surfaces abélienne définie sur $\mathbb{F}_q$, de polynôme de Weil f_X et trace $\mathrm{Tr}(X)$.

Soit D une courbe absolument irréductible sur X et soit $\tilde{D}$ sa normalisée. Alors f_X divise $f_{\mathrm{Jac}(\tilde{D})}$ (ou le contraire).

- Soit D une courbe irréductible de genre π_D sur une surface abélienne simple X, alors $\pi_D \geqslant 2$.
- Soit D une courbe irréductible de genre π sur une surface abélienne simple X, alors

$$\#D(\mathbb{F}_q) \leqslant q + 1 - \mathrm{Tr}(X) + (\pi - 2)m.$$

IV. Une nouvelle borne

Théorème 4 (Aubry, B., Herbaut, Perret, 2019)

Soit X une surface abélienne simple qui ne contient pas des courbes absolument irréductibles de genre $\pi \leqslant \ell$. Alors, pour $1 < r < \sqrt{q}$ la distance minimale du code $\mathcal{C}(X, rH, S)$ satisfait :

$$d(X, rH, S) \geqslant \#S - r\sqrt{\frac{H^2}{2\ell}}\left(q + 1 - \mathrm{Tr}(X) + (\ell - 1)m\right).$$

Remarque : $d_{min} - \#S \underset{q\to\infty}{\sim} -r\sqrt{\frac{H^2}{2\ell}}q$, la borne pour $\ell = 2$ est meilleure de celle pour $\ell = 1$!

Question : Est-ce qu'ils existent des surfaces abéliennes qui ne contiennent pas des courbes absolument irréductibles de genre arithmétique 0, 1 ni 2?

OUI !

IV. Surfaces abéliennes sans courbes de petit genre

Lemme

Une surface abélienne X ne contient pas des courbes absolument irréductibles de genre arithmétique 0, 1 *ni* 2 $\iff$ *X est simple et non isogène à la Jacobienne d'une courbe de genre 2.*

IV. Surfaces abéliennes sans courbes de petit genre

Lemme

Une surface abélienne X ne contient pas des courbes absolument irréductibles de genre arithmétique 0, 1 ni 2 $\iff$ X est simple et non isogène à la Jacobienne d'une courbe de genre 2.

Théorème (Weil)

Soit (X, λ) une surface abélienne principalement polarisée définie sur le corps fini $\mathbb{F}_q$. Alors (X, λ) est soit

1. *la Jacobienne polarisée d'une courbe de genre 2 sur $\mathbb{F}_q$,*
2. *le produit de deux courbes elliptiques polarisées sur $\mathbb{F}_q$,*
3. *la restriction de Weil d'une courbe elliptique polarisée sur une extension quadratique de $\mathbb{F}_q$.*

IV. Surfaces abéliennes sans courbes de petit genre

Lemme

Une surface abélienne X ne contient pas des courbes absolument irréductibles de genre arithmétique 0, 1 ni 2 $\iff$ X est simple et non isogène à la Jacobienne d'une courbe de genre 2.

Théorème (Weil)

Soit (X, λ) une surface abélienne principalement polarisée définie sur le corps fini $\mathbb{F}_q$. Alors (X, λ) est soit

1. *la Jacobienne polarisée d'une courbe de genre 2 sur $\mathbb{F}_q$,*
2. *le produit de deux courbes elliptiques polarisées sur $\mathbb{F}_q$,*
3. *la restriction de Weil d'une courbe elliptique polarisée sur une extension quadratique de $\mathbb{F}_q$.*

IV. Surfaces abéliennes sans courbes de petit genre

Lemme

Une surface abélienne X ne contient pas des courbes absolument irréductibles de genre arithmétique 0, 1 *ni* 2 $\iff$ *X est simple et non isogène à la Jacobienne d'une courbe de genre 2.*

Surfaces abéliennes qui pourraient avoir la propriété que nous cherchons :

- les restrictions de Weil d'une courbe elliptique polarisée sur une extension quadratique de $\mathbb{F}_q$

IV. Surfaces abéliennes sans courbes de petit genre

Lemme

Une surface abélienne X ne contient pas des courbes absolument irréductibles de genre arithmétique 0, 1 *ni* 2 $\iff$ X *est simple et non isogène à la Jacobienne d'une courbe de genre 2.*

Surfaces abéliennes qui pourraient avoir la propriété que nous cherchons :

- les restrictions de Weil d'une courbe elliptique polarisée sur une extension quadratique de $\mathbb{F}_q$
- les surfaces abéliennes définies sur $\mathbb{F}_q$ qui n'admettent pas de polarisation principale

IV. Surfaces abéliennes sans courbes de genre $\leqslant 2$

Proposition 1 (Aubry, B., Herbaut, Perret, 2019)

(i) *Soit X une surface n'admettant pas de polarization principale, alors elle ne contient pas des courbes absolument irréductibles de genre arithmétique* 0, 1 *ni* 2.

(ii) *Soit X le restriction de Weil de $\mathbb{F}_{q^2}$ à $\mathbb{F}_q$ d'une courbe elliptique E définie sur $\mathbb{F}_{q^2}$. Alors X ne contient pas des courbes absolument irréductibles de genre* 0, 1 *ni* 2 *si et seulement si l'une des conditions suivantes est satisfaite :*

(1) $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 1$;
(2) $p > 2$ *et* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 2$;
(3) $p \equiv 11 \mod 12$ *ou* $p = 3$, $q = \square$ *et* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$;
(4) $p = 2$, $q \neq \square$ *et* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$;
(5) $q = 2$ *ou* $q = 3$, *et* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q$.

Remarques conclusives

- ✓ La théorie de l'intersection est un outil puissant pour l'étude des codes sur les surfaces et pourrait être appliquée à l'étude des codes sur les variétés de toute dimension.
- ✓ Les surfaces sans courbes de petit genre semblent intéressantes pour construire des bons codes.
- ✓ Les fibrations sur des courbes de genre grand et avec peu de points rationnels pourraient donner de très bons codes.

Quelques idées pour la suite

I) Codes sur les 3-folds. Appliquer notre méthode aux codes sur les variétés de dimension 3 ($O(q^3)$ points rationnels).

II) Fibrations. Donner des exemples de courbes algébriques de genre grand avec peu de points rationnels et des fibrations sur ces courbes.

III) Surfaces abéliennes. Donner des exemples de surfaces abéliennes qui ne contiennent pas des courbes absolument irréductibles de genre $\leqslant 3$.

Merci de votre attention !

(Des questions ?)

In this work more questions arise than answers given,
for which of course we do not apologise.