Paramètres des codes correcteurs sur les surfaces de Hirzebruch

Jade Nardi

13 avril 2018

Références clés

- Cícero Carvalho, Victor G.L.Neumann - *Projective Reed–Muller type codes on rational normal scrolls*. 2015.
- Johan P.Hansen - *Toric varieties Hirzebruch surfaces and error-correcting codes*. 2002
- Alain Couvreur, Iwan Duursma - *Evaluation codes from smooth quadric surfaces and twisted Segre varieties*. 2012.

A la manière des *codes Reed-Muller projectifs*, on va construire des codes correcteurs en **évaluant des polynômes** sur des surfaces avec de bonnes propriétés, les **surfaces de Hirzebruch**.

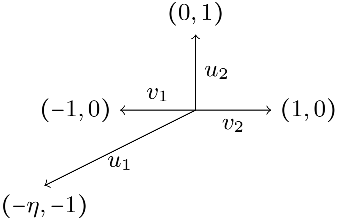
Objectifs :

- Déterminer les paramètres des codes construits ainsi,
- En déduire quelques propriétés sur les courbes maximales de la surface.

Soit $\eta \in \mathbb{N}$. On définit la surface de Hirzebruch $\mathcal{H}_\eta$ de paramètre η.

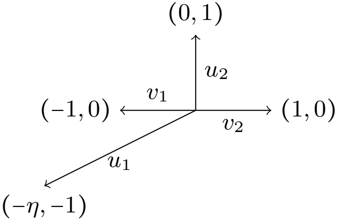
Soit $\eta \in \mathbb{N}$. On définit la surface de Hirzebruch $\mathcal{H}_\eta$ de paramètre η.

- 1^e **point de vue : torique**
  C'est la variété torique associée à l'éventail



Soit $\eta \in \mathbb{N}$. On définit la surface de Hirzebruch $\mathcal{H}_\eta$ de paramètre η.

- 1^e **point de vue : torique**
  C'est la variété torique associée à l'éventail

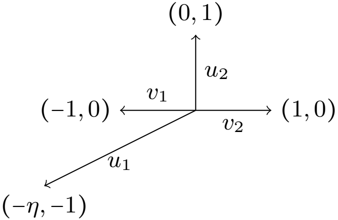


- 2^e **point de vue : quotient**
  On fait agir $\mathbb{G}_m \times \mathbb{G}_m$ sur $\left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right)$: on note (t_1,t_2) les coordonnées sur le premier $\mathbb{A}^2$, (x_1,x_2) pour le second et $(\lambda,\mu) \in \mathbb{G}_m \times \mathbb{G}_m$.

$$(\lambda,\mu)\cdot(t_1,t_2,x_1,x_2) = (\lambda t_1, \lambda t_2, \mu\lambda^{-\eta} x_1, \mu x_2).$$

Soit $\eta \in \mathbb{N}$. On définit la surface de Hirzebruch $\mathcal{H}_\eta$ de paramètre η.

- 1^e **point de vue : torique**
  C'est la variété torique associée à l'éventail



- 2^e **point de vue : quotient**
  On fait agir $\mathbb{G}_m \times \mathbb{G}_m$ sur $\left(\mathbb{A}^2 \setminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \setminus \{(0,0)\}\right)$: on note (t_1,t_2) les coordonnées sur le premier $\mathbb{A}^2$, (x_1,x_2) pour le second et $(\lambda,\mu) \in \mathbb{G}_m \times \mathbb{G}_m$.

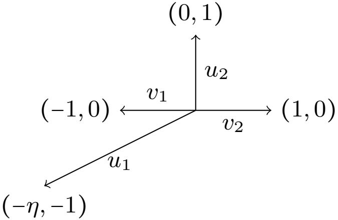
$$(\lambda,\mu)\cdot(t_1,t_2,x_1,x_2) = (\lambda t_1, \lambda t_2, \mu\lambda^{-\eta}x_1, \mu x_2).$$

  $\mathcal{H}_\eta$ peut être définie comme le quotient

$$\left(\mathbb{A}^2 \setminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \setminus \{(0,0)\}\right) / \mathbb{G}_m^2.$$

Soit $\eta \in \mathbb{N}$. On définit la surface de Hirzebruch $\mathcal{H}_\eta$ de paramètre η.

- 1^e **point de vue : torique**
  C'est la variété torique associée à l'éventail



- 2^e **point de vue : quotient**
  On fait agir $\mathbb{G}_m \times \mathbb{G}_m$ sur $\left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right)$: on note (t_1, t_2) les coordonnées sur le premier $\mathbb{A}^2$, (x_1, x_2) pour le second et $(\lambda, \mu) \in \mathbb{G}_m \times \mathbb{G}_m$.

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

  $\mathcal{H}_\eta$ peut être définie comme le quotient

$$\left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) / \mathbb{G}_m^2.$$

- 3^e **point de vue : plongée dans** $\mathbb{P}^{\eta+3}$ (Exemples et nbre de $\mathbb{F}_q$ points)

On va construire un code similaire à Reed-Muller, en évaluant des **polynômes**.
L'*anneau de Cox* de $\mathcal{H}_\eta$ sur $\mathbb{F}_q$ est l'anneau $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
On le munit d'une **graduation**, c'est-à-dire on définit le *degré d'un polynôme* homogène.

On va construire un code similaire à Reed-Muller, en évaluant des **polynômes**.
L'*anneau de Cox* de $\mathcal{H}_\eta$ sur $\mathbb{F}_q$ est l'anneau $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
On le munit d'une **graduation**, c'est-à-dire on définit le *degré d'un polynôme* homogène.

Un monôme $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ est de bidegré (δ_T, δ_X) si

$$\begin{cases} \delta_T & = c_1 + c_2 - \eta d_1, \\ \delta_X & = d_1 + d_2. \end{cases} \tag{1}$$

On note $R(\delta_T, \delta_X)$ le $\mathbb{F}_q$-ev des polynômes de bidegré (δ_T, δ_X).

On va construire un code similaire à Reed-Muller, en évaluant des **polynômes**.
L'*anneau de Cox* de $\mathcal{H}_\eta$ sur $\mathbb{F}_q$ est l'anneau $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
On le munit d'une **graduation**, c'est-à-dire on définit le *degré d'un polynôme* homogène.

Un monôme $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ est de bidegré (δ_T, δ_X) si

$$\begin{cases} \delta_T & = c_1 + c_2 - \eta d_1, \\ \delta_X & = d_1 + d_2. \end{cases} \tag{1}$$

On note $R(\delta_T, \delta_X)$ le $\mathbb{F}_q$-ev des polynômes de bidegré (δ_T, δ_X). Alors

$$R = \bigoplus_{(\delta_T, \delta_X) \in \mathbb{Z}^2} R(\delta_T, \delta_X)$$

Remarque : $R(\delta_T, \delta_X)$ n'est pas réduit à zéro si et seulement si

$$\delta_X \geq 0 \text{ et } \delta := \delta_T + \eta \delta_X \geq 0.$$

Cela permet de travailler sans plonger la surface dans un projectif et ouvre des perspectives pour des codes sur d'autres variétés toriques.

On va **évaluer les polynômes** en les points rationnels de la surface $\mathcal{H}_\eta$.
On rappelle que les points de la surface de Hirzebruch sont les orbites sous l'action

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu\lambda^{-\eta} x_1, \mu x_2).$$

Un point est *rationnel* si l'orbite contient au moins un représentant rationnel.

On va **évaluer les polynômes** en les points rationnels de la surface $\mathcal{H}_\eta$.
On rappelle que les points de la surface de Hirzebruch sont les orbites sous l'action

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

Un point est *rationnel* si l'orbite contient au moins un représentant rationnel.

Soit $F \in R(\delta_T, \delta_X)$ et P un point de $\mathcal{H}_\eta$, On pose $F(P) = F(t_1, t_2, x_1, x_2)$, où (t_1, t_2, x_1, x_2) est l'unique représentant de P qui est de l'une des ces formes :

- $(1, a, 1, b)$ avec $a,\ b \in \mathbb{F}_q$,
- $(0, 1, 1, b)$ avec $b \in \mathbb{F}_q$,
- $(1, a, 0, 1)$ avec $a \in \mathbb{F}_q$,
- $(0, 1, 0, 1)$.

On va **évaluer les polynômes** en les points rationnels de la surface $\mathcal{H}_\eta$.
On rappelle que les points de la surface de Hirzebruch sont les orbites sous l'action

$$(\lambda,\mu)\cdot(t_1,t_2,x_1,x_2) = (\lambda t_1, \lambda t_2, \mu\lambda^{-\eta}x_1, \mu x_2).$$

Un point est *rationnel* si l'orbite contient au moins un représentant rationnel.

Soit $F \in R(\delta_T,\delta_X)$ et P un point de $\mathcal{H}_\eta$, On pose $F(P) = F(t_1,t_2,x_1,x_2)$, où (t_1,t_2,x_1,x_2) est l'unique représentant de P qui est de l'une des ces formes :

- $(1,a,1,b)$ avec a, $b \in \mathbb{F}_q$,
- $(0,1,1,b)$ avec $b \in \mathbb{F}_q$,
- $(1,a,0,1)$ avec $a \in \mathbb{F}_q$,
- $(0,1,0,1)$.

On veut que, sur chaque $\mathbb{A}^2$, la coordonnée non nulle la plus à gauche vaille 1.

Le code $C_\eta(\delta_T, \delta_X)$ est définie comme l'image de l'application

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T, \delta_X) & \to & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P \in \mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{2}$$

Le code $C_\eta(\delta_T, \delta_X)$ est définie comme l'image de l'application

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T, \delta_X) & \rightarrow & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P \in \mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{2}$$

On n'a absolument pas besoin de la structure de la variété pour construire ou implémenter un tel code. Il suffit de construire l'ensemble des polynômes et d'évaluer en les $(q+1)^2$ points $(1, a, 1, b)$, $(0, 1, 1, b)$, $(1, a, 0, 1)$ et $(0, 1, 0, 1)$.

On va considérer la dimension comme une donnée combinatoire facile à calculer.

Rappel : Un monôme $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ est de bidegré (δ_T, δ_X) si

$$d_1 + d_2 = \delta_X \text{ et } c_1 + c_2 - \eta d_1 = \delta_T$$

A (δ_T, δ_X) donné, un monôme est totalement déterminé par le couple (d_2, c_2) avec

$$0 \leq d_2 \leq \delta_X \text{ et } 0 \leq c_2 \leq \delta_T + \eta(\delta_X - d_2) = \delta - \eta d_2$$

L'ensemble des couples (d_2, c_2) est donc à l'intersection de ces 4 hyperplans, ce qui forme un polygone que l'on note $P(\delta_T, \delta_X)$.

$$P(\delta_T, \delta_X) = \{(d_2, c_2) \in \mathbb{N}^2 \mid 0 \leq d_2 \leq \delta_X \text{ et } 0 \leq c_2 \leq \delta_T + \eta(\delta_X - d_2) = \delta - \eta d_2\}$$

On note A l'abscisse des sommets les plus à droite.

$$A = A(\eta, \delta_T, \delta_X) = \min\left(\delta_X, \frac{\delta}{\eta}\right) = \begin{cases} \delta_X & \text{si } \delta_T \geq 0, \\ \frac{\delta}{\eta} = \delta_X + \frac{\delta_T}{\eta} & \text{sinon.} \end{cases}$$

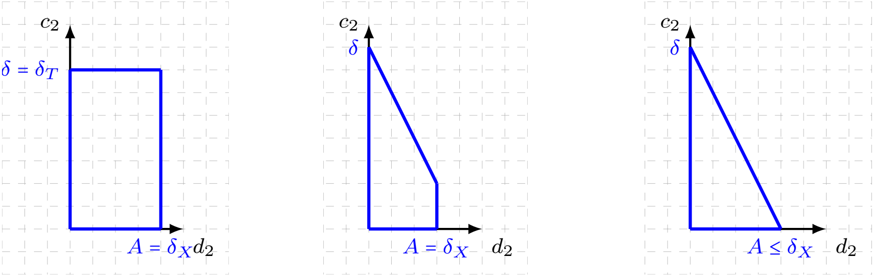
Ce n'est pas toujours un entier !

$$P(\delta_T, \delta_X) = \{(d_2, c_2) \in \mathbb{N}^2 \mid 0 \le d_2 \le \delta_X \text{ et } 0 \le c_2 \le \delta_T + \eta(\delta_X - d_2) = \delta - \eta d_2\}$$

On note A l'abscisse des sommets les plus à droite.

$$A = A(\eta, \delta_T, \delta_X) = \min\left(\delta_X, \frac{\delta}{\eta}\right) = \begin{cases} \delta_X & \text{si } \delta_T \ge 0, \\ \frac{\delta}{\eta} = \delta_X + \frac{\delta_T}{\eta} & \text{sinon.} \end{cases}$$

Ce n'est pas toujours un entier !



$\eta = 0$
e.g. $\mathcal{P}(7,4)$

$\eta > 0$, $\delta_T > 0$
e.g. $\mathcal{P}(2,3)$ in $\mathcal{H}_2$

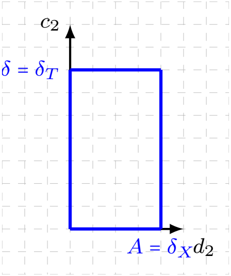
$\eta > 0$, $\delta_T \le 0$
e.g. $\mathcal{P}(-2,5)$ in $\mathcal{H}_2$

$$P(\delta_T, \delta_X) = \{(d_2, c_2) \in \mathbb{N}^2 \mid 0 \leq d_2 \leq \delta_X \text{ et } 0 \leq c_2 \leq \delta_T + \eta(\delta_X - d_2) = \delta - \eta d_2\}$$

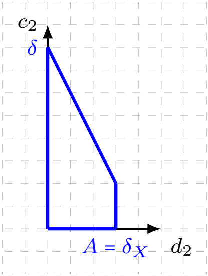
On note A l'abscisse des sommets les plus à droite.

$$A = A(\eta, \delta_T, \delta_X) = \min\left(\delta_X, \frac{\delta}{\eta}\right) = \begin{cases} \delta_X & \text{si } \delta_T \geq 0, \\ \frac{\delta}{\eta} = \delta_X + \frac{\delta_T}{\eta} & \text{sinon.} \end{cases}$$

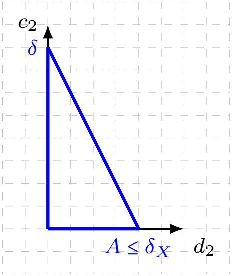
Ce n'est pas toujours un entier !



$\eta = 0$
e.g. $\mathcal{P}(7, 4)$



$\eta > 0$, $\delta_T > 0$
e.g. $\mathcal{P}(2, 3)$ in $\mathcal{H}_2$



$\eta > 0$, $\delta_T \leq 0$
e.g. $\mathcal{P}(-2, 5)$ in $\mathcal{H}_2$

On exhibe la dimension comme le cardinal d'un sous-ensemble des points entier de ce polygone. Posons

$$\mathcal{K}(\delta_T,\delta_X) = \left\{ (\alpha,\beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} 0 \leq \alpha \leq \min(\lfloor A \rfloor, q-1)\} \cup \{A\} \cap \mathbb{N} \\ 0 \leq \beta \leq \min(\delta - \eta\alpha, q) - 1 \text{ or } \beta = \delta - \eta\alpha \end{array} \right\}.$$

Alors

$$\mathcal{K}(\delta_T,\delta_X) = P(\delta_T,\delta_X) \cap ((\{d_2 \leq q-1\} \cup \{d_2 = A\}) \cap (\{c_2 \leq q-1\} \cup \{c_2 = \delta - \eta d_2)\})).$$

Faisons un dessin.

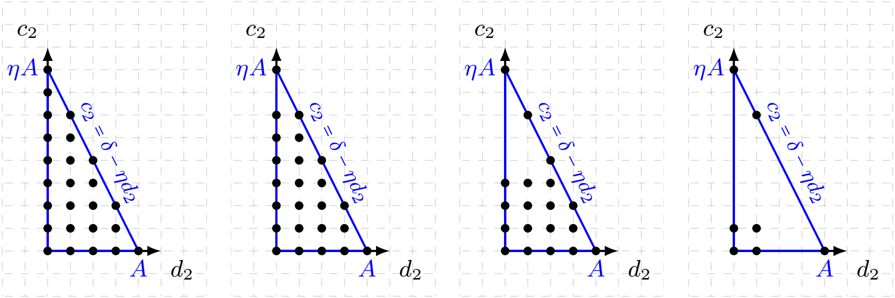
On exhibe la dimension comme le cardinal d'un sous-ensemble des points entier de ce polygone. Posons

$$\mathcal{K}(\delta_T, \delta_X) = \left\{ (\alpha, \beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} 0 \leq \alpha \leq \min(\lfloor A \rfloor, q-1)\} \cup \{A\} \cap \mathbb{N} \\ 0 \leq \beta \leq \min(\delta - \eta\alpha, q) - 1 \text{ or } \beta = \delta - \eta\alpha \end{array} \right\}.$$

Alors

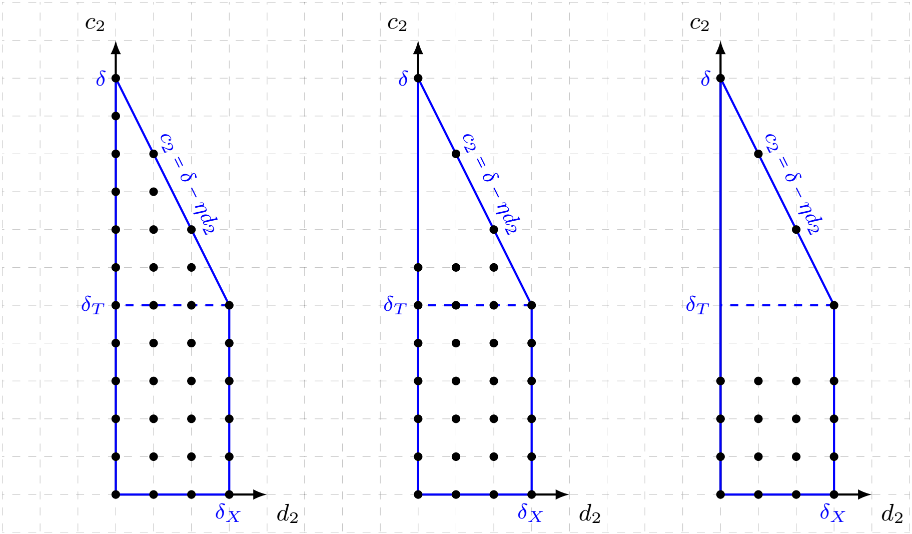
$$\mathcal{K}(\delta_T, \delta_X) = P(\delta_T, \delta_X) \cap ((\{d_2 \leq q-1\} \cup \{d_2 = A\}) \cap (\{c_2 \leq q-1\} \cup \{c_2 = \delta - \eta d_2)\})).$$

Faisons un dessin.



(a) $q = 11$ (b) $q = 7$ (c) $q = 4$ (d) $q = 2$

Figure – $\mathcal{P}(-2, 5)$ dans $\mathcal{H}_2$ pour différentes valeurs de q.



(a) $\delta < q = 13$ (b) $\delta_T \leq q = 7 \leq \delta$ (c) $\delta_X < q = 4 < \delta_T$

Figure – $\mathcal{P}(5,3)$ dans $\mathcal{H}_2$

Théorème

La dimension du code $C_\eta(\delta_T, \delta_X)$ vaut

$$\dim C_\eta(\delta_T, \delta_X) = \#\mathcal{K}(\delta_T, \delta_X)$$

Théorème

La dimension du code $C_\eta(\delta_T, \delta_X)$ vaut

$$\dim C_\eta(\delta_T, \delta_X) = \#\mathcal{K}(\delta_T, \delta_X)$$

Formule explicite de la dimension du code

Sur $\mathcal{H}_0$,

$$\dim C_0(\delta_T, \delta_X) = (\min(\delta_T, q) + 1)\,(\min(\delta_X, q) + 1)\,.$$

Sur $\mathcal{H}_\eta$ pour $\eta \geq 1$, on pose

$$m = \min(\lfloor A \rfloor, q-1),\ h = \begin{cases} \min(\delta_T, q) + 1 & \text{si } \delta_T \geq 0 \text{ et } q \leq \delta_X, \\ 1 & \text{si } \delta_T \leq 0,\ q \leq A \text{ et } \eta \mid \delta_T, \\ 0 & \text{sinon,} \end{cases}$$

$$s = \frac{\delta - q}{\eta} \text{ et } \tilde{s} = \begin{cases} \lfloor s \rfloor & \text{si } s \in [0, m], \\ -1 & \text{si } s < 0, \\ m & \text{si } s > m. \end{cases}$$

Alors

$$\dim C_\eta(\delta_T, \delta_X) = (q+1)(\tilde{s}+1) + (m - \tilde{s})\left(\delta + 1 - \eta\left(\frac{m + \tilde{s} + 1}{2}\right)\right) + h.$$

Exemple utile pour la suite : Cas où l'évaluation est surjective.
Montrons que si δ_T, $\delta_X \geq q$, alors l'application d'évaluation $\mathrm{ev}_{(\delta_T,\delta_X)}$ est surjective. En effet,

$$\mathcal{K}(\delta_T,\delta_X) = \left\{ (\alpha,\beta) \in \mathbb{N}^2 \;\middle|\; \begin{array}{c} \alpha \in [\![0,q-1]\!] \cup \{\delta_X\} \\ \beta \in [\![0,q-1]\!] \cup \{\delta - \eta\alpha\} \end{array} \right\},$$

d'où $\dim C_\eta(\delta_T,\delta_X) = \#\mathcal{K}(\delta_T,\delta_X) = (q+1)^2 = N$.

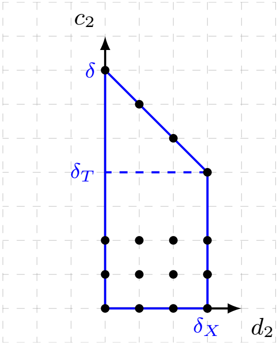


Figure – $\mathcal{P}(3,4)$ avec $q = 3$ dans $\mathcal{H}_1$

On note $d_\eta(\delta_T, \delta_X)$ la distance minimale du code $C_\eta(\delta_T, \delta_X)$. On veut minorer le poids des mots du code.

Soit $F \in R(\delta_T, \delta_X) \smallsetminus \ker \mathrm{ev}_{(\delta_T, \delta_X)}$, on pose $N_F = \#\mathcal{Z}(F)(\mathbb{F}_q)$, le nombre de $\mathbb{F}_q$-points sur la courbe définie par $F = 0$.

On note $d_\eta(\delta_T, \delta_X)$ la distance minimale du code $C_\eta(\delta_T, \delta_X)$. On veut minorer le poids des mots du code.
Soit $F \in R(\delta_T, \delta_X) \smallsetminus \ker \mathrm{ev}_{(\delta_T, \delta_X)}$, on pose $N_F = \#\mathcal{Z}(F)(\mathbb{F}_q)$, le nombre de $\mathbb{F}_q$-points sur la courbe définie par $F = 0$.
Pour tout couple couple $(\varepsilon_T, \varepsilon_X)$, on peut considérer l'application **surjective**

$$\mathrm{ev}_{(\varepsilon_T, \varepsilon_X), F} : \left\{ \begin{array}{rcl} R(\varepsilon_T, \varepsilon_X) & \to & \mathbb{F}_q^{N_F} \\ G & \mapsto & (G(Q))_{Q \in \mathcal{Z}(F)(\mathbb{F}_q)} \end{array} \right. .$$

$$N_F = \dim \left({R(\varepsilon_T, \varepsilon_X)} \big/ {\ker \mathrm{ev}_{(\varepsilon_T, \varepsilon_X), F}} \right).$$

On pose $\langle F \rangle_{(\varepsilon_T, \varepsilon_X)}$ le sev $FR(\varepsilon_T - \delta_T, \varepsilon_X - \delta_X) \subset R(\varepsilon_T, \varepsilon_X)$ engendré par F.

On note $d_\eta(\delta_T,\delta_X)$ la distance minimale du code $C_\eta(\delta_T,\delta_X)$. On veut minorer le poids des mots du code.

Soit $F \in R(\delta_T,\delta_X) \setminus \ker \mathrm{ev}_{(\delta_T,\delta_X)}$, on pose $N_F = \#\mathcal{Z}(F)(\mathbb{F}_q)$, le nombre de $\mathbb{F}_q$-points sur la courbe définie par $F = 0$.

Pour tout couple couple $(\varepsilon_T,\varepsilon_X)$, on peut considérer l'application **surjective**

$$\mathrm{ev}_{(\varepsilon_T,\varepsilon_X),F} : \begin{cases} R(\varepsilon_T,\varepsilon_X) & \to & \mathbb{F}_q^{N_F} \\ G & \mapsto & (G(Q))_{Q\in\mathcal{Z}(F)(\mathbb{F}_q)} \end{cases}.$$

$$N_F = \dim\left(R(\varepsilon_T,\varepsilon_X) \big/ \ker \mathrm{ev}_{(\varepsilon_T,\varepsilon_X),F} \right).$$

On pose $\langle F\rangle_{(\varepsilon_T,\varepsilon_X)}$ le sev $FR(\varepsilon_T-\delta_T,\varepsilon_X-\delta_X) \subset R(\varepsilon_T,\varepsilon_X)$ engendré par F.

Puisque $\ker \mathrm{ev}_{(\varepsilon_T,\varepsilon_X)} + \langle F\rangle_{(\varepsilon_T,\varepsilon_X)} \subset \ker \mathrm{ev}_{(\varepsilon_T,\varepsilon_X),F}$, on a $\tilde{N}_F \geq N_F$ avec

$$\tilde{N}_F = \dim\left(R(\varepsilon_T,\varepsilon_X) \big/ \ker \mathrm{ev}_{(\varepsilon_T,\varepsilon_X)} + \langle F\rangle_{(\varepsilon_T,\varepsilon_X)} \right).$$

$$\Rightarrow d_\eta(\delta_T,\delta_X) \geq \min_{F\in\mathrm{Vect}\,\Delta(\delta_T,\delta_X)} N - \tilde{N}_F. \tag{3}$$

C'est cette quantité que l'on minore, à l'aide d'arguments de bases de Gröbner.

Formule explicite pour la distance minimale

Soit $\eta \geq 0$, $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ with $\delta \geq 0$. A moins que

$$\eta \geq 1, \quad \delta_T < 0, \quad \eta \mid \delta_T, \quad \text{et } q \leq \frac{\delta}{\eta}, \tag{H}$$

le code $C_\eta(\delta_T, \delta_X)$ sur la surface de Hirzebruch $\mathcal{H}_\eta$ a pour distance minimale

- Si $\eta \geq 1$,
  - Si $q > \delta$, alors
  $$d_\eta(\delta_T, \delta_X) = \begin{cases} (q + \mathbb{1}_{\delta_X = 0})(q - \delta + 1) & \text{si } \delta_T \geq 0 \text{ ou } (\delta_T < 0 \text{ et } \eta \geq 2) \\ (q - \delta)(q + 1) & \text{si } \delta_T < 0 \text{ et } \eta = 1 \end{cases}$$
  - Si $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, alors
  $$d_\eta(\delta_T, \delta_X) = q - \left\lfloor \frac{\delta - q}{\eta} \right\rfloor$$
  - Si $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$,
  $$d_\eta(\delta_T, \delta_X) = \max(q - \delta_X + 1, 1)$$
- Si $\eta = 0$,
$$d_\eta(\delta_T, \delta_X) = \max(q - \delta_X + 1, 1) \max(q - \delta_T + 1, 1)$$

Courbes maximales

Ecrivons $\mathbb{F}_q = \{\xi_1, \xi_2, \dots, \xi_q\}$.

- Si $\eta \geq 1$,
  - Si $q > \delta$, posons
$$F(T_1, T_2, X_1, X_2) = \begin{cases} X_1^{\delta_X} \prod_{i=1}^{\delta_T+\delta_X} (T_2 - \xi_i T_1) & \text{si } \delta_T \geq 0 \text{ ou } \eta \geq 2 \\ X_1^{-\delta_T} X_2^{\delta_X+\delta_T} \prod_{i=1}^{\delta_T+\delta_X} (T_2 - \xi_i T_1) & \text{si } \delta_T < 0 \text{ et } \eta = 1 \end{cases}$$
  - Si $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, posons $s = \lfloor \frac{\delta - q}{\eta} \rfloor$ et
$$F(T_1, T_2, X_1, X_2) = T_2^{\delta_T + \eta(\delta_X - s) - q} \prod_{i=1}^{s} (X_2 - \xi_i T_1^\eta X_1) \prod_{a \in \mathbb{F}_q} (T_2 - a T_1)$$
  - Si $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$, posons $m_X = \min(q, \delta_X)$ et
$$F(T_1, T_2, X_1, X_2) = X_2^{\delta_X - m_X} T_2^{\delta_T} \prod_{i=1}^{m_X} (X_2 - \xi_i X_1 T_1^\eta)$$
- si $\eta = 0$, posons $m_T = \min(q, \delta_T)$ and $m_X = \min(q, \delta_X)$ et
$$F(T_1, T_2, X_1, X_2) = X_2^{\delta_X - m_X} T_2^{\delta_T - m_T} \prod_{i=1}^{m_X} (X_2 - \xi_i X_1 T_1^\eta) \prod_{j=1}^{m_T} (T_2 - \xi_j T_1)$$

Les mots de code associés à ces polynômes atteignent la distance minimale.

Majoration du nombre de points rationnels des courbes

Soit $\eta \geq 0$ et $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ avec $\delta = \delta_T + \eta\delta_X \geq 0$. On suppose que (H) n'est pas vraie. Soit $\mathcal{C}$ une courbe de la surface de Hirzebruch $\mathcal{H}_\eta$ qui ne contient pas tous les $\mathbb{F}_q$-points de $\mathcal{H}_\eta$ et de bidegré (δ_T, δ_X) (c'est-à-dire de classe de Picard $\delta_T\mathcal{F} + \delta_X\sigma$). Alors

- Si $\eta \geq 1$,
  - Si $q > \delta$, alors
$$\#\mathcal{C}(\mathbb{F}_q) \leq \begin{cases} (q+1)\delta_T & \text{si } \delta_X = 0 \text{ et } \delta_T \geq 0, \\ q(\delta+1)+1 & \text{si } \delta_X \neq 0 \text{ et } (\delta_T \geq 0 \text{ ou } (\delta_T < 0 \text{ et } \eta \geq 2)), \\ (q+1)(\delta+1) & \text{si } \delta_T < 0 \text{ et } \eta = 1. \end{cases}$$
  - Si $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, alors
$$\#\mathcal{C}(\mathbb{F}_q) \leq q^2 + q + 1 + \left\lfloor \frac{\delta - q}{\eta} \right\rfloor.$$
  - Si $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$ et $q \geq \delta_X$,
$$\#\mathcal{C}(\mathbb{F}_q) \leq q^2 + q + \delta_X.$$
- Si $\eta = 0$,
$$\#\mathcal{C}(\mathbb{F}_q) \leq (q+1)^2 - \max(q - \delta_X + 1, 1)\max(q - \delta_T + 1, 1).$$

Penchons-nous sur le cas $\delta_T < 0$. On pose $C_\eta^\star(\delta_T, \delta_X)$ le code obtenu par poinçonnage de $C_\eta(\delta_T, \delta_X)$ en les points $\mathcal{Z}(X_1)$.

Penchons-nous sur le cas $\delta_T < 0$. On pose $C_\eta^\star(\delta_T,\delta_X)$ le code obtenu par poinçonnage de $C_\eta(\delta_T,\delta_X)$ en les points $\mathcal{Z}(X_1)$.

Proposition - Paramètres du code poinçonné

Soit $\eta \geq 1$, $\delta_T < 0$ et $\delta_X > 0$. Le $C_\eta^\star(\delta_T,\delta_X)$ a longueur $q(q+1)$ et a la même dimension et distance minimale que $C_\eta(\delta_T,\delta_X)$.

Preuve : Un monôme $M = T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \in R(\delta_T,\delta_X)$ sur $\mathcal{H}_\eta$ satisfait

$$0 \leq c_1 + c_2 = \delta_T + \eta d_1 < \eta d_1.$$

Donc $d_1 > 0$ et M s'annule sur $X_1 = 0$.

Penchons-nous sur le cas $\delta_T < 0$. On pose $C^\star_\eta(\delta_T, \delta_X)$ le code obtenu par poinçonnage de $C_\eta(\delta_T, \delta_X)$ en les points $\mathcal{Z}(X_1)$.

Proposition - Paramètres du code poinçonné

Soit $\eta \geq 1$, $\delta_T < 0$ et $\delta_X > 0$. Le $C^\star_\eta(\delta_T, \delta_X)$ a longueur $q(q+1)$ et a la même dimension et distance minimale que $C_\eta(\delta_T, \delta_X)$.

Preuve : Un monôme $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \in R(\delta_T, \delta_X)$ sur $\mathcal{H}_\eta$ satisfait

$$0 \leq c_1 + c_2 = \delta_T + \eta d_1 < \eta d_1.$$

Donc $d_1 > 0$ et M s'annule sur $X_1 = 0$.

η	δ_T	δ_X	Paramètres de $C^\star_\eta(\delta_T, \delta_X)$
1	-1	2	[12,3,8]
1	-1	3	[12,6,4]
2	-1	1	[12,2,9]
2	-1	3	[12,10,2]
2	-2	2	[12,4,6]
2	-2	3	[12,8,3]

1. On pose la relation d'équivalence sur les monômes de bidegré (δ_T, δ_X)

$$M \equiv M' \Leftrightarrow M - M' \in \ker \mathrm{ev}_{(\delta_T, \delta_X)},$$

1. On pose la relation d'équivalence sur les monômes de bidegré (δ_T, δ_X)

$$M \equiv M' \Leftrightarrow M - M' \in \ker \mathrm{ev}_{(\delta_T, \delta_X)},$$

2. Caractériser les monômes qui ont la même évaluation,

1. On pose la relation d'équivalence sur les monômes de bidegré (δ_T, δ_X)

$$M \equiv M' \Leftrightarrow M - M' \in \ker \mathrm{ev}_{(\delta_T, \delta_X)},$$

2. Caractériser les monômes qui ont la même évaluation,
3. Choisir une famille de représentants des monômes sous $\equiv$,

1. On pose la relation d'équivalence sur les monômes de bidegré (δ_T, δ_X)
$$M \equiv M' \iff M - M' \in \ker \mathrm{ev}_{(\delta_T, \delta_X)},$$
2. Caractériser les monômes qui ont la même évaluation,
3. Choisir une famille de représentants des monômes sous $\equiv$,
4. Montrer que cette famille est en fait une base de $R(\delta_T, \delta_X)$ modulo le noyau.

Proposition

Soient (d_2, c_2), $(d_2', c_2') \in \mathcal{P}(\delta_T, \delta_X)$. On pose

$$M = M(d_2, c_2) = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \text{ et } M' = M(d_2', c_2') = T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'}.$$

Alors $M \equiv M'$ si et seulement si

$$q - 1 \mid d_i - d_i', \tag{C1}$$

$$q - 1 \mid c_j - c_j', \tag{C2}$$

$$d_i = 0 \iff d_i' = 0, \tag{C3}$$

$$c_j = 0 \iff c_j' = 0. \tag{C4}$$

Proposition

Soient (d_2, c_2), $(d_2', c_2') \in \mathcal{P}(\delta_T, \delta_X)$. On pose

$$M = M(d_2, c_2) = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \text{ et } M' = M(d_2', c_2') = T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'}.$$

Alors $M \equiv M'$ si et seulement si

$$q - 1 \mid d_i - d_i', \tag{C1}$$
$$q - 1 \mid c_j - c_j', \tag{C2}$$
$$d_i = 0 \Leftrightarrow d_i' = 0, \tag{C3}$$
$$c_j = 0 \Leftrightarrow c_j' = 0. \tag{C4}$$

Idée de la preuve : On peut se convaincre sans trop de difficulté que les conditions sont suffisantes. Pour montrer que c'est nécessaire, on remarque que $M(1, x, 1, 1) = M'(1, x, 1, 1)$ pour tout $x \in \mathbb{F}_q$, ce qui implique que $x^{c_2} = x^{c_2'}$ et donc

$$T_2^q - T_2 \mid T_2^{c_2'} - T_2^{c_2},$$

ce qui donne la condition sur c_2.

Proposition

Soient (d_2, c_2), $(d_2', c_2') \in \mathcal{P}(\delta_T, \delta_X)$. On pose

$$M = M(d_2, c_2) = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \text{ et } M' = M(d_2', c_2') = T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'}.$$

Alors $M \equiv M'$ si et seulement si

$$q - 1 \mid d_i - d_i', \tag{C1}$$
$$q - 1 \mid c_j - c_j', \tag{C2}$$
$$d_i = 0 \Leftrightarrow d_i' = 0, \tag{C3}$$
$$c_j = 0 \Leftrightarrow c_j' = 0. \tag{C4}$$

Idée de la preuve : On peut se convaincre sans trop de difficulté que les conditions sont suffisantes. Pour montrer que c'est nécessaire, on remarque que $M(1, x, 1, 1) = M'(1, x, 1, 1)$ pour tout $x \in \mathbb{F}_q$, ce qui implique que $x^{c_2} = x^{c_2'}$ et donc

$$T_2^q - T_2 \mid T_2^{c_2'} - T_2^{c_2},$$

ce qui donne la condition sur c_2. On fait de même en $(1, 1, 1, x)$ pour d_2 puis on utilise la définition du bidegré pour avoir les conclusions sur d_1 et c_1.

Proposition [Rappel]

$$T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \equiv T_1^{c'_1}T_2^{c'_2}X_1^{d'_1}X_2^{d'_2} \Leftrightarrow \begin{cases} q-1 & \mid d_i - d'_i, \\ q-1 & \mid c_j - c'_j, \\ d_i = 0 & \Leftrightarrow d'_i = 0, \\ c_j = 0 & \Leftrightarrow c'_j = 0. \end{cases}$$

Dessin ! Interprétation de l'ensemble de points que l'on a choisi.

Proposition [Rappel]

$$T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \equiv T_1^{c'_1} T_2^{c'_2} X_1^{d'_1} X_2^{d'_2} \Leftrightarrow \begin{cases} q-1 & \mid d_i - d'_i, \\ q-1 & \mid c_j - c'_j, \\ d_i = 0 & \Leftrightarrow d'_i = 0, \\ c_j = 0 & \Leftrightarrow c'_j = 0. \end{cases}$$

Dessin ! Interprétation de l'ensemble de points que l'on a choisi.

$$\Delta(\delta_T, \delta_X) = \{ M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{K}(\delta_T, \delta_X) \}$$

Proposition

$\Delta(\delta_T, \delta_X)$ forme un système de représentants des monômes de $R(\delta_T, \delta_X)$ modulo $\equiv$.

Proposition [Rappel]

$$T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \equiv T_1^{c'_1}T_2^{c'_2}X_1^{d'_1}X_2^{d'_2} \Leftrightarrow \begin{cases} q-1 & \mid d_i - d'_i, \\ q-1 & \mid c_j - c'_j, \\ d_i = 0 & \Leftrightarrow d'_i = 0, \\ c_j = 0 & \Leftrightarrow c'_j = 0. \end{cases}$$

Dessin ! Interprétation de l'ensemble de points que l'on a choisi.

$$\Delta(\delta_T, \delta_X) = \{M(\alpha,\beta) \mid (\alpha,\beta) \in \mathcal{K}(\delta_T,\delta_X)\}$$

Proposition

$\Delta(\delta_T, \delta_X)$ forme un système de représentants des monômes de $R(\delta_T, \delta_X)$ modulo $\equiv$.

Comment passer à la dimension ?

Proposition [Rappel]

$$T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \equiv T_1^{c'_1}T_2^{c'_2}X_1^{d'_1}X_2^{d'_2} \Leftrightarrow \begin{cases} q-1 & \mid d_i - d'_i, \\ q-1 & \mid c_j - c'_j, \\ d_i = 0 & \Leftrightarrow d'_i = 0, \\ c_j = 0 & \Leftrightarrow c'_j = 0. \end{cases}$$

Dessin ! Interprétation de l'ensemble de points que l'on a choisi.

$$\Delta(\delta_T, \delta_X) = \{M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{K}(\delta_T, \delta_X)\}$$

Proposition

$\Delta(\delta_T, \delta_X)$ forme un système de représentants des monômes de $R(\delta_T, \delta_X)$ modulo $\equiv$.

Comment passer à la dimension ? On définit une application linéaire $\pi_{(\delta_T, \delta_X)}$ de $R(\delta_T, \delta_X)$ qui à chaque monôme associe son représentant dans $\Delta(\delta_T, \delta_X)$.

Théorème

L'application $\pi_{(\delta_T, \delta_X)}$ est la projection de $R(\delta_T, \delta_X)$ le long de $\ker \mathrm{ev}_{(\delta_T, \delta_X)}$ sur $\mathrm{Vect}(\Delta(\delta_T, \delta_X))$. De plus, $\Delta(\delta_T, \delta_X)$ est libre modulo $\ker \mathrm{ev}_{(\delta_T, \delta_X)}$.

Ceci conclut la preuve pour la dimension !

Pour calculer la dimension, on s'est ramené à un problème sur les monômes. On va faire de même pour la distance minimale via les bases de Gröbner.

Pour calculer la dimension, on s'est ramené à un problème sur les monômes. On va faire de même pour la distance minimale via les bases de Gröbner.

Soit R un anneau de polynômes. Un *ordre monomial* est un ordre total $<$ sur les monômes tel que pour tous monômes M, N, P,

$$M < N \Rightarrow MP < NP \text{ et } M < MP.$$

Pour calculer la dimension, on s'est ramené à un problème sur les monômes. On va faire de même pour la distance minimale via les bases de Gröbner.

Soit R un anneau de polynômes. Un *ordre monomial* est un ordre total $<$ sur les monômes tel que pour tous monômes M, N, P,

$$M < N \Rightarrow MP < NP \text{ et } M < MP.$$

Pour chaque polynôme $F \in R$, on note son *terme dominant* $\mathrm{LT}(F)$.

Pour calculer la dimension, on s'est ramené à un problème sur les monômes. On va faire de même pour la distance minimale via les bases de Gröbner.

Soit R un anneau de polynômes. Un *ordre monomial* est un ordre total $<$ sur les monômes tel que pour tous monômes M, N, P,

$$M < N \;\Rightarrow\; MP < NP \text{ et } M < MP.$$

Pour chaque polynôme $F \in R$, on note son *terme dominant* $\mathrm{LT}(F)$.
Soit I un idéal de R, muni d'un ordre monomial $<$. L'*idéal monomial* $\mathrm{LT}(I) \subset R$ associé à I est l'idéal engendré par les termes dominants $\mathrm{LT}(F)$ des polynômes $F \in I$, c'est-à-dire

$$\mathrm{LT}(I) = \langle \mathrm{LT}(F) \mid F \in I \rangle$$

Pour calculer la dimension, on s'est ramené à un problème sur les monômes. On va faire de même pour la distance minimale via les bases de Gröbner.

Soit R un anneau de polynômes. Un *ordre monomial* est un ordre total $<$ sur les monômes tel que pour tous monômes M, N, P,

$$M < N \Rightarrow MP < NP \text{ et } M < MP.$$

Pour chaque polynôme $F \in R$, on note son *terme dominant* $\mathrm{LT}(F)$.
Soit I un idéal de R, muni d'un ordre monomial $<$. L'*idéal monomial* $\mathrm{LT}(I) \subset R$ associé à I est l'idéal engendré par les termes dominants $\mathrm{LT}(F)$ des polynômes $F \in I$, c'est-à-dire

$$\mathrm{LT}(I) = \langle \mathrm{LT}(F) \mid F \in I \rangle$$

Un sous-ensemble G de R est une *base de Gröbner* de I si G engendre l'idéal I et les termes dominants des polynômes de G engendrent $\mathrm{LT}(I)$.

Pour calculer la dimension, on s'est ramené à un problème sur les monômes. On va faire de même pour la distance minimale via les bases de Gröbner.

Soit R un anneau de polynômes. Un *ordre monomial* est un ordre total $<$ sur les monômes tel que pour tous monômes M, N, P,

$$M < N \Rightarrow MP < NP \text{ et } M < MP.$$

Pour chaque polynôme $F \in R$, on note son *terme dominant* $\mathrm{LT}(F)$.
Soit I un idéal de R, muni d'un ordre monomial $<$. L'*idéal monomial* $\mathrm{LT}(I) \subset R$ associé à I est l'idéal engendré par les termes dominants $\mathrm{LT}(F)$ des polynômes $F \in I$, c'est-à-dire

$$\mathrm{LT}(I) = \langle \mathrm{LT}(F) \mid F \in I \rangle$$

Un sous-ensemble G de R est une *base de Gröbner* de I si G engendre l'idéal I et les termes dominants des polynômes de G engendrent $\mathrm{LT}(I)$.

Le résultat qui nous intéresse : une base du quotient

Soit I un idéal de R de base de Gröbner G. Alors, en posant π la projection canonique de R sur R/I, l'ensemble

$$\{\pi(M) \mid M \text{ monômes de } R \text{ tels que pour tout } g \in G,\ \mathrm{LT}(g) \nmid M\}$$

est une base de l'espace vectoriel R/I.

Exhibons l'idéal qui va nous intéresser.

Considérons l'application sur l'anneau R

$$\mathrm{ev} : \left\{ \begin{array}{rcl} R & \to & \mathbb{F}_q^N \\ F = \sum\limits_{(\delta_T,\delta_X)} F_{(\delta_T,\delta_X)} & \mapsto & \sum\limits_{(\delta_T,\delta_X)} \mathrm{ev}_{(\delta_T,\delta_X)}\left(F_{(\delta_T,\delta_X)}\right) \end{array} \right. ,$$

et son noyau $\mathcal{I} = \ker \mathrm{ev} \subset R$.

C'est un idéal gradué $\mathcal{I} = \bigoplus\limits_{(\delta_T,\delta_X)\in\mathbb{Z}\times\mathbb{N}} \mathcal{I}(\delta_T,\delta_X)$, où $\mathcal{I}(\delta_T,\delta_X) = \ker \mathrm{ev}_{(\delta_T,\delta_X)}$.

Exhibons l'idéal qui va nous intéresser.
Considérons l'application sur l'anneau R

$$\mathrm{ev} : \left\{ \begin{array}{rcl} R & \to & \mathbb{F}_q^N \\ F = \sum\limits_{(\delta_T,\delta_X)} F_{(\delta_T,\delta_X)} & \mapsto & \sum\limits_{(\delta_T,\delta_X)} \mathrm{ev}_{(\delta_T,\delta_X)}\left(F_{(\delta_T,\delta_X)}\right) \end{array} \right. ,$$

et son noyau $\mathcal{I} = \ker \mathrm{ev} \subset R$.
C'est un idéal gradué $\mathcal{I} = \bigoplus\limits_{(\delta_T,\delta_X)\in\mathbb{Z}\times\mathbb{N}} \mathcal{I}(\delta_T,\delta_X)$, où $\mathcal{I}(\delta_T,\delta_X) = \ker \mathrm{ev}_{(\delta_T,\delta_X)}$.

On pose un ordre monomial sur R.

$$T_1^{c_1'}T_2^{c_2'}X_1^{d_1'}X_2^{d_2'} < T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2}$$

si $d_1'+d_2' < d_1+d_2$ ou $\left| \begin{array}{rl} d_1'+d_2' & = d_1+d_2 \\ d_2' & < d_2 \end{array} \right.$ ou $\left| \begin{array}{rl} d_1' & = d_1 \\ d_2' & = d_2 \\ c_2' & < c_2 \end{array} \right.$ ou $\left| \begin{array}{rl} d_1' & = d_1 \\ d_2' & = d_2 \\ c_2' & = c_2 \\ c_1' & < c_1 \end{array} \right.$

Soit $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$. On pose

$$\mathcal{G}(\delta_T, \delta_X) = \{M - M' \mid M,\ M' \text{ monômes de } R(\delta_T, \delta_X) \text{ tels que } M \equiv M'\}$$

et

$$\mathcal{G} = \bigcup_{(\delta_T, \delta_X)} \mathcal{G}(\delta_T, \delta_X).$$

Soit $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$. On pose

$$\mathcal{G}(\delta_T, \delta_X) = \{M - M' \mid M,\ M' \text{ monômes de } R(\delta_T, \delta_X) \text{ tels que } M \equiv M'\}$$

et

$$\mathcal{G} = \bigcup_{(\delta_T, \delta_X)} \mathcal{G}(\delta_T, \delta_X).$$

Proposition

$\mathcal{G}$ est une base de Gröbner de $\mathcal{I}$.

Soit $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$. On pose

$$\mathcal{G}(\delta_T, \delta_X) = \{M - M' \mid M,\ M' \text{ monômes de } R(\delta_T, \delta_X) \text{ tels que } M \equiv M'\}$$

et

$$\mathcal{G} = \bigcup_{(\delta_T, \delta_X)} \mathcal{G}(\delta_T, \delta_X).$$

Proposition

$\mathcal{G}$ est une base de Gröbner de $\mathcal{I}$.

Puisque $\mathcal{I}$ est homogène, on a ${}^{R}\!/_{I} = \bigoplus_{(\delta_T, \delta_X)} \left({}^{R(\delta_T, \delta_X)}\!/_{I(\delta_T, \delta_X)} \right)$.

Soit $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$. On pose

$$\mathcal{G}(\delta_T, \delta_X) = \{M - M' \mid M,\ M' \text{ monômes de } R(\delta_T, \delta_X) \text{ tels que } M \equiv M'\}$$

et

$$\mathcal{G} = \bigcup_{(\delta_T, \delta_X)} \mathcal{G}(\delta_T, \delta_X).$$

Proposition

$\mathcal{G}$ est une base de Gröbner de $\mathcal{I}$.

Puisque $\mathcal{I}$ est homogène, on a $R \big/ I = \bigoplus_{(\delta_T, \delta_X)} \left(R(\delta_T, \delta_X) \big/ I(\delta_T, \delta_X) \right)$.

Application à notre cas

Pour tout $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ tel que $\delta \geq 0$, une base d'un supplémentaire de $\mathcal{I}(\delta_T, \delta_X)$ dans $R(\delta_T, \delta_X)$ est $\{M \text{ monômes de } R(\delta_T, \delta_X) \mid \forall\, g \in \mathcal{G},\ \mathrm{LT}(g) \nmid M\}$.

Soit $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$. On pose

$$\mathcal{G}(\delta_T, \delta_X) = \{M - M' \mid M,\ M' \text{ monômes de } R(\delta_T, \delta_X) \text{ tels que } M \equiv M'\}$$

et

$$\mathcal{G} = \bigcup_{(\delta_T, \delta_X)} \mathcal{G}(\delta_T, \delta_X).$$

Proposition

$\mathcal{G}$ est une base de Gröbner de $\mathcal{I}$.

Puisque $\mathcal{I}$ est homogène, on a $R \big/ I = \bigoplus_{(\delta_T, \delta_X)} \left(R(\delta_T, \delta_X) \big/ I(\delta_T, \delta_X) \right)$.

Application à notre cas

Pour tout $(\delta_T, \delta_X) \in \mathbb{Z} \times \mathbb{N}$ tel que $\delta \geq 0$, une base d'un supplémentaire de $\mathcal{I}(\delta_T, \delta_X)$ dans $R(\delta_T, \delta_X)$ est $\{M \text{ monômes de } R(\delta_T, \delta_X) \mid \forall\, g \in \mathcal{G},\ \mathrm{LT}(g) \nmid M\}$.

Proposition

$\Delta(\delta_T, \delta_X)$ est exactement l'ensemble des monômes de $R(\delta_T, \delta_X)$ qui ne sont divisibles par le terme dominant d'aucun polynôme de $\mathcal{G}$.

Soit $(\varepsilon_T, \varepsilon_X) \in \mathbb{N}^2$ tel que $\varepsilon_T,\ \varepsilon_X \geq q$. On pose

$$\Delta(\varepsilon_T, \varepsilon_X)_F = \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\}.$$

Minoration de la distance minimale

La distance minimale vérifie $d_\eta(\delta_T, \delta_X) \geq \min_{M \in \Delta(\delta_T, \delta_X)} \#\Delta(\varepsilon_T, \varepsilon_X)_M$.

Soit $(\varepsilon_T, \varepsilon_X) \in \mathbb{N}^2$ tel que $\varepsilon_T,\ \varepsilon_X \geq q$. On pose

$$\Delta(\varepsilon_T, \varepsilon_X)_F = \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\}.$$

Minoration de la distance minimale

La distance minimale vérifie $d_\eta(\delta_T, \delta_X) \geq \min\limits_{M \in \Delta(\delta_T, \delta_X)} \#\Delta(\varepsilon_T, \varepsilon_X)_M$.

Esquissons la preuve.

On a posé $\langle F \rangle_{(\varepsilon_T, \varepsilon_X)}$ le sev $FR(\varepsilon_T - \delta_T, \varepsilon_X - \delta_X) \subset R(\varepsilon_T, \varepsilon_X)$ engendré par F.

$$\tilde{N}_F = \dim \left(R(\varepsilon_T, \varepsilon_X) \big/ \ker \mathrm{ev}_{(\varepsilon_T, \varepsilon_X)} + \langle F \rangle_{(\varepsilon_T, \varepsilon_X)} \right).$$

$$\Rightarrow d_\eta(\delta_T, \delta_X) \geq \min_{F \in \mathrm{Vect}\, \Delta(\delta_T, \delta_X)} N - \tilde{N}_F. \qquad (4)$$

On veut minorer cette quantité.

Soit $(\varepsilon_T, \varepsilon_X) \in \mathbb{N}^2$ tel que $\varepsilon_T,\ \varepsilon_X \geq q$. On pose

$$\Delta(\varepsilon_T, \varepsilon_X)_F = \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\}.$$

Minoration de la distance minimale

La distance minimale vérifie $d_\eta(\delta_T, \delta_X) \geq \min\limits_{M \in \Delta(\delta_T, \delta_X)} \#\Delta(\varepsilon_T, \varepsilon_X)_M$.

Esquissons la preuve.

On a posé $\langle F \rangle_{(\varepsilon_T, \varepsilon_X)}$ le sev $FR(\varepsilon_T - \delta_T, \varepsilon_X - \delta_X) \subset R(\varepsilon_T, \varepsilon_X)$ engendré par F.

$$\tilde{N}_F = \dim \left(R(\varepsilon_T, \varepsilon_X) \Big/ \ker \mathrm{ev}_{(\varepsilon_T, \varepsilon_X)} + \langle F \rangle_{(\varepsilon_T, \varepsilon_X)} \right).$$

$$\Rightarrow d_\eta(\delta_T, \delta_X) \geq \min_{F \in \mathrm{Vect}\, \Delta(\delta_T, \delta_X)} N - \tilde{N}_F. \tag{4}$$

On veut minorer cette quantité. On sait que

$$\Delta(\varepsilon_T, \varepsilon_X) = \{M \text{ monômes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, g \in \mathcal{G},\ LT(g) \nmid M\}$$

est une base $R(\varepsilon_T, \varepsilon_X)$ modulo $\mathcal{I}(\varepsilon_T, \varepsilon_X)$. Par surjectivité, $\#\Delta(\varepsilon_T, \varepsilon_X) = N$.

Soit $(\varepsilon_T, \varepsilon_X) \in \mathbb{N}^2$ tel que ε_T, $\varepsilon_X \geq q$. On pose

$$\Delta(\varepsilon_T, \varepsilon_X)_F = \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\}.$$

Minoration de la distance minimale

La distance minimale vérifie $d_\eta(\delta_T, \delta_X) \geq \min_{M \in \Delta(\delta_T, \delta_X)} \#\Delta(\varepsilon_T, \varepsilon_X)_M$.

Esquissons la preuve.

On a posé $\langle F\rangle_{(\varepsilon_T, \varepsilon_X)}$ le sev $FR(\varepsilon_T - \delta_T, \varepsilon_X - \delta_X) \subset R(\varepsilon_T, \varepsilon_X)$ engendré par F.

$$\tilde{N}_F = \dim \left(R(\varepsilon_T, \varepsilon_X) \big/ \ker \mathrm{ev}_{(\varepsilon_T, \varepsilon_X)} + \langle F\rangle_{(\varepsilon_T, \varepsilon_X)} \right).$$

$$\Rightarrow d_\eta(\delta_T, \delta_X) \geq \min_{F \in \mathrm{Vect}\, \Delta(\delta_T, \delta_X)} N - \tilde{N}_F. \tag{4}$$

On veut minorer cette quantité. On sait que

$$\Delta(\varepsilon_T, \varepsilon_X) = \{M \text{ monômes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, g \in \mathcal{G},\ LT(g) \nmid M\}$$

est une base $R(\varepsilon_T, \varepsilon_X)$ modulo $\mathcal{I}(\varepsilon_T, \varepsilon_X)$. Par surjectivité, $\#\Delta(\varepsilon_T, \varepsilon_X) = N$.

Sachant que F est homogène, l'idéal $\mathcal{I} + \langle F\rangle$ est homogène.

Soit $(\varepsilon_T, \varepsilon_X) \in \mathbb{N}^2$ tel que $\varepsilon_T,\ \varepsilon_X \geq q$. On pose

$$\Delta(\varepsilon_T, \varepsilon_X)_F = \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\}.$$

Minoration de la distance minimale

La distance minimale vérifie $d_\eta(\delta_T, \delta_X) \geq \min\limits_{M \in \Delta(\delta_T, \delta_X)} \#\Delta(\varepsilon_T, \varepsilon_X)_M$.

Esquissons la preuve.

On a posé $\langle F \rangle_{(\varepsilon_T, \varepsilon_X)}$ le sev $FR(\varepsilon_T - \delta_T, \varepsilon_X - \delta_X) \subset R(\varepsilon_T, \varepsilon_X)$ engendré par F.

$$\tilde{N}_F = \dim \left({R(\varepsilon_T, \varepsilon_X)} \big/ {\ker \mathrm{ev}_{(\varepsilon_T, \varepsilon_X)} + \langle F \rangle_{(\varepsilon_T, \varepsilon_X)}} \right).$$

$$\Rightarrow d_\eta(\delta_T, \delta_X) \geq \min_{F \in \mathrm{Vect}\, \Delta(\delta_T, \delta_X)} N - \tilde{N}_F. \tag{4}$$

On veut minorer cette quantité. On sait que

$$\Delta(\varepsilon_T, \varepsilon_X) = \{M \text{ monômes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, g \in \mathcal{G},\ LT(g) \nmid M\}$$

est une base $R(\varepsilon_T, \varepsilon_X)$ modulo $\mathcal{I}(\varepsilon_T, \varepsilon_X)$. Par surjectivité, $\#\Delta(\varepsilon_T, \varepsilon_X) = N$.

Sachant que F est homogène, l'idéal $\mathcal{I} + \langle F \rangle$ est homogène.

Soit $\widehat{\mathcal{G}}$ une base de Gröbner de $\mathcal{I} + \langle F \rangle$ contenant $\mathcal{G} \cup \{F\}$.

Alors $\tilde{\Delta}(\varepsilon_T, \varepsilon_X) = \{M$ monônes de $R(\varepsilon_T, \varepsilon_X)$ tels que $\forall\, h \in \widehat{\mathcal{G}},\ LT(h) \nmid M\}$ est une base de $R(\varepsilon_T, \varepsilon_X)$ modulo $\mathcal{I}(\varepsilon_T, \varepsilon_X) + \langle F \rangle_{(\varepsilon_T, \varepsilon_X)}$ de cardinal $\tilde{N}_F$.

On a donc

$$\Delta(\varepsilon_T, \varepsilon_X) = \{M \text{ monômes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, g \in \mathcal{G},\ LT(g) \nmid M\}$$

de cardinal N et

$$\tilde{\Delta}(\varepsilon_T, \varepsilon_X) = \{M \text{ monônes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, h \in \widehat{\mathcal{G}},\ LT(h) \nmid M\}$$

de cardinal $\tilde{N}_F$. De plus,

$$\Delta(\varepsilon_T, \varepsilon_X) \smallsetminus \tilde{\Delta}(\varepsilon_T, \varepsilon_X) = \{M \in \Delta(\varepsilon_T, \varepsilon_X) \text{ tq } \exists\, g \in \hat{\mathcal{G}} \smallsetminus \mathcal{G},\ \mathrm{LT}(g) \mid M\}.$$

Sachant que $F \in \widehat{\mathcal{G}} \smallsetminus \mathcal{G}$, on a
$\Delta(\varepsilon_T, \varepsilon_X)_F \underset{\text{rappel}}{=} \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\} \subset \Delta(\varepsilon_T, \varepsilon_X) \smallsetminus \tilde{\Delta}(\varepsilon_T, \varepsilon_X)$.
D'où $\#\Delta(\varepsilon_T, \varepsilon_X)_F \leq N - \tilde{N}_F$.

On a donc

$$\Delta(\varepsilon_T, \varepsilon_X) = \{M \text{ monômes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, g \in \mathcal{G},\ LT(g) \nmid M\}$$

de cardinal N et

$$\tilde{\Delta}(\varepsilon_T, \varepsilon_X) = \{M \text{ monônes de } R(\varepsilon_T, \varepsilon_X) \text{ tels que } \forall\, h \in \widehat{\mathcal{G}},\ LT(h) \nmid M\}$$

de cardinal $\tilde{N}_F$. De plus,

$$\Delta(\varepsilon_T, \varepsilon_X) \setminus \tilde{\Delta}(\varepsilon_T, \varepsilon_X) = \{M \in \Delta(\varepsilon_T, \varepsilon_X) \text{ tq } \exists\, g \in \hat{\mathcal{G}} \setminus \mathcal{G},\ \mathrm{LT}(g) \mid M\}.$$

Sachant que $F \in \widehat{\mathcal{G}} \setminus \mathcal{G}$, on a
$\Delta(\varepsilon_T, \varepsilon_X)_F \underset{\text{rappel}}{=} \{N \in \Delta(\varepsilon_T, \varepsilon_X) \mid \mathrm{LT}(F) \mid N\} \subset \Delta(\varepsilon_T, \varepsilon_X) \setminus \tilde{\Delta}(\varepsilon_T, \varepsilon_X)$.
D'où $\#\Delta(\varepsilon_T, \varepsilon_X)_F \leq N - \tilde{N}_F$.

Pour terminer, remarquons que $\Delta(\varepsilon_T, \varepsilon_X)_F = \Delta(\varepsilon_T, \varepsilon_X)_{\mathrm{LT}(F)}$.