Codes correcteurs sur les surfaces de Hirzebruch

Jade Nardi

Jeudi 7 février

Cadre : Théorie de l'information créée par Shannon $\sim$ 1950

But : Améliorer/Préserver la qualité des systèmes de transmissions de données à travers l'espace (réseaux téléphoniques, communications par satellite) ou le temps (bandes magnétiques, disques optiques, etc.).

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

2	93	01	13	155	363	83
Sexe	Année	Mois	Depart.	Commune	Rang	Clé

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

2	93	01	13	155	363	83
Sexe	Année	Mois	Depart.	Commune	Rang	Clé

Clé $\equiv 97 - N \ [97]$ où N est le nombre formé des 13 premiers chiffres.

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

2	93	01	13	155	363	83
Sexe	Année	Mois	Depart.	Commune	Rang	Clé

Clé $\equiv 97 - N \ [97]$ où N est le nombre formé des 13 premiers chiffres.
S'il y a une erreur, disons $2\,93\,01\,\mathbf{1}5\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ et $68 + 83 \not\equiv 0 \ [97]$
Clé courte + / - Pas de correction

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

2	93	01	13	155	363	83
Sexe	Année	Mois	Depart.	Commune	Rang	Clé

Clé $\equiv 97 - N \ [97]$ où N est le nombre formé des 13 premiers chiffres.
S'il y a une erreur, disons $2\,93\,01\,\mathbf{1}5\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ et $68 + 83 \not\equiv 0 \ [97]$
Clé courte + / - Pas de correction

Exemple 2 : Envoyer trois fois le message
On veut envoyer le message 001. On envoie $m = 001001001$.

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

2	93	01	13	155	363	83
Sexe	Année	Mois	Depart.	Commune	Rang	Clé

Clé $\equiv 97 - N \ [97]$ où N est le nombre formé des 13 premiers chiffres.
S'il y a une erreur, disons $2\,93\,01\,\mathbf{1}5\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ et $68 + 83 \not\equiv 0 \ [97]$
Clé courte + / - Pas de correction

Exemple 2 : Envoyer trois fois le message
On veut envoyer le message 001. On envoie $m = 001001001$.
S'il y a une erreur et le destinataire reçoit $\tilde{m} = 001\mathbf{1}01001$, il peut la détecter et la corriger.

On veut transmettre un message m qui risque d'être détérioré lors de la transmission. On veut que le destinataire puisse détecter s'il y a une erreur voire la corriger.
Idée : Ajouter de la **redondance**.

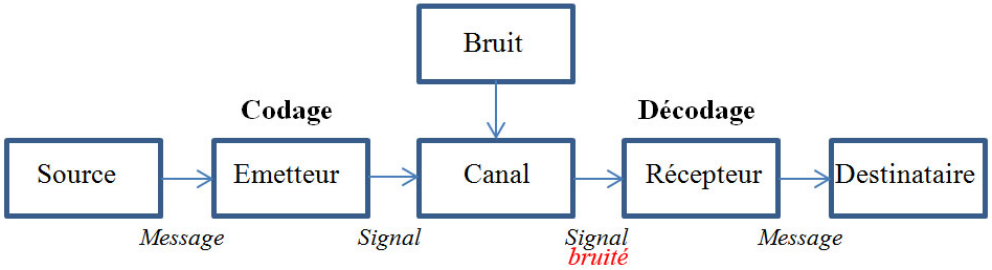
Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

2	93	01	13	155	363	83
Sexe	Année	Mois	Depart.	Commune	Rang	Clé

Clé $\equiv 97 - N \ [97]$ où N est le nombre formé des 13 premiers chiffres.
S'il y a une erreur, disons $2\,93\,01\,\mathbf{1}5\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ et $68 + 83 \not\equiv 0 \ [97]$
Clé courte + / - Pas de correction

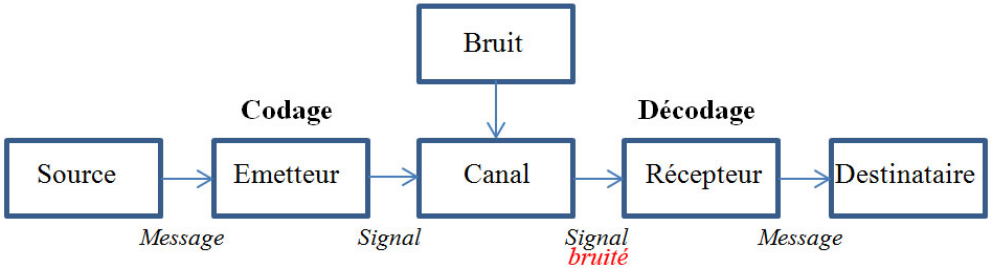
Exemple 2 : Envoyer trois fois le message
On veut envoyer le message 001. On envoie $m = 001001001$.
S'il y a une erreur et le destinataire reçoit $\tilde{m} = 001\mathbf{1}01001$, il peut la détecter et la corriger.
A partir de deux erreurs, on n'a plus de garantie. Si $\tilde{m} = \mathbf{1}01\mathbf{1}01\mathbf{0}01$, m ou 101101101 ?
Correction d'une erreur + / - Longueur du message envoyé

Soit p un nombre premier, $e \in \mathbb{N}$ et $q = p^e$.



Message à transmettre : vecteur $m \in (\mathbb{F}_q)^k$.

Soit p un nombre premier, $e \in \mathbb{N}$ et $q = p^e$.

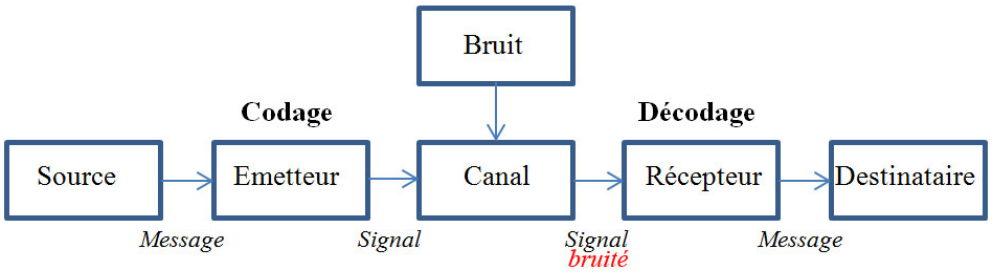


Message à transmettre : vecteur $m \in (\mathbb{F}_q)^k$.
Encodage : Fonction injective

$$E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$$

Si l'encodage est linéaire, cela définit un *sous-espace vectoriel* C de $(\mathbb{F}_q)^n$ de dimension k.

Soit p un nombre premier, $e \in \mathbb{N}$ et $q = p^e$.

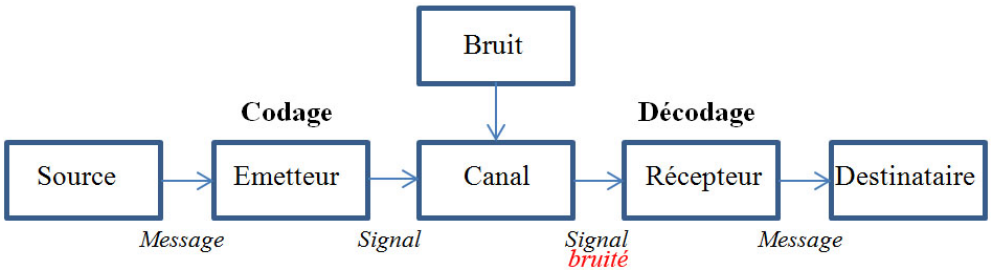


Message à transmettre : vecteur $m \in (\mathbb{F}_q)^k$.
Encodage : Fonction injective

$$E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$$

Si l'encodage est linéaire, cela définit un *sous-espace vectoriel* C de $(\mathbb{F}_q)^n$ de dimension k.
Transmission du mot du code $E(m) = x$ à travers le canal (transmissions indépendantes et sans effacement)
Message reçu : $y = x + e$.

Soit p un nombre premier, $e \in \mathbb{N}$ et $q = p^e$.



Message à transmettre : vecteur $m \in (\mathbb{F}_q)^k$.
Encodage : Fonction injective

$$E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$$

Si l'encodage est linéaire, cela définit un *sous-espace vectoriel* C de $(\mathbb{F}_q)^n$ de dimension k.
Transmission du mot du code $E(m) = x$ à travers le canal (transmissions indépendantes et sans effacement)
Message reçu : $y = x + e$.
Décodage :

$$D : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^k$$

tel que $D \circ E = Id$
Fait correspondre à tout vecteur reçu y de F un vecteur corrigé qui soit l'un des mots de code le plus vraisemblablement émis.

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.
Soit $x \in C$. Le poids du mot x est donné par

$$\omega(x) = \#\{i \in \{1, \ldots, n\},\ x_i \neq 0\}$$

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.
Soit $x \in C$. Le poids du mot x est donné par

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$$

Soient $x,\ y \in C$. La *distance de Hamming* entre x et y est définie par

$$d(x, y) = \#\{i \in \{1, \dots, n\},\ x_i \neq y_i\}$$

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.
Soit $x \in C$. Le poids du mot x est donné par

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$$

Soient $x,\ y \in C$. La *distance de Hamming* entre x et y est définie par

$$d(x, y) = \#\{i \in \{1, \dots, n\},\ x_i \neq y_i\} = \omega(x - y)$$

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.
Soit $x \in C$. Le poids du mot x est donné par

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$$

Soient $x,\ y \in C$. La *distance de Hamming* entre x et y est définie par

$$d(x, y) = \#\{i \in \{1, \dots, n\},\ x_i \neq y_i\} = \omega(x - y)$$

La *distance minimale du code* C est définie par

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$$

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.
Soit $x \in C$. Le poids du mot x est donné par

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$$

Soient $x,\ y \in C$. La *distance de Hamming* entre x et y est définie par

$$d(x, y) = \#\{i \in \{1, \dots, n\},\ x_i \neq y_i\} = \omega(x - y)$$

La *distance minimale du code* C est définie par

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\} = \min_{x \in C} \omega(x)$$

Définition

Un *code linéaire* C sur $\mathbb{F}_q$ de longueur n est un sous-espace vectoriel $\mathbb{F}_q^n$. On note k sa dimension.
Soit $x \in C$. Le poids du mot x est donné par

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$$

Soient $x,\ y \in C$. La *distance de Hamming* entre x et y est définie par

$$d(x, y) = \#\{i \in \{1, \dots, n\},\ x_i \neq y_i\} = \omega(x - y)$$

La *distance minimale du code* C est définie par

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\} = \min_{x \in C} \omega(x)$$

Un code linéaire de longueur n, de dimension k et de distance minimale d est dit $[n, k, d]$.
On dit qu'il a un *taux de correction* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.
On définit le taux de transmission $\kappa = \frac{k}{n}$ et la distance relative $\delta = \frac{d}{n}$.

Te taux de transmission : $\kappa = \frac{k}{n}$
Distance relative $\delta = \frac{d}{n}$

Borne de Singleton : $\delta + \kappa \leq 1 + \frac{1}{n}$.

Te taux de transmission : $\kappa = \frac{k}{n}$
Distance relative $\delta = \frac{d}{n}$

Borne de Singleton : $\delta + \kappa \leq 1 + \frac{1}{n}$.

Borne asymptotique de Gilbert-Varshamov : A q fixé et quand $n \to +\infty$,

$$\sup_{C\ q-\text{aire}} \{\kappa(C) \mid \delta(C) = \delta\} \geq 1 - H_q(\delta)$$

où $H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$.

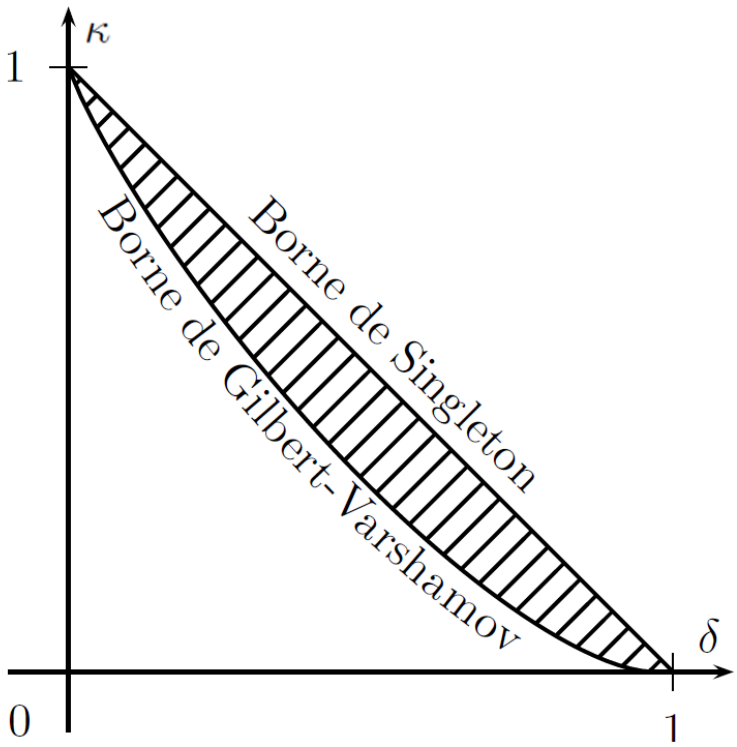
Te taux de transmission : $\kappa = \frac{k}{n}$
Distance relative $\delta = \frac{d}{n}$

Borne de Singleton : $\delta + \kappa \leq 1 + \frac{1}{n}$.

Borne asymptotique de Gilbert-Varshamov : A q fixé et quand $n \to +\infty$,

$$\sup_{C\ q-\text{aire}} \{\kappa(C) \mid \delta(C) = \delta\} \geq 1 - H_q(\delta)$$

où $H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$.



Soit $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$ et $k \leq n$. On considère le **code de Reed-Solomon**

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)),\ f \in \mathbb{F}_q[X]_{\leq k-1}\}$$

C'est un code de type $[n, k, n-k+1]$.

Soit $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$ et $k \leq n$. On considère le **code de Reed-Solomon**

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)),\ f \in \mathbb{F}_q[X]_{\leq k-1}\}$$

C'est un code de type $[n, k, n-k+1]$.

Preuve pour la distance minimale :
Soit $(f(\alpha_1), \ldots, f(\alpha_n))$ un mot de poids minimal non nul. Soit $I = \{i \in \{1, \ldots, n\} \mid f(\alpha_i) = 0\}$. Alors, puisque $\deg f \leq k-1$, $\#I \leq k-1$. Donc $d \geq n - (k-1)$. De plus, pour

$$f(X) = \prod_{i=1}^{k-1} (X - \alpha_i)$$

le mot du code associé à f est exactement de poids $n - (k-1)$. Donc $d \leq n - (k-1)$.

Soit $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$ et $k \leq n$. On considère le **code de Reed-Solomon**

$$C = \{(f(\alpha_1), \ldots, f(\alpha_n)),\ f \in \mathbb{F}_q[X]_{\leq k-1}\}$$

C'est un code de type $[n, k, n-k+1]$.

Preuve pour la distance minimale :
Soit $(f(\alpha_1), \ldots, f(\alpha_n))$ un mot de poids minimal non nul. Soit $I = \{i \in \{1, \ldots, n\} \mid f(\alpha_i) = 0\}$. Alors, puisque $\deg f \leq k-1$, $\#I \leq k-1$. Donc $d \geq n - (k-1)$. De plus, pour

$$f(X) = \prod_{i=1}^{k-1} (X - \alpha_i)$$

le mot du code associé à f est exactement de poids $n - (k-1)$. Donc $d \leq n - (k-1)$.

En d'autres termes, la distance minimale est égale à

$$n - \max\{i \mid f(\alpha_i) = 0\}$$

Connaître la distance minimale du code est équivalent à connaitre le nombre maximal de zéros des polynômes que l'on considère.

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 : quotient**
  On fait agir $\bar{\mathbb{F}} \times \bar{\mathbb{F}}$ 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 $(\lambda, \mu) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$.

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

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

- 1^e **point de vue : quotient**
  On fait agir $\bar{\mathbb{F}} \times \bar{\mathbb{F}}$ 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 $(\lambda, \mu) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$.

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

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

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

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

- 1^e **point de vue : quotient**
  On fait agir $\bar{\mathbb{F}} \times \bar{\mathbb{F}}$ 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 $(\lambda, \mu) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$.

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

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

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

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

On va construire un code type Reed-Solomon, en évaluant des **polynômes** de $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
On munit R d'une **graduation**, c'est-à-dire on donne un *degré* à chaque monôme.

On va construire un code type Reed-Solomon, en évaluant des **polynômes** de $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
On munit R d'une **graduation**, c'est-à-dire on donne un *degré* à chaque monôme.
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 type Reed-Solomon, en évaluant des **polynômes** de $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
On munit R d'une **graduation**, c'est-à-dire on donne un *degré* à chaque monôme.
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

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

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 $\mathbb{F}_q$-*rationnel* si l'orbite contient au moins un représentant à coordonnées dans $\mathbb{F}_q$.

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 $\mathbb{F}_q$-*rationnel* si l'orbite contient au moins un représentant à coordonnées dans $\mathbb{F}_q$.

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 $\mathbb{F}_q$-*rationnel* si l'orbite contient au moins un représentant à coordonnées dans $\mathbb{F}_q$.

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.

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 $\mathbb{F}_q$-*rationnel* si l'orbite contient au moins un représentant à coordonnées dans $\mathbb{F}_q$.

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

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \begin{cases} R(\delta_T,\delta_X) & \to & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P\in\mathcal{H}\eta(\mathbb{F}_q)}. \end{cases} \tag{3}$$

Déterminons la **dimension** du code

$$\dim\left(R(\delta_T,\delta_X)\big/_{\ker \mathrm{ev}_{(\delta_T,\delta_X)}}\right)$$

La stratégie :

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

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

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

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T,\delta_X) & \to & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P\in\mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{3}$$

Déterminons la **dimension** du code

$$\dim\left(R(\delta_T,\delta_X)\big/_{\ker \mathrm{ev}_{(\delta_T,\delta_X)}}\right)$$

La stratégie :

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,

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

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T,\delta_X) & \to & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P\in\mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{3}$$

Déterminons la **dimension** du code

$$\dim\left(R(\delta_T,\delta_X)/\ker \mathrm{ev}_{(\delta_T,\delta_X)}\right)$$

La stratégie :

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 $\equiv$,

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

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T,\delta_X) & \to & \mathbb{F}_q^N \\ F & \mapsto & (F(P))_{P\in\mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{3}$$

Déterminons la **dimension** du code

$$\dim\left(R(\delta_T,\delta_X)/\ker \mathrm{ev}_{(\delta_T,\delta_X)}\right)$$

La stratégie :

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 $\equiv$,
4. Montrer que cette famille est en fait une base de $R(\delta_T, \delta_X)$ modulo le noyau.

On rappelle qu'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

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

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

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

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

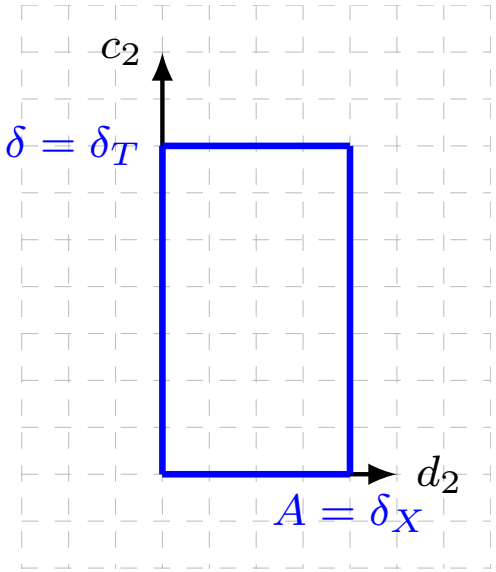
Ce n'est pas toujours un entier !

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

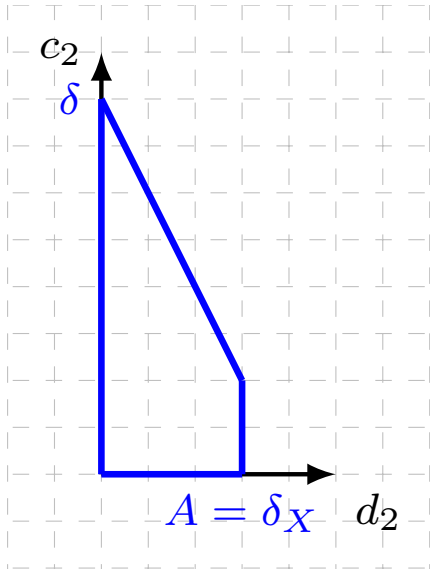
On note A l'abscisse des sommets les plus à droite.

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

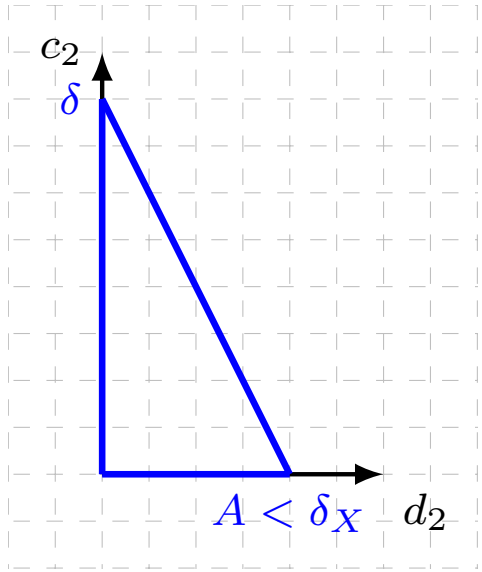
Ce n'est pas toujours un entier !



$\eta = 0$
e.g. $\mathcal{P}(7, 4)$ in $\mathcal{H}_0$



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



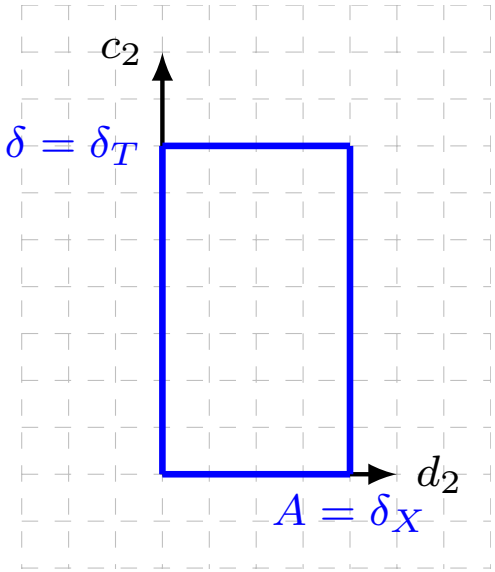
$\eta > 0$, $\delta_T \leq 0$
e.g. $\mathcal{P}(-2, 5)$ in $\mathcal{H}_2$

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

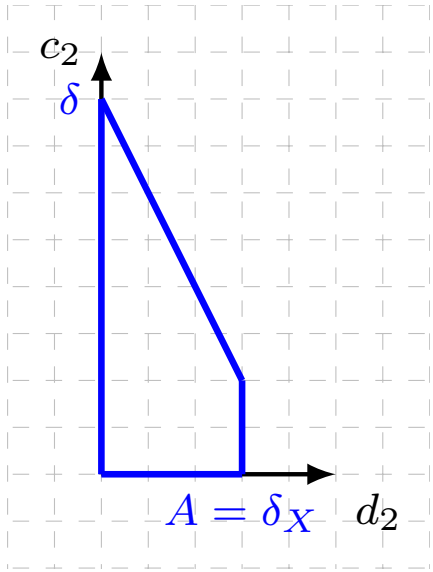
On note A l'abscisse des sommets les plus à droite.

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

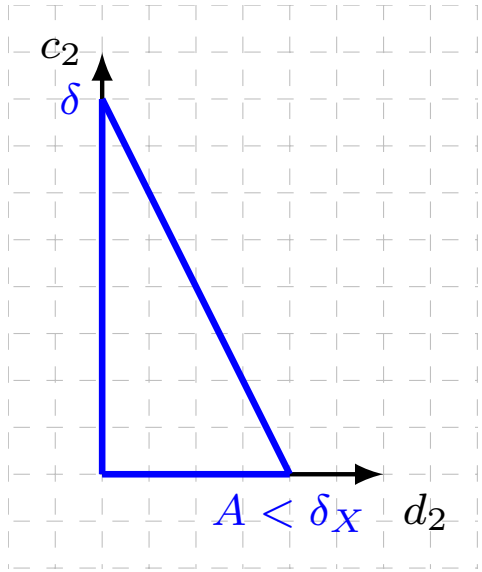
Ce n'est pas toujours un entier !



$\eta = 0$
e.g. $\mathcal{P}(7, 4)$ in $\mathcal{H}_0$



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



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

Choisir des représentants des monômes modulo le noyau revient à choisir des points dans le polygone.

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

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

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 : Puisqu'un élément $x \in \overline{\mathbb{F}_q}$ appartient à $\mathbb{F}_q$ si et seulement si $x^q - x = 0$, on peut se convaincre que les conditions sont suffisantes.

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 : Puisqu'un élément $x \in \overline{\mathbb{F}_q}$ appartient à $\mathbb{F}_q$ si et seulement si $x^q - x = 0$, on peut se convaincre 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 : Puisqu'un élément $x \in \overline{\mathbb{F}_q}$ appartient à $\mathbb{F}_q$ si et seulement si $x^q - x = 0$, on peut se convaincre 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

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

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

Pourquoi ces conditions (C3) et (C4) ?

Prenons $q = 3$, $\eta = 0$ et $(\delta_T, \delta_X) = (0, 4)$.

$$M = X_1^2 X_2^2 \text{ et } M' = X_2^4$$

Alors $M(1, 1, 0, 1) = 0$ alors que $M'(1, 1, 0, 1) = 1$.

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

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

Pourquoi ces conditions (C3) et (C4) ?
Prenons $q = 3$, $\eta = 0$ et $(\delta_T, \delta_X) = (0, 4)$.

$$M = X_1^2 X_2^2 \text{ et } M' = X_2^4$$

Alors $M(1, 1, 0, 1) = 0$ alors que $M'(1, 1, 0, 1) = 1$.

Ces conditions ne jouent que quand on évalue des points avec des coordonnées nulles.

Proposition [Rappel]

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

$$M \equiv M' \Leftrightarrow \begin{cases} q-1 & \mid d_i - d_i', \\ q-1 & \mid c_j - c_j', \\ d_i = 0 & \Leftrightarrow d_i' = 0, \\ c_j = 0 & \Leftrightarrow c_j' = 0. \end{cases}$$

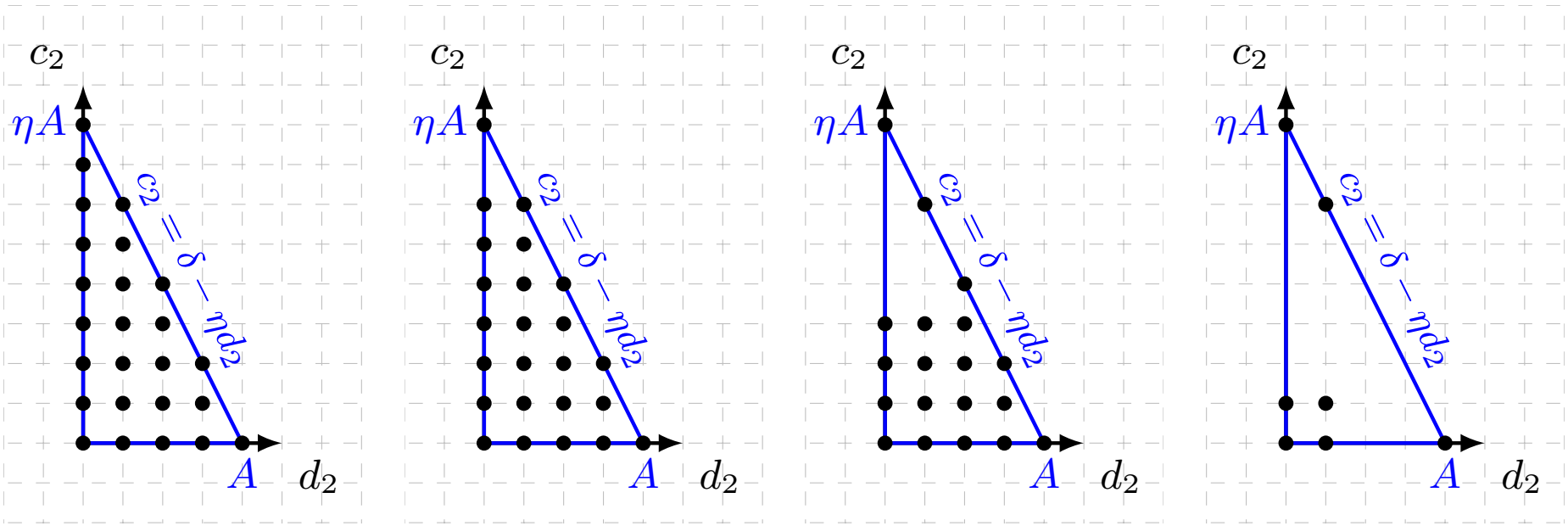
On choisit des points dans le polygone. Dessin !

Proposition [Rappel]

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

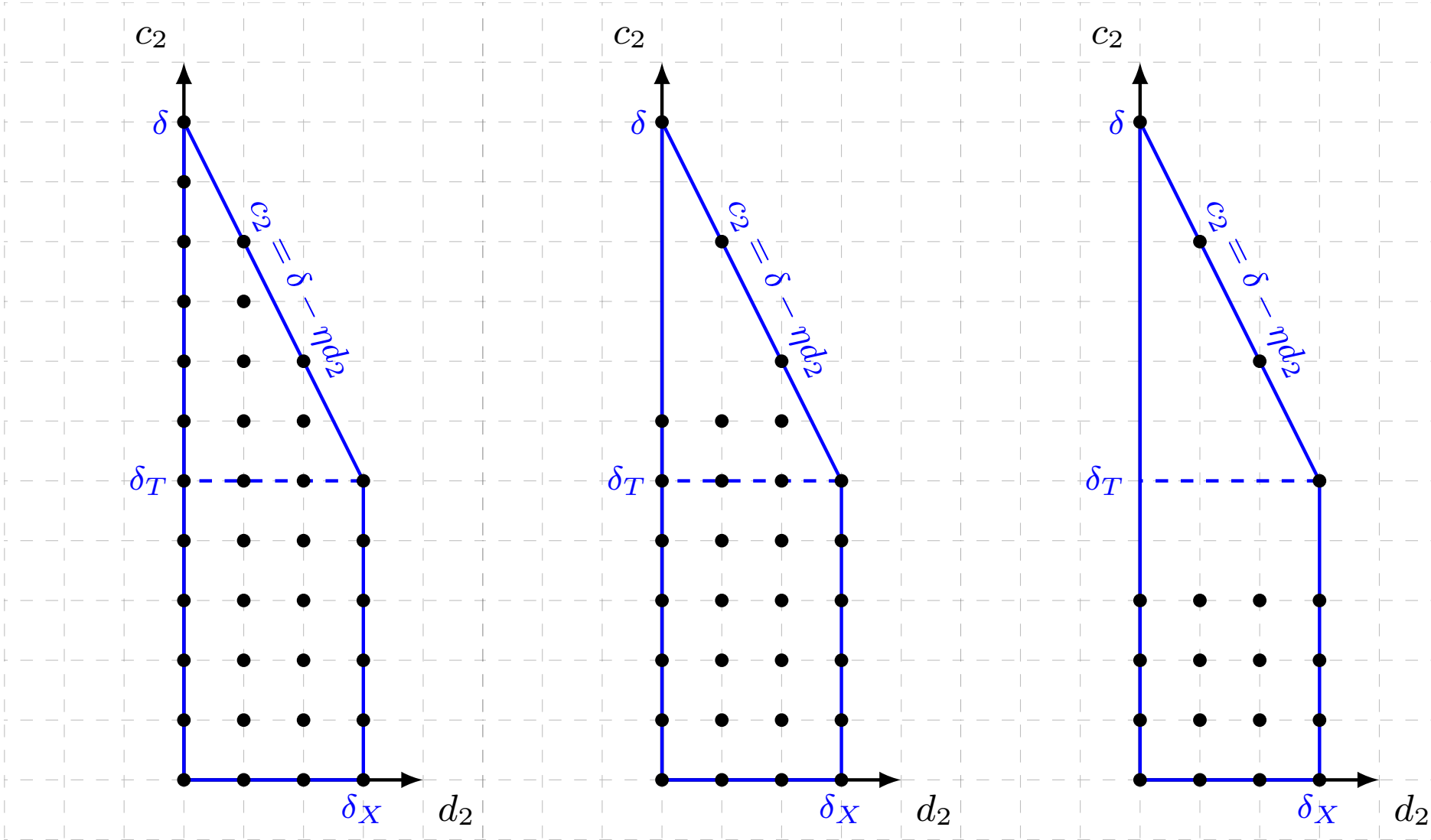
$$M \equiv M' \Leftrightarrow \begin{cases} q-1 & \mid d_i - d_i', \\ q-1 & \mid c_j - c_j', \\ d_i = 0 & \Leftrightarrow d_i' = 0, \\ c_j = 0 & \Leftrightarrow c_j' = 0. \end{cases}$$

On choisit des points dans le polygone. 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 $\mathcal{H}_2$

$$\Delta(\delta_T, \delta_X) = \{M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{P}(\delta_T, \delta_X) \text{ choisi dans le polygone.}\}$$

Proposition

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

$$\Delta(\delta_T, \delta_X) = \{M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{P}(\delta_T, \delta_X) \text{ choisi dans le polygone.}\}$$

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 ?

$$\Delta(\delta_T, \delta_X) = \{M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{P}(\delta_T, \delta_X) \text{ choisi dans le polygone.}\}$$

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 $\ker \mathrm{ev}_{(\delta_T, \delta_X)}$.

$$\Delta(\delta_T, \delta_X) = \{M(\alpha, \beta) \mid (\alpha, \beta) \in \mathcal{P}(\delta_T, \delta_X) \text{ choisi dans le polygone.}\}$$

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 $\ker \mathrm{ev}_{(\delta_T, \delta_X)}$.

Corollaire

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

$$\dim C_\eta(\delta_T, \delta_X) = \#\Delta(\delta_T, \delta_X)$$

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

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

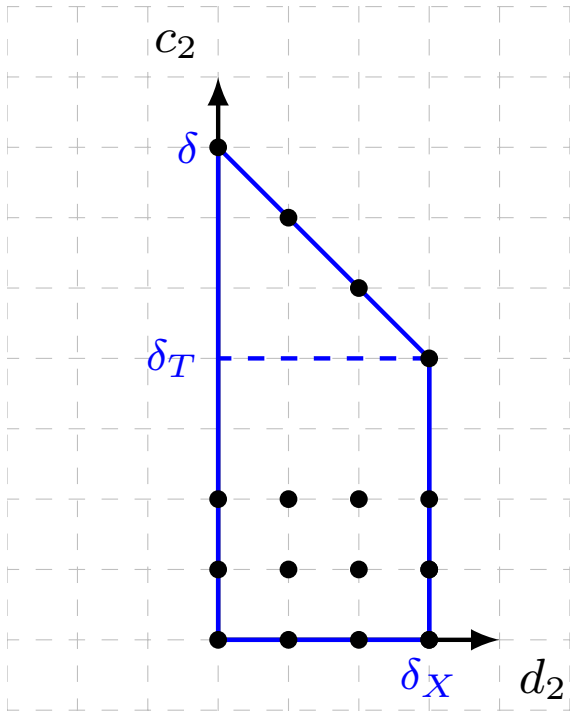


Figure – $\mathcal{P}(3,4)$ avec $q=3$ dans $\mathcal{H}_1$

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

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

Par définition,

$$d_\eta(\delta_T, \delta_X) = \min_{F \in R(\delta_T,\delta_X)\setminus \ker \mathrm{ev}_{(\delta_T,\delta_X)}} \omega(\mathrm{ev}_{(\delta_T,\delta_X)}(F)).$$

Par définition,

$$d_\eta(\delta_T, \delta_X) = \min_{F \in R(\delta_T, \delta_X) \setminus \ker \mathrm{ev}_{(\delta_T, \delta_X)}} \omega(\mathrm{ev}_{(\delta_T, \delta_X)}(F)).$$

De plus, on munit l'ensemble des monômes de R d'une **relation d'ordre totale**. Cela nous permet de définir le **terme dominant** d'un polynôme F, que l'on note $\mathrm{LT}(F)$.

Par définition,

$$d_\eta(\delta_T, \delta_X) = \min_{F \in R(\delta_T, \delta_X) \setminus \ker \mathrm{ev}_{(\delta_T, \delta_X)}} \omega(\mathrm{ev}_{(\delta_T, \delta_X)}(F)).$$

De plus, on munit l'ensemble des monômes de R d'une **relation d'ordre totale**. Cela nous permet de définir le **terme dominant** d'un polynôme F, que l'on note $\mathrm{LT}(F)$.
Soit $(\epsilon_T, \epsilon_X) \in \mathbb{N}^2$ tel que $\epsilon_T,\ \epsilon_X \geq q$. On pose

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

Minoration de la distance minimale

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

Par définition,

$$d_\eta(\delta_T, \delta_X) = \min_{F \in R(\delta_T,\delta_X) \setminus \ker \mathrm{ev}_{(\delta_T,\delta_X)}} \omega(\mathrm{ev}_{(\delta_T,\delta_X)}(F)).$$

De plus, on munit l'ensemble des monômes de R d'une **relation d'ordre totale**. Cela nous permet de définir le **terme dominant** d'un polynôme F, que l'on note $\mathrm{LT}(F)$.
Soit $(\epsilon_T, \epsilon_X) \in \mathbb{N}^2$ tel que $\epsilon_T,\ \epsilon_X \geq q$. On pose

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

Minoration de la distance minimale

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

Esquissons la preuve.
Pour $F \in R(\delta_T, \delta_X) \setminus \ker \mathrm{ev}_{(\delta_T,\delta_X)}$, on pose

$$\mathcal{Z}(F) = \{P \in \mathcal{H}_\eta \mid F(P) = 0\} \text{ et } N_F = \#\mathcal{Z}(F)(\mathbb{F}_q).$$

- D'abord on remarque que $\mathrm{ev}_{(\delta_T,\delta_X)}(F) = \mathrm{ev}_{(\delta_T,\delta_X)}\left(\pi_{(\delta_T,\delta_X)}(F)\right)$ et donc

$$d_\eta(\delta_T, \delta_X) = \min_{F \in \mathrm{Vect}\ \Delta(\delta_T,\delta_X)} \omega(\mathrm{ev}_{(\delta_T,\delta_X)}(F)) = \min_{F \in \mathrm{Vect}\ \Delta(\delta_T,\delta_X)} N - N_F.$$

On veut minorer $N - N_F$ uniformément en $F \in \mathrm{Vect}\,\Delta(\delta_T, \delta_X)$.

Minoration de la distance minimale

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

Suite de la preuve.

- Pour tout $F \in \operatorname{Vect} \Delta(\delta_T, \delta_X)$, on considère l'application **surjective**

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

$$N_F = \dim \left(R(\epsilon_T, \epsilon_X) \Big/ \ker \operatorname{ev}_{(\epsilon_T,\epsilon_X),F} \right).$$

- On pose $\langle F \rangle_{(\epsilon_T,\epsilon_X)}$ le sev $FR(\epsilon_T - \delta_T, \epsilon_X - \delta_X) \subset R(\epsilon_T, \epsilon_X)$ engendré par F.
  Puisque $\ker \operatorname{ev}_{(\epsilon_T,\epsilon_X)} + \langle F \rangle_{(\epsilon_T,\epsilon_X)} \subset \ker \operatorname{ev}_{(\epsilon_T,\epsilon_X),F}$, on a $\tilde{N}_F \geq N_F$ avec

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

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

Grosso modo, $N - \tilde{N}_F$ est la dimension des polynômes qui ne sont pas dans le noyau mais qui sont divisibles par F. On montre par ailleurs qu'il suffit de compter le nombre de monômes qui ne sont pas divisibles par le terme dominant de F, i.e.

$$N - \tilde{N}_F = \#\left\{ N \in \Delta(\epsilon_T, \epsilon_X) \mid \operatorname{LT}(F) \mid N \right\} = \#\Delta(\epsilon_T, \epsilon_X)_F$$

Minoration de la distance minimale

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

Suite de la preuve.

- Pour tout $F \in \operatorname{Vect} \Delta(\delta_T, \delta_X)$, on considère l'application **surjective**

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

$$N_F = \dim \left(R(\epsilon_T, \epsilon_X) \Big/ \ker \operatorname{ev}_{(\epsilon_T,\epsilon_X),F} \right).$$

- On pose $\langle F \rangle_{(\epsilon_T,\epsilon_X)}$ le sev $FR(\epsilon_T - \delta_T, \epsilon_X - \delta_X) \subset R(\epsilon_T, \epsilon_X)$ engendré par F.
  Puisque $\ker \operatorname{ev}_{(\epsilon_T,\epsilon_X)} + \langle F \rangle_{(\epsilon_T,\epsilon_X)} \subset \ker \operatorname{ev}_{(\epsilon_T,\epsilon_X),F}$, on a $\tilde{N}_F \geq N_F$ avec

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

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

Grosso modo, $N - \tilde{N}_F$ est la dimension des polynômes qui ne sont pas dans le noyau mais qui sont divisibles par F. On montre par ailleurs qu'il suffit de compter le nombre de monômes qui ne sont pas divisibles par le terme dominant de F, i.e.

$$N - \tilde{N}_F = \#\left\{ N \in \Delta(\epsilon_T, \epsilon_X) \mid \operatorname{LT}(F) \mid N \right\} = \#\Delta(\epsilon_T, \epsilon_X)_F$$

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

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

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 $\mathbb{F}_q = \{\xi_1, \xi_2, \ldots, \xi_q\}$. Les mots de code associés à ces polynômes atteignent la distance minimale.

- 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

$$F(T_1, T_2, X_1, X_2) = T_2^{\delta_T + \eta(\delta_X - s) - q} \prod_{i=1}^{s} (X_2 - \xi_i T_1^{\eta} X_1) \prod_{a \in \mathbb{F}_q} (T_2 - aT_1)$$

  - 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

$$F(T_1, T_2, X_1, X_2) = X_2^{\delta_X - m_X} T_2^{\delta_T - m_T} \prod_{i=1}^{m_X} (X_2 - \xi_i X_1 T_1^{\eta}) \prod_{j=1}^{m_T} (T_2 - \xi_j T_1)$$

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 $\eta = 0$,

$$\#\mathcal{C}(\mathbb{F}_q) \leq (q+1)^2 - \max(q - \delta_X + 1, 1)\max(q - \delta_T + 1, 1).$$

Nous sommes dans le cas contraire à l'étude classique des codes. On se sert de notre connaissance du code pour en déduire les courbes maximales de la surface, et non le contraire !

Les codes permettent d'obtenir des résultats géométriques sur la surface considérée.

Nous sommes dans le cas contraire à l'étude classique des codes. On se sert de notre connaissance du code pour en déduire les courbes maximales de la surface, et non le contraire !

Les codes permettent d'obtenir des résultats géométriques sur la surface considérée.

Merci pour votre attention !