Introduction aux codes correcteurs et lien avec la géométrie algbérique

Jade Nardi

Jeudi 23 mars

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.).

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.).

Deux approches :

- Probabiliste (Shannon) : Il existe des codes avec le meilleur taux de transmission souhaitable rendant la probabilité d'erreur aussi petite que l'on veut.

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.).

Deux approches :

- Probabiliste (Shannon) : Il existe des codes avec le meilleur taux de transmission souhaitable rendant la probabilité d'erreur aussi petite que l'on veut.
  $\rightsquigarrow$ Non constructif

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.).

Deux approches :

- Probabiliste (Shannon) : Il existe des codes avec le meilleur taux de transmission souhaitable rendant la probabilité d'erreur aussi petite que l'on veut.
  $\rightsquigarrow$ Non constructif
- Algébrique (Golay et Hamming) : Construire explicitement des systèmes remplissant ces conditions $\Rightarrow$ Théorie des codes correcteurs d'erreurs.

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**.

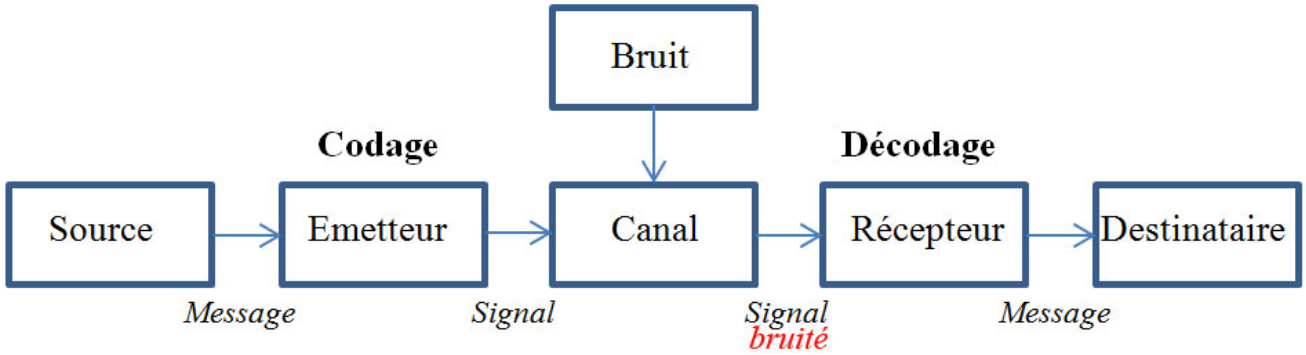
Exemple 1 : Clé du numéro de sécurité sociale - 15 chiffres

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

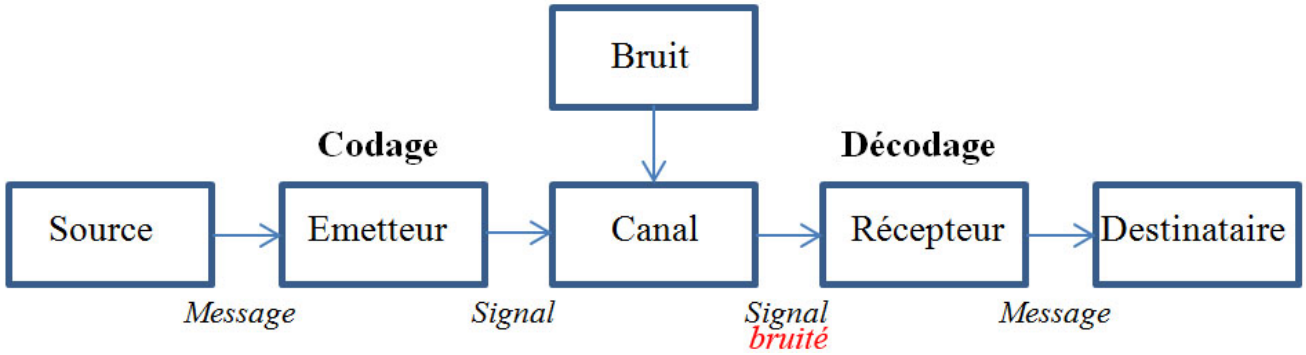
Exemple 2 : Envoyer trois fois le message
On veut envoyer le message 001. On envoie $m = 001001001$.
S'il y a une erreur et le destinataire reçoit $\tilde{m} = 001\mathbf{1}01001$, il peut la détecter et la corriger.
A partir de deux erreurs, on n'a plus de garantie. Si $\tilde{m} = \mathbf{1}01\mathbf{1}01\mathbf{0}01$, 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 $q = p^e$.

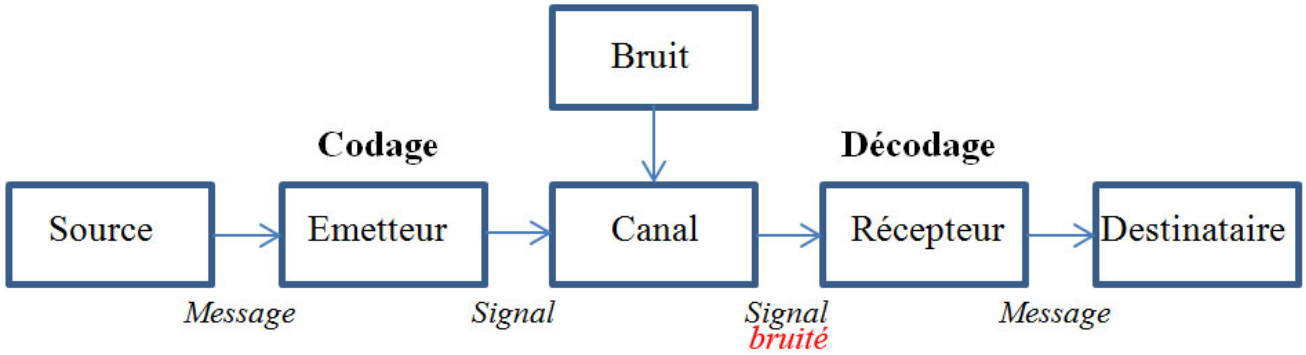


Message à transmettre : vecteur $m \in (\mathbb{F}_q)^k$.
Encodage : Fonction injective

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

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 $q = p^e$.

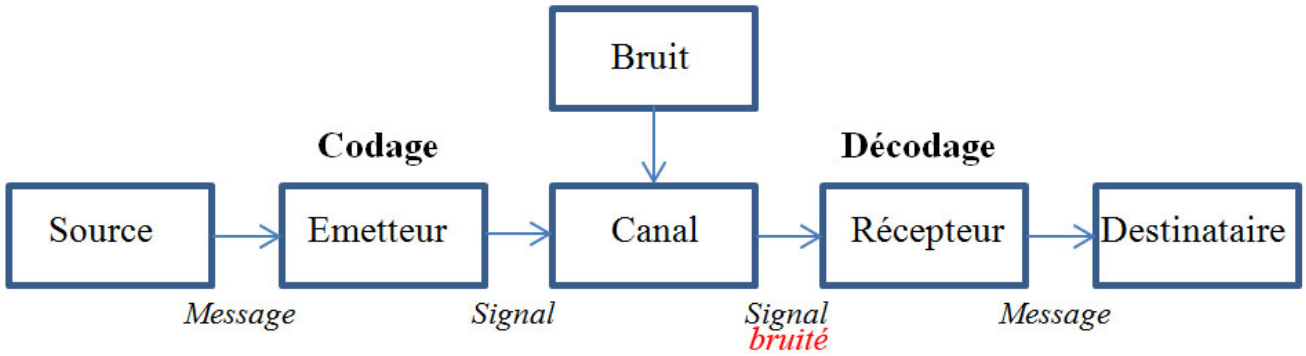


Message à transmettre : vecteur $m \in (\mathbb{F}_q)^k$.
Encodage : Fonction injective

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

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

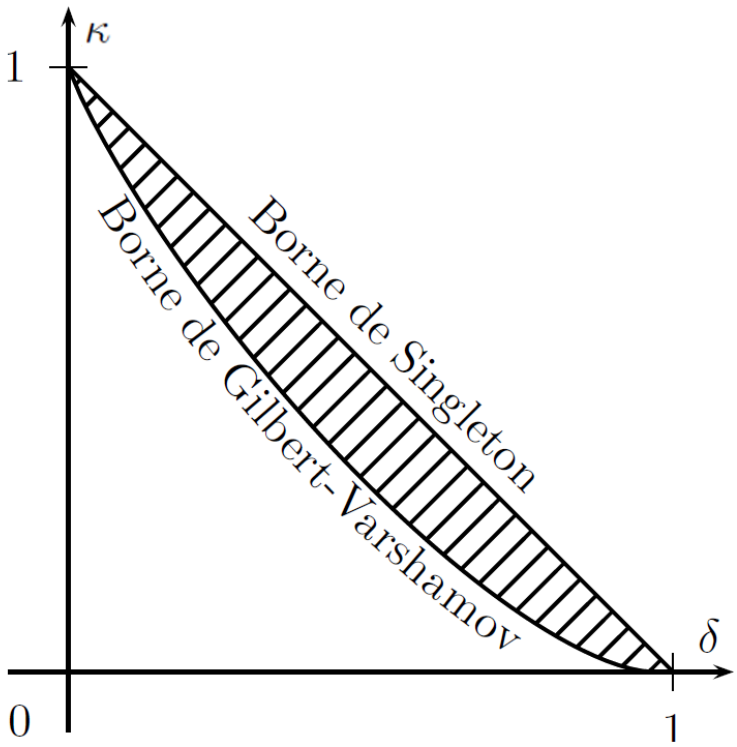
Te taux de transmission : $\kappa = \frac{k}{n}$
Distance relative $\delta = \frac{d}{n}$

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



On peut définir un code linéaire grâce à sa **matrice génératrice**

$$G = \mathrm{Mat}_{\mathcal{B}}\left(E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n\right)$$

Donc $C = \mathrm{Im}\, G$.

On peut définir un code linéaire grâce à sa **matrice génératrice**

$$G = \mathrm{Mat}_{\mathcal{B}}\left(E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n\right)$$

Donc $C = \mathrm{Im}\, G$.
Puisque G est injective, on peut la mettre sous **forme systématique**

$$G \sim (I_k, A_{n-k})$$

On peut définir un code linéaire grâce à sa **matrice génératrice**

$$G = \mathrm{Mat}_{\mathcal{B}}\left(E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n\right)$$

Donc $C = \mathrm{Im}\, G$.
Puisque G est injective, on peut la mettre sous **forme systématique**

$$G \sim (I_k, A_{n-k})$$

On peut le définir grâce à la **matrice de contrôle** H qui vérifie

$$\forall x \in (\mathbb{F}_q)^n,\ H(x) = 0 \iff x \in C$$

Si $G = (I_k, A_{n-k})$, alors $H = (-A_{n-k}^t, I_{n-k})$.

On peut définir un code linéaire grâce à sa **matrice génératrice**

$$G = \mathrm{Mat}_{\mathcal{B}}\left(E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n\right)$$

Donc $C = \mathrm{Im}\, G$.
Puisque G est injective, on peut la mettre sous **forme systématique**

$$G \sim (I_k, A_{n-k})$$

On peut le définir grâce à la **matrice de contrôle** H qui vérifie

$$\forall x \in (\mathbb{F}_q)^n,\ H(x) = 0 \iff x \in C$$

Si $G = (I_k, A_{n-k})$, alors $H = (-A_{n-k}^t, I_{n-k})$.
Distance minimale : Nombre minimum de colonnes de H dont une combinaison linéaire est nulle.

On peut définir un code linéaire grâce à sa **matrice génératrice**

$$G = \mathrm{Mat}_{\mathcal{B}}\left(E : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n\right)$$

Donc $C = \mathrm{Im}\, G$.
Puisque G est injective, on peut la mettre sous **forme systématique**

$$G \sim (I_k, A_{n-k})$$

On peut le définir grâce à la **matrice de contrôle** H qui vérifie

$$\forall x \in (\mathbb{F}_q)^n,\ H(x) = 0 \iff x \in C$$

Si $G = (I_k, A_{n-k})$, alors $H = (-A_{n-k}^t, I_{n-k})$.
Distance minimale : Nombre minimum de colonnes de H dont une combinaison linéaire est nulle.
Décodage : On reçoit $y = x + e$. Alors $H(y) = H(e)$. Si $\omega(e) \leq t$, alors il y a exactement $\omega(e)$ colonnes, $c_1, \ldots, c_{\omega(e)}$ de H telles que

$$H(e) = \alpha_1 c_1 + \cdots + \alpha_{\omega(e)} c_{\omega(e)}$$

et on corrige $x = y - \alpha_1 e_1 + \cdots + \alpha_{\omega(e)} e_{\omega(e)}$ où $\{e_i\}$ est le base canonique de $(\mathbb{F}_q)^n$.

Exemple : Code de Hamming $[7, 4, 3]$ sur $\mathbb{F}_2$. On veut envoyer le message $m = 1101$.

Exemple : Code de Hamming $[7, 4, 3]$ sur $\mathbb{F}_2$. On veut envoyer le message $m = 1101$. On envoie

$$x = mG = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}}_{\text{matrice génératrice}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Exemple : Code de Hamming $[7, 4, 3]$ sur $\mathbb{F}_2$. On veut envoyer le message $m = 1101$. On envoie

$$x = mG = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}}_{\text{matrice génératrice}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Matrice de contrôle :

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Alors $H.G^t = 0$.

Exemple : Code de Hamming $[7, 4, 3]$ sur $\mathbb{F}_2$. On veut envoyer le message $m = 1101$.
On envoie

$$x = mG = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}}_{\text{matrice génératrice}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Matrice de contrôle :

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Alors $H.G^t = 0$.
Si on reçoit $y = \begin{pmatrix} \mathbf{0} & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$.

$$H\, y^t = \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}}_{\text{syndrome}} = c_1$$

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 $[n, k, n-k+1]$.

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 $d \leq n - (k-1)$.

Matrice génératrice :

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}$$

Comment décoder ?

Message envoyé : $x = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg f \leq k-1$.

Message reçu : $y = (y_1, \ldots, y_n)$ avec $e \leq t$ erreurs.

Comment décoder ?

Message envoyé : $x = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg f \leq k-1$.

Message reçu : $y = (y_1, \ldots, y_n)$ avec $e \leq t$ erreurs.

On calcule le polynôme d'interpolation L tel que $L(\alpha_i) = y_i$ avec $\deg L \leq n-1$.

Comment décoder ?

Message envoyé : $x = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg f \leq k-1$.
Message reçu : $y = (y_1, \ldots, y_n)$ avec $e \leq t$ erreurs.
On calcule le polynôme d'interpolation L tel que $L(\alpha_i) = y_i$ avec $\deg L \leq n-1$. On cherche un polynôme E de la forme

$$E = \prod_{i \in I} (X - \alpha_i)$$

où l'ensemble I est exactement le lieu des erreurs.

Comment décoder ?

Message envoyé : $x = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg f \leq k-1$.
Message reçu : $y = (y_1, \ldots, y_n)$ avec $e \leq t$ erreurs.
On calcule le polynôme d'interpolation L tel que $L(\alpha_i) = y_i$ avec $\deg L \leq n-1$. On cherche un polynôme E de la forme

$$E = \prod_{i \in I} (X - \alpha_i)$$

où l'ensemble I est exactement le lieu des erreurs. Alors

$$E(\alpha_i)L(\alpha_i) = E(\alpha_i)f(\alpha_i)$$

Comment décoder ?

Message envoyé : $x = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg f \leq k-1$.
Message reçu : $y = (y_1, \ldots, y_n)$ avec $e \leq t$ erreurs.
On calcule le polynôme d'interpolation L tel que $L(\alpha_i) = y_i$ avec $\deg L \leq n-1$. On cherche un polynôme E de la forme

$$E = \prod_{i \in I} (X - \alpha_i)$$

où l'ensemble I est exactement le lieu des erreurs. Alors

$$E(\alpha_i)L(\alpha_i) = E(\alpha_i)f(\alpha_i)$$

On note $g(X) = P(X)E(X)$. On détermine g et E grâce aux relations

$$g(\alpha_i) = E(\alpha_i)L(\alpha_i)$$

$\Rightarrow$ système à $(e+1) + (k-1+e+1)$ inconnues.

Comment décoder ?

Message envoyé : $x = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg f \leq k-1$.
Message reçu : $y = (y_1, \ldots, y_n)$ avec $e \leq t$ erreurs.
On calcule le polynôme d'interpolation L tel que $L(\alpha_i) = y_i$ avec $\deg L \leq n-1$. On cherche un polynôme E de la forme

$$E = \prod_{i \in I} (X - \alpha_i)$$

où l'ensemble I est exactement le lieu des erreurs. Alors

$$E(\alpha_i)L(\alpha_i) = E(\alpha_i)f(\alpha_i)$$

On note $g(X) = P(X)E(X)$. On détermine g et E grâce aux relations

$$g(\alpha_i) = E(\alpha_i)L(\alpha_i)$$

$\Rightarrow$ système à $(e+1) + (k-1+e+1)$ inconnues.
Or $e \leq \frac{d-1}{2} = \frac{n-k}{2}$ donc $k + 2e + 1 \leq k + n - k + 1 = k + 1 \leq n$.
Mais f est unique $\Rightarrow$ Unique couple (g, E)
Donc $f = g/E$.

Variété algébrique affine définie sur un corps $\mathbb{F}$: Lieu de zéros d'un ensemble de polynômes de $\mathbb{F}[X_1, \ldots, X_n]$.

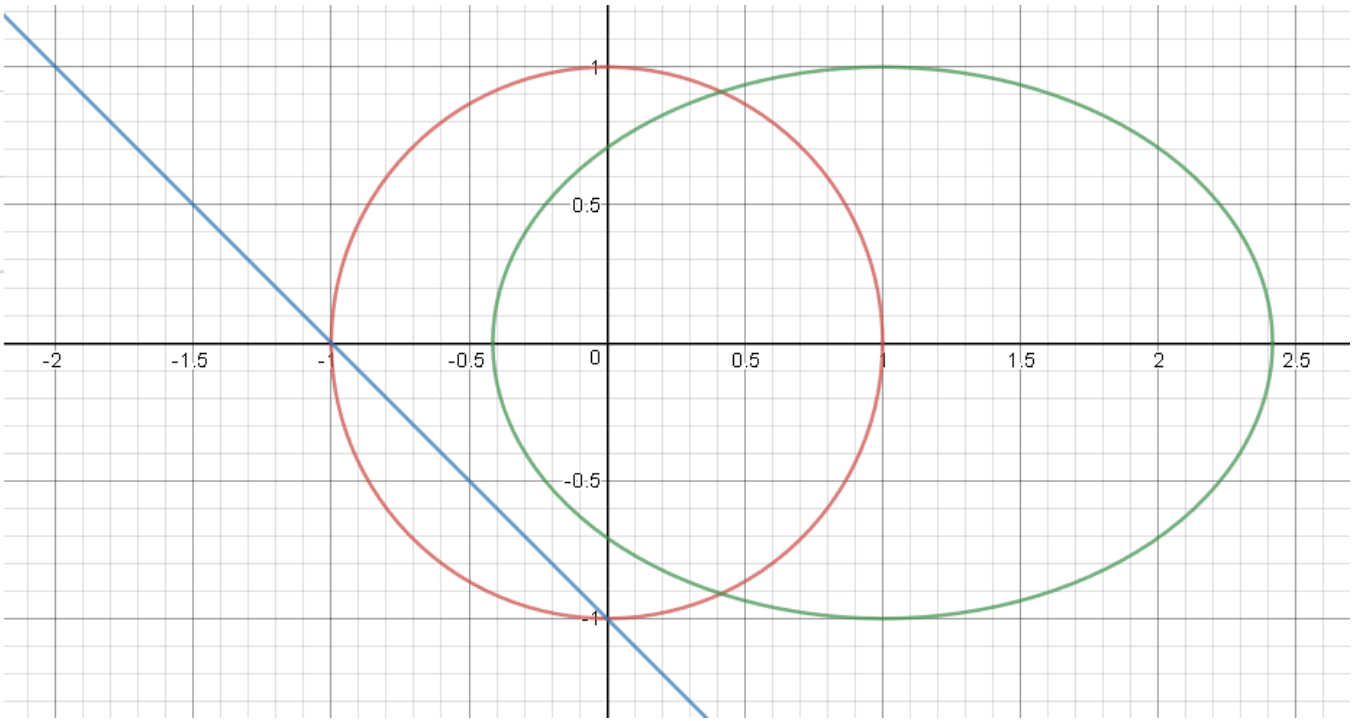
Variété algébrique affine définie sur un corps $\mathbb{F}$: Lieu de zéros d'un ensemble de polynômes de $\mathbb{F}[X_1, \ldots, X_n]$.

$$\text{Variétés algébriques dans } \mathbb{F}^n \leftrightarrow \text{idéaux de } \mathbb{F}[X_1, \ldots, X_n]$$

Exemples :

Espace affine $\mathbb{A}^n$ associée à l'idéal nul

1. $x^2 + y^2 - 1 = 0$
2. $x + y + 1 = 0$
3. $(x-1)^2 + 2y^2 - 2 = 0$



On définit l'espace projective de dimension n comme

$$\mathbb{P}^n(\mathbb{F}) = \mathbb{F}^{n+1} \setminus \{0\} / \sim$$

i.e. $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists\, \lambda \in \mathbb{F}^*$ tel que $\forall\, i \in \{1, \ldots, n\}$, $x_i = \lambda y_i$

On définit l'espace projective de dimension n comme

$$\mathbb{P}^n(\mathbb{F}) = \mathbb{F}^{n+1} \setminus \{0\} / \sim$$

i.e. $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists\, \lambda \in \mathbb{F}^*$ tel que $\forall\, i \in \{1, \ldots, n\}$, $x_i = \lambda y_i$

On note $[x_0 : x_1 : \ldots : x_n]$ un représentant de cette classe d'équivalence.
Cela revient à dire que les points de $\mathbb{P}^n$ sont les droites vectorielles de $\mathbb{F}^{n+1}$.

On définit l'espace projective de dimension n comme

$$\mathbb{P}^n(\mathbb{F}) = \mathbb{F}^{n+1} \setminus \{0\} / \sim$$

i.e. $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists\, \lambda \in \mathbb{F}^*$ tel que $\forall\, i \in \{1, \ldots, n\}$, $x_i = \lambda y_i$

On note $[x_0 : x_1 : \ldots : x_n]$ un représentant de cette classe d'équivalence.
Cela revient à dire que les points de $\mathbb{P}^n$ sont les droites vectorielles de $\mathbb{F}^{n+1}$.
Avantage : Toutes les droites de $\mathbb{P}^n$ se coupent une fois !

Théorème [Bezout]

Deux courbes algébriques projectives planes de degrés m et n, définies sur un corps algébriquement clos $\mathbb{F}$ et sans composante irréductible commune, ont exactement mn points d'intersections, comptés avec leur multiplicité.

Variété algébrique projective définie sur un corps $\mathbb{F}$: Lieu de zéros d'un ensemble de polynômes homogènes de $\mathbb{F}[X_0, \ldots, X_n]$.

Variété algébrique projective définie sur un corps $\mathbb{F}$: Lieu de zéros d'un ensemble de polynômes homogènes de $\mathbb{F}[X_0, \ldots, X_n]$.

Pourquoi *homogènes* ?
Un polynôme $f \in \mathbb{F}[X_0, \ldots, X_n]$ est dit *homogène de degré* d si pour tout $\lambda \in \mathbb{F}$,

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$$

Si $[x_0 : \ldots : x_n]$ est un zéro de f, on veut que toutes les éléments de son orbite $\{(\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in \mathbb{F}^*\}$ soient aussi zéros de f.

Variété algébrique projective définie sur un corps $\mathbb{F}$: Lieu de zéros d'un ensemble de polynômes homogènes de $\mathbb{F}[X_0, \ldots, X_n]$.

Pourquoi *homogènes* ?
Un polynôme $f \in \mathbb{F}[X_0, \ldots, X_n]$ est dit *homogène de degré* d si pour tout $\lambda \in \mathbb{F}$,

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$$

Si $[x_0 : \ldots : x_n]$ est un zéro de f, on veut que toutes les éléments de son orbite $\{(\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in \mathbb{F}^*\}$ soient aussi zéros de f.

Variétés algébriques projective dans $\mathbb{P}^n(\mathbb{F})$ $\leftrightarrow$ idéaux homogènes de $\mathbb{F}[X_0, \ldots, X_n]$

Soit V une variété algébrique définie sur $\mathbb{F}$. On note $V(\mathbb{F})$ l'ensemble de ses points $\mathbb{F}$-rationnels, c'est-à-dire, dont les coordonnées sont dans $\mathbb{F}$.

Soit V une variété algébrique définie sur $\mathbb{F}$. On note $V(\mathbb{F})$ l'ensemble de ses points $\mathbb{F}$-rationnels, c'est-à-dire, dont les coordonnées sont dans $\mathbb{F}$.

Exemples :

1. $V = \mathbb{P}^n$ sur $\mathbb{F}_q$. $V(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$.
2. $V : X^2 + Y^2 = 1$ dans $\mathbb{F}_2^2$. $V(\mathbb{F}_2) = \{(0,1),(1,0)\}$.
3. $V : X^2 + Y^2 = -1$ sur $\mathbb{R}^2$. $V(\mathbb{R}) = \varnothing$.
4. $V : X^2 + Y = 0$ sur $\mathbb{F}_3^2$. $V(\mathbb{F}_3) = \{(0,0),(1,2),(2,2)\}$.

Soit V une variété algébrique définie sur $\mathbb{F}$. On note $V(\mathbb{F})$ l'ensemble de ses points $\mathbb{F}$-rationnels, c'est-à-dire, dont les coordonnées sont dans $\mathbb{F}$.

Exemples :

1. $V = \mathbb{P}^n$ sur $\mathbb{F}_q$. $V(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$.
2. $V : X^2 + Y^2 = 1$ dans $\mathbb{F}_2^2$. $V(\mathbb{F}_2) = \{(0,1),(1,0)\}$.
3. $V : X^2 + Y^2 = -1$ sur $\mathbb{R}^2$. $V(\mathbb{R}) = \varnothing$.
4. $V : X^2 + Y = 0$ sur $\mathbb{F}_3^2$. $V(\mathbb{F}_3) = \{(0,0),(1,2),(2,2)\}$.

Définition

Soit $V \subset \mathbb{A}^r$ (resp. $\mathbb{P}^r$) une variété algébrique affine (resp. projective) définie sur $\mathbb{F}_q$. Soit $\mathcal{P} = \{P_1, \ldots, P_n\} \subset V(\mathbb{F}_q)$ et $\mathcal{F}$ un sous-espace vectoriel de $\mathbb{F}_q[X_1, \ldots, X_r]$ (resp. de $\mathbb{F}_q[X_0, \ldots, X_r]^h$). Le *code d'évaluation* $C_{\mathcal{P}}(\mathcal{F})$ est défini comme l'image de l'application

$$\mathrm{ev} : \left\{ \begin{array}{ccc} \mathcal{F} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array} \right.$$

Soit V une variété algébrique définie sur $\mathbb{F}$. On note $V(\mathbb{F})$ l'ensemble de ses points $\mathbb{F}$-rationnels, c'est-à-dire, dont les coordonnées sont dans $\mathbb{F}$.

Exemples :

1. $V = \mathbb{P}^n$ sur $\mathbb{F}_q$. $V(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$.
2. $V : X^2 + Y^2 = 1$ dans $\mathbb{F}_2^2$. $V(\mathbb{F}_2) = \{(0,1),(1,0)\}$.
3. $V : X^2 + Y^2 = -1$ sur $\mathbb{R}^2$. $V(\mathbb{R}) = \varnothing$.
4. $V : X^2 + Y = 0$ sur $\mathbb{F}_3^2$. $V(\mathbb{F}_3) = \{(0,0),(1,2),(2,2)\}$.

Définition

Soit $V \subset \mathbb{A}^r$ (resp. $\mathbb{P}^r$) une variété algébrique affine (resp. projective) définie sur $\mathbb{F}_q$. Soit $\mathcal{P} = \{P_1, \ldots, P_n\} \subset V(\mathbb{F}_q)$ et $\mathcal{F}$ un sous-espace vectoriel de $\mathbb{F}_q[X_1, \ldots, X_r]$ (resp. de $\mathbb{F}_q[X_0, \ldots, X_r]^h$). Le *code d'évaluation* $C_{\mathcal{P}}(\mathcal{F})$ est défini comme l'image de l'application

$$\mathrm{ev} : \left\{ \begin{array}{ccc} \mathcal{F} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array} \right.$$

On veut que cette application soit injective !

Soit V une variété algébrique définie sur $\mathbb{F}$. On note $V(\mathbb{F})$ l'ensemble de ses points $\mathbb{F}$-rationnels, c'est-à-dire, dont les coordonnées sont dans $\mathbb{F}$.

Exemples :

1. $V = \mathbb{P}^n$ sur $\mathbb{F}_q$. $V(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$.
2. $V : X^2 + Y^2 = 1$ dans $\mathbb{F}_2^2$. $V(\mathbb{F}_2) = \{(0,1),(1,0)\}$.
3. $V : X^2 + Y^2 = -1$ sur $\mathbb{R}^2$. $V(\mathbb{R}) = \varnothing$.
4. $V : X^2 + Y = 0$ sur $\mathbb{F}_3^2$. $V(\mathbb{F}_3) = \{(0,0),(1,2),(2,2)\}$.

Définition

Soit $V \subset \mathbb{A}^r$ (resp. $\mathbb{P}^r$) une variété algébrique affine (resp. projective) définie sur $\mathbb{F}_q$. Soit $\mathcal{P} = \{P_1, \ldots, P_n\} \subset V(\mathbb{F}_q)$ et $\mathcal{F}$ un sous-espace vectoriel de $\mathbb{F}_q[X_1, \ldots, X_r]$ (resp. de $\mathbb{F}_q[X_0, \ldots, X_r]^h$). Le *code d'évaluation* $C_{\mathcal{P}}(\mathcal{F})$ est défini comme l'image de l'application

$$\mathrm{ev} : \left\{ \begin{array}{ccc} \mathcal{F} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array} \right.$$

On veut que cette application soit injective !
$\Rightarrow$ Code de longueur $n = \#\mathcal{P}$ et de dimension $\dim \mathcal{F}$.

Soit V une variété algébrique définie sur $\mathbb{F}$. On note $V(\mathbb{F})$ l'ensemble de ses points $\mathbb{F}$-rationnels, c'est-à-dire, dont les coordonnées sont dans $\mathbb{F}$.

Exemples :

1. $V = \mathbb{P}^n$ sur $\mathbb{F}_q$. $V(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$.
2. $V : X^2 + Y^2 = 1$ dans $\mathbb{F}_2^2$. $V(\mathbb{F}_2) = \{(0,1),(1,0)\}$.
3. $V : X^2 + Y^2 = -1$ sur $\mathbb{R}^2$. $V(\mathbb{R}) = \varnothing$.
4. $V : X^2 + Y = 0$ sur $\mathbb{F}_3^2$. $V(\mathbb{F}_3) = \{(0,0),(1,2),(2,2)\}$.

Définition

Soit $V \subset \mathbb{A}^r$ (resp. $\mathbb{P}^r$) une variété algébrique affine (resp. projective) définie sur $\mathbb{F}_q$. Soit $\mathcal{P} = \{P_1, \ldots, P_n\} \subset V(\mathbb{F}_q)$ et $\mathcal{F}$ un sous-espace vectoriel de $\mathbb{F}_q[X_1, \ldots, X_r]$ (resp. de $\mathbb{F}_q[X_0, \ldots, X_r]^h$). Le *code d'évaluation* $C_{\mathcal{P}}(\mathcal{F})$ est défini comme l'image de l'application

$$\mathrm{ev} : \begin{cases} \mathcal{F} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{cases}$$

On veut que cette application soit injective !
$\Rightarrow$ Code de longueur $n = \#\mathcal{P}$ et de dimension $\dim \mathcal{F}$.

Cas important pour les codeurs : Si D est un diviseur sur V, on peut considérer $C_{V(\mathbb{F}_q)}(L(D))$.
$\Longrightarrow$ Codes de Goppa (~ 1980)

C'est une généralisation du code de Reed-Solomon.

- $V = \mathbb{A}^1$ sur $\mathbb{F}_q$.
- $\mathcal{P} = A^1(\mathbb{F}_q)$
- $\mathcal{F} = \mathbb{F}_q[X]_{\leq k-1}$

C'est une généralisation du code de Reed-Solomon.

- $V = \mathbb{A}^1$ sur $\mathbb{F}_q$.
- $\mathcal{P} = A^1(\mathbb{F}_q)$
- $\mathcal{F} = \mathbb{F}_q[X]_{\leq k-1}$

Pourquoi généraliser ?

- Pouvoir considérer des variétés avec plus de points $\Rightarrow$ Codes plus longs
- Utiliser nos connaissances sur une variété pour établir les paramètres du code

C'est une généralisation du code de Reed-Solomon.

- $V = \mathbb{A}^1$ sur $\mathbb{F}_q$.
- $\mathcal{P} = A^1(\mathbb{F}_q)$
- $\mathcal{F} = \mathbb{F}_q[X]_{\leq k-1}$

Pourquoi généraliser ?

- Pouvoir considérer des variétés avec plus de points $\Rightarrow$ Codes plus longs
- Utiliser nos connaissances sur une variété pour établir les paramètres du code

Et la distance minimale ?
Soit V une variété algébrique et f un polynôme. Notons H l'hypersurface $f = 0$.

$$\#\{P \in V(\mathbb{F}) \mid f(P) = 0\} = \#(V \cap H)(\mathbb{F})$$

C'est une généralisation du code de Reed-Solomon.

- $V = \mathbb{A}^1$ sur $\mathbb{F}_q$.
- $\mathcal{P} = A^1(\mathbb{F}_q)$
- $\mathcal{F} = \mathbb{F}_q[X]_{\leq k-1}$

Pourquoi généraliser ?

- Pouvoir considérer des variétés avec plus de points $\Rightarrow$ Codes plus longs
- Utiliser nos connaissances sur une variété pour établir les paramètres du code

Et la distance minimale ?
Soit V une variété algébrique et f un polynôme. Notons H l'hypersurface $f = 0$.

$$\#\{P \in V(\mathbb{F}) \mid f(P) = 0\} = \#(V \cap H)(\mathbb{F})$$

Borner la distance minimale revient à borner le nombre de points rationnels sur les sous-variétés *hypersurfaciques* de V.

C'est une généralisation du code de Reed-Solomon.

- $V = \mathbb{A}^1$ sur $\mathbb{F}_q$.
- $\mathcal{P} = A^1(\mathbb{F}_q)$
- $\mathcal{F} = \mathbb{F}_q[X]_{\leq k-1}$

Pourquoi généraliser ?

- Pouvoir considérer des variétés avec plus de points $\Rightarrow$ Codes plus longs
- Utiliser nos connaissances sur une variété pour établir les paramètres du code

Et la distance minimale ?
Soit V une variété algébrique et f un polynôme. Notons H l'hypersurface $f = 0$.

$$\#\{P \in V(\mathbb{F}) \mid f(P) = 0\} = \#(V \cap H)(\mathbb{F})$$

Borner la distance minimale revient à borner le nombre de points rationnels sur les sous-variétés *hypersurfaciques* de V.

Faire travailler de concert géométrie algébrique et théorie des codes permet de construire des nouveaux codes dont les paramètres sont régis par la géométrie.

Pour $\mathcal{F} = \mathbb{F}_q[X_0, \ldots, X_r]_s^h$ et $\mathcal{P} = X(\mathbb{F}_q)$, on note le code $C_X(s)$.

Pour $\mathcal{F} = \mathbb{F}_q[X_0, \ldots, X_r]_s^h$ et $\mathcal{P} = X(\mathbb{F}_q)$, on note le code $C_X(s)$.

Lemme

Soit $s < q$. Le code $C_{\mathbb{P}^1}(s)$ a pour paramètre $[q+1, s+1, q+1-s]$.

- $\#\mathbb{P}^1(\mathbb{F}_q) = q+1$,
- $\#\mathbb{F}_q[X_0, X_1]_s^h = s+1$
- Même argument pour la distance minimale que pour Reed-Solomon

Pour $\mathcal{F} = \mathbb{F}_q[X_0, \ldots, X_r]_s^h$ et $\mathcal{P} = X(\mathbb{F}_q)$, on note le code $C_X(s)$.

Lemme

Soit $s < q$. Le code $C_{\mathbb{P}^1}(s)$ a pour paramètre $[q+1, s+1, q+1-s]$.

- $\#\mathbb{P}^1(\mathbb{F}_q) = q+1$,
- $\#\mathbb{F}_q[X_0, X_1]_s^h = s+1$
- Même argument pour la distance minimale que pour Reed-Solomon

On considère sur $\mathbb{P}^3$ la quadrique hyperbolique $\mathcal{H}$ donnée par l'équation $X_0X_3 - X_1X_2 = 0$ et le plongement de Segre :

$$\phi : \begin{cases} \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ ((u_0 : u_1), (v_0 : v_1)) & \mapsto & (u_0v_0 : u_0v_1 : u_1v_0 : u_1v_1) \end{cases}$$

Pour $\mathcal{F} = \mathbb{F}_q[X_0, \ldots, X_r]_s^h$ et $\mathcal{P} = X(\mathbb{F}_q)$, on note le code $C_X(s)$.

Lemme

Soit $s < q$. Le code $C_{\mathbb{P}^1}(s)$ a pour paramètre $[q+1, s+1, q+1-s]$.

- $\#\mathbb{P}^1(\mathbb{F}_q) = q+1$,
- $\#\mathbb{F}_q[X_0, X_1]_s^h = s+1$
- Même argument pour la distance minimale que pour Reed-Solomon

On considère sur $\mathbb{P}^3$ la quadrique hyperbolique $\mathcal{H}$ donnée par l'équation $X_0X_3 - X_1X_2 = 0$ et le plongement de Segre :

$$\phi : \begin{cases} \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ ((u_0 : u_1), (v_0 : v_1)) & \mapsto & (u_0v_0 : u_0v_1 : u_1v_0 : u_1v_1) \end{cases}$$

Proposition

1. La quadrique $\mathcal{H}$ est isomorphe à $\mathbb{P}^1 \times \mathbb{P}^1$ par le plongement de Segre.

Pour $\mathcal{F} = \mathbb{F}_q[X_0, \ldots, X_r]_s^h$ et $\mathcal{P} = X(\mathbb{F}_q)$, on note le code $C_X(s)$.

Lemme

Soit $s < q$. Le code $C_{\mathbb{P}^1}(s)$ a pour paramètre $[q+1, s+1, q+1-s]$.

- $\#\mathbb{P}^1(\mathbb{F}_q) = q+1$,
- $\#\mathbb{F}_q[X_0, X_1]_s^h = s+1$
- Même argument pour la distance minimale que pour Reed-Solomon

On considère sur $\mathbb{P}^3$ la quadrique hyperbolique $\mathcal{H}$ donnée par l'équation $X_0X_3 - X_1X_2 = 0$ et le plongement de Segre :

$$\phi : \begin{cases} \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ ((u_0 : u_1), (v_0 : v_1)) & \mapsto & (u_0v_0 : u_0v_1 : u_1v_0 : u_1v_1) \end{cases}$$

Proposition

1. La quadrique $\mathcal{H}$ est isomorphe à $\mathbb{P}^1 \times \mathbb{P}^1$ par le plongement de Segre.
2. $\mathbb{F}_q[X_0, \ldots, X_3]_s^h / I_{\mathcal{H}}(s) \xrightarrow{\sim} \mathbb{F}_{q\,s}[U_0, U_1]_s^h \otimes \mathbb{F}_q[V_0, V_1]_s^h$

Définition

Soient C et C' deux codes linéaires de paramètres respectifs $[n, k, d]$ et $[n', k', d']$. On définit le produit tensoriel de C et C' comme le sous-espace vectoriel de ${\mathbb{F}_q}^n \otimes {\mathbb{F}_q}^{n'}$ engendré par les tenseurs élémentaires $\{c \otimes c'\}_{c \in C,\, c' \in C'}$.

$\Rightarrow$ Matrices dont les lignes sont des mots de C et les colonnes des mots de C'.
C'est un code linéaire de paramètre $[nn', kk', dd']$.

Définition

Soient C et C' deux codes linéaires de paramètres respectifs $[n, k, d]$ et $[n', k', d']$. On définit le produit tensoriel de C et C' comme le sous-espace vectoriel de ${\mathbb{F}_q}^n \otimes {\mathbb{F}_q}^{n'}$ engendré par les tenseurs élémentaires $\{c \otimes c'\}_{c \in C,\, c' \in C'}$.

$\Rightarrow$ Matrices dont les lignes sont des mots de C et les colonnes des mots de C'.
C'est un code linéaire de paramètre $[nn', kk', dd']$.

Proposition

$C_{\mathcal{H}}(s) \cong C_{\mathbb{P}^1}(s) \otimes C_{\mathbb{P}^1}(s)$ a pour paramètre $[(q+1)^2, (s+1)^2, (q+1-s)^2]$.

Définition

Soient C et C' deux codes linéaires de paramètres respectifs $[n, k, d]$ et $[n', k', d']$. On définit le produit tensoriel de C et C' comme le sous-espace vectoriel de ${\mathbb{F}_q}^n \otimes {\mathbb{F}_q}^{n'}$ engendré par les tenseurs élémentaires $\{c \otimes c'\}_{c \in C,\, c' \in C'}$.

$\Rightarrow$ Matrices dont les lignes sont des mots de C et les colonnes des mots de C'.
C'est un code linéaire de paramètre $[nn', kk', dd']$.

Proposition

$C_{\mathcal{H}}(s) \cong C_{\mathbb{P}^1}(s) \otimes C_{\mathbb{P}^1}(s)$ a pour paramètre $[(q+1)^2, (s+1)^2, (q+1-s)^2]$.

Corollaire

Soit X une courbe obtenue comme intersection de la quadrique hyperbolique $\mathcal{H}$ et d'une surface de degré s dans $\mathbb{P}^3$ qui ne contienne pas $\mathcal{H}$. Alors

$$\#X(\mathbb{F}_q) \leq 2s(q+1) - s^2$$

et on a égalité ssi X est l'union de s lignes de la forme $\phi(\{a\} \times \mathbb{P}^1)$ et de s lignes de la forme $\phi(\mathbb{P}^1 \times \{a\})$.

Théorème - Hasse-Weil ($\sim$ 1940)

Soit C une courbe projective lisse de genre g définie sur $\mathbb{F}_q$.

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Théorème - Hasse-Weil ($\sim$ 1940)

Soit C une courbe projective lisse de genre g définie sur $\mathbb{F}_q$.

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Pour le cas d'égalité, Hasse-Weil donne uniquement

$$\#X(\mathbb{F}_q) \leq 2s(q+1)$$

Théorème - Hasse-Weil ($\sim$ 1940)

Soit C une courbe projective lisse de genre g définie sur $\mathbb{F}_q$.

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Pour le cas d'égalité, Hasse-Weil donne uniquement

$$\#X(\mathbb{F}_q) \leq 2s(q+1)$$

Esquisse de la preuve : la surface de degré s est définie par la donnée d'un polynôme homogène f de degré s sur $\mathbb{P}^3$ qui n'appartient pas à $I_{\mathcal{H}}(s)$
Un point $P \in X(\mathbb{F}_q)$ si et seulement si $P \in \mathcal{H}(\mathbb{F}_q)$ et $f(P) = 0$.

Théorème - Hasse-Weil ($\sim$ 1940)

Soit C une courbe projective lisse de genre g définie sur $\mathbb{F}_q$.

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Pour le cas d'égalité, Hasse-Weil donne uniquement

$$\#X(\mathbb{F}_q) \leq 2s(q+1)$$

Esquisse de la preuve : la surface de degré s est définie par la donnée d'un polynôme homogène f de degré s sur $\mathbb{P}^3$ qui n'appartient pas à $I_{\mathcal{H}}(s)$
Un point $P \in X(\mathbb{F}_q)$ si et seulement si $P \in \mathcal{H}(\mathbb{F}_q)$ et $f(P) = 0$.

$\Rightarrow$ Majorer $\#X(\mathbb{F}_q)$ revient à majorer le nombre de zéros du mot de code $\mathrm{ev}\, f$ associé à f, c'est-à-dire minorer son poids.
Or le poids minimal d'un code est donné par
$n - d = (q+1)^2 - (q+1-s)^2 = 2s(q+1) - s^2$.

Merci pour votre attention !