ACCQ204 14 Décembre 2015

Cours 2

Enseignant: Aslan Tchamkerten *Crédit: Rita Ibrahim & Wenceslas Godel*

Codes linéaires

1 Le besoin de structure

Shannon promet l'existence de codes très bons mais il ne nous dit rien sur comment les construire.

Idée: Se restreindre à une classe de codes dont la complexité de codage ou décodage est faible.

Code sur un alphabet $[q] = \{1, 2, \ldots, q\}$

$C : [q]^k \longrightarrow [q]^n$

La mise en mémoire requiert: $n \times q^k$! Prohibitif (chaque message comporte n bits).

Idée: Imposer de la structure sur C pour limiter la mémoire.

Definition 1 *Soit $\mathbb{F}_q$ un corps.*
C est un code linéaire si c'est un sous-espace vectoriel de $\mathbb{F}_q^n$. On le note $[n, k, d]_q$.

Remarque À partir de maintenant tous les codes que l'on va étudier seront des codes linéaires.

2 Rappels sur le corps finis

Theorem 2 *Tout corps fini a cardinalité p^s où p est un nombre entier et $s \geq 1$ entier.*

Exemple 3 $\mathbb{F} = (\{0, 1\}, +, \cdot)$
$\mathbb{F} = (\{0, 1, \ldots, p-1\}, +_p, \cdot_p)$ *Les opérations sont réalisées modulo p.*

Theorem 4 $\forall q = p^s \ \exists!$ *corps avec q éléments (sans compter les isomorphismes).*

Theorem 5 *Tout corps fini a un élément* π*, appelé élément "primitif" de* $\mathbb{F}$ *t.q.* $S = \{0, \pi^0, \pi^1, \ldots, \pi^{q-2}\}$.

2.1 Polyômes et corps finis

Definition 6 *Étant donné* $\mathbb{F}_q$*, on définit* $\mathbb{F}_q[X] = \{\sum_0^\infty \alpha_i X^i, \alpha_i \in \mathbb{F}_q\}$.

Definition 7 $P(X) = \sum_1^d \alpha_i X^i, \alpha_d \neq 0$*, d est le degré de P(X).*

Exemple 8 $\mathbb{F}_q[X]$ *avec les lois d'addition et de multiplication est un anneau.*

Definition 9 $\alpha \in \mathbb{F}_q$ *est une racine de P(X) si* $P(\alpha) = 0$.

Theorem 10 (Fondamental de l'algèbre) *Un polynôme non nul de degré d a au plus d racines (peu importe* $\mathbb{F}_q$*).*

Definition 11 $P(X) \in \mathbb{F}_q[X]$ *est dit "irréductible" si pour tout* $Q_1(X), Q_2(X) \in \mathbb{F}_q[X]$ *tq.* $Q_1(X) \cdot Q_2(X) = P(X)$*, on a* $min(deg(Q_1), deg(Q_2)) = 0$.

Exemple 12 $X^2 + X + 1$ *irréductible sur* $\mathbb{F}_2$.
$X^2 + 1 = (X+1) \cdot (X+1)$ *n'est pas irréductible sur* $\mathbb{F}_2$.

3 Extensions d'un corps

$\mathbb{F}_q \overset{extension}{\longrightarrow} F_{q^m} \overset{isomorphe}{\leftrightarrow} \mathbb{F}_q^m$.
$\mathbb{F}_q^m = \{(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) : \alpha_i \in F_q \forall i,$ avec les règles d'addition $+$ et de multiplication $\cdot\}$
$+ : (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \times (\beta_0, \beta_1, \ldots, \beta_{m-1}) \longmapsto (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \ldots, \alpha_{m-1} + \beta_{m-1})$
L'addition des polyômes revient à l'addition des vecteurs.

$\cdot$: multiplication des polyômes modulo $E(X)$ où $E(X)$ est un polynôme irréductible de degré m. Cela assure que l'on reste dans l'ensemble des polyômes de degré $m-1$ et que chaque élément a un inverse. Parfois $\mathbb{F}_q^m$ est noté $\mathbb{F}_q / E(X)$.

Remarque Si $|\mathbb{F}_q| < \infty$, $\exists$ des polyômes irréductibles de n'importe quel degré.

4 Retour aux codes linéaires

Definition 13 *Le rang d'une matrice* $\in \mathbb{F}_q^{k\times n}$ *est le nombre* <u>maximal</u> *de lignes (ou colonnes) indépendantes.*

Definition 14 *Une matrice est dite* <u>de rang plein</u> *si son rang est* $min(k, n)$.

Theorem 15 *Si* $S \subset \mathbb{F}_q^n$ *est un sous espace-linéaire*

1. $|S| = q^k, k \geq 1$, *k étant la dimension de S.*
2. $\exists v_1, v_2, \ldots, v_k \in S$ *appelés base de S tq.* $\forall x \in S$,
   $x = \sum_1^k a_i vi = (a_1, a_2, \ldots, a_k) \cdot G$
   avec $G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}$ *appelée matrice "génératrice" de S.*
3. $\exists H$ *matrice* $\in \mathbb{F}_q^{(n-k)\times n}$ *de rang plein tq.* $H \cdot x^T = 0, \forall x \in S$
   H étant la matrice de parité.
4. $G \perp H \Leftrightarrow G \cdot H^T = 0$.

Lemma 16 *Soit* $k \leq n$ *G une matrice* $k \times n$ *génératrice de* S_1, *H une matrice de parité de dimension* $(n-k) \times n$ *du sous-espace* S_2 *tq.* $G \cdot H^T = 0$. *G et H sont supposées de rang plein.*
<u>Alors</u> $S_1 = S_2$.

Preuve

1. <u>$S_1 \subseteq S_2$</u>
   $c \in S_1 \Rightarrow \exists y \in \mathbb{F}_q^n$ tq. $c = y \cdot G \Rightarrow c \cdot H^T = y \cdot G \cdot H^T = 0$ car $G \cdot H^T = 0$
   $\Rightarrow c \in S_2$.
2. <u>$S_2 \subseteq S_1$</u>
   H est de rang plein $\Rightarrow dim\,(Ker\,(H)) = n - dim\,(Im\,(H))$. Or $Ker\,(H) = S_2$ et $dim\,(Im\,(H)) = n-k$. Donc $dim\,(Ker\,(H)) = k \Rightarrow dim\,(S_2) = k$.
   De plus G de rang plein $\Rightarrow dim\,(S_1) = k$.
   $\overset{1}{\rightarrow} S_1 = S_2$.

■

Exemple 17

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

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

$G \cdot H^T = 0$.

Conséquence 18 *Tout code linéaire* $[n, k, d]_q$ *peut-être représenté avec:* $min\,(n \cdot k, (n-k) \cdot n) = \mathcal{O}\,(n^2) \neq exp\,(\mathcal{O}\,(n))!$

Complexité du codage: $C\,(m) = m \cdot G$, où m est un vecteur-ligne de taille k et G une matrice de taille $k \times n$.
La complexité est en $\mathcal{O}\,(k \times n)$.

5 Distance minimale d'un code linéaire

Proposition 19 *Pour un code* $C\,[n, k, d]_q$, $d = \min_{c \neq 0 \in C}\ wt(C)\,.$

Preuve $d \triangleq \min_{x,y \in C, x \neq y}\ \Delta\,(x, y) = \min_{x,y \in C, x \neq y}\ \Delta\,(x - y, 0)$
Or $\Delta\,(x - y, 0) = wt\,(x - y)$.
Donc $d = \min_{c \in C, c \neq 0}\ wt\,(c)\,.$
En effet, la borne inférieure de la quantité $\Delta\,(x - y, 0)$ est atteinte car si l'on prend deux éléments, on peut toujours arriver à obtenir c. Par exemple, on choisit $x = c, y = 0$. ■

Proposition 20 *Pour un code* $[n, k, d]_q$ *de matrice de parité H, d est le nombre de colonnes linéairement dépendantes (preuve:* $Hc^T = 0$ *pour tout élément dans le code et donc le c de poids minimal correspondra au nombre minimal de colonnes linéairement dépendantes).*

6 Code de Hamming

Definition 21 *Pour tout entier $r \geq 2$ un code de Hamming (binaire) a pour matrice de parité H_r telle que :*

$$H_r = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & . & 1 \\ 0 & 1 & 1 & 0 & 0 & . & 1 \\ 0 & 0 & 0 & 1 & 1 & . & 1 \\ . & . & . & . & . & . & 1 \end{pmatrix}$$

où la $i^{ème}$ colonne est la représentation de i en binaire ($1 \leq i \leq 2^r - 1$) sur r bits. Donc $r = n - k$, i.e., $k = n - r$.

Proposition 22 *Pour tout $r \geq 2$ le code de Hamming a distance minimale égale à 3.*

Preuve Les colonnes de la matrice sont deux à deux indépendantes, donc $d \geq 3$. De plus $H_r^1 + H_r^2 + H_r^3 = 0$ et donc $d = 3$. ■

Observation 23 (Code et borne de Hamming) *Par la borne de Hamming*

$$|C| \cdot \mathrm{Vol}(n, \lfloor \frac{d-1}{2} \rfloor) \leq 2^n$$

Pour $d = 3$ on a

$$|C| \leq 2^n \cdot \frac{1}{n+1}$$

car $\mathrm{Vol}(n, 1) = n + 1$. *Il suit que*

$$\log_2(|C|) \leq n - \log_2(n+1).$$

Pour le code de Hamming,

$$n = 2^r - 1 \Rightarrow r = \log_2(n+1)$$

et donc

$$\log_2 |C| = k = n - r = n - \log_2(n+1).$$

On déduis que les codes de Hamming atteignent la borne de Hamming.

Observation 24 *Un code atteignant la borne de Hamming est dit parfait. Il existe d'autres codes parfait, par exemple, le code $[n, 1, n]_2$, ainsi que d'autres codes du a Golay.*

6.1 Décodage code de Hamming

1. Algo 1 : MAP. la complexité est en $2^{O(n)}$! (besoin de lister tous les mots codes).

2. Algo 2 : Dans le cas où une erreur se produit au maximum par mot code envoyé on a $y = C + e$ avec

$$e = \begin{pmatrix} 0 \\ . \\ 0 \\ 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}$$

Alors

$$Hy = Hc + He = He$$

ce qui correspond à la i^{eme} colonne de H (i étant la position du 1 dans e et donc de l'erreur dans y).

Complexité: $O(n \log_2(n))$ (un seul calcul matriciel à faire).

Remarque: Hy est appelé le syndrôme de y.

7 Codes MDS : maximum distance separable

Rappel : la borne du singleton nous dit que pour tout code

$$d \leq n - k + 1 \Rightarrow r + \delta \leq 1 \Rightarrow r \leq 1 - \delta.$$

Definition 25 *Un code est dit MDS (maximum distance separable) si* $d = n - k + 1$.

Proposition 26 *Si un code est MDS alors tout ensemble de k coordonnées les mots codes restrincts à ces coordonnés sont distinctes (i.e. les k composantes de tout mot code définissent le mot code).*

Preuve Voir preuve borne de Singleton. ■

Definition 27 *Soit C un code avec q^k mots codes sur $\mathbb{F}_q$ et de longueur n. Soit J un sous-ensemble de $\{1, 2, .., n\}$ de coordonnées. J est un* ensemble d'information *si pour tout mot code, les composantes de J le détermine entièrement.*

Corollary 28 *Pour un code MDS, tout J avec $|J| = k$ est un ensemble d'information.*

Conjecture 1 *Tout code linéaire $[n, k]_q$ MDS satisfait $n \leq q+1$ si $1 < k < q$ sauf si q est pair et $k = 3$ ou $k = q - 1$ auquel cas on a $n \leq q + 2$.*