ACCQ204 14 Décembre 2015

Cours 2

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

Bornes Fondamentales et codes linéaires

1 Introduction

Un code $\mathcal{C} \subseteq \Sigma^n$ sur un alphabet Σ est noté $(n, k, d)_q$ où

- $q = |\Sigma|$ est la taille de l'alphabet
- $|\mathcal{C}| \geq q^k$
- $\Delta(\mathcal{C}) \geq d$.

Parfois on utilise la notation (n, M, d) avec $M = q^k$.

Le but de ce cours est la charactérisation de la région de faisabilité de $(n, k, d)_q$. Bien que ce problème reste partiellement ouvert, on établira des conditions nécessaires et des conditions suffisantes pour l'existence de codes pour des paramétres donnés. En particilier, on s'intéresse aux paires (R, δ) atteignables où $R \triangleq \liminf_{n\to\infty} \frac{k(n)}{n}$ et $\delta \triangleq \liminf_{n\to\infty} \frac{d(n)}{n}$.[1]

2 Bornes Supérieures

Theorem 1 (Singleton) *Pour tout $q \geq 2$ on a $k+d \leq n+1$ d'où $R+\delta \leq 1$.*

Preuve
Soit $(n, k, d)_q$ un code. On définit la projection sur les $k-1$ premières composantes

$$\pi : \Sigma^n \to \Sigma^{k-1} \quad \pi(x^n) \triangleq x_1, x_2 ... x_{k-1}.$$

[1] Il est clair que R est une fonction non-croissante de δ.

Puisque $|\mathcal{C}| \geq q^k$ on a $|\mathcal{C}| > q^{k-1}$ et par le principe des niches de pigeons il existe x^n et y^n tels que $\pi(x^n) = \pi(y^n)$ et donc tels que $\Delta(x^n, y^n) \leq n - (k-1) = n - k + 1$. Par suite

$$d \leq \Delta(\mathcal{C}) \leq \Delta(x^n, y^n) \leq n - k + 1.$$

■

Theorem 2 (Hamming) *Pour tout entier $q \geq 2$ et $R, \delta \in [0,1]$ on a*

$$R + \frac{H(\frac{\delta}{2})}{\log_2(q)} \leq 1.$$

Preuve Soit $d = \lfloor \delta n \rfloor$. Pour tout $x, y \in \mathcal{C}$ on a

$$\text{Ball}(x, \lfloor (d-1)/2 \rfloor) \cap \text{Ball}(y, \lfloor (d-1)/2 \rfloor) = \emptyset$$

d'où $|\mathcal{C}| \cdot \text{Vol}(n, \lfloor (d-1)/2 \rfloor]) \leq q^n$ et donc

$$q^k \cdot 2^{n(H(\frac{\delta}{2}) - o(1))} \leq q^n.$$

En fixant le rapport $R = k/n$ et en prenant la limite $n \to \infty$ le résultat suit.
■

Theorem 3 (Plotkin) *Pour tout $R, \delta \in [0,1]$*

$$R \leq \begin{cases} 1 - \frac{\delta}{\theta} & \delta \leq \theta \\ 0 & \delta > \theta \end{cases}$$

avec $\theta \triangleq 1 - \frac{1}{q}$.

Preuve
Cas $\delta > \theta$: Soit $\Delta(\mathcal{C}) \geq d$ et $|\mathcal{C}| = q^k$. On considère la quantité auxiliaire

$$S \triangleq \sum_{x,y \in \mathcal{C}} \Delta(x,y) \geq dq^k(q^k - 1). \tag{1}$$

On remarque que S est une somme de contributions de colonnes de la matrice $q^k \times n$ correspondant aux q^k mots codes écrit en ligne:

$$\begin{pmatrix} x_1(1) & x_2(1) & . & . & . & x_n(1) \\ x_1(2) & . & . & . & . & x_n(2) \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ x_1(q^k) & . & . & . & . & x_n(q^k) \end{pmatrix}$$

On peut donc écrire

$$S = S_1 + S_2 + ... + S_l + ... + S_n$$

avec S_l la contribution de la l-ième colonne.

Calcul de S_l: Soit ${n_i}^l$ le nombre de fois où l'élément i apparait dans la colonne l. Afin de calculer S_l on somme la contribution de chaque élément $i \in \Sigma$ de la colonne l. Cette contribution est le produit entre le nombre d'apparitions de i dans la colonne l et le nombre d'apparitions d'éléments différents de i dans la colonne l. Il suit que

$$S_l = \sum_{i=1}^{q} {n_i}^l(q^k - {n_i}^l) = \sum_{i=1}^{q} {n_i}^l(q^k) - \sum_{i=1}^{q} {n_i}^2 = q^{2k} - \sum_{i=1}^{q} {n_i}^2.$$

D'après l'inégalité de Cauchy-Schwarz on a $\left|\sum_{i=1}^{q} n_i m_i\right|^2 \leq \sum_{i=1}^{q} |n_i|^2 \cdot \sum_{i=1}^{q} |m_i|^2$ et donc pour $m_i = 1$ l'inégalité s'écrit $\left|\sum_{i=1}^{q} n_i\right|^2 \leq \sum_{i=1}^{q} |n_i|^2 \cdot n$. Cette inégalité donne $S_l \leq q^{2k} - \frac{q^{2k}}{q}$ et on conclut

$$S = \sum_{l=1}^{n} S_l \leq n(q^{2k} - \frac{q^{2k}}{q}) = nq^{2k}(1 - \frac{1}{q}). \tag{2}$$

De (1) et (2) on déduit

$$nq^{2k}(1 - \frac{1}{q}) \geq dq^k(q^k - 1)$$

ou de manière équivalente

$$q^k \leq \frac{d}{d - \theta n} = \frac{qd}{qd - (q-1)n} \tag{3}$$

qui implique que pour $\theta < \delta$ on a $R = 0$.
Cas $\delta \leq \theta$: On prend n' tel que $\theta n' \approx d$, plus précisément on définit $n' = \lfloor \frac{d}{\theta} - \frac{1}{q-1} \rfloor$.

On groupe les mots code qui sont les même sur les $n - n'$ premières positions et on définit les sous-codes

$$\mathcal{C}_x \triangleq \{(c_{n-n'+1}, \ldots, c_n) : (c_1, c_2, \ldots, c_n) \in \mathcal{C}\ , (c_1, c_2, \ldots, c_{n-n'}) = x\}$$

En appliquant (3) au code $\mathcal{C}_x$ en remplaçant q^k par $|\mathcal{C}_x|$ et n par n' on obtient[2]

$$|\mathcal{C}_x| \leq \frac{qd}{qd - (q-1)n'} \leq qd$$

où la deuxième inégalite suit de la définition de n' qui guarantit que $qd - (q-1)n' \geq 1$. On déduit que

$$|\mathcal{C}| = \sum_{x \in q^{n-n'}} |\mathcal{C}_x| \leq qd \cdot q^{n-n'} = q^{n - \frac{d}{\theta} + O(\log_q d)}$$

d'où $R \leq 1 - \frac{\delta}{\theta}$. ■

3 Bornes Inférieures

Theorem 4 (Gilbert-Varshamov) *$R \geq$ 1- H(δ) pour $0 \leq \delta \leq \frac{1}{2}$ (on suppose ici que $q = 2$, la généralisation à $q \geq 3$ est immédiate).*

Preuve
Fixer $0 \leq \delta \leq \frac{1}{2}$ et considérer $d = \delta n$ (n suffisament grand).
On considère la construction suivante:

- Initialisation : $\mathcal{C} \leftarrow \emptyset$, $S = \{0,1\}^n$ = espace entier
- while $S \neq \emptyset$ do
  - choisir $x \in S$
  - $\mathcal{C} \leftarrow \mathcal{C} \cup \{x\}$
  - $S \leftarrow S \backslash \text{Ball}(x, d-1)$

[2]On peut appliquer (3) car clairement $\Delta(\mathcal{C}_x) \geq d$ et notre choix de n' satisfait $\theta n' < d$.

- end while
- output $\mathcal{C}$

Propriétés:

- $\Delta(\mathcal{C}) \geq d$
- $|\mathcal{C}| \geq \frac{2^n}{\text{Vol}(n,d-1)}$

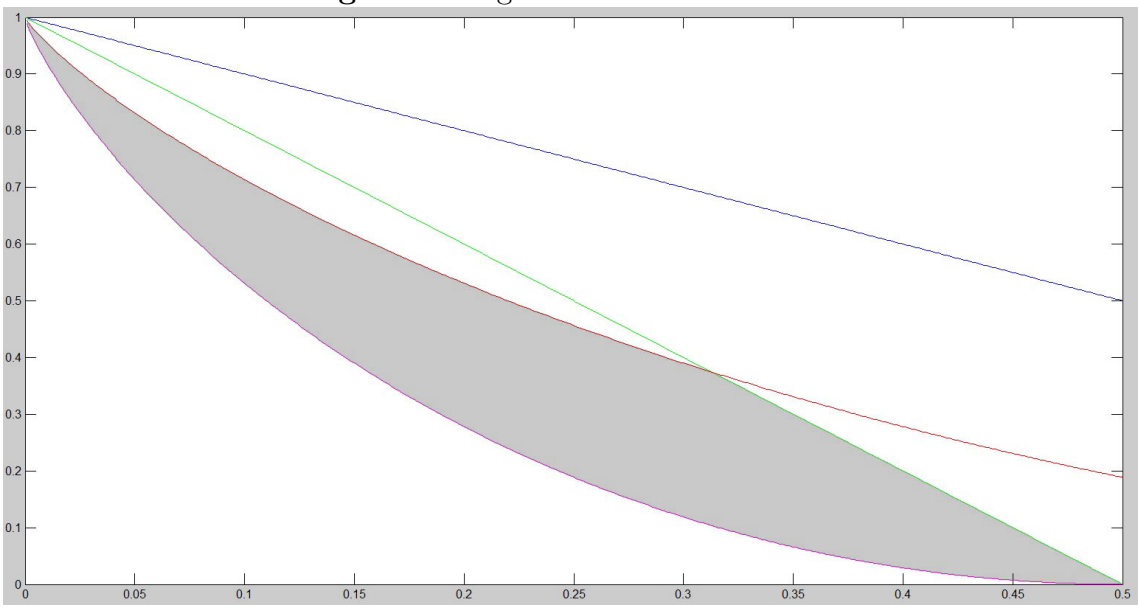
Puisque $\text{Vol}(n, d-1) \approx 2^{nH(\delta)}$ on a $R \geq 1 - H(\delta)$. ■

4 Comparaison pour $q = 2$

- Singleton: $R + \delta \leq 1$ (bleu)
- Hamming: R + $H(\delta/2) \leq 1$ (rouge)
- Plotkin: R $\leq \max\{1 - 2\delta, 0\}$ (vert)
- Gilbert-Varshamov: $R \geq 1 - H(\delta)$ (courbe jaune)

La frontiére entre (R, δ) atteignables et non-atteignables est inclue dans la région grisée. Notons qu'il existe de meilleurs bornes, par exemple la borne supérieure d'Elias-Bassalygo est meilleure que la borne Plotkin-Hamming.

Figure 1: Région de faisabilité



Remarque

- Modèle pire-des-scénarios de Hamming: on peut corriger $\leq \frac{\delta}{2}$ erreurs (taux normalisé) à taux $R \geq 1 - H(\delta)$ (Gilbert-Varshamov). Par Hamming, tout code corrigeant $\leq \frac{\delta}{2}$ erreurs a un taux $R \leq 1 - H(\frac{\delta}{2})$.
- Modèle probabiliste de Shannon: on peut corriger $\frac{\delta}{2} \pm \varepsilon$ erreurs avec probabilité $1 - \varepsilon$ et taux maximal $1 - H(\frac{\delta}{2})$.

5 Codes linéaires

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 5 *Soit $q = p^s$ avec p premier et s entier ≥ 1*
C est un code linéaire si c'est un sous-espace linéaire ou s.e.v de $\{1, 2, \ldots, q\}^n$.
On le note $[n, k, d]_q$.

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

6 Corps finis

$F = (S, +, \cdot)$

1. $+$ et $\cdot$ satisfont certaines conditions:
   - fermés,
   - commutatifs,
   - et admettent des identités ("0" pour $+$ et "1" pour $\cdot$).
2. Inverses: $\forall\ a \in S \Rightarrow$ unique inverse -a
   $\forall\ a \neq 0 \in S \Rightarrow$ unique inverse a^{-1}.
3. Distributivité: $a \cdot (a + b) = ab + ac$.

Theorem 6 *Tout corps fini a cardinalité p^s où p est un nombre entier et $s \geq 1$ entier.*

Exemple 7 $F = (\{0, 1\}, +, \cdot)$
$F = (\{0, 1, \ldots, p-1\}, +_p, \cdot_p)$ *Les opérations sont réalisées modulo p.*

Theorem 8 $\forall q = p^s\ \exists!$ *corps avec q éléments (sans compter les isomorphismes).*

Remarque $(S, \cdot, +)$ et $(S', \odot, \oplus)$
ϕ isomorphisme
$\phi : S \longrightarrow S'$ conserve les opérations.

Theorem 9 *Tout corps fini a un élément π, appelé élément "primitif" de F tq. $S = \{0, \pi^0, \pi^1, \ldots, \pi^{q-2}\}$.*

7 Polyômes et corps finis

Definition 10 *Étant donné F_q, on définit $F_q[X] = \{\sum_0^\infty \alpha_i X^i, \alpha_i \in F_q\}$.*

Definition 11 *$P(X) = \sum_1^d \alpha_i X^i, \alpha_d \neq 0$, d est le degré de P(X).*

Exemple 12 *Les $F_q[X]$ avec les lois d'addition et de multiplication sont des anneaux.*

Definition 13 *$\alpha \in F_q$ est une racine de P(X) si $P(\alpha) = 0$.*

Theorem 14 (Fondamental de l'algèbre) *Un polynôme non nul de degré d a au plus d racines (peu importe F_q).*

Definition 15 *$P(X) \in F_q[X]$ est dit "irréductible" si pour tout $Q_1(X), Q_2(X) \in F_q[X]$ tq. $Q_1(X) \cdot Q_2(X) = P(X)$, on a $min(deg(Q_1), deg(Q_2)) = 0$.*

Remarque Les polynômes irréductibles sur l'ensemble des polynômes jouent le même rôle que les nombres premiers sur l'ensemble des entiers.

Exemple 16 *$X^2 + X + 1$ irréductible sur F_2.*
$X^2 + 1 = (X + 1) \cdot (X + 1)$ n'est pas irréductible sur F_2.

8 Extensions d'un corps

$F_q \longrightarrow F_q^m \overset{isomorphe}{\leftrightarrow} F_{q^m}$.
Avec F_{q^m} on n'insiste plus sur la représentation vectorielle mais polynômiale.
$F_q^m = \{(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})\}, \forall i, \alpha_i \in F_q$.
E(X) est un polynôme irréductible de degré m.
$+ : (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \times (\beta_0, \beta_1, \ldots, \beta_{m-1}) \longmapsto (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \ldots, \alpha_{m-1} + \beta_{m-1})$
On peut considérer commme représentation alternative: $P(X) = \sum_0^{m-1} \alpha_i X^i$.
Alors l'addition des polyômes revient à l'addition des vecteurs.
$\cdot$: multiplication des polyômes modulo E(X).
Cela nous assure que l'on reste dans l'ensemble des polyômes de degré m-1.
On note $F/E(X)$.
Remarque Si $|F| < \infty$, $\exists$ des polyômes irréductibles de n'importe quel degré.

9 Sous-espace linéaire

Definition 17 *$S \subseteq F_q^n$ est un sous-espace linéaire si:*

- $\forall x, y \in S, x + y \in S$.
- $\forall (a, x) \in F_q \times S, ax \in S$.

Exemple 18 F_3^3
$S = \{(0,0,1), (1,0,1), (2,0,2), (0,1,1), (0,2,2), (1,2,2), (1,2,0), (2,1,0), (2,2,1)\}$
$(1,0,1) + (0,2,2) = (1,2,0) \in S$.
$2 \cdot (2,0,2) = (1,0,1) \in S$.

Definition 19 $B = \{v_1, v_2, \ldots, v_l\}, v_i \in S$
$span(B) = \left\{ \sum_1^l a_i v_i | a_i \in F_q \right\}$.

Definition 20 *Le rang d'une matrice $\in F_q^{k \times n}$ est le nombre <u>maximal</u> de lignes (ou colonnes) indépendantes.*

Exemple 21 $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

Definition 22 *Une matrice est dite <u>de rang plein</u> si son rang est $min(k, n)$.*

Theorem 23 *Si $S \subseteq F_q^n$ 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 $G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}$, *matrice "génératrice" de S.*
3. $\exists H$ *matrice* $\in F_q^{(n-k) \times n}$ *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 24 *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.*

Alors $S_1 = S_2$.

Preuve

1. $\underline{S_1 \subseteq S_2}$
   $c \in S_1 \Rightarrow \exists y \in F_q^n$ 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. $\underline{S_2 \subseteq S_1}$
   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 $\Rightarrow dim\,(S_1) = k$.

   $\stackrel{1}{\rightarrow} S_1 = S_2$.

■

Exemple 25

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

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

$G \cdot H^T = 0$.

Conséquence 26 *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: $m \in F_q^q \Rightarrow C\,(m) = m \cdot G$, où m est un vecteur-ligne de taille k et G une matrice de taille $k \times n$.
La complexité est en $\mathcal{O}\,(k \times n)$.

10 Distance minimale d'un code linéaire

Proposition 27 *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 28 *Pour un code* $[n,k,d]_q$ *de matrice de parité H, d est le nombre de colonnes linéairement dépendantes (⇒ cf. exercice).*