ACCQ204 11 Jan. 2016
Cours 4
Enseignant: Aslan Tchamkerten *Crédit: Sergey Zakharenko*

1 Décodage en liste

Definition:
Soit $0 \leqslant \rho \leqslant 1$ et $L \geqslant 1$.
Un code $C \subseteq \Sigma^n$ est (ρ, L)-liste décodable, si $\forall y \in \Sigma^n$

$$|\{c \in C : \Delta(c, y) \leqslant \rho n\}| \leqslant L$$

Remarque:
Le décodage est dit "efficace" si $L = e^{o(n)}$.
Ce décodage peut être utilisé de plusieurs façon. Par exemple, si $|\,\text{liste}\,| = 1$, déclarer l'unique élément et si $|\,\text{liste}\,| \geq 2$, déclarer "erreur." Un autre exemple est de déterminer le message envoyé dans la liste à l'aide d'information extérieure, si telle est disponible.
Théorème:
Soit $q \geqslant 2$ entier et $0 < \rho < 1 - \frac{1}{q}$

i. Pour tout entier $L \geqslant 1$ et $R \leqslant 1 - H_q(\rho) - \frac{1}{L}$ il existe un code (ρ, L)-décodable.

ii. Si un (ρ, L) code a taux $R \geqslant 1 - H_q(\rho) + \varepsilon$ alors $L \geqslant 2^{\Omega(\varepsilon n)}$.

Remarques: avec $L = cste$ il est possible de corriger jusqu'a ρn erreurs avec un taux $1 - H_q(\rho) - 1/L$ (L n'a pas besoin de grandir comme $e^{o(n)}$!!!). Si le taux est $> 1 - H_q(\rho)$ alors corriger une fraction $\rho > 0$ d'erreurs implique une liste immense $L = e^{\Omega n}$.
Preuve:

i. $|C| = q^k$ et $\forall m$ et on génère chaque mot code indépendamment aléatoirement $C(m) \sim$ uniform$[q]^n$. On défini l'évènement erreur

$$\mathcal{E} = \{\exists m_{\alpha_1}, \dots m_{\alpha_{L+1}} \text{ et } y \in [q]^n \text{ tel que } C(m_{\alpha_i}) \in \mathcal{B}(y, \rho n) \forall i = 1 \dots L+1\}$$

On va montrer que si $R \leq 1 - H_q(\rho) - 1/L$ alors $P(\mathcal{E}) < 1$, et il s'ensuit que $\exists$ un code C t.q. $\forall y$, $\mathcal{B}(y, \rho n)$ contient au plus L mots codes. On a

$$\mathcal{E} = \bigcup_{\alpha_1 \dots \alpha_{L+1}, y} \mathcal{E}(\alpha_1, \dots, \alpha_{L+1}, y)$$

où on définit

$$\mathcal{E}(\alpha_1, \dots, \alpha_{L+1}, y) = \{C(m_{\alpha_i}) \in \mathcal{B}(y, \rho n), \forall i = 1 \dots L+1\}.$$

On a

$$P(C(m_{\alpha_i}) \in \mathcal{B}(y, \rho n)) = \frac{\text{Vol}_q(n, \rho n)}{q^n} \leqslant \frac{q^{nH_q(\rho)}}{q^n} = q^{-n(1-H_q(\rho))}$$

et donc

$$P(\mathcal{E}(\alpha_1, \dots, \alpha_{L+1}, y)) \leqslant q^{-n(L+1)(1-H_q(\rho))}.$$

Par la borne de l'union on déduit donc

$$P(\mathcal{E}) \leqslant \binom{q^k}{L+1} q^n q^{-n(L+1)(1-H_q(\rho))}.$$

Or sait que $\binom{a}{b} \leqslant a^b$ et $k = R \cdot n$, d'où

$$P(\mathcal{E}) \leqslant q^{-n(L+1)[1-H_q(p)-\frac{1}{L+1}-R]} = q^{-n(L+1)[(1-H_q(\rho)-\frac{1}{L}-R)+(\frac{1}{L}-\frac{1}{L+1})]}$$

En supposant

$$1 - H_q(\rho) - \frac{1}{L} - R \geqslant 0$$

et puisque $\frac{1}{L} - \frac{1}{L+1} = \frac{1}{L(L+1)}$, on conclut

$$P(\mathcal{E}) \leqslant q^{-\frac{n}{L}} < 1$$

concluant la preuve.

ii. On va montrer que si C a taux $R \geqslant 1 - H_q(\rho) + \varepsilon \Rightarrow \exists y \in [q]^n$ t.q. $|C \cap \mathcal{B}(y, \rho n)| = q^{\Omega(n)}$.
On fixe code C avec taux $R \geqslant 1 - H_q(\rho) + \varepsilon$, et on fixe $c \in C$.
Choisissons Y aléatoirement sur uniforme$[q]^n$.

$$P(c \in \mathcal{B}(Y, \rho n)) = P(Y \in \mathcal{B}(\mathbf{c}, \rho \mathbf{n})) = \frac{\mathrm{vol}_q(n, \rho n)}{q^n} \geqslant \frac{q^{n(H_q(\rho)-o(1))}}{q^n}$$

$$\mathbb{E}[|C \cap \mathcal{B}(Y, \rho n)|] = \sum_{c \in C} \mathbb{E}[1\{c \in \mathcal{B}(Y, \rho n)\}]$$

$$\mathbb{E}[1\{c \in \mathcal{B}(Y, \rho n)\}] = P(c \in \mathcal{B}(Y, \rho n)) \geqslant q^{-n(1-H_q(\rho)+o(1))}$$

Puisque $|C| = q^{Rn}$, il suit que

$$\mathbb{E}[|C \cap \mathcal{B}(Y, \rho n)|] \geqslant q^{n(R-1+H_q(\rho)-o(1))} = q^{\Omega(n)} \text{ si } R \geqslant 1 - H_q(\rho) + \varepsilon$$

$$\Rightarrow \forall C \exists y : |C \cap \mathcal{B}(y, \rho n)| \geqslant q^{\Omega(n)} \text{ si } R \geqslant 1 - H_q(\rho) + \varepsilon.$$