ACCQ204 Décembre 2018

Enseignant: Aslan Tchamkerten

1 But: atteindre $\delta, R > 0$

Vu:

- Hamming: $[n, n - \log_2(n+1), 3]_2$ d'où $R = 1 - O((\log n)/n)$ et $\delta = O(1/n)$. Taux élevé, distance faible, faible complexité.
- RS: code possible (c.f. exos) $[n = 2^t, n/2, n/2+1]_{n=2^t=q}$ d'où $R, \delta \to 1/2$ mais $q = n$...

  Idée 1: codes BCH ("sous-ensemble-sous-corps" d'un code RS), mais $R > 0$ et $\delta \to 0$

  Idée 2: partir d'un code RS et écrire chaque symbol sur t bits. On obtient donc un code $[n \log_2 n, (n \log_2 n)/2, n/2+1]_2$. D'où $R \to 1/2$ mais $\delta \to 0$. En effet la distance minimale reste inchangée car les symboles sont "codés" avec un code de distance 1. Et si on augmentait cette distance par un véritable code correcteur d'erreurs? Ceci aboutit aux codes dit "concaténés".

2 Codes concaténés

Soit $q \geq 2, k \geq 1$ entiers et $Q = q^k$.

Soit

$$C_{out} : [Q]^K \to [Q]^N$$

code dit extérieur et

$$C_{in} : [q]^k \to [q]^n$$

code dit intérieur

Pour un message

$$m = (m_1, \ldots, m_K)$$

on a

$$C_{out}(m) = [C_{out}(m)_1, \ldots, C_{out}(m)_N]$$

et ensuite on utilise C_{in} et on obtient

$$[C_{in}(C_{out}(m)_1), \ldots, C_{in}(C_{out}(m)_N)] \equiv C_{in} \circ C_{out}(m)$$

le concaténation de codes C_{in} et C_{out}.

Theorem 1 *$C_{in} \circ C_{out}$ est un code $[n \cdot N, k \cdot K, d \cdot D]_q$. De plus, si C_{in} et C_{out} sont linéaires, alors $C_{in} \circ C_{out}$ est linéaire.*

Corollary 1 *Si C_{out} et C_{in} ont les taux R et r et distances δ_{out} et δ_{in}, respectivement, alors $C_{in} \circ C_{out}$ a taux $R \cdot r$ et distance minimale $\delta_{out} \cdot \delta_{in}$.*

2.1 Borne de Zyablov

On va voir que par concaténation on peut construire des codes à faible complexité et atteignant $\delta, R > 0$ sur un alphabet de dimension donnée (qui ne grandit pas avec la longueur de bloc).

1. From Exercise 6 Assignment 2 there exists linear codes over $[q]$ whose asymptotic rate $r = \lim_{n\to\infty} \frac{k(n)}{n}$ and relative minimum distance $\delta = \lim_{n\to\infty} \frac{d(n)}{n}$ satisfy the Gilbert-Varshamov bound
$$r \geq 1 - H_q(\delta).$$
Pick n large enough so that there exists a code such that
$$r(n) \geq 1 - H_q(\delta) - \varepsilon. \tag{1}$$
We assume here that we have access to this n, through an oracle.
Given a $k \times n$ generator matrix of a linear code, it takes it takes $O(q^k kn)$ time to generate each codeword (there are q^k codewords and each of them takes $O(kn)$ to be written using the generator matrix). Therefore it takes $O(q^k kn^2)$ to evaluate the minimum distance of a linear code. Since there are $q^{O(kn)}$ possible matrices, it takes $q^{O(kn)}O(q^k kn^2) = q^{O(kn)}$ to find a code with minimum distance satisfying (1).

2. Let C_{in} be the code found in the previous item. The minimum distance of this code thus satisfies
$$\delta_{in} \geq H_q^{-1}(1 - r - \varepsilon).$$
Let C_{out} be a RS code therefore satisfying
$$\delta_{out} = 1 - R.$$
The concatenated code $(\mathcal{R}, \delta)$ thus satisfies
$$\mathcal{R} = rR$$
and
$$\delta \geq (1 - R)H_q^{-1}(1 - r - \varepsilon).$$
Expressing R as a function of δ and r we get
$$R \geq 1 - \frac{\delta}{H_q^{-1}(1 - r - \varepsilon)}.$$
Therefore we can achieve
$$\mathcal{R} \geq r\left(1 - \frac{\delta}{H_q^{-1}(1 - r - \varepsilon)}\right).$$
Optimizing over r we get the Zyablov bound
$$\mathcal{R} \geq \sup_r r\left(1 - \frac{\delta}{H_q^{-1}(1 - r - \varepsilon)}\right)$$
which is below the GV bound for any $\delta \in (0, 1/2)$.

2.2 Décodage simple de code concaténés

On suppose que C_{in} a distance minimale d et C_{out} distance minimale D. On considère décoder C_{in} puis ensuite C_{out}.

- Si le $i$ème bloc contient $< d/2$ erreurs il sera décodé juste.
- Si il y a moins de $D/2$ blocs erronés, alors $C_{in} \circ C_{out}$ sera décodé juste.

Si le nombre total d'erreurs est $< d \cdot D/4$ alors le nombre de blocs avec au moins $d/2$ erreurs est au plus $D/2$.

Donc on peut corriger jusqu'a $d \cdot D/4$ et on sait qu'on peut corriger jusqu'a $d \cdot D/2$. Le décodage simple n'est donc pas optimal.

3 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

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

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

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

où on définit

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

On a

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

et donc

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

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

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

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