February 14, 2019

REMINDERS:

(•) HW0 due Th 11:59pm

(•) HW1 out Th (due in 1 week)

(•) Video topic + group composition due in 2 weeks (11:59pm, Mar 5)

RECAP:

→ $[n, k, d]_q$ code

→ Code family $\mathcal{C} = \{C_i\}_{i \geq 1}$, C_i is $(n_i, k_i, d_i)_q$ code $(n_{i+1} > n_i)$

$$R(\mathcal{C}) = \lim_{i \to \infty} \frac{k_i}{n_i} \qquad \delta(C) = \lim_{i \to \infty} \frac{d_i}{n_i}$$

→ $[2^r - 1, 2^r - r - 1, 3]_2$ - Hamming code : $H_r = \begin{array}{c} \quad 1 \;\; \cdots \;\; i \;\; \cdots \;\; 2^r-1 \\ r\updownarrow \begin{pmatrix} & & \boxed{\,\,} & & \end{pmatrix} \end{array}$ Binary(i)

↳ Can correct upto 1 error in $O(n^2)$ time

Need proof reader for today.

↳ Proof reader for [Sec 3.1, 3.2] → Vemuri (?) {we'll use the material next lecture}

TODAY:

(•) Dual of a linear code

↳ Hadamard code → $R = 0$, $\delta = 1/2$

⇒ Q: Can we get $R > 0$, $\delta > 0$ at the same time?

↳ YES! Gilbert - Varshamov bound

(•) Digression: → q-ary entropy fn

→ Volume of a Hamming ball

(•) Gilbert - Varshamov construction / bound

Dual of a linear code

Def: Let H be a parity check matrix for an $[n, k]_q$ code C. Dual of C $(C^\perp)$ as the code generated by H.

⇒ $C^\perp$ is $[n, n-k]_q$ ← rank-nullity thm

Ex: $C_{H,r}^\perp \triangleq C_{sim,r}$ (simplex code) ← H_r as gen. matrix

Hadamard code → $C_{Had,r}$ $\xleftarrow{\text{gen}}$ $H'_r = \begin{pmatrix} 0 & \\ \vdots & H_r \\ 0 & \end{pmatrix}$

$C_{sim,r} = [2^r - 1, r, ?]_2$ code

$C_{Had,r} = [2^r, r, ?]_2$ code

Prop: $d(C_{Sim,r}),\ d(C_{Had,r}) = 2^{r-1} = \dfrac{2^r}{2}$

$$\Rightarrow R(C_{Had,r}) = \lim_{r\to\infty} \frac{r}{2^r} = 0$$

$$\delta(C_{Had,r}) = \lim_{r\to\infty} \frac{2^{r-1}}{2^r} = \frac{1}{2}$$

Pf (for $C_{Had,r}$) Argue that any non-zero codeword $\bar{c} \in C_{Had,r}$ has $wt(\bar{c}) \geq 2^{r-1}$.

↳ <u>ALL</u> non-zero codeword $\bar{c}$, $wt(\bar{c}) = 2^{r-1}$

Consider $\bar{x} \in \mathbb{F}_2^r \setminus \{\bar{0}\} \Rightarrow \exists\, i$ s.t $x_i = 1$.

$$\bar{x} \longmapsto \underset{\substack{\| \\ 1}}{(x_1, \ldots, x_i, \ldots, x_r)} \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ H_r^0 & H_r^1 & \cdots & H_r^{2^r-1} \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} \; i$$

<u>Claim</u>: Can partition the columns in pairs (l_1, l_2) s.t

2^{r-1} such pairs. $\Leftarrow$ $H_r^{l_1}[i] \neq H_r^{l_2}[i]$ & agree in other rows

$$H_r^{l_1} = H_r^{l_2} + \bar{e}_i$$

<u>Note</u>: $c_l = \langle \bar{x}, H_r^l \rangle$

Consider a pair (l_1, l_2)

$$\bar{c} \quad [\ \cdots\ \underset{c_{l_1}}{\overset{l_1}{|}}\ \cdots\ \underset{c_{l_2}}{\overset{l_2}{|}}\ \cdots\ ]$$

$$c_{l_1} = \langle \bar{x}, \bar{H}_r^{l_1} \rangle = \langle \bar{x}, \bar{H}_r^{l_2} + \bar{e}_i \rangle = \underbrace{\langle \bar{x}, \bar{H}_r^{l_2} \rangle}_{c_{l_2}} + \underbrace{\langle \bar{x}, \bar{e}_i \rangle}_{\substack{\| \\ x_i = 1}}$$

$\Rightarrow c_{l_1} = c_{l_2} \oplus 1 \Rightarrow (c_{l_1}, c_{l_2})$ <u>exactly</u> one of them is a 1.

$\Rightarrow$ exactly 2^{r-1} positions in $\bar{c} = 1$ ∎

<u>Big Q</u>: Optimal tradeoff between R and δ?

$\rightarrow$ $R(C_{H,r}) = 1,\quad \delta(C_{H,r}) = 0$

$\quad\ R(C_{Had,r}) = 0,\quad \delta(C_{Had,r}) = \frac{1}{2}$

Q1: Can we get $R > 0$ <u>and</u> $\delta >$

Q2: Can we get $R > 0$ & $\delta > \frac{1}{2}$?

A1: Yes (Gilbert-Varshamov bound)

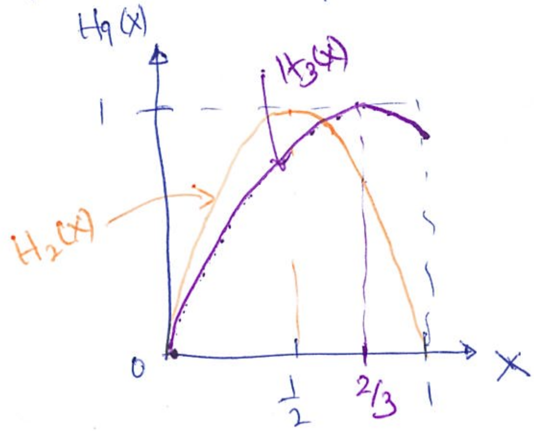
A2: NO (Plotkin bound)

Def: q-ary entropy fn $\quad q \geq 2 \quad 0 \leq x \leq 1$

$$H_q(x) = x \log_q (q-1) - x \log_q x - (1-x) \log_q (1-x)$$

~~Sep~~ Special case $(q=2)$ $\quad H(x) = H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$

" Shannon's entropy for the distr $\{x, 1-x\}$



Volume of a Hamming ball

$$B_q(\bar{x}, r) = |\{\bar{y} \in [q]^n : \Delta(\bar{x}, \bar{y}) \leq r\}|$$

$$= \sum_{i=0}^{r} \binom{n}{i} (q-1)^i = \underline{\underline{Vol_q(r, n)}}$$

PROP: $q \geq 2, \quad 0 \leq p \leq 1 - \frac{1}{q}$

(i) $Vol_q(pn, n) \leq q^{H_q(p)n}$

(ii) $Vol_q(pn, n) \geq q^{H_q(p)n - o(n)}$

$f(n) \in o(g(n))$

$\equiv \lim_{n \to \infty} \frac{f(n)}{g(n)} = 0$

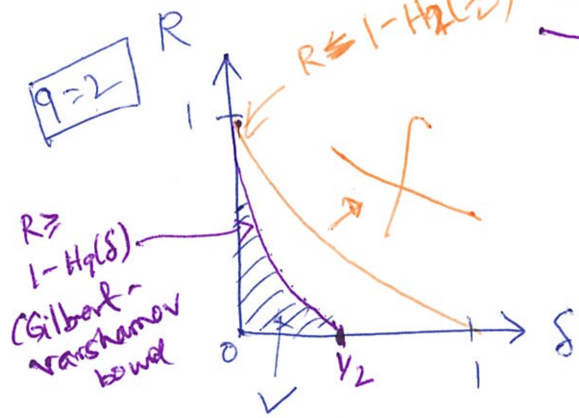
Recall Hamming bound:

$$\frac{k}{n} \leq 1 - \frac{\log_q Vol_q\left(\left\lfloor \frac{d-1}{2} \right\rfloor, n\right)}{n} \approx Vol_q\left(\frac{\delta n}{2}, n\right)$$

$d = \delta \cdot n$

$$\Rightarrow R \leq 1 - \frac{\log_q q^{H_q(\frac{\delta}{2})n - o(n)}}{n} = 1 - \frac{\left(H_q(\frac{\delta}{2})n - o(n)\right)}{n}$$

$$= 1 - H_q\left(\frac{\delta}{2}\right) + \underbrace{\frac{o(n)}{n}}_{= o(1)}$$



Pf (i) $\quad \mathrm{Vol}_q(pn,n) \leq q^{H_q(p)\cdot n}$

$$\Leftrightarrow \quad 1 \geq \mathrm{Vol}_q(pn,n)\cdot q^{-H_q(p)\cdot n}$$

Claim: $p \leq 1-\frac{1}{q} \Leftrightarrow \frac{p}{(q-1)(1-p)} \leq 1$

$$1 = (p+(1-p))^n$$

Binomial expansion $\rightarrow$ $$= \sum_{i=0}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

$$\geq \sum_{i=0}^{pn} \binom{n}{i} p^i (1-p)^{n-i}$$

$$= \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i}$$

$$= \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i (1-p)^n \cdot \left(\frac{p}{(q-1)(1-p)}\right)^i$$

Claim $\longrightarrow$ $$\geq \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i \underbrace{(1-p)^n \left(\frac{p}{(q-1)(1-p)}\right)^{pn}}_{= q^{-H_q(p)n}}$$

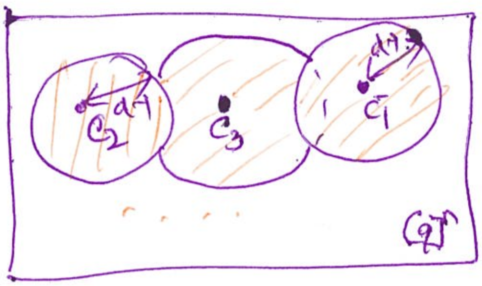
$$= q^{-H_q(p)n} \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i$$

$$= q^{-H_q(p)n} \cdot \mathrm{Vol}_q(pn,n) \quad \blacksquare$$

Gilbert - Varshamov bound:

Thm: Let $q \geq 2$. For every $0 \leq \delta \leq 1 - \frac{1}{q}$, $0 < \varepsilon \leq 1 - H_q(\delta)$;
$\exists$ a (linear) code with relative distance δ, $R \geq 1 - H_q(\delta) - \varepsilon$

2 proofs:
- $\to$ Greedy construction ($\varepsilon = 0$) $\Rightarrow$ not necessarily linear (Gilbert)
- $\to$ Randomized " ($\varepsilon > 0$) $\to$ linear code (Varshamov)



Algo: (1) $C \leftarrow \phi$
(2) While $\exists\ \bar{u} \in [q]^n$ s.t. $\Delta(\bar{u}, \bar{w}) \geq d \ \forall \bar{w} \in C$
Add u to C
(3) Output C

Claim: C has distance $\geq d$. Runtime: $q^{O(n)}$

Prop: $|C| \geq q^{n(1 - H_q(\delta))} \equiv R \geq 1 - H_q(\delta)$

Pf: Note: $\bigcup_{\bar{c} \in C} B(\bar{c}, d-1) = [q]^n$ $\qquad \left| \bigcup_{i=1}^{m} A_i \right| \leq \sum_{i=1}^{m} |A_i|$

$$\Rightarrow \left| \bigcup_{\bar{c} \in C} B_q(\bar{c}, d-1) \right| = q^n$$

$$q^n \leq \sum_{\bar{c} \in C} |B_q(\bar{c}, d-1)|$$
$$= \sum_{\bar{c} \in C} Vol_q(d-1, n)$$
$$= |C|\, Vol_q(d-1, n)$$
$$\leq |C|\, Vol_q(\underbrace{d}_{=\delta n}, n)$$
$$\leq |C|\, q^{H_q(\delta) \cdot n}$$

$$\Rightarrow |C| \geq q^{n(1 - H_q(\delta))}$$

∎