Feb 23

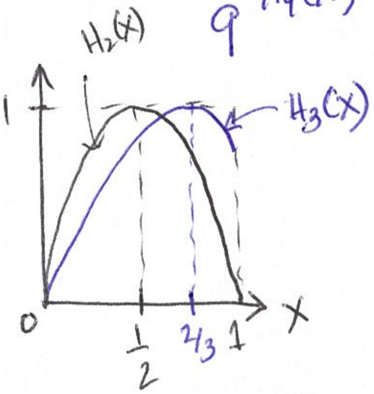
REMINDERS:

(∘) HW 1 due by 11:59 pm tonight
  (→) Read piazza posts for clarifications
(∘) Video topic (subit via Google form) by 11:59 pm NEXT Wed
  (→) Not submitting this means ZERO ON REST of the project.
(∘) HW 2 out next Wed

RECAP: $q \geq 2$ $\quad 0 \leq x \leq 1$

(∘) q-ary entropy fn: $H_q(x) = x \log_q (q-1) - x \log_q x - (1-x) \log_q (1-x)$

NOTE (not covered on Mon)



$$q^{H_q(x)} = \frac{q^{\log_q (q-1)^x}}{q^{\log_q x^x} \cdot q^{\log_q (1-x)^{1-x}}} = \frac{(q-1)^x}{x^x \cdot (1-x)^{1-x}}$$

$$= \frac{1}{(1-x)} \cdot \left(\frac{(q-1)(1-x)}{x} \right)^x \quad \text{—— } (*)$$

(∘) Volume of a Hamming ball: $Vol_q(r,n) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$

(∘) PROPOSITION: $q \geq 2$, $0 \leq p \leq 1 - \frac{1}{q}$

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

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

(∘) Big Goal: Optimal tradeoff b/w R & δ
  → Hamming code $R = 1, \delta = 0$ $\quad$ Q: $R > 0, \delta > 0$?
  → Hadamard code $R = 0, \delta = \frac{1}{2}$

Volunteer for proof reading today? John

PLAN for today: (i) Prove PROPOSITION (i)
(ii) Gilbert-Varshamov bound ($\Rightarrow R > 0, \delta > 0$)

(Recall) Hamming bound:

$d = \delta n$

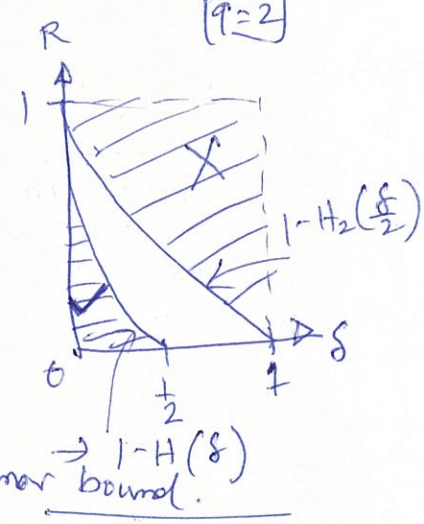
$\delta \le 1 - \frac{1}{q}$

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

$$\le 1 - \frac{\log_q q^{H_q(\frac{\delta}{2})n - o(n)}}{n}$$

$$= 1 - \frac{H_q(\frac{\delta}{2})n - o(n)}{n}$$

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



Pf of (1) Show $Vol_q(pn, n) \le q^{H_q(p)n}$

$q \ge 2$

$0 \le p \le 1 - \frac{1}{q}$

$$\equiv \quad 1 \ge Vol_q(pn, n) \cdot q^{-H_q(p)n}$$

Assume pn is an integer

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

Binomial expansion theorem

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

Claim: $p \le 1 - \frac{1}{q} \iff \frac{p}{(q-1)(1-p)} \le 1$

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

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

$$= \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i \cdot \Big(\underbrace{\frac{p}{(q-1)(1-p)}}_{\le 1}\Big)^i (1-p)^n$$

$$\ge \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i \underbrace{\left(\frac{p}{(q-1)(1-p)}\right)^{pn} (1-p)^n}_{= q^{-H_q(p)n} \text{ from } (*)}$$

$$= q^{-H_q(p)n} \cdot \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i = q^{-H_q(n)} \cdot Vol_q(pn, n) \quad \blacksquare$$

Gilbert-Varshamov bound (GV bound)

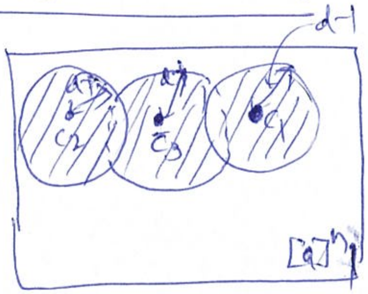
THM: Let $q \geq 2$. For every $0 \leq \delta \leq 1-\frac{1}{q}$, $0 \leq \varepsilon \leq 1 - H_q(\delta)$, $\exists$ a (linear) code with relative distance δ, and

$$R \geq 1 - H_q(\delta) - \varepsilon$$

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

Greedy construction

$d = \delta n$. $C \subseteq [q]^n$



Algo: (1) $C \leftarrow \phi$

(2) While $\exists\ \bar{u} \in [q]^n$ s.t $\Delta(\bar{u}, \bar{c}) \geq d$ for all $\bar{c} \in C$

Add $\bar{u}$ to C

(3) return C

Claim 1: Algo terminates. [Time $q^{O(n)}$]

Claim 2: The code C that is output has distance $\geq d$.

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

Pf:

$$\bigcup_{\bar{c} \in C} B(\bar{c}, d-1) = [q]^n \text{ (as Algo has terminated)}$$

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

$$\Rightarrow q^n \leq \sum_{\bar{c} \in C} |B(\bar{c}, d-1)|$$

$$= \sum_{\bar{c} \in C} Vol_q(d-1, n) = |C| \cdot Vol_q(d-1, n)$$

$$\leq |C|\ Vol_q(d, n)$$

$$= |C|\ Vol_q(\delta n, n) \qquad [\delta \leq 1 - \tfrac{1}{q}]$$

$$\leq |C| \cdot q^{H_q(\delta) \cdot n}$$

$$\Rightarrow |C| \geq \frac{q^n}{q^{H_q(\delta) \cdot n}} = q^{n(1-H_q(\delta))} \qquad \blacksquare$$