Feb 27 — 1 min checkin

REMINDERS

- Video topic due (via G form) by 11:59pm THIS WEDNESDAY!
  - ↳ If your group does not submit the form EVERYONE in the group gets ZERO ON rest of project
  - ↳ 0 submissions as of 7:45pm on Sunday
- HW 1 grading should be by tonight
- Impossible Project Finale (5:10 pm in NSC 225)

RECAP

- BIG Q: Optimal tradeoff between $R(C)$ & $\delta(C)$?
- So far: possible → $R(C)=1,\ \delta(C)=0$ via Hamming codes
  $R(C)=0,\ \delta(C)=\frac{1}{2}$ via Hadamard codes
- Q1: Can we simultaneously get $R(C)>0,\ \delta(C)>0$?

Plan for today

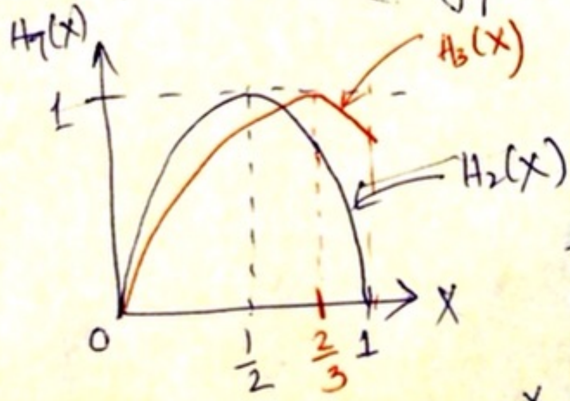
- q-ary entropy function
- Volume of a Hamming ball
- (If we have time) Gilbert-Varshamov bound (answers Q1 above positively)

$a\log b = \log b^a$

$x^{\log_x y} = y$

Def: q-ary entropy function $\qquad q \geq 2 \qquad 0 \leq x \leq 1$

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



$$H(x) = H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$$

Shannon's entropy function for distribution

0	w.p. x
1	w.p. $1-x$

Fact: $H_q\left(1-\frac{1}{q}\right) = 1$

$H_q(0) = 0$

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

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

Volume of a Hamming ball

Reminder $B_q(\bar{x}, r) = \{\bar{y} \in [q]^n \mid \Delta(\bar{x}, \bar{y}) \le r\}$

$x \in [q]^n$

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

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

Proposition $q \ge 2$, $0 \le p \le 1 - \frac{1}{q}$

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

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

little-oh $f(n) \in o(g(n))$

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

(Recall) Hamming bound

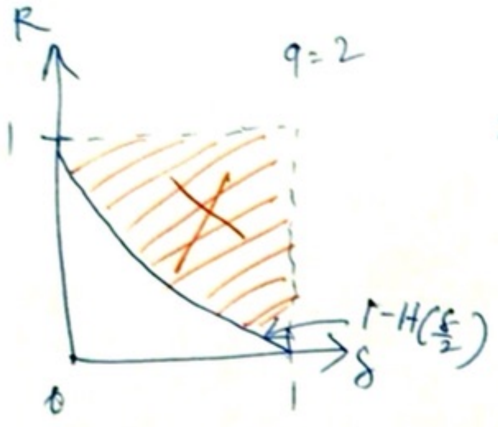
$$R = \frac{k}{n} \le 1 - \frac{\log_q Vol_q\left(\left\lfloor \frac{d-1}{2} \right\rfloor, n\right)}{n}$$

$\approx Vol_q\left(\frac{\delta n}{2}, n\right)$

$d = \delta n$

by (ii) above

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



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

$\frac{o(n)}{n}$

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

$$\lesssim 1 - H_q\left(\frac{\delta}{2}\right)$$

Pf of (ii) in book ← please read this $n! \approx \left(\frac{n}{e}\right)^n$

Pf of (i) $\quad \mathrm{Vol}_q(pn, n) \le q^{H_q(p)\cdot n}$ $\quad \Big| \; \frac{1}{a^b} = a^{-b}$

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

$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$

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

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

$\boxed{\frac{a}{b} \le \frac{c}{d} \Rightarrow \frac{a}{b+a} \le \frac{c}{d+c}}$

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

Binomial expansion Thm. $\rightarrow$

$$= \sum_{i=0}^{n} \binom{n}{i} p^i (1-p)^{n-i} \quad \left(\begin{matrix} pn \text{ is} \\ \text{an int.}\end{matrix}\right)$$

All summands ≥ 0

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

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

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

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

$1 \ge q^{-H_q(p)n}\cdot \mathrm{Vol}_q(pn, n)$ ✓

$$= \sum_{i=0}^{pn} \binom{n}{i} (q-1)^i \left(\underbrace{\left(\frac{p}{(q-1)(1-p)}\right)^p \cdot (1-p)}_{\text{by }(\#) \rightarrow\, = q^{-H_q(p)}}\right)^n$$

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

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

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

Gilbert - Varshamov bound (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 rel. distance δ and

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