Feb 21 **REMINDERS:**

- (•) Clarification on erasures added to HW 1 webpage
- (•) Reminders about HW instructions:
  - (–) Only four sources allowed. PERIOD
    - ↳ If you used an unallowed source follow instructio on ~~week~~ HW 1 webpage
  - (–) Can collaborate in groups of size ≤ 3
    - ↳ Only to the extent of discussing ideas
- (•) Reading assignment: Book [Sec 3.1, 3.2]

RECAP:

- (•) Family of codes
- (•) Can get $R(C) = 1$, $\delta(C) = 0$ $\left\{ \text{via } [2^r-1, 2^r-1-r, 3]_2 \text{ Hamming code} \right\}$.
- (•) Can correct for t errors for any linear code in $O(n^{t+2})$ time

---

PROOF READER: Ben

Volunteer for proof reading Sec 3.1 + 3.2? ← Aman

PLAN FOR TODAY:

- (•) Dual of a linear code
  - ↳ ~~Deale of e Hamming code~~ Hadamard code: $R(C) \to 0$, $\delta(C)$ ~~$R(C)$~~ $= \frac{1}{2}$
- ⇒ Q: Can we get $R(C) > 0$, ~~$R(C)$~~ $\delta(C) > 0$
  - A: Yes! Via Gilbert-Varshamov bound (on Wed)
- (•) (Necessary) Digression: q-ary entropy function
  - → Volume of a Hamming ball

Def (Dual of a linear code) Let H be a parity check matrix for an $[n,k]_q$ code C.

Dual of C (denoted by $C^{\perp}$) is the code generated by H

$\Rightarrow$ $C^{\perp}$ is an $[n, n-k]_q$ code

↑ rank nullity Theorem

Example: $C_{H,r}^{\perp} \overset{\text{def}}{=} C_{sim,r}$ (simplex code) ← H_r as the generator matrix

$C_{Had,r} \xleftarrow[\text{matrix}]{\text{generator}} H'_r = \left(\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \;\; H_r \right) \updownarrow r$, width $\longleftrightarrow 2^r$

↗ Hadamard code.

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

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

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

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

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

Pf (for $C_{Had,r}$) Goal: Argue every non-zero codeword has Ham wt. $\geq 2^{r-1}$ + $\exists$ some non-zero codeword with Ham wt. $= 2^{r-1}$

We'll show: EVERY non-zero codeword in $C_{Had,r}$ has wt $= 2^{r-1}$

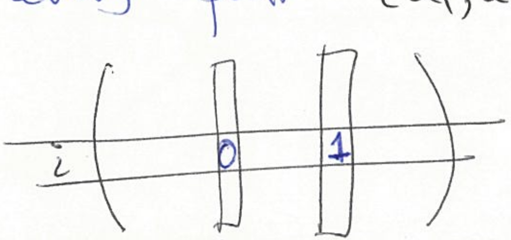
$\bar{x} \in \mathbb{F}_2^r \setminus \{\bar{0}\} \Rightarrow \exists\, i \in [r]$ s.t $x_i = 1$

$$C_{Had,r}(\bar{x}) = (x_1, \ldots, x_r) \begin{pmatrix} \uparrow & \uparrow & & \uparrow & & \uparrow \\ H_r^0 & H_r^1 & \cdots & H_r^j & \cdots & H_r^{2^r-1} \\ \downarrow & \downarrow & & \downarrow & & \downarrow \end{pmatrix}$$

$0 \leq j \leq 2^r - 1$

Claim: Can partition the columns of H'_r s.t for every pair (ℓ_1, ℓ_2)

$$(*) \begin{cases} H_r^{\ell_1}[i] \neq H_r^{\ell_2}[i] \ \& \\ H_r^{\ell_1}[i'] = H_r^{\ell_2}[i'] \text{ for all } i' \neq i. \end{cases}$$



Pf (sketch) of Claim: for every $\ell_1 \in [n]$ s.t $H_r^{\ell_1}[i] = 0$ ← 2^{r-1} ways to pick ℓ_1 ← as each vector in $\{0,1\}^r$ is present as a column to H'_r exactly once.

(*) holds by construction. $\Leftarrow$ let ℓ_2 be s.t $H_r^{\ell_2} = H_r^{\ell_1} + \bar{e_i}$

Rest of the pf:

$C_{Had,r}(\bar{x})$ → ℓ_1 position ← $\langle \bar{x}, H_r^{\ell_1} \rangle$

$C_{Had,r}(\bar{x})$ → ℓ_2 position ← $\langle \bar{x}, H_r^{\ell_2} \rangle$

$\langle \bar{x}, H_r^{\ell_1} \rangle + \langle \bar{x}, H_r^{\ell_2} \rangle = \langle \bar{x}, H_r^{\ell_1} + H_r^{\ell_2} \rangle = \langle \bar{x}, \bar{e}_i \rangle = x_i = 1$ ▪

Big Q: optimal tradeoff between R & δ?

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

Q1: Can we get $R > 0, \delta > 0$?

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

A1: Yes: Gilbert-Varshamov bound (Wed)

A2: No: Plotkin bound (Fri/Mon)

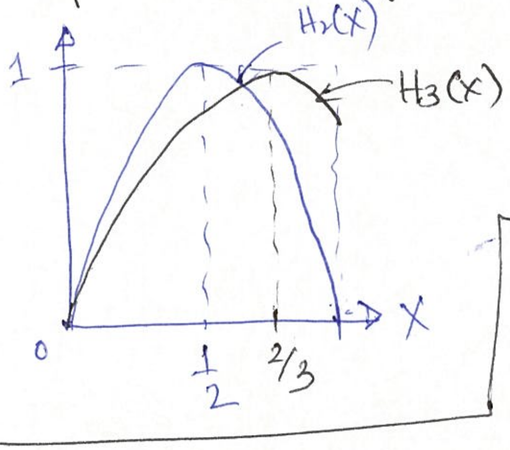
Def: q-ary entropy function $\quad q \geq 2, \ 0 \leq x \leq 1$

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

→ special case $q = 2$ $\quad H(x) = H_2(x) = -x \log_2 x - (1-x) \log_2 (1-$

↑ Shannon's entropy function for the distribut

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



$$H_q(1 - \tfrac{1}{q}) = 1$$

Volume of a Hamming ball

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

$$|B_q(\bar{x}, r)| = |\{\bar{y} \in [q]^n \mid \Delta(\bar{x}, \bar{y}) \leq r\}|$$
$$= \sum_{i=0}^{r} \binom{n}{i} (q-1)^i = Vol_q(r, n)$$

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

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

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

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