TI-Lecture-5-5-2020

5 May, 2020 13:58

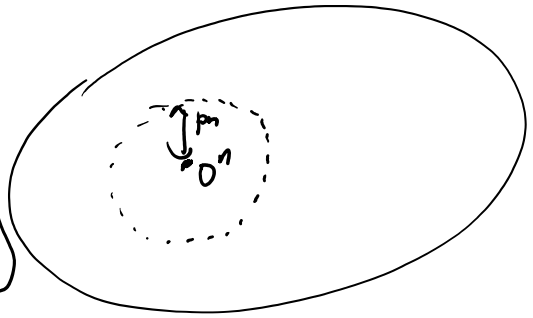
Varshamov ... random matrix $G$, $k \times n$

$\rightarrow [n, (1-H(p))n, pn]$

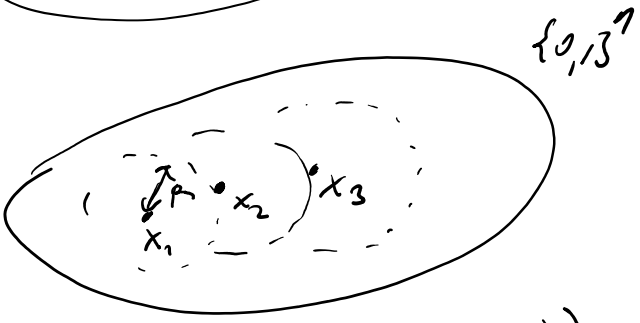
W.h.p $G$ generates

$x \in \{0,1\}^n$

$Pr\left[C(x) = xG \in Ball(0^n, pn)\right]$




Gilbert ... greedy

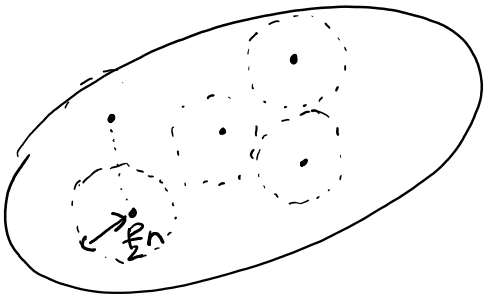



Hamming bound:

$[n, k, pn]$ ... code then $k \leq \left(1 - H\left(\frac{p}{2}\right)\right)n$

$\leq$ VI

$\leq ((1 - H(p))n)$




$Vol(n, \frac{p}{2}n) \cdot 2^k \leq 2^n$

$Vol(n, \frac{p}{2}n)$

VI

$2^{H(\frac{p}{2})n}$

$n$

$$\frac{2^{nH(\frac{p}{2})}}{n} \cdot 2^k \leq 2^n$$

$$2^k \leq n \cdot 2^{n - H(\frac{p}{2})n}$$

$$2^k \leq n \cdot 2^{(1-H(\frac{p}{2}))n}$$

$$k \leq \left(1 - H\left(\frac{p}{2}\right)\right)n + \lg n$$

$$\left(1 - H\left(\frac{p}{2}\right) + \frac{\lg n}{n}\right) n$$

$\hookrightarrow 0$

$$\therefore \quad k \leq \left(1 - H\left(\frac{p}{2}\right)\right)n$$

$[n, (1-H(p))n, pn]$ Gilbert - Varshamov

$\frac{pn-1}{2}$ ... errors

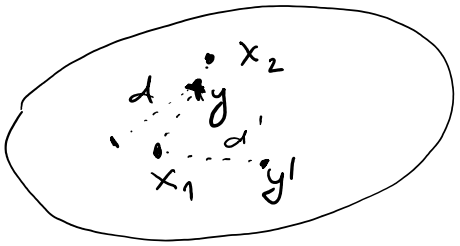
ω.

$[n, (1-H(p))n, \dots]$ Shannon.

$\hookrightarrow$ $pn$ errors

---

$d$ ... distance $\frac{d-1}{2}$ errors




$$\frac{d-1}{2} \leq d' \leq d$$

multiple codewords at distance $\leq d'$ from $y$.

- list decoding : on input $y$, find all codewords up-to distance $d' \to L$

RS : $d' \simeq (1-\varepsilon)d$ $\quad |L| \le$ small

$\exists$ alg. for list-decoding

- local decoding


- decode all the bits $n, k$
- $x_i$ ? decode $x_i$ given $i$.

Ex: Hadamard codes $[2^k, k, \frac{1}{2}\cdot 2^k]_2$

$2^k = n$ $\quad \lg n = k$ $\quad \frac{1}{2}n$

$x \in \{0,1\}^k$ $\quad y \in \{0,1\}^{2^k}$

$y = \dots y_a \dots$ $\quad a \in \{0,1\}^k$

$y_a = \langle x, a \rangle_{\mod 2} = \sum_{i=1}^{k} x_i \cdot a_i \mod 2$

$x, x'$ $\quad C(x) + C(x') = C(x+x')$ $\quad GF[2]$

each codeword except for $0^n$, has exactly $\frac{1}{2}$ of coordinates set to 1.

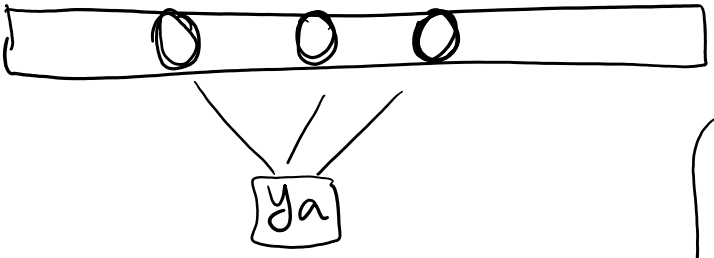
fix $x \neq 0^k$ think of $a$ as variable

$x$ 0 1 0 1 1 1 0

$a$ 1 0 1 1 1 0 0

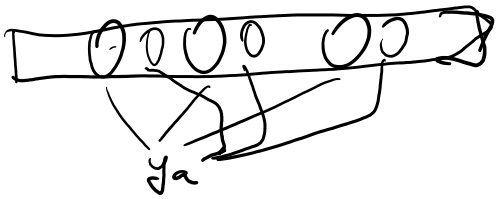

- for given coordinate $a \in \{0,1\}^k$ decode $y_a$

$e_i = (0\ldots0\underset{i}{1}0\ldots0) \rightsquigarrow x_i$ $\quad y_{e_i} = x_i$




[deterministic alg doesn't work]

$\forall a$ probabilistic procedure decodes $y_a$ correctly with high prob. over the random choices of the procedure




decoding alg: on input $a \in \{0,1\}^n$, pick random $r \in \{0,1\}^k$

$\rightarrow$ output $y_r \oplus y_{r+a}$

Claim: If the # of errors $\leq \frac{1}{5}$ then the output is correct with probability $\geq \frac{3}{5}$.

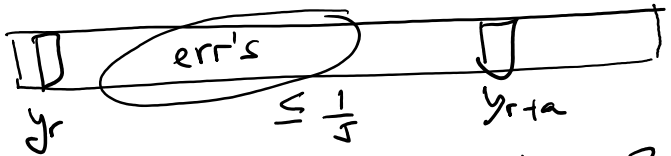

$\rightarrow$ no corruption than the alg. outputs always the correct value.

$$y_r = \sum x_i r_i \quad \oplus \quad y_{r+a} = \sum x_i (r+a)_i \pmod 2$$

$$y_a = \sum x_i a_i \qquad y_a + y_r = y_{a+r}$$

$$y_r + y_{r+a} = \sum x_i r_i + \sum x_i \underbrace{(r+a)_i}_{r_i + a_i} = \sum x_i \underbrace{(r_i + a_i + r_i)}_{a_i}$$

$$= \sum x_i a_i = y_a$$




$r' = r + a$

$\Pr_r[y_r \text{ corrupted}] \le \frac{1}{5}$ $\Pr_r[y_{r+a} \text{ corrupted}] \le \frac{1}{5}$

$\Pr_r[y_r \text{ or } y_{r+a} \text{ is corrupted}] \le \frac{1}{5} + \frac{1}{5} \le \frac{2}{5}$

for fixed $a$
repeat the procedure $l$-times and output the most frequent value.

The probability of error $\le 2^{-cl}$.

$l = O(\log k)$

$\frac{1}{k^2}$

---

## Communication Complexity

Alice

$x \in \{0,1\}^n$

Bob

$y \in \{0,1\}^n$

They want to compute some fun $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$f(x,y)$

**Q:** How much communication they have to perform to calculate $f(x,y)$?

Ex: 1) $\sum x_i + \sum y_i \mod 2$ — 2 bits

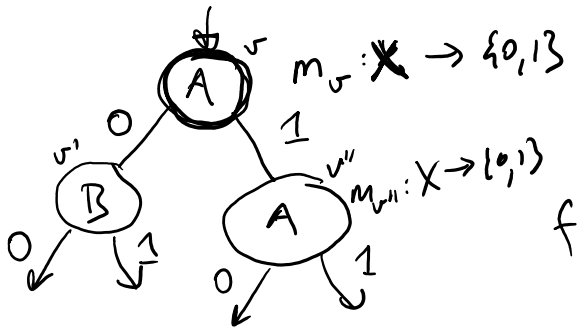
2) $EQ(x,y) = [x \doteq y]$ — $n+1$ bits suffice, cannot be improved (determ.)

3) $DISJ(x,y) = [\exists i;\ x_i = y_i = 1]$ — $n+1$ bits suffices, cannot be improved

protocol

$m_{v'} : Y \to \{0,1\}$

depth = communication cost




A B

$f : X \times Y \to Z$

$f(x,y) = z$

15:45