TI-Lecture-7-4-2020

7 April, 2020 13:47

Thm (Chernoff): Let $0 < p < 1$ & $0 < \alpha < 1$.

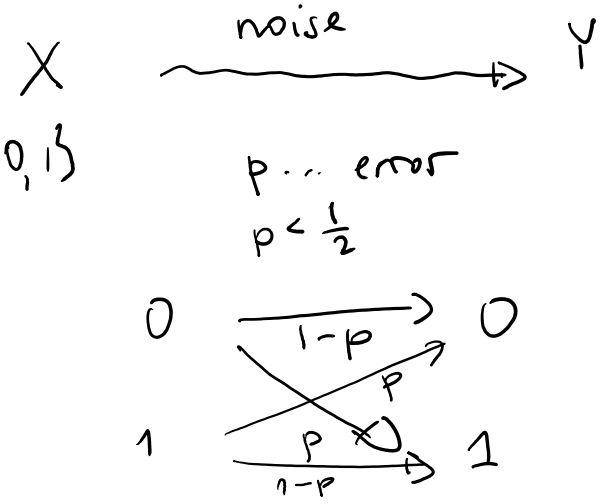
There exists $c_{p\alpha} > 0$ s.t. $\forall n \geq 1$ and

sequence $X_1, \dots X_n$ of indep. r.vars's

where $X_i = \begin{cases} 0 & 1-p \\ 1 & p \end{cases}$

$$Pr\left[\left| \sum X_i - pn \right| \geq \alpha n \right] \leq 2 \cdot e^{-c_{p\alpha} n}$$

Lemma: $\forall n, r \geq 1 \quad \frac{2^{H(r/n)n}}{n} \leq Vol(n,r) \leq 2^{H(\frac{r}{n})n}$.



binary symmetric channel

$E(X_1, X_2, \dots X_k) \xrightarrow{enc} M_1, \dots M_n \rightsquigarrow M_1' \dots M_n' \xrightarrow{dec} X_1 \dots X_k$

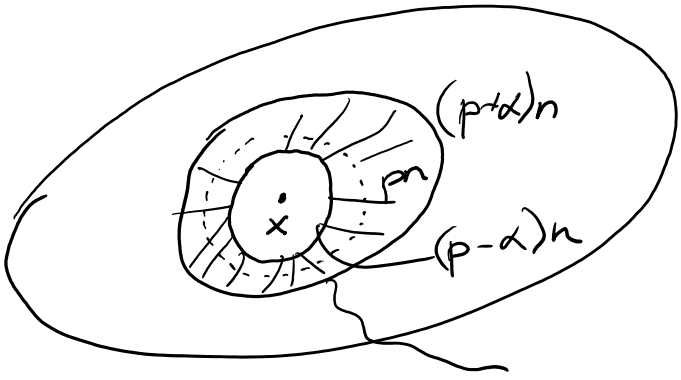
k ... minimize n rate $R = \frac{k}{n}$

Thm: (Shannon) Binary symmetric channel with error prob. $p < \frac{1}{2}$. Let $0 < R < 1 - H(p)$. $\forall \varepsilon > 0$ $\forall n$ large enough there exists $C \subseteq \{0,1\}^n$ $|C| = 2^{Rn}$ & the prob. of incorrect decoding of transmitted codeword is $\leq \varepsilon$.

$C_1, C_2, \ldots C_n \ldots$ prob. of incorrect decody $\varepsilon_n = 2^{-\Theta(n)}$.

$n \rightsquigarrow r$

pn errors in expectation



$\mathrm{Vol}(n, r)$ = volume of a ball of radius r

$\mathrm{Vol}(n, r) \leq 2^{H(\frac{r}{n})n}$

$\mathrm{Vol}(n, (p+\alpha)n) \leq 2^{H(p+\alpha)n}$

Pf: fix n, p given, $H(p+\alpha) + R < 1$ ✍

p given

$H(p+\alpha)+R < 1$

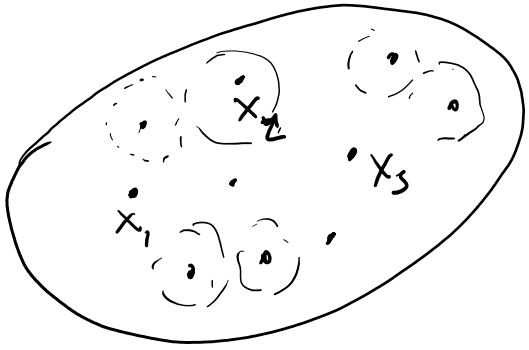
pick α s.t.

$R < 1 - H(p)$

$R < 1 - H(p+\alpha)$

by continuity of H

C_n we will construct it at random



$\{0,1\}^n$

$|C_n| = 2^{Rn}$

1) pick C_n at random
2) pick $x \in C_n$ at random
3) send $x \overset{\text{noisy}}{\rightsquigarrow} y$
4) decode $y \longrightarrow x'$ closest elt' in C_n.

$\Pr[x' \neq x] \leq 2^{-cn}$.

$2^{Rn} - 1$

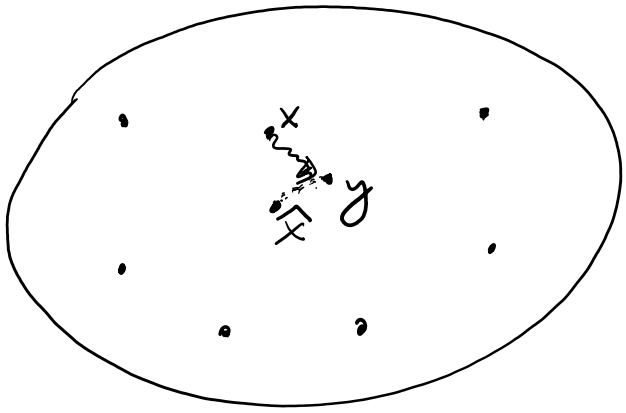
$R = \frac{k}{n}$

$R' = \left(R - \frac{1}{n}\right)$

$|C'| = 2^{R'n} = 2^{Rn-1}$

$\Pr[\text{incorrect dec.}] \leq 2 \cdot 2^{-cn}$.

decoding



w.h.p. noise in $y \leq (p+\alpha)n$

$\geq 1 - 2e^{-c_p \alpha^2 n}$

decode incorrectly only if $\exists \hat{x} \in C_n$ s.t.

$$\Delta_{Ham}(\hat{x}, y) \leq \Delta_{Ham}(x, y) \leq (p+\alpha)n .$$

pick x

$x \to y$ $\quad y$ independent of $C_n \setminus \{x\}$.

$$Pr[\exists \hat{x} \in C_n ; \Delta_{Ham}(\hat{x}, y) \leq (p+\alpha)n]$$

$$\leq \underbrace{\left(2^{Rn}-1\right)}_{|C_n \setminus \{x\}| \leq 1} \cdot \frac{Vol(n(p+\alpha)n)}{2^n}$$

$$\leq 2^{Rn} \cdot \frac{2^{H(p+\alpha)n}}{2^n} = \frac{2^{(R+H(p+\alpha))n}}{2^n}$$

$R + H(p+\alpha) < 1$

$\delta = 1 - R - H(p+\alpha) > 0$

$$= 2^{-\delta n}$$

→ Prob of incorrect decoding when C, $x \in C$, noisy y is picked at random $\leq 2^{-\delta n} + 2e^{-c_p \alpha^2 n}$

$\leq 2^{-\Theta(n)}$. $(*)$

$\exists C_n$ s.t. Pr of incorrect decoding for $x \in C$ and noise pick at random $\leq (*)$

by Markov $\exists C_n' \subseteq C_n$

$\exists C_n' \subseteq C_n \quad |C_n'| \geq \frac{|C_n|}{2} \geq 2^{Rn-1} \approx 2^{Rn}$

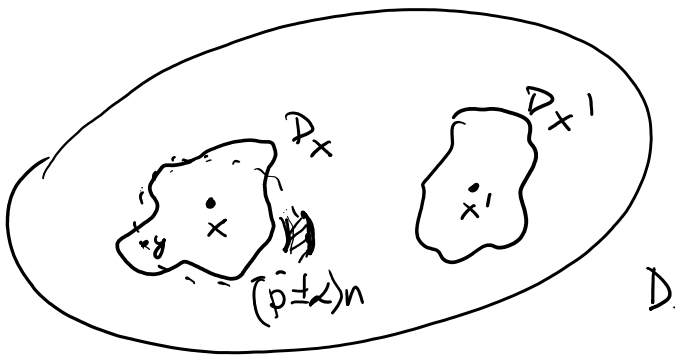
$\forall x \in C_n' \quad$ Pr [decoding incorrect when x sent] $\leq 2 \cdot (*)$

- error correcting codes

Thm (Shannon): Let $0 < p < \frac{1}{2}$, $R > 1 - H(p)$ $\delta \in (0,1)$. $\forall n$ large enough $\forall C_n \subseteq \{0,1\}^n$ $|C_n| \geq 2^{Rn}$ then the average $\frac{x \in C_n}{\text{probability}}$ of incorrect decoding $\geq 1 - \delta$.

Pf:

Pf:



$\{0,1\}^n$

$D_x = \{y \in \{0,1\}^n, y \text{ is decoded into } x\}$

$\bigcup_{x \in C} D_x \qquad \sum_{x \in C} |D_x| \leq 2^n \qquad D_x$'s are disjoint.

Probab. of decoding correctly?

$2^{-(p-\alpha)n}$

pick $\alpha > 0$ s.t. $R > 1 - H(p) + \alpha \cdot \log \frac{1-p}{p}$

$0 > 1 - R - H(p) + \alpha \cdot \log \frac{1-p}{p}$

$x \in C$ e ... error vector at random

$y = x + e$ (coordinate wise over GF_2)

$\Pr_{x,e}[x+e \text{ is decoded correctly}]$

$\leq \Pr_{x,e}[x+e \text{ is decoded correctly} \wedge |e| \in [(p-\alpha)n, (p+\alpha)n]]$

$+ \Pr_{x,e}[x+e \text{ — " — } \wedge |e| \notin [(p-\alpha)n, (p+\alpha)n]]$

$\leq 2e^{-c_{\alpha,p} n}$

(*)

(*)

$$(*) = \Pr_{X,E}\left[X+E \in D_X \;\&\; |E| \in \left[(p-\alpha)n, (p+\alpha)n\right]\right]$$

$$= \sum_{\substack{x \in C \\ e \in \{e \in \{0,1\}^n,\ |e| \in [(p-\alpha)n, (p+\alpha)n]\} \\ x+e \in D_x}} \Pr[X=x \;\&\; E=e] = (**)$$

$$|e| \in \left[(p-\alpha)n, (p+\alpha)n\right] \Pr[E=e] \le (1-p)^{n-(p-\alpha)n} p^{(p-\alpha)n}$$

$e = 0101110010101110 = p^8 \cdot (1-p)^6$ (ex c)

$$(**) \le \sum \Pr[E=e] \le (1-p)^{n-(p-\alpha)n} \cdot p^{(p-\alpha)n}$$

$$\Pr[X=x \;\&\; E=e] = \Pr[X=x] \cdot \Pr[E=e]$$

$$\Pr[X=x] = 2^{-Rn} \le p^{(p-\alpha)n} \cdot (1-p)^{n-(p-\alpha)n}$$

$$(**) = \sum_{(x,e)\ \ldots\ x+e \in D_x} \ldots \le \left(\sum |D_x|\right) \cdot 2^{-Rn} \cdot p^{(p-\alpha)n} \cdot (1-p)^{n-(p-\alpha)n}$$

$$\le 2^n$$

$$\le 2^n \cdot 2^{-Rn} \cdot 2^{-H(p)n} \cdot \left(\frac{1-p}{p}\right)^{\alpha n} \le 2^{-cn}$$

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

$$p^{pn}(1-p)^{n-pn} \cdot p^{-\alpha n}(1-p)^{\alpha n}$$

$n \cdot \underbrace{\left(1 - K - \pi(p) + \alpha\sqrt{p}\right)}_{<0}$,

$\underbrace{p^{pn}(1-p)^{n-pn}}_{2^{-H(p)n}} \cdot \underbrace{p^{-\alpha n}\cdot(1-p)^{\alpha n}}_{\left(\frac{1-p}{p}\right)^{\alpha n}}$

$\Rightarrow \quad Pr_{x,e}\left[\, x+e \text{ decoded correctly} \,\right] \leq 2 \cdot e^{-c_p \alpha^2 n} + 2^{-cn}$