April 23, 2019

REMINDERS

(•) Video due in 1 week (11:59pm next Tue)
(•) 3rd proof reading schedule starts next Tue
(•) Guest lecture ~~next Tue~~ on THURSDAY: Coding for cloud (Sai)

RECAP:

(•) Can achieve BSC_p capacity (rate $= 1 - H(p) - \varepsilon$) with:
- (#) poly time encoding
- (#) poly time decoding

Can make this $O(N)$ using expander codes.

- (#) $2^{-\Omega(N)}$ decoding error prob.
- (#) $N \geq 2^{\Omega(1/\varepsilon)}$

Question: Can we get above BUT with $N = \text{poly}(\frac{1}{\varepsilon})$?

TODAY (Proof reader: Vihari)

(•) Make a start towards answering above Q. (enc/dec time $O(N \log N)$)

(•) Polar codes (Arikan '08)
- ↳ Reduction to (linear) compression
- ↳ Information theory primer

Notation (+ Main Result)

Ex 11.1 (Thm 11.1.2) get rid of this using code concat

BSC_p: i/p: $\overline{X} = (X_1, \ldots, X_n) \in \{0,1\}^n$

o/p: $\overline{Y} = (Y_1, \ldots, Y_n) \in \{0,1\}^n$

$\overline{Y} = \overline{X} + \overline{Z}$, $\overline{Z} = (Z_1, \ldots, Z_n) \in \text{Bern}(p)^n$

k, n depend on ε

Want to be true for all large enough n

Want to be exp(-n)

THM: $\forall\ 0 \leq p < \frac{1}{2}$, $\exists$ a poly func $n_0(\cdot)$ s.t. $\forall\ \varepsilon > 0$

$\exists\ k, n$, $E: \mathbb{F}_2^k \to \mathbb{F}_2^n$; $D: \mathbb{F}_2^n \to \mathbb{F}_2^k$ s.t.

1. Length & rate: $k \geq (1 - H(p) - \varepsilon)\, n$; $\frac{1}{\varepsilon} \leq n \leq n_0(\frac{1}{\varepsilon})$
2. Runtimes: E & D run in $O(n \log n)$
3. Failure prob: $\forall\ \overline{m} \in \mathbb{F}_2^k$; $\Pr_{\overline{Z} \in \text{Bern}(p)^n}[D(E(\overline{m}) + \overline{Z}) \neq \overline{m}] \leq \varepsilon$.

Reduction to linear compression

"Thm": If $\exists$ an efficient linear compression $\bar{Z} \in \mathrm{Bern}(p)^n$

$\implies \exists$ ______ coding scheme for BSC_p

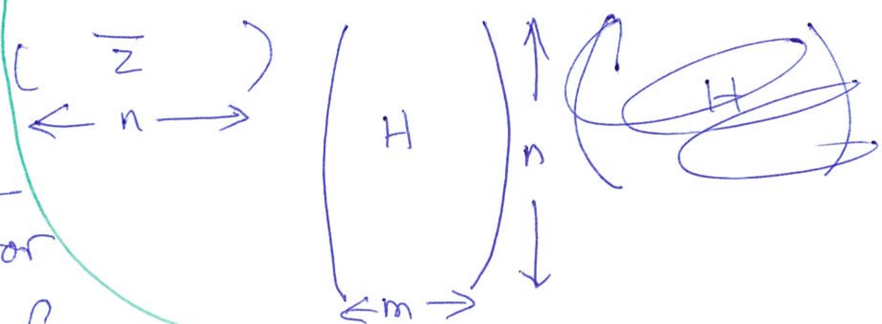
Linear compression scheme: $(n \geq m)$ $H \in \mathbb{F}_2^{n \times m}$; $D : \mathbb{F}_2^{m} \to \mathbb{F}_2^{n}$

rate: $\frac{m}{n}$

(H, D) is a τ-error linear compression scheme:

(•) H has full rank. (compression: $\bar{Z} \cdot H$)

(•) $\Pr_{\bar{Z} \sim \mathrm{Bern}(p)^n} \left[D(\bar{Z} \cdot H) \neq \bar{Z} \right] \leq \tau.$



Prop: (H, D) be a τ-error linear compression for $\mathrm{Bern}(p)^n$

$\in \mathbb{F}_2^{n \times m}$

Let $G \in \mathbb{F}_2^{k \times n}$, $G^* \in \mathbb{F}_2^{n \times k}$ be full rank matrices s.t.

These $\exists$ by standard LA arguments

(i) $G \cdot H = 0$ (ii) $G \cdot G^* = I_k$

gen matrix

transpose of parity check matrix

H^T is the parity check matrix $\implies k + m = n \implies R = 1 - \frac{m}{n}$

→ Let enc function $E : \mathbb{F}_2^k \to \mathbb{F}_2^n$ s.t. $E(\bar{x}) = \bar{x} \cdot G$

→ Let dec ______ $D' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ s.t.

$$D'(\bar{Y}) = (\bar{Y} - D(\bar{Y} \cdot H)) \cdot G^*$$

$\implies \forall \bar{m} \in \mathbb{F}_2^k$, $\Pr_{\bar{Z} \in \mathrm{Bern}(p)^n} \left(D'(E(\bar{m}) + \bar{Z}) \neq \bar{m} \right) \leq \tau.$

Enc complexity: mat · vect complexity for G

Dec complexity: ______ for H & G^*

$\Big\}$ $O(n^2)$ [for polar codes $O(n \log n)$]

(•) Linear compression $\mathrm{Bern}(p)^n \implies$ coding for BSC_p (Ex 6.11)

Pf of Prop: Assume $\bar{z}$ (error pattern) s.t. $D(\bar{z}\cdot H) = \bar{z}$

(argue D' works) Fix any $\bar{m} \in \mathbb{F}_2^k$

$$D'(E(\bar{m})+\bar{z}) = \Big(E(\bar{m})+\bar{z} - D\big((E(\bar{m})+\bar{z})\cdot H\big)\Big)\cdot G^*$$

Def of D' →

Def of E → $= \Big(\bar{m}\cdot G + \bar{z} - D\big((\bar{m}G+\bar{z})\cdot H\big)\Big)\cdot G^*$

from (i) → $= \big(\bar{m}\cdot G + \bar{z} - D(\bar{z}\cdot H)\big)\cdot G^*$

by (*) → $= (m\cdot G + \bar{z} - \bar{z})\cdot G^*$

by (ii) → $= \bar{m}\cdot G\cdot G^*$

$= \bar{m}$

$\vdots$

$= \bar{m}$

$\Rightarrow$ Dec error prob $\leq \Pr_{\bar{z}\in \mathrm{Bern}(p)^n} (D(\bar{z}\cdot H) \neq \bar{z}) \leq \tau$.

Modified Goal: Design an ε-error linear compression scheme for $\mathrm{Bern}(p)^n$ with rate $H(p)+\varepsilon$

Information theory background (App E)

r.v. Z with distribution $\mathcal{D}$ $\quad \mathrm{supp}(\mathcal{D}) = \{z \mid \underbrace{\Pr[Z=z]}_{\Pr(z)} \neq 0\}$

$= \mathrm{supp}(Z)$

$$H(Z) \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{z\sim\mathcal{D}} \log_2 \frac{1}{\Pr(z)} = \sum_{z\in \mathrm{supp}(Z)} \Pr(z) \log_2 \frac{1}{\Pr(z)}$$

$(0\cdot \log_2 \frac{1}{0} = 0)$

$Z_0 = \begin{cases} 1 & \text{wp } p \\ 0 & \text{o/w} \end{cases}$ $\quad H(Z_0) = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{1-p} = H_2(p)$

Z' is uniform over $\{0,1\}^n$; $H(Z') = n$

Z'' ———— " $\{z_1, \ldots, z_N\}$: $H(Z'') = \log_2 N$

Prop 1: ~~Z is~~ $|\mathrm{supp}(Z)| = N \Rightarrow H(Z) \leq \log_2 N$

Prop 2: $H(Z) \geq 0$, $H(Z) = 0 \Leftrightarrow Z$ is def. $\equiv |\mathrm{supp}(Z)| = 1$

Prop 3: $Z \sim \mathrm{Bern}(p)^n$, $H(Z) = H_2(p)\cdot n$

Joint + Conditional entropy

r.v.s ~~##~~ X & Y (co-related)

$$H(X,Y) = \sum_{x,y} \underbrace{Pr(x,y)}_{\substack{\shortparallel \\ Pr[X=x,\, Y=y]}} \cdot \log_2 \frac{1}{Pr(x,y)}$$

X & Y are indep $\quad Pr(x,y) = Pr(x) \cdot Pr(y)$

$$\begin{aligned}
H(X,Y) &= \sum_{x,y} Pr(x,y) \log_2 \frac{1}{Pr(x) \cdot Pr(y)} \\
&= \sum_{x,y} Pr(x,y) \log_2 \frac{1}{Pr(x)} + \sum_{x,y} Pr(x,y) \log_2 \frac{1}{Pr(y)} \\
&= \sum_{x} Pr(x) \log_2 \frac{1}{Pr(x)} + \sum_{y} Pr(y) \log_2 \frac{1}{Pr(y)} \\
&= H(X) + H(Y)
\end{aligned}$$

Let $Z = (Z_1, \dots, Z_n)$ s.t. all Z_i are indep $(\in \text{Bern}(p))$

$$H(Z) = \sum_{i=1}^{n} H(Z_i) = n \cdot H_2(p) \Rightarrow (\text{Prop } 3)$$

In general $\quad pr(y|x) = \dfrac{Pr(x,y)}{Pr(x)} \Rightarrow Pr(x,y) = pr(y|x)\, Pr(x)$

$$\begin{aligned}
\Rightarrow H(X,Y) &= \sum_{x,y} Pr(x,y) \log_2 \frac{1}{Pr(y|x)\, Pr(x)} \\
&= \sum_{x,y} Pr(x,y) \log_2 \frac{1}{Pr(x)} + \sum_{x,y} Pr(y|x) Pr(x) \log_2 \frac{1}{Pr(y|x)} \\
&= \sum_{x} Pr(x) \log_2 \frac{1}{Pr(x)} + \sum_{x} Pr(x) \sum_{y} Pr(y|x) \log_2 \frac{1}{Pr(y|x)} \\
&= H(X) + \sum_{x} Pr(x)\, H(Y | X=x) \\
&= H(X) + \underbrace{\mathop{\mathbb{E}}_{x} H(Y | X=x)}_{\stackrel{\text{def}}{=} H(Y|X)}
\end{aligned}$$

Def: $\quad H(Y|X) = \mathop{\mathbb{E}}_{x} H(Y|X=x)$

Chain rule: $\quad H(X,Y) = H(X) + H(Y|X)$

$$H(Z_1, \ldots, Z_n) = H(Z_1) + H(Z_2 \mid Z_1) + H(Z_3 \mid Z_1, Z_2) + \cdots + H(Z_n \mid Z_1, Z_2, \ldots, Z_n)$$

X & Y are indep

$$H(X, Y) = H(X) + H(Y)$$

$$\Rightarrow \quad H(Y \mid X) = H(Y)$$