ITCS: CS 229r — 2/26/2019

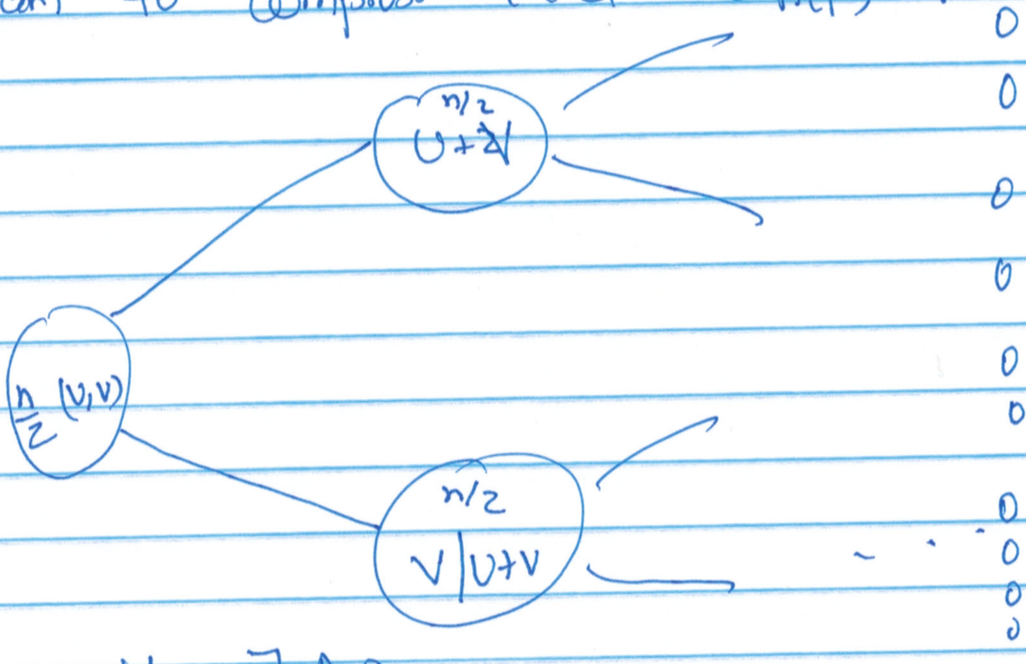
LECTURE 9

TODAY:

POLAR CODING (contd.)
- DECODING
- TOWARDS ANALYSIS (of Entropy Theorem)
  - MARTINGALES
  - LOCAL VS. GLOBAL POLARIZATION

Review of Last lecture

(1) Want to compress i.i.d Bern(p) variable.



(2) Theorem: $\forall p, c \; \exists A, B$ polys s.t.

② Key Theorem (to be proved):

$\forall p, c<\alpha, \exists \beta<1$ s.t. $\forall t$

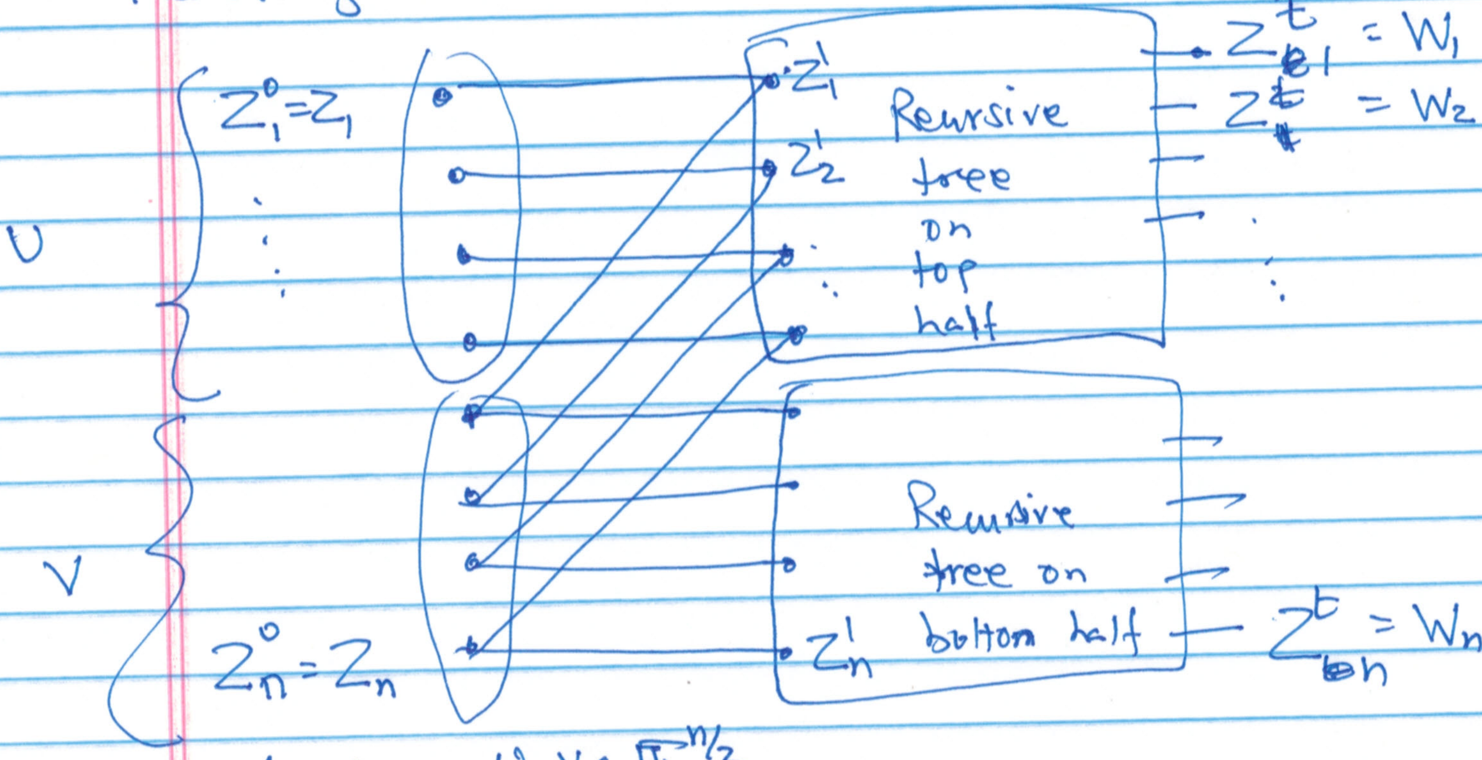
$$\Pr_{j\in[2^t]}\left[H(W_j \mid W_{<j}) \in (c^{-t}, 1-c^{-t})\right] \le O(\beta^t)$$

③ How to decode?

$S \triangleq \{j \mid H(W^j \mid W_{<j}) \ge c^{-t}\}$.

DECODING

(i) Redrawing the "tree



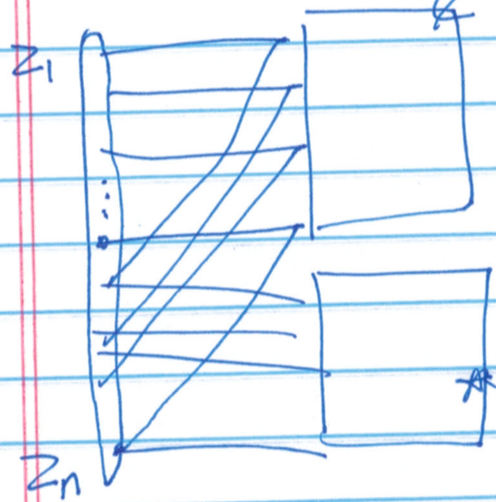
$z=(U,V)$ $\quad U,V\in \mathbb{F}_2^{n/2}$

$$W = P_n(U,V) = \left(P_{n/2}(U+V), P_{\frac{n}{2}}(V)\right)$$

Output W_S.

Decoding Idea

Decode top first (recursively)

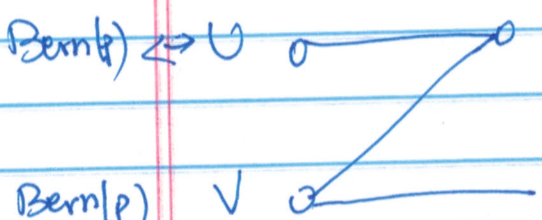


Decode bottom next

. top decoding : "obvious".

- bottom? : Need to exploit knowledge of top decoding!
(Else impossible!)
why?

- how? can compute revised "bias" of bits.



$$\Pr[V=1 \mid U+V=1] = \frac{1}{2}$$

$$\Pr[V=1 \mid U+V=0] \approx O(p^2) \quad [\text{as } p \to$$

$$= \frac{p^2}{p^2 + (1-p)^2}$$

- But now bits not identical!

$[\Pr[Z_{\frac{n}{2}+1} = 1] = 1/2,\ \Pr[Z_{n/2+2} = 1] = p^2$ etc. $]$.

[illegible]

DECODE $(W; (p_1, \ldots, p_n))$ $\quad W \in \{0,1,?\}^n ; 0 \le p_i \le 1$

- $\hat{U}+\hat{V} = \text{Decode}\left(W[1..\frac{n}{2}]; q_1 \ldots q_{\frac{n}{2}}\right)$

$$q_i \triangleq p_i\left(1 - p_{\frac{n}{2}+i}\right) + p_{\frac{n}{2}+i}\left(1-p_i\right)$$

- $\hat{V} = \text{Decode}\left(W[\frac{n}{2}+1..n]; r_1 \ldots r_{\frac{n}{2}}\right)$

$$r_i = \frac{p_{\frac{n}{2}+i}\left(1-p_i\right)}{q_i} \quad \text{if } (\hat{U}+\hat{V})_i = 1$$

$$= \frac{p_i\, p_{\frac{n}{2}+i}}{1-q_i} \quad \text{if } (U+V)_i = 0$$

- Output $(\hat{U}, \hat{V})$.

Base Case?

Decode $(W; p_1)$ $\quad n=1$

if $W_1 = 0/1$ output W_1

else $(W_1 = ?)$ output 1 if $p_1 \ge 1/2$

0 o.w.

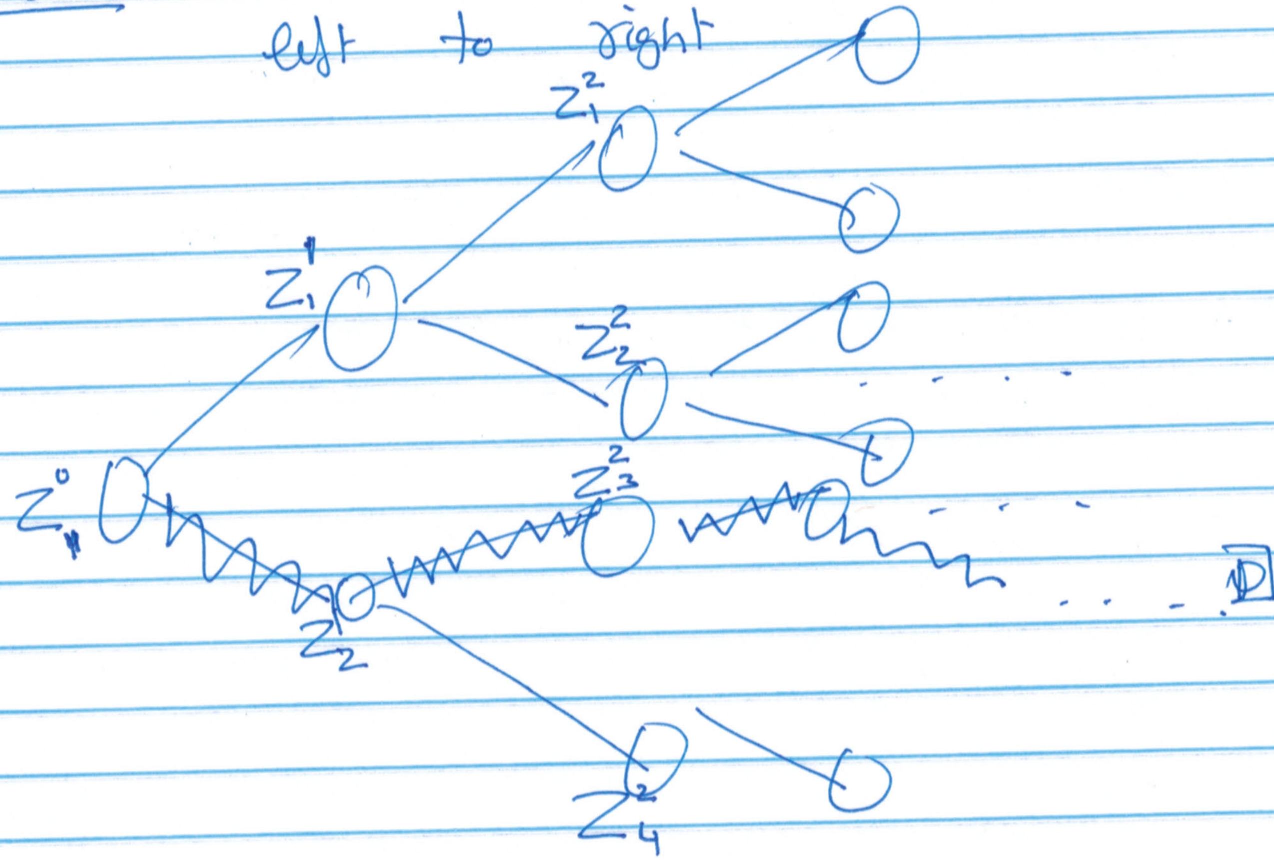
Key Analysis Ingredient:

- Biases are correct conditioned on things above, as we move left to right.

$\boxtimes$

Proof of Polarization Theorem

"Perspective: take random walk on tree from left to right



- follow entropy $H(Z_j^i \mid Z_{<j}^i) \triangleq X_i$

- Theorem (to be proved)

$$\Pr_{\text{walk}}\left[X_i \in (c^{-t}, 1-c^{-t})\right] \le O(\beta^t)$$

Fact: $\forall \alpha$ $\mathbb{E}[X_i \mid X_0 \ldots X_{i-1} = \alpha] = \alpha$ "Martingale"
($\Leftarrow$ $(u,v) \to (u+v, v)$ is invertible).

Our martingale is "bounded": $X_i \in [0,1]$ $\forall i$.

What we see (almost imm.)

Local Polarization:

① $\forall \tau > 0$ $\exists \sigma > 0$ s.t. [Variance in middle]

$$\mathrm{Var}(X_i \mid X_1 \ldots X_{i-1}) \geq \sigma \quad \text{if} \quad X_{i-1} \in (\tau, 1-\tau).$$

② $\forall c < \infty$ $\exists \tau > 0$ $\exists \theta > 0$ s.t. $\forall i$ [Suction at ends].

$$\Pr\left[X_i < \frac{X_{i-1}}{c}\right] \geq \theta \quad \text{if} \quad X_i \leq \tau$$

[similarly for $\bar{X}_i = 1 - X_i$].

Key Lemma: Local Polarization $\Rightarrow$ Strong Polarization (condition of Theorem).

Lemma : Our Martingale is Locally Polarizing

Proof Idea: Pretend it's all prob. (not conditional)

① if $U, V \sim \mathrm{Bern}(p)$

$\mathrm{bias}(U+V) = 2p(1-p) > p \Rightarrow$ Variance.

2 (Suction at high end)

$p = \frac{1}{2} - \delta \qquad \delta \to 0$

$\Rightarrow H(p) = 1 - \delta^2$

& $p' = 2p(1-p) = \frac{1}{2} - \delta^2$

$\Rightarrow H(p') = 1 - \delta^4$

$\cdot\left(\bar{X}_i = \delta^2 \Rightarrow \bar{X}_{i+1} = \delta^4\right.$ more than good enough)

Suction at low end:

$p = \delta \Rightarrow H(p) \approx \delta \cdot \log 1/\delta$

$p' = 2p(1-p) \approx 2p$

$H(p') \approx 2\delta \log \frac{1}{2\delta}$

$\Rightarrow 2H(p) - H(p') \approx 2\delta \log \frac{1}{\delta} - 2\delta \log \frac{1}{2\delta}$

$\approx 2\delta \approx \frac{H(p)}{\log H(p)} = o(h(p))$

Proof of Key Lemma

Part 1

$$\phi_t \triangleq \min\{\sqrt{X_t}, \sqrt{1-X_t}\}$$

then $\exists \beta' < 1$ s.t. $\forall \phi_t$ $\mathbb{E}[\phi_{t+1}] \le \beta' \cdot \phi_t$

- Proof of claim: $\xrightarrow{\text{Calculation}}$

$$\Rightarrow \mathbb{E}[\phi_t] \le (\beta')^t \Rightarrow \Pr[\phi_t \ge (\beta')^{t/2}] \le (\beta')^{t/2}$$

$$\Rightarrow \Pr[X_t \in \underbrace{((\beta')^{t/2}, 1-(\beta')^{t/2})}_{\text{not good enough}}] \le \underbrace{(\beta')^{t/2}}_{\text{good!}}$$

2. if $X_t \le (\beta')^{t/2}$ then $X_{2t} < c^{-2t}$ whp.

roughly: ~~While~~ $\exists \tau_0$ s.t. with $X_{t'} < \tau_0$ $\Pr\left[X_{t'+1} < \frac{X_{t'}}{c^{10}}\right] \ge \frac{1}{2}$

$$\Pr[\exists t' \in [t, 2t] \text{ s.t. } X_{t'} > \tau_0] \le \frac{(\beta')^{t/2}}{\tau_0} \quad [\text{Doob's Ineq.}]$$

if $X_{t'} < \tau_0$ $\forall t'$ .. then falls w.p. $\frac{1}{2}$ by c^{10}; doubles w.p. $\frac{1}{2}$ [...]