LECTURE 17

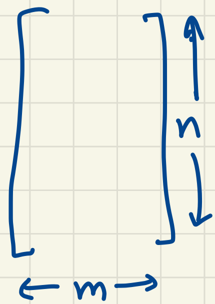
TODAY

POLAR CODES (contd.)

- Polarization Theorem (statement)
- Analysis of Code (mod Theorem)
- Encoding + Decoding

Review from last time:

① **Needed: Linear Compressor**

$H =$ 

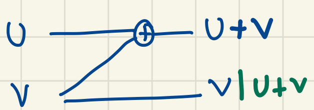
; ① $m \le (H(p)+\epsilon)\,n$

② Decomp. $D(zH) = z$ whp

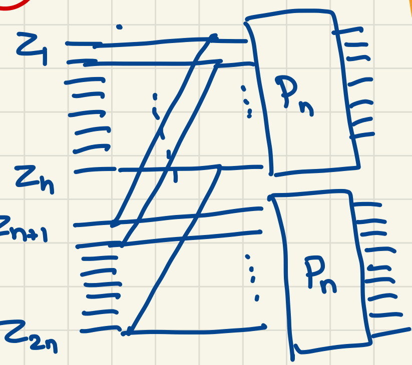
③ run time poly$(1/\epsilon)$.

② **Polarization Method:**

2a Single Step

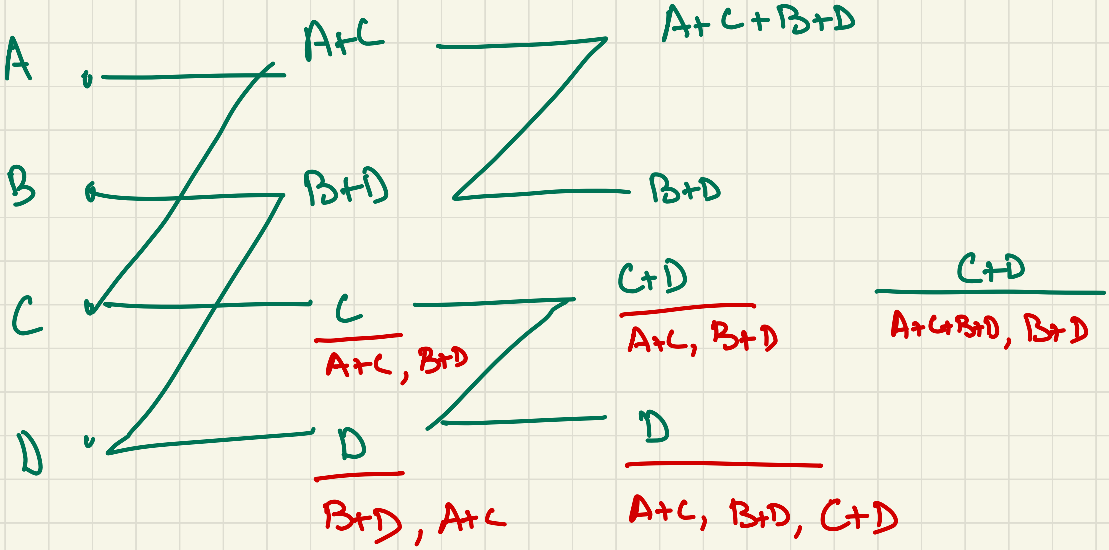


2b n-Step



$\bar{z} = (\bar{u}, \bar{v}) \Rightarrow$

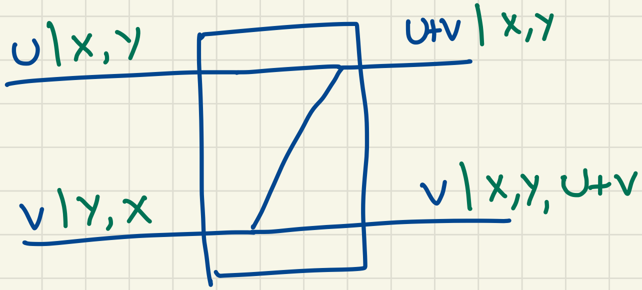
$P_{2n}(\bar{z}) = \left(P_n(\bar{u}+\bar{v}),\ P_n(\bar{v})\right)$



A
B
C
D
A+C
B+D
C
A+C, B+D
D
B+D, A+C
A+C+B+D
B+D
C+D
A+C, B+D
D
A+C, B+D, C+D
C+D
A+C+B+D, B+D

Analysis: (will analyze)

locally



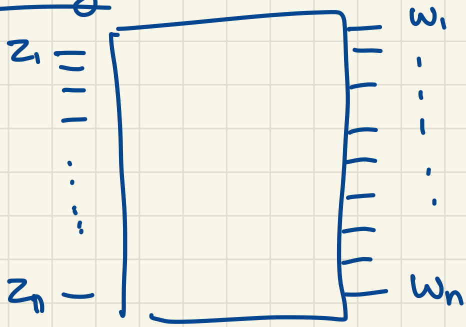
$(U, X), (V, Y)$ iid

$H(U|X) = H(U|X,Y)$

$H(V|Y) = H(V|X,Y)$

(so everything gets conditioned on X, Y).

globally



$H(W_i | W_{<i})$

Defn: (ϵ, τ, δ) - polarization

$H(W_i|W_{<i}) \in [0, 1]$

$\overset{?}{\in} (\tau, 1-\delta)$

$$\Pr_{i \in [n]}\left[H(W_i | W_{<i}) \in (\tau, 1-\delta) \right] \leq \epsilon$$

Lemma: (ϵ, τ, δ) - polarization $\Rightarrow$ for $H = P|_S$

$$m = |S| \leq \left(H(p) + (\epsilon + 2\delta) \right) \cdot n$$

$$\exists D \quad \Pr\left[D(HZ) \neq Z \right] \leq n \cdot \tau$$

Thm: $\forall c \ \exists \alpha > 0$ s.t. have $(n^{-\alpha}, n^{-c}, n^{-c})$ - polarization

implications: $\epsilon = n^{-\alpha} \Rightarrow n = \left(\frac{1}{\epsilon}\right)^{1/\alpha} = \text{poly}(1/\epsilon)$

τ, δ very small.

Prove Thm
Prove Lemma
Encode, Decode

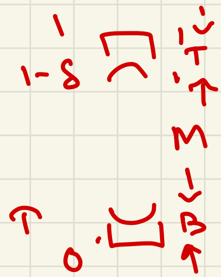
TODO LIST

Proof of Lemma:

$$T_{op} \triangleq \{ i \mid H(W_i \mid W_{<i}) \geq 1-\delta \}$$

$$B_{ottom} \triangleq \{ i \mid H(W_i \mid W_{<i}) \leq \tau \}$$

$$M \triangleq \{ i \mid H(W_i \mid W_{<i}) \in (\tau, 1-\delta) \}$$



1. $|T| + |B| + |M| = n$
2. $|M| \leq \epsilon n$
3. $|T| \leq \dfrac{H(p)\cdot n}{1-\delta} \leq H(p)\cdot n + 2\delta n$ (Chain Rule+).

$\delta \leq \frac{1}{4}$

$$H(w_1 \ldots w_n) = n \cdot H(p) = \sum_i H(w_i \mid w_{<i}) \geq \sum_{i \in T} H(w_i \mid w_{<i}) \geq (1-\delta)|T|$$

$$S \triangleq T \cup M$$

- $|S| \leq (H(p) + \epsilon + \delta)\, n$
- $H(W_{\bar{S}} \mid W_S) \leq n \cdot \tau$

$\Rightarrow \exists$ (ineff.) alg $\tilde{D}$ s.t. $\Pr[\tilde{D}(W_S) \neq W_{\bar{S}}] \leq n\tau$

* see exercise.

$H(W_i \mid W_{<i}) \leq \tau$ if i is erased

$W_1 \to$ is in $T \cup M$ $\Rightarrow$ it is known.

else $H(W_1 \mid \phi) < \tau$ $\Rightarrow$ we will guess W_1

$$\boxed{\begin{aligned} H(W_{\bar{S}} \mid W_S) &= \sum_{i \in \bar{S}} H(W_i \mid \underbrace{W_S, W_{<i,\bar{S}}}) \\ &\leq \sum_{i \in \bar{S}} H(W_i \mid W_{<i}) \\ &\leq \tau \cdot |\bar{S}| \leq \tau \cdot n \end{aligned}}$$

Exercise: Let X, Y be jointly distributed.

Prove $\exists$ predictor $P = P(y)$ s.t.

$$\Pr_{(X,Y)}\left[P(Y) \neq X \right] \leq H(X \mid Y)$$

———— x ————

Apply with $Y = W|_S$ & $X = W|_{\bar{S}}$

———— x ————

TBD:

1. Encoding + Decoding given S
2. Proof of Thm
3. Computing S

Exercise

Describe matrix P_n s.t.

$P_n(Z) = Z \cdot P_n$

Plan:

1. Today
2. Next lecture
3. Never; still OK; like being given generator of code ... still non-trivial to encode decode.

———— x ————

Base case

$$D(\hat{w}_i, P_1)$$

$$\hat{w}_1 \in \{0, 1, ?\}$$

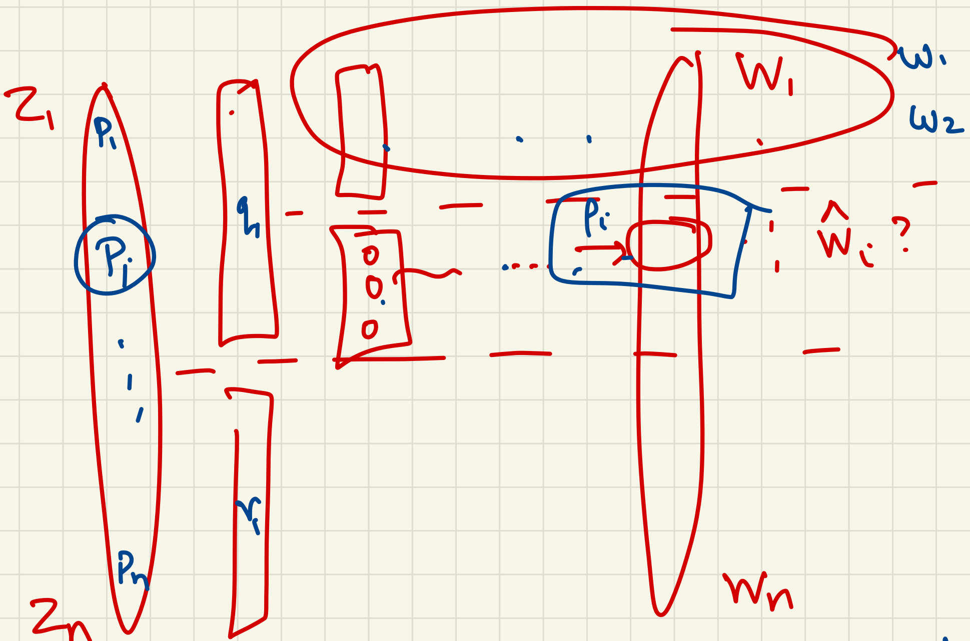
$\hat{w}_1 = 0$ output 0

$P_i = \underbrace{H(w_i \mid w_{<i})}_{= w_{<i}}$

$\hat{w}_1 = 1$ output 1

$\bar{w}_1 = ?$ if $\left.\begin{array}{l} P_1 < \frac{1}{2} \Rightarrow 0 \\ P_1 \geq \frac{1}{2} \Rightarrow 1 \end{array}\right\}$

$P_1 =$ ~~H~~ Bias of bit conditioned thing above



$D(\hat{W}_i ; P_i)$ $\sum_{i \notin S} H(W_i \mid W_{<i} = w_{<i})$

P_i = Bias of $W_i \mid W_{<i} = w_{<i}$

$\max(P_i, 1-P_i) \leq H(P_i)$

$\underline{H(W_i \mid W_{<i}) = ?}$

$H(\underline{\underline{W_i}} \mid W_{<i} = w_{<i})$ ← decoding alg.