Today
- Polar Codes II

CS5.318.1
Coding Theory
Lecture 22 (2022-11-16)
Instructor: Prahladh Harsha.

Recap Polar Codes from last lecture

(1) Linear Compression Scheme for $(Ber(p))^n$

$H : \{0,1\}^n \to \{0,1\}^m \qquad m \le (H(p)+\varepsilon)n$

Decompressor : D s.t

$$\Pr_{Z \sim (Ber(p))^n}\left[D(HZ) \neq Z\right] \le \varepsilon.$$

n, RT of D - poly$(1/\varepsilon)$

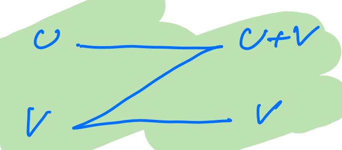
(2) P- invertible matrix. ; $W = PZ$

Defn: $\underbrace{|S_\tau| = \{i \in [n] \mid H(W_i \mid W_{<i}) \ge \tau\}}_{\text{unpredictable bits.}}$

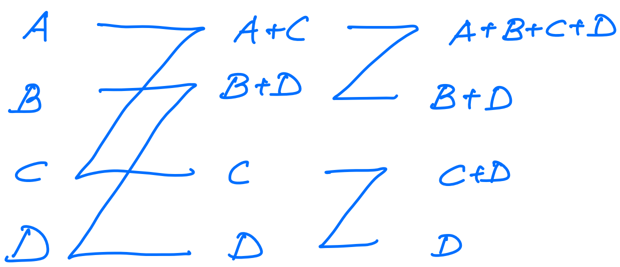
(ε, τ)- Polarizing matrix if $|S_\tau| \le (H(p)+\varepsilon)n$

(3) Arikan's construction:

$P_2 : \{0,1\}^2 \to \{0,1\}^2$



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



Defn: (ε, τ)-polarization if

$$\Pr_{i\in[n]}\left[H(W_i \mid W_{<i}) \in (\tau, 1-\tau)\right] \le \varepsilon.$$

Lemma: (ε, τ)-polarization $\Rightarrow$ Linear compression scheme w/ $m = |S| = (H(p)+\varepsilon+2\tau)n$ $(\tau \le 1/2)$

& Decompressor D s.t.

$$\Pr\left[D(HZ) \ne Z\right] \le \tau \cdot n.$$

Theorem: $\forall c\ \exists \alpha$ Arikan's matrix satisfies $\left(\frac{1}{n^\alpha}, \frac{1}{n^c}\right)$-polarization

Consequence of Lemma + Thm: we obtain $n = \mathrm{poly}\left(\frac{1}{\varepsilon}\right)$.

$$\varepsilon = \frac{1}{n^\alpha} \qquad n = \left(\frac{1}{\varepsilon}\right)^{1/\alpha} = \mathrm{poly}\left(\frac{1}{\varepsilon}\right),$$

$\rightarrow$ Decompresser

$\rightarrow$ Find S

} both can be done in $\mathrm{poly}\left(\frac{1}{\varepsilon}\right)$-time (but not in today's lecture).

Proof of Lemma:

$$H = \{ i \in [n] \mid H(W_i \mid W_{<i}) \geq 1 - \tau \}$$
$$L = \{ i \in [n] \mid H(W_i \mid W_{<i}) \leq \tau \}$$
$$M = \{ i \in [n] \mid H(W_i \mid W_{<i}) \in (\tau, 1-\tau) \}$$

(ε, τ)-polarization $\Rightarrow$ $|M| \leq \varepsilon n$

① $|H| + |L| + |M| = n$

② $|H|(1-\tau) \leq H(p) n \Rightarrow |H| \leq \dfrac{H(p) n}{1-\tau}$

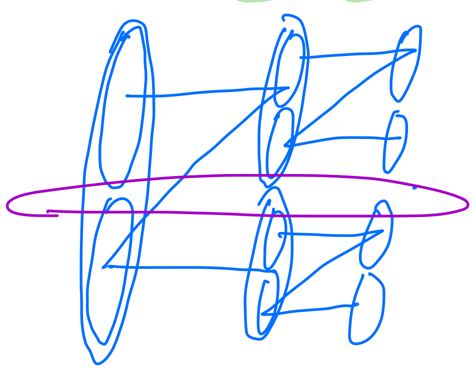
$$\leq H(p)(1+2\tau) n$$
$$\leq (H(p) + 2\tau) n.$$

$$S \triangleq H \cup M$$
$$|S| \leq (H(p) + 2\tau + \varepsilon) n$$

Compressor $\quad Z \mapsto (PZ)|_S$ $\quad \boxtimes$.

Theorem: $\forall c\ \exists \alpha$ Arikan's matrix satisfies $\left(\frac{1}{n^\alpha}, \frac{1}{n^c}\right)$-polarization

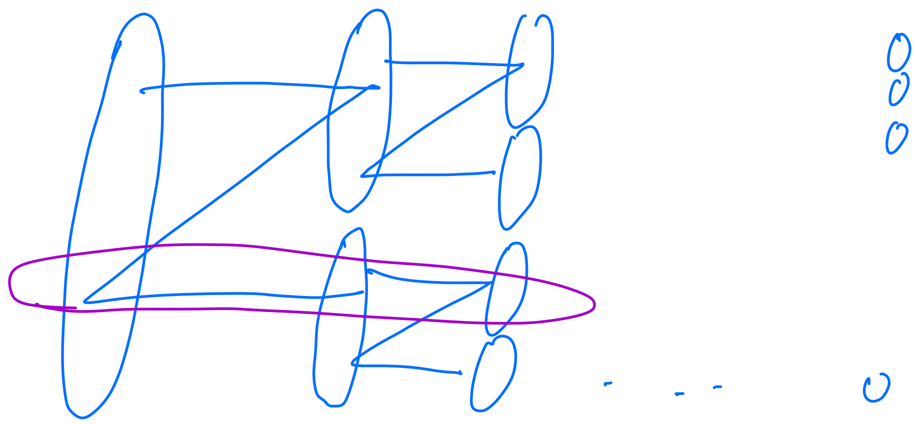
i



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

Want to prove this.

$$\Pr_{i \in [n]} \left[H(W_i \mid W_{<i}) \in \left(\frac{1}{n^{100}}, 1 - \frac{1}{n^{100}}\right) \right] \leq \frac{1}{n^{0.001}}$$



$Z^{(0)} = Z$ $\quad Z^{(1)}$ $\quad Z^{(2)}$ $\quad \dots \quad$ $Z^{(t)} = W$

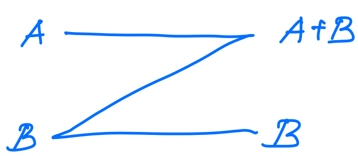
$t = \log n$

Pick $i \in_R [n]$, $\quad X_j \triangleq H(Z_i^{(j)} \mid Z_{<i}^{(j)})$

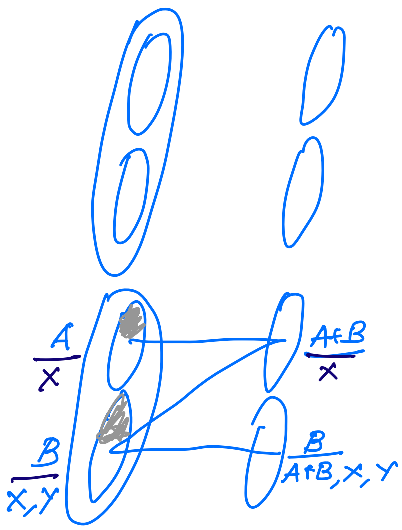
$X_0, X_1, \dots X_t$ – Arikan's martingale.

<u>Def:</u> $X_0, X_1, \dots X_t$ – martingale in M
if $\forall j \in \{1, \dots t\}$, $\forall a_0, \dots a_{j-1} \in M$
$$\mathbb{E}[X_j \mid X_0 = a_0, X_1 = a_1, \dots X_{j-1} = a_{j-1}] = a_{j-1}$$

In our setting
$$X_0 = H(p)$$



$$H(A,B) = H(A+B, B)$$
$$H(A) + H(B|A) = H(A+B) + H(B|A+B)$$
$$H(A) + H(B) = H(A+B) + H(B|A+B)$$



Initial sum

$$H(A|X) + H(B|X,Y)$$
$$= H(A|X) + H(B|Y)$$

Ending Sum

$$H(A+B|X) + H(B|A+B, X, Y)$$

$$H(A,B|X,Y) = H(A+B, B|X,Y)$$

RHS: $H(A+B|X,Y) + H(B|A+B, X, Y)$

LHS $= H(A|X,Y) + H(B|A, X, Y)$

$= H(A|X) + H(B|Y)$

Want to prove:

Strong Polarization ($t = \log n$)

$$\Pr\left[X_t \in (2^{-100t}, 1 - 2^{-100t})\right] \leq \frac{1}{2^{0.001t}}$$

Examples of martingales in $[0,1]$

(1) $X_0 = \frac{1}{2}$; $X_t = \begin{cases} X_{t-1} + \frac{1}{2^{t+1}} & \text{w/p } \frac{1}{2} \\ X_{t-1} - \frac{1}{2^{t+1}} & \text{w/ } \frac{1}{2} \end{cases}$

(2) $X_0 = p$ $\quad X_{t+1} = \begin{cases} X_t + \frac{1}{2}\min\{X_t, 1-X_t\} & \text{w/ } \frac{1}{2} \\ X_t - \frac{1}{2}\min\{X_t, 1-X_t\} & \text{w/ } \frac{1}{2}. \end{cases}$

(3) $X_0 = \alpha$ $\quad X_{t+1} = \begin{cases} X_t^2 & \text{w/ } 1/2 \\ 2X_t - X_t^2 & \text{w/ } 1/2. \end{cases}$

Local Polarization: $X_0, X_1 \ldots X_t$ · martingale satisfies local polarization.

(i) Variance in the Middle:

$\forall \tau, \exists \sigma, \forall t$

$$\mathrm{Var}(X_t \mid X_{t-1} \in (\tau, 1-\tau)) \geq \sigma^2$$

(ii) Suction at the ends.

$\forall c > 1, \exists \tau, \forall t$

0-end : $\Pr\left[X_t < \frac{X_{t-1}}{c} \,\middle|\, X_{t-1} < \tau\right] \geq 1/2.$

1-end : $\Pr\left[1 - X_t < \frac{1 - X_{t-1}}{c} \,\middle|\, 1 - X_{t-1} < \tau\right] \geq 1/2.$

Thm: Arikan's martingale satisfies local polarization

(calculus involving entropy fn. + Taylor approx)

will skip

Thm. Local Polarization $\Rightarrow$ Strong Polarization.

(Recall Strong Polarization)

$$\Pr\left[X_t \in (2^{-100t}, 1 - 2^{-100t})\right] \leq \frac{1}{2^{0.001t}})$$

Proof sketch of local $\Rightarrow$ strong.

$$\Phi_t = \min\{\sqrt{X_t}, \sqrt{1-X_t}\}$$

Claim: $\exists\, \beta < 1$, s.t. $\mathbb{E}[\Phi_t \mid X_{t-1}] \leq \beta \cdot \Phi_{t-1}$

(variance in the middle section^2 at ends).

skip proof.

$$\mathbb{E}[\Phi_t] \leq \beta^t$$

$$\Pr[\Phi_t \geq \beta^{t/2}] \leq \beta^{t/2} \quad \text{(by Markov)}$$

i.e. $\Pr[\min(X_t, 1-X_t) \geq \beta^t] \leq \beta^{t/2}$.

i.e. $\Pr[X_t \in (\beta^t, 1-\beta^t)] \leq \beta^{t/2}$

$\beta \approx 1$

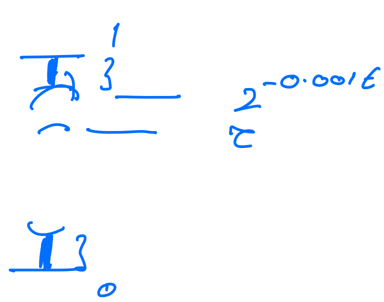
$\beta = 2^{-0.0001}$

$$\underbrace{(2^{-0.0001t}, 1-2^{-0.0001t})}_{\text{not good enough}} \quad \underbrace{\leq 2^{-0.00005t}}_{\text{good}}$$

Semi-strong polarization.

<u>Two phases</u>

(1) $t/2$ phases obtain semi-strong polarization



(2) Next $t/2$ phases:

with probability $e^{t/2}/\varepsilon$, the martingale never crosses ε.

- but in this case it shrinks by factor c at least $1/2$ the time & doubles at most $1/2$ the time.

$\boxtimes$