

Constant Weight Polar Codes through Periodic Markov Processes

Boaz Shuval, Ido Tal

Technion

Big Picture First

- ▶ Previous work:
 - ▶ Polar coding for **aperiodic** processes with memory
 - ▶ Generally, **no polarization** for **periodic** processes
 - ▶ Specifically, counterexample for period 4
- ▶ This work: for **periodic** or **aperiodic** processes
 - ▶ Period is odd $\implies$ polarization
 - ▶ Fix initial state of Markov chain $\implies$ polarization
 - ▶ Fix initial phase of Markov chain $\implies$ polarization
- ▶ Applications:
 - ▶ Balanced codewords
 - ▶ Constant weight codewords
 - ▶ Codewords in a weight range

Setting: Finite Irreducible Markov (FIM) Processes

- ▶ **Process:**

$$(X_j, Y_j, S_j)_{j=1}^N$$

- ▶ **Finite number of states:** $S_j \in \mathcal{S}$, where $|\mathcal{S}| < \infty$
- ▶ **Hidden state:** S_j is **unknown** to encoder and decoder

- ▶ **Probability distribution:**

$$P(x_j, y_j, s_j | s_{j-1})$$

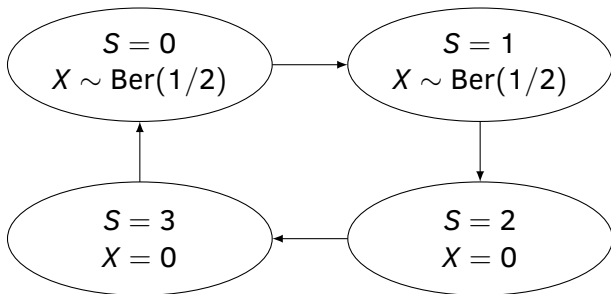
- ▶ **Stationary:** same for all j
- ▶ **Markov:**

$$P(x_j, y_j, s_j | s_{j-1}) = P(x_j, y_j, s_j | \{x_\ell, y_\ell, s_\ell\}_{\ell < j})$$

- ▶ **State sequence:** ~~aperiodic~~ irreducible Markov chain

Periodic Processes do not Polarize [Şaşoğlu Tal:2019]

Counterexample:

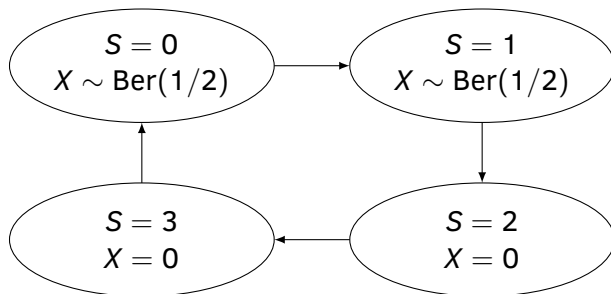


No polarization: for all $\frac{5N}{8} < i \leq \frac{6N}{8}$,

$$\left| H(U_i | U_1^{i-1}) - \frac{1}{2} \right| \leq \epsilon_N, \quad \lim_{N \rightarrow \infty} \epsilon_N = 0$$
$$\left| H(U_i | U_1^{i-1}, S_0) - \frac{1}{2} \right| \leq \epsilon_N, \quad \lim_{N \rightarrow \infty} \epsilon_N = 0$$

Periodic Processes do not Polarize [Şaşoğlu Tal:2019]

Counterexample:

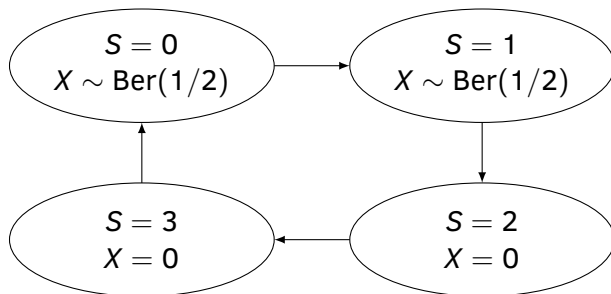


Moreover, for $N \geq 8$ and all $\frac{5N}{8} < i \leq \frac{6N}{8}$,

$$H(U_i | U_1^{i-1}, \mathbf{S}_0) = 1/2$$

Periodic Processes do not Polarize [Şaşoğlu Tal:2019]

Counterexample:



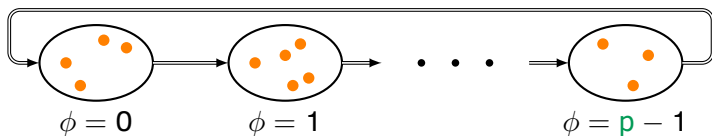
Moreover, for $N \geq 8$ and all $\frac{5N}{8} < i \leq \frac{6N}{8}$,

$$H(U_i | U_1^{i-1}, \mathbf{S}_0) = 1/2$$

However,

$$H(U_i | U_1^{i-1}, \mathbf{S}_0 = \mathbf{s}_0) = \begin{cases} 0, & \mathbf{s}_0 \in \{1, 3\} \\ 1, & \mathbf{s}_0 \in \{0, 2\} \end{cases}$$

Stationary Irreducible Periodic Markov Processes



- ▶ Markov state: $P(s_j | s_{j-1}) = P(s_j | s_{j-1}, s_{j-2}, \dots)$
- ▶ Periodic:
 - ▶ States partitioned to p phases
 - ▶ **Phase** of s is $\phi(s) = \varphi$
 - ▶ $P(S_{j+1} = s' | S_j = s) > 0$ only if $\phi(s') \equiv \phi(s) + 1 \pmod{p}$
- ▶ Irreducible $\implies$ unique positive stationary distribution π
- ▶ Stationary $\implies$ existence of:

$$\mathcal{H}_{X|Y} = \lim_{N \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N)$$

$$\mathcal{H}_X = \lim_{N \rightarrow \infty} \frac{1}{N} H(X_1^N)$$

H , Z , and K Conditioned on an Event

For

- ▶ binary random variable U
- ▶ general random variables W, Q
- ▶ event A

we have

$$H(W|Q, A) = - \sum_{w,q} P_{W,Q|A}(w, q) \log_2 P_{W|Q,A}(w|q)$$

$$Z(U|Q, A) = 2 \sum_q \sqrt{P_{U,Q|A}(0, q) P_{U,Q|A}(1, q)}$$

$$K(U|Q, A) = \sum_q |P_{U,Q|A}(0, q) - P_{U,Q|A}(1, q)|$$

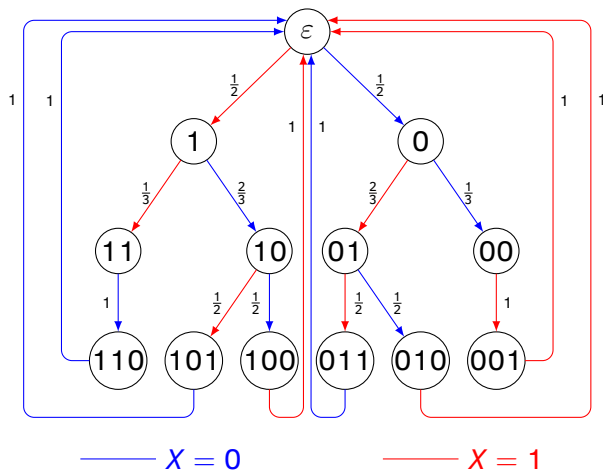
Main Theorem: Fix Phases of Initial, Final States $\implies$ Periodic Processes Polarize

- ▶ Let $(X_j, Y_j, S_j)_j$ be a FIM process, where $(S_j)_j$ has period $\mathbf{p}$
- ▶ For $N = 2^n$, denote by U_1^N the polar transform of X_1^N
- ▶ Fix $0 \leq \varphi < \mathbf{p}$
- ▶ Set $\Psi_0 \subseteq \mathcal{S}$ s.t. $\phi(s_0) = \varphi$ for all $s_0 \in \Psi_0$
- ▶ Set $\Psi_N \subseteq \mathcal{S}$ s.t. $\phi(s_N) = \varphi + N \bmod \mathbf{p}$ for all $s_N \in \Psi_N$
- ▶ Denote $\mathbf{A}_N \triangleq \{s_0 \in \Psi_0 \text{ and } s_N \in \Psi_N\}$

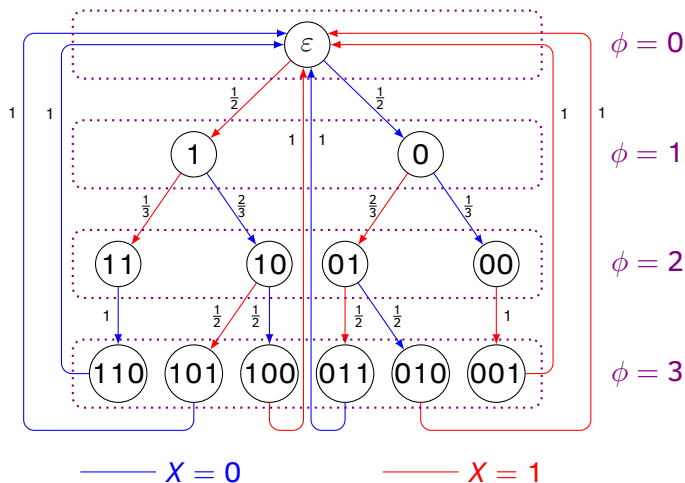
Then, for $0 < \beta < 1/2$,

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : Z(U_i | U_1^{i-1}, Y_1^N, \mathbf{A}_N) < 2^{-N^\beta} \right\} \right| = 1 - \mathcal{H}_{X|Y},$$
$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : K(U_i | U_1^{i-1}, \mathbf{A}_N) < 2^{-N^\beta} \right\} \right| = \mathcal{H}_X$$

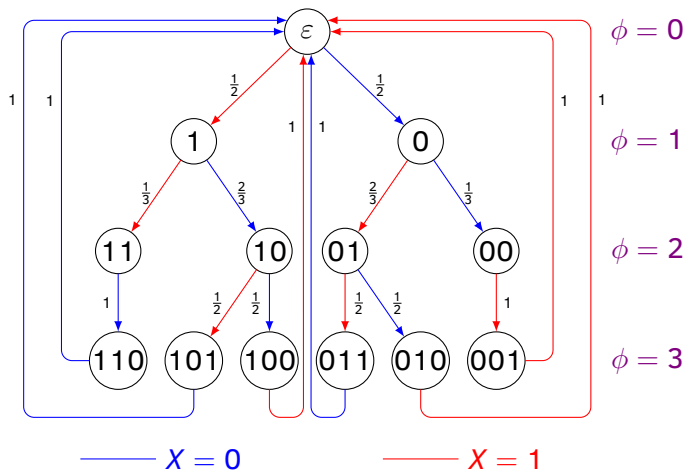
Example: Balanced Codewords



Example: Balanced Codewords

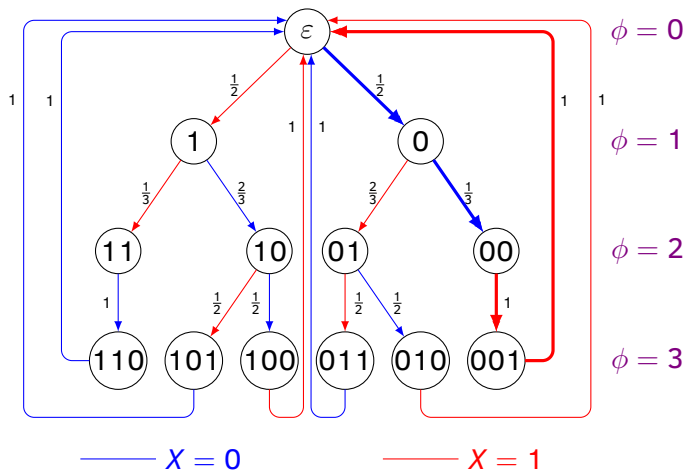


Example: Balanced Codewords



$$p = 4, \quad N = 16, \quad \varphi = 0, \quad \Psi_0 = \Psi_N = \{\varepsilon\}$$

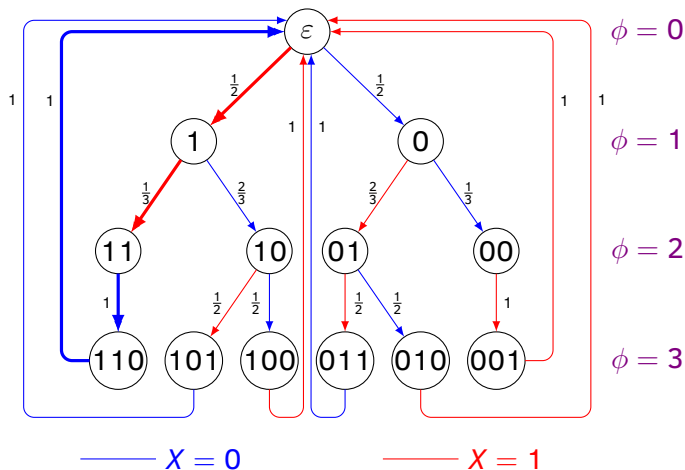
Example: Balanced Codewords



$p = 4$, $N = 16$, $\varphi = 0$, $\Psi_0 = \Psi_N = \{\varepsilon\}$

0011

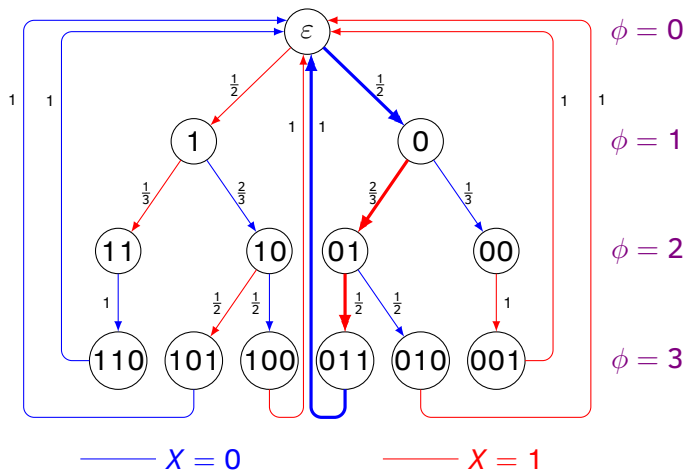
Example: Balanced Codewords



$p = 4$, $N = 16$, $\varphi = 0$, $\Psi_0 = \Psi_N = \{\varepsilon\}$

0011 1100

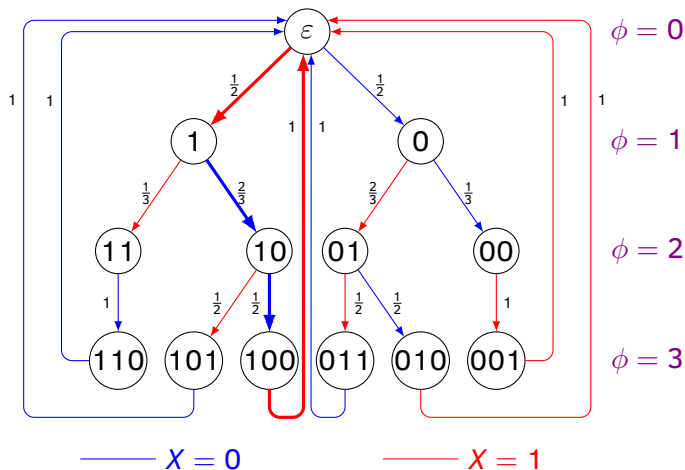
Example: Balanced Codewords



$p = 4$, $N = 16$, $\varphi = 0$, $\Psi_0 = \Psi_N = \{\varepsilon\}$

0011 1100 0110

Example: Balanced Codewords

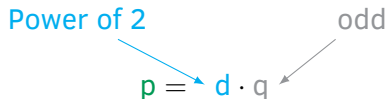


$p = 4$, $N = 16$, $\varphi = 0$, $\Psi_0 = \Psi_N = \{\epsilon\}$

0011 1100 0110 1001

Proof Outline

- ▶ Factor



and denote

$$\mathcal{S}(\Delta) = \{s \in \mathcal{S} : \phi(s) \equiv \Delta \pmod{d}\}$$

- ▶ “Simpler” case: under event

$$D(\Delta) = \{S_0 \in \mathcal{S}(\Delta)\}$$

- ▶ Establish slow polarization
- ▶ Establish fast polarization
- ▶ General case:
 - ▶ Recall: $A_N \triangleq \{S_0 \in \Psi_0 \text{ and } S_N \in \Psi_N\}$
 - ▶ Show that $A_N \subseteq D(\Delta)$ for some Δ
 - ▶ Use “simpler” case to establish result

Interlude: What Went Wrong in the Counterexample?

Why in counterexample, $H(U_i|U_1^{i-1}, \mathbf{S}_0) = 1/2$?

Interlude: What Went Wrong in the Counterexample?

Why in counterexample, $H(U_i|U_1^{i-1}, \mathbf{S}_0) = 1/2$?

► Recall:

$$H(U_i|U_1^{i-1}, \mathbf{S}_0 = s_0) = \begin{cases} 0, & s_0 \in \{1, 3\} \\ 1, & s_0 \in \{0, 2\} \end{cases}$$

- If $S_0 \in \{1, 3\}$, then $S_N \in \{1, 3\}$
- If $S_0 \in \{2, 4\}$, then $S_N \in \{2, 4\}$

Interlude: What Went Wrong in the Counterexample?

Why in counterexample, $H(U_i|U_1^{i-1}, \mathbf{S}_0) = 1/2$?

► Recall:

$$H(U_i|U_1^{i-1}, \mathbf{S}_0 = s_0) = \begin{cases} 0, & s_0 \in \{1, 3\} \\ 1, & s_0 \in \{0, 2\} \end{cases}$$

- If $S_0 \in \{1, 3\}$, then $S_N \in \{1, 3\}$
- If $S_0 \in \{2, 4\}$, then $S_N \in \{2, 4\}$
- Hence, in the polar transform, we are either pairing
 - $H = 1$ with $H = 1 \implies H^- = H^+ = 1$
 - $H = 0$ with $H = 0 \implies H^- = H^+ = 0$

Interlude: What Went Wrong in the Counterexample?

Why in counterexample, $H(U_i|U_1^{i-1}, \mathbf{S}_0) = 1/2$?

► Recall:

$$H(U_i|U_1^{i-1}, \mathbf{S}_0 = s_0) = \begin{cases} 0, & s_0 \in \{1, 3\} \\ 1, & s_0 \in \{0, 2\} \end{cases}$$

- If $S_0 \in \{1, 3\}$, then $S_N \in \{1, 3\}$
- If $S_0 \in \{2, 4\}$, then $S_N \in \{2, 4\}$
- Hence, in the polar transform, we are either pairing
 - $H = 1$ with $H = 1 \implies H^- = H^+ = 1$
 - $H = 0$ with $H = 0 \implies H^- = H^+ = 0$
- **Problem:** we never pair $H \geq 1/2$ with $H \leq 1/2$
- $\implies$ Expected entropy is stuck at $1/2$

Interlude: What Went Wrong in the Counterexample?

Why in counterexample, $H(U_i|U_1^{i-1}, \mathbf{S}_0) = 1/2$?

► Recall:

$$H(U_i|U_1^{i-1}, \mathbf{S}_0 = s_0) = \begin{cases} 0, & s_0 \in \{1, 3\} \\ 1, & s_0 \in \{0, 2\} \end{cases}$$

- If $S_0 \in \{1, 3\}$, then $S_N \in \{1, 3\}$
- If $S_0 \in \{2, 4\}$, then $S_N \in \{2, 4\}$
- Hence, in the polar transform, we are either pairing
 - $H = 1$ with $H = 1 \implies H^- = H^+ = 1$
 - $H = 0$ with $H = 0 \implies H^- = H^+ = 0$
- **Problem:** we never pair $H \geq 1/2$ with $H \leq 1/2$
- $\implies$ Expected entropy is stuck at $1/2$

Remember
this for later

Slow Polarization: Convergence to $H_\infty(\Delta)$ and $\hat{H}_\infty(\Delta)$

For a given $0 \leq \Delta < d$, $N = 2^n$, and $1 \leq i \leq N$, denote

$$\hat{H}_n(\Delta) = H(U_i|Q_i, S_0, S_N, D(\Delta))$$

$$H_n(\Delta) = H(U_i|Q_i, D(\Delta))$$

where $Q_i = (U_1^{i-1}, Y_1^N)$

Slow Polarization: Convergence to $H_\infty(\Delta)$ and $\hat{H}_\infty(\Delta)$

For a given $0 \leq \Delta < d$, $N = 2^n$, and $1 \leq i \leq N$, denote

$$\hat{H}_n(\Delta) = H(U_i|Q_i, S_0, S_N, D(\Delta))$$

$$H_n(\Delta) = H(U_i|Q_i, D(\Delta))$$

where $Q_i = (U_1^{i-1}, Y_1^N)$

Lemma

Fix $0 \leq \Delta < d$. Then,

$$(\hat{H}_n(\Delta))_{n=1}^\infty \xrightarrow{L_1, a.s.} \hat{H}_\infty(\Delta) \in [0, 1]$$

$$(H_n(\Delta))_{n=1}^\infty \xrightarrow{L_1, a.s.} H_\infty(\Delta) \in [0, 1]$$

Slow Polarization: Convergence to $H_\infty(\Delta)$ and $\hat{H}_\infty(\Delta)$

For a given $0 \leq \Delta < d$, $N = 2^n$, and $1 \leq i \leq N$, denote

$$\hat{H}_n(\Delta) = H(U_i|Q_i, S_0, S_N, D(\Delta))$$

$$H_n(\Delta) = H(U_i|Q_i, D(\Delta))$$

where $Q_i = (U_1^{i-1}, Y_1^N)$

Lemma

Fix $0 \leq \Delta < d$. Then,

$$(\hat{H}_n(\Delta))_{n=1}^\infty \xrightarrow{L_1, a.s.} \hat{H}_\infty(\Delta) \in [0, 1]$$

$$(H_n(\Delta))_{n=1}^\infty \xrightarrow{L_1, a.s.} H_\infty(\Delta) \in [0, 1]$$

Proof sketch: $\hat{H}_n(\Delta)$ is a bounded sub-martingale;
 $H_n(\Delta)$ is a bounded super-martingale

Slow Polarization: $\hat{H}_\infty(\Delta) \in \{0, 1\}$

$$p = d \cdot q$$

Define

$$\mathcal{S}_N^2(\Delta) = \{(s_0, s_N) : \phi(s_0) \equiv \Delta \pmod{d}, \\ \phi(s_N) - \phi(s_0) \equiv N \pmod{p}\}$$

Slow Polarization: $\hat{H}_\infty(\Delta) \in \{0, 1\}$

$$p = d \cdot q$$

Define

$$\mathcal{S}_N^2(\Delta) = \{(s_0, s_N) : \phi(s_0) \equiv \Delta \pmod{d}, \\ \phi(s_N) - \phi(s_0) \equiv N \pmod{p}\}$$

Recalling $\hat{H}_n(\Delta) = H(U_i|Q_i, S_0, S_N, D(\Delta))$,

$$\hat{H}_n(\Delta) = d \cdot \sum_{(s_0, s_N) \in \mathcal{S}_N^2(\Delta)} \pi(s_0, s_N) \underbrace{H(U_i|Q_i, S_0 = s_0, S_N = s_N)}_{\gamma(s_0, s_N)}$$

Slow Polarization: $\hat{H}_\infty(\Delta) \in \{0, 1\}$

$$p = d \cdot q$$

Define

$$\mathcal{S}_N^2(\Delta) = \{(s_0, s_N) : \phi(s_0) \equiv \Delta \pmod{d}, \\ \phi(s_N) - \phi(s_0) \equiv N \pmod{p}\}$$

Recalling $\hat{H}_n(\Delta) = H(U_i|Q_i, s_0, s_N, D(\Delta))$,

$$\hat{H}_n(\Delta) = d \cdot \sum_{(s_0, s_N) \in \mathcal{S}_N^2(\Delta)} \pi(s_0, s_N) \underbrace{H(U_i|Q_i, s_0 = s_0, s_N = s_N)}_{\gamma(s_0, s_N)}$$

By the pigeon hole principle, we can have **neither**

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \forall (s_0, s_N) \in \mathcal{S}_N^2(\Delta)$$

nor

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \forall (s_0, s_N) \in \mathcal{S}_N^2(\Delta)$$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Define

$$\begin{aligned} \mathcal{S}_N^3(\Delta) = \{ (s_0, s_N, s_{2N}) : & \phi(s_0) \equiv \Delta \pmod{d}, \\ & \phi(s_N) - \phi(s_0) \equiv N \pmod{p}, \\ & \phi(s_{2N}) - \phi(s_N) \equiv N \pmod{p} \} \end{aligned}$$

¹[ŞaşoğluTal:2019, Lemma 11], [Şaşoğlu:2017, Lemma 2.2]

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Define

$$\begin{aligned} \mathcal{S}_N^3(\Delta) = \{ (s_0, s_N, s_{2N}) : & \phi(s_0) \equiv \Delta \pmod{d}, \\ & \phi(s_N) - \phi(s_0) \equiv N \pmod{p}, \\ & \phi(s_{2N}) - \phi(s_N) \equiv N \pmod{p} \} \end{aligned}$$

Let $N > d$. For polarization to $\{0, 1\}$ it suffices to show¹ that if

$$\epsilon \leq \hat{H}_n(\Delta) \leq 1 - \epsilon$$

there exists $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with probability $\geq \mu > 0$ s.t.

$$\gamma(s_0, s_N) \leq \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) \geq \hat{H}_n(\Delta)$$

or

$$\gamma(s_0, s_N) \geq \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) \leq \hat{H}_n(\Delta)$$

¹[ŞaşoğluTal:2019, Lemma 11], [Şaşoğlu:2017, Lemma 2.2]

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Assume the contrary: for all $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$, either

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) < \hat{H}_n(\Delta) \quad (1)$$

or

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) > \hat{H}_n(\Delta) \quad (2)$$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Assume the contrary: for all $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$, either

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) < \hat{H}_n(\Delta) \quad (1)$$

or

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) > \hat{H}_n(\Delta) \quad (2)$$

- Recall q odd, d power of 2
- Chinese Remainder Theorem $\implies$ exists $0 \leq \varphi < p$, s.t.

$$\varphi \equiv \Delta \pmod{d} \quad \text{and} \quad \varphi \equiv -2 \pmod{q}$$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Assume the contrary: for all $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$, either

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) < \hat{H}_n(\Delta) \quad (1)$$

or

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) > \hat{H}_n(\Delta) \quad (2)$$

- ▶ Recall q odd, d power of 2
- ▶ Chinese Remainder Theorem $\implies$ exists $0 \leq \varphi < p$, s.t.

$$\varphi \equiv \Delta \pmod{d} \quad \text{and} \quad \varphi \equiv -2 \pmod{q}$$

- ▶ Fix $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Assume the contrary: for all $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$, either

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) < \hat{H}_n(\Delta) \quad (1)$$

or

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) > \hat{H}_n(\Delta) \quad (2)$$

- ▶ Recall q odd, d power of 2
- ▶ Chinese Remainder Theorem $\implies$ exists $0 \leq \varphi < p$, s.t.

$$\varphi \equiv \Delta \pmod{d} \quad \text{and} \quad \varphi \equiv -2 \pmod{q}$$

- ▶ Fix $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$
- ▶ Assume w.l.o.g. (1) holds $\implies \gamma(s_0, s_N) < \hat{H}_n(\Delta)$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Assume the contrary: **for all** $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$, either

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) < \hat{H}_n(\Delta) \quad (1)$$

or

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) > \hat{H}_n(\Delta) \quad (2)$$

- ▶ Recall q odd, d power of 2
- ▶ Chinese Remainder Theorem $\implies$ exists $0 \leq \varphi < p$, s.t.

$$\varphi \equiv \Delta \pmod{d} \quad \text{and} \quad \varphi \equiv -2 \pmod{q}$$

- ▶ Fix $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$
- ▶ Assume w.l.o.g. (1) holds $\implies \gamma(s_0, s_N) < \hat{H}_n(\Delta)$
- ▶ By (1), for any $(s_0, s_N, a_0) \in \mathcal{S}_N^3(\Delta) \implies \gamma(s_N, a_0) < \hat{H}_n(\Delta)$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Assume the contrary: **for all** $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$, either

$$\gamma(s_0, s_N) < \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) < \hat{H}_n(\Delta) \quad (1)$$

or

$$\gamma(s_0, s_N) > \hat{H}_n(\Delta) \quad \text{and} \quad \gamma(s_N, s_{2N}) > \hat{H}_n(\Delta) \quad (2)$$

- ▶ Recall q odd, d power of 2
- ▶ Chinese Remainder Theorem $\implies$ exists $0 \leq \varphi < p$, s.t.

$$\varphi \equiv \Delta \pmod{d} \quad \text{and} \quad \varphi \equiv -2 \pmod{q}$$

- ▶ Fix $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$
- ▶ Assume w.l.o.g. (1) holds $\implies \gamma(s_0, s_N) < \hat{H}_n(\Delta)$
- ▶ By (1), for any $(s_0, s_N, a_0) \in \mathcal{S}_N^3(\Delta) \implies \gamma(s_N, a_0) < \hat{H}_n(\Delta)$
- ▶ By (1), for any $(s_N, a_0, a_1) \in \mathcal{S}_N^3(\Delta) \implies \gamma(a_0, a_1) < \hat{H}_n(\Delta)$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

$$p = d \cdot q$$

Recap:

- ▶ Fixed $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$, and
$$\varphi \equiv \Delta \pmod{d} \quad \text{and} \quad \varphi \equiv -2 \pmod{q}$$
- ▶ Assumed w.l.o.g. $\gamma(s_0, s_N) < \hat{H}_n(\Delta)$
- ▶ Showed for any $(s_N, a_0, a_1) \in \mathcal{S}_N^3(\Delta)$, $\gamma(a_0, a_1) < \hat{H}_n(\Delta)$

Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

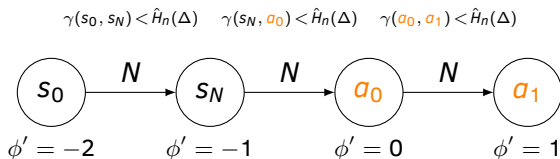
$$p = d \cdot q$$

Recap:

- ▶ Fixed $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$, and
 $\varphi \equiv \Delta \pmod{d}$ and $\varphi \equiv -2 \pmod{q}$
- ▶ Assumed w.l.o.g. $\gamma(s_0, s_N) < \hat{H}_n(\Delta)$
- ▶ Showed for any $(s_N, a_0, a_1) \in \mathcal{S}_N^3(\Delta)$, $\gamma(a_0, a_1) < \hat{H}_n(\Delta)$

Next,

- ▶ Define $\phi'(s) = \phi(s) \pmod{q}$
- ▶ Choose n s.t. Euler's totient of q divides $n \implies$



Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

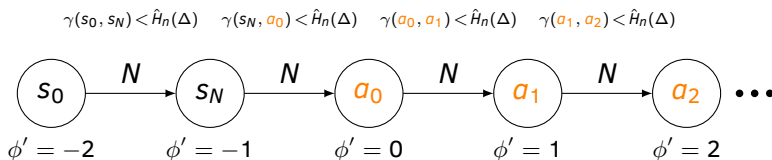
$$p = d \cdot q$$

Recap:

- ▶ Fixed $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$, and
 $\varphi \equiv \Delta \pmod{d}$ and $\varphi \equiv -2 \pmod{q}$
- ▶ Assumed w.l.o.g. $\gamma(s_0, s_N) < \hat{H}_n(\Delta)$
- ▶ Showed for any $(s_N, a_0, a_1) \in \mathcal{S}_N^3(\Delta)$, $\gamma(a_0, a_1) < \hat{H}_n(\Delta)$

Next,

- ▶ Define $\phi'(s) = \phi(s) \pmod{q}$
- ▶ Choose n s.t. Euler's totient of q divides $n \implies$



Slow Polarization: $\hat{H}_\infty(\Delta) \rightarrow \{0, 1\}$

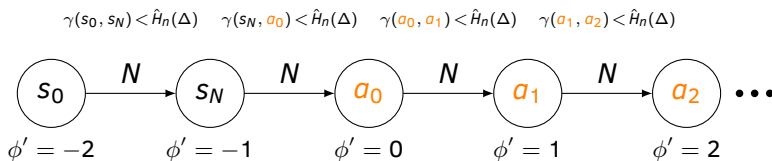
$$p = d \cdot q$$

Recap:

- ▶ Fixed $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ with $\phi(s_0) = \varphi$, and
 $\varphi \equiv \Delta \pmod{d}$ and $\varphi \equiv -2 \pmod{q}$
- ▶ Assumed w.l.o.g. $\gamma(s_0, s_N) < \hat{H}_n(\Delta)$
- ▶ Showed for any $(s_N, a_0, a_1) \in \mathcal{S}_N^3(\Delta)$, $\gamma(a_0, a_1) < \hat{H}_n(\Delta)$

Next,

- ▶ Define $\phi'(s) = \phi(s) \pmod{q}$
- ▶ Choose n s.t. Euler's totient of q divides $n \implies$



Induction $\implies \forall (s, s') \in \mathcal{S}_N^2(\Delta)$, $\gamma(s, s') < \hat{H}_n(\Delta) \implies$ **Contradiction!**

Slow Polarization: Tying Things Together

Proposition: For $0 \leq \Delta < d$, $0 < \epsilon < 1$, and $N = 2^n$:

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : H(U_i | U_1^{i-1}, Y_1^N, D(\Delta)) < \epsilon \right\} \right| && H_n(\Delta) \\ &= \lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : H(U_i | U_1^{i-1}, Y_1^N, S_0, S_N, D(\Delta)) < \epsilon \right\} \right| \\ &= 1 - \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N, S_0, S_N, D(\Delta)) && \hat{H}_n(\Delta) \\ &= 1 - \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N, D(\Delta)) \\ &= 1 - \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N) \\ &= 1 - \mathcal{H}_{X|Y} \end{aligned}$$

Slow Polarization: Tying Things Together

Proposition: For $0 \leq \Delta < d$, $0 < \epsilon < 1$, and $N = 2^n$:

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : H(U_i | U_1^{i-1}, Y_1^N, D(\Delta)) > 1 - \epsilon \right\} \right| && H_n(\Delta) \\ &= \lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : H(U_i | U_1^{i-1}, Y_1^N, S_0, S_N, D(\Delta)) > 1 - \epsilon \right\} \right| \\ &= \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N, S_0, S_N, D(\Delta)) && \hat{H}_n(\Delta) \\ &= \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N, D(\Delta)) \\ &= \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N) \\ &= \mathcal{H}_{X|Y} \end{aligned}$$

Fast Polarization for “Simpler” Case – Given $D(\Delta)$

Proposition: Fix $0 < \beta < 1/2$ and $0 \leq \Delta < d$. Then, for $N = 2^n$,

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : Z(U_i | Q_i, D(\Delta)) < 2^{-N^\beta} \right\} \right| = 1 - \mathcal{H}_{X|Y}$$

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : K(U_i | Q_i, S_0, S_N, D(\Delta)) < 2^{-N^\beta} \right\} \right| = \mathcal{H}_{X|Y}$$

Reminder: This is not yet our Main Theorem; we still need to go from $D(\Delta)$ to $A_N \triangleq \{S_0 \in \Psi_0 \text{ and } S_N \in \Psi_N\}$

Proof Sketch

$$M(\Delta) \triangleq \frac{1}{d \cdot \min\{\pi_s : s \in \mathcal{S}(\Delta)\}}, \quad 0 \leq \Delta \leq d$$

Proof Sketch

$$M(\Delta) \triangleq \frac{1}{d \cdot \min\{\pi_s : s \in \mathcal{S}(\Delta)\}}, \quad 0 \leq \Delta \leq d$$

Markov + irreducibility + stationarity + periodicity $\implies$

Mixing Lemma:

- Fix $0 \leq \Delta < d$ and $N = 2^n \geq d$
- Let $A, B \subseteq \mathcal{X}^N \times \mathcal{Y}^N$

Then,

$$\begin{aligned} \mathbb{P} \left((X_1^N, Y_1^N) \in A \quad \text{and} \quad (X_{N+1}^{2N}, Y_{N+1}^{2N}) \in B \middle| D(\Delta) \right) \\ \leq M(\Delta) \cdot \mathbb{P} \left((X_1^N, Y_1^N) \in A \middle| D(\Delta) \right) \\ \cdot \mathbb{P} \left((X_{N+1}^{2N}, Y_{N+1}^{2N}) \in B \middle| D(\Delta) \right) \end{aligned}$$

Proof Sketch

$$M(\Delta) \triangleq \frac{1}{d \cdot \min\{\pi_s : s \in \mathcal{S}(\Delta)\}}, \quad 0 \leq \Delta \leq d$$

Mixing Lemma $\implies$

Lemma: Fix $0 \leq \Delta < d$ and $N = 2^n \geq d$. Then,

$$\begin{aligned} Z_n^-(\Delta) &\leq 2 \cdot M(\Delta) \cdot Z_n(\Delta) & \text{and} & & Z_n^+(\Delta) &\leq M(\Delta) \cdot (Z_n(\Delta))^2 \\ \hat{K}_n^-(\Delta) &\leq d \cdot M(\Delta) \cdot (\hat{K}_n(\Delta))^2 & \text{and} & & \hat{K}_n^+(\Delta) &\leq 2 \cdot \hat{K}_n(\Delta) \end{aligned}$$

This yields the proposition

From $D(\Delta)$ to A_N

Recall:

$$Z(U|Q, \mathbf{A}) = 2 \sum_q \sqrt{P_{U,Q|\mathbf{A}}(0, q) P_{U,Q|\mathbf{A}}(1, q)}$$

$$K(U|Q, \mathbf{A}) = \sum_q |P_{U,Q|\mathbf{A}}(0, q) - P_{U,Q|\mathbf{A}}(1, q)|$$

Lemma: Let

- ▶ U be a binary random variable
- ▶ Q general random variable
- ▶ $A_1, A_2, \dots, A_\ell$ mutually exclusive events

Denote

$$C = A_1 \cup A_2 \cup \dots \cup A_\ell$$

Then,

$$Z(U|Q, \mathbf{C}) \geq \sum \mathbb{P}(A_j|\mathbf{C}) Z(U|Q, A_j)$$

$$K(U|Q, \mathbf{C}) \leq \sum \mathbb{P}(A_j|\mathbf{C}) K(U|Q, A_j)$$

From $D(\Delta)$ to A_N

Recall 1: fast polarization for $D(\Delta)$

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : Z(U_i | Q_i, D(\Delta)) < 2^{-N^\beta} \right\} \right| = 1 - \mathcal{H}_{X|Y}$$
$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : K(U_i | Q_i, S_0, S_N, D(\Delta)) < 2^{-N^\beta} \right\} \right| = \mathcal{H}_{X|Y}$$

Recall 2: for $C = A_1 \cup A_2 \cup \dots \cup A_\ell$,

$$Z(U|Q, C) \geq \sum \mathbb{P}(A_j | C) Z(U|Q, A_j)$$

$$K(U|Q, C) \leq \sum \mathbb{P}(A_j | C) K(U|Q, A_j)$$

From $D(\Delta)$ to A_N

$$\Psi_{0,N} = \Psi_0 \times \Psi_N$$

Recall 1: fast polarization for $D(\Delta)$

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : Z(U_i | Q_i, D(\Delta)) < 2^{-N^\beta} \right\} \right| = 1 - \mathcal{H}_{X|Y}$$

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : K(U_i | Q_i, S_0, S_N, D(\Delta)) < 2^{-N^\beta} \right\} \right| = \mathcal{H}_{X|Y}$$

Recall 2: for $C = A_1 \cup A_2 \cup \dots \cup A_\ell$,

$$Z(U|Q, C) \geq \sum \mathbb{P}(A_j | C) Z(U|Q, A_j)$$

$$K(U|Q, C) \leq \sum \mathbb{P}(A_j | C) K(U|Q, A_j)$$

For Z , take

For K , take

$$C = \{(S_0, S_N) \in \mathcal{S}_N^2(\Delta)\} = D(\Delta)$$

$$C = \{(S_0, S_N) \in \Psi_{0,N}\} = A_N$$

$$A_1 = \{(S_0, S_N) \in \Psi_{0,N}\} = A_N$$

$$A_{S_0, S_N} = \{(S_0, S_N) = (s_0, s_N)\}$$

$$A_2 = \{(S_0, S_N) \in \mathcal{S}_N^2(\Delta) \setminus \Psi_{0,N}\}$$

$$\subseteq D(\Delta)$$


$$(s_0, s_N) \in \Psi_{0,N}$$