

# Constant Weight Polar Codes through Periodic Markov Processes

Boaz Shuval, Ido Tal

The Andrew and Erna Viterbi Faculty of Electrical and Computer Engineering,  
Technion, Haifa 32000, Israel.

Email: {bshuval@, idotal@ee.}technion.ac.il

**Abstract**—Constant weight codes can arise from an input process sampled from a periodic Markov chain. A previous result showed that, in general, polarization does *not* occur for input-output processes with an underlying *periodic* Markov chain. In this work, we show that if we fix the initial state of an underlying periodic Markov chain, polarization *does* occur. Fixing the initial state is aligned with ensuring a constant weight code.

## I. INTRODUCTION

Polar codes have been shown to achieve the capacity or information rate of many channel models [1]–[12]. Specifically, in [4], [5], polar codes were shown to achieve the information rate of input-output processes with an underlying finite-state, *aperiodic*, and irreducible Markov (FAIM) process. Moreover, in [4, Theorem 4] it was shown by a counter-example that aperiodicity is a necessary condition. In this paper, we prove that polarization does occur for periodic processes, provided that the initial state is fixed. This setting is natural in the context of codewords constrained to be of a constant weight.

An example of an irreducible Markov chain of period  $p = 4$  for producing sequences of constant weight  $N/2$  (i.e., normalized weight  $1/2$ ) is given in Figure 1. This holds if the initial state is  $\varepsilon$  and the sequence length  $N$  is a multiple of 4. A few things to note:

- We produce only a subset of the sequences of weight  $N/2$ .
- All sequences of length 4 have probability  $1/6$ , where  $6 = \binom{4}{2}$  is the number of sequences of length 4 and weight 2.
- The number of states can be drastically reduced, while producing the same set of sequences at the same probabilities, see Figure 2.
- Enlarging the period  $p$  from 4 to a larger number will allow us to produce a larger subset of sequences of weight  $N/2$ , at the expense of more states.
- If the sequence length  $N$  is not a multiple of the period  $p$ , we must also constrain the final state to be in a certain set. For example, in Figure 1 and  $N = 6$ , the final state must be either ‘10’ or ‘01’. That is, of weight 1.
- For  $\alpha = a/b$  rational, a similar graph can be constructed for sequences of weight  $\lfloor \alpha N \rfloor$ , when  $N$  is not a multiple of  $b$ . The same holds for weight  $\lceil \alpha N \rceil$ . This again requires constraining the final state to be of a certain weight.
- For  $\alpha \leq \beta$  rational, a similar graph can be constructed for sequences of weight between  $\alpha N$  and  $\beta N$ . Now, generally, the final state is constrained to have a range of weights.
- For positive integers  $a$  and  $b$ , the aperiodic graph in Figure 3 can ensure sequences whose weight modulo

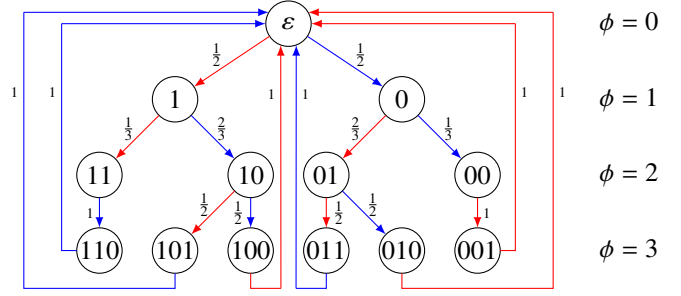


Fig. 1. Markov chain for producing sequences of weight  $N/2$ . Labels for blue and red arrows are ‘0’ and ‘1’, respectively. Transition probabilities between states are shown on the arrows. The state  $\varepsilon$  is the start and end state, at which the output is ensured to have weight  $N/2$ . The chain has period  $p = 4$ ; each horizontal layer of the graph is a different phase  $\phi$ .

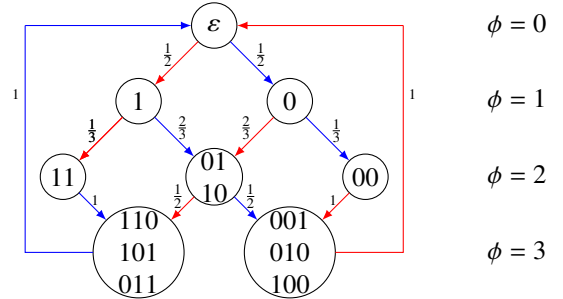


Fig. 2. Condensed Markov chain for producing sequences of weight  $N/2$ . Here, states from Figure 1 of the same phase and weight are merged. The probability of a blue (red) edge from a node with phase  $\phi$  and weight  $w$  to a node with phase  $\phi + 1$  and weight  $w + 1$  is the number of valid sequences, i.e. length 4 and weight 2, whose weight in the prefix of length  $\phi + 1$  is  $w$  ( $w + 1$ ) divided by the number of valid sequences whose weight in the prefix of length  $\phi$  is  $w$ .

$b$  is  $a$ . This is obtained by fixing the initial state to be ‘0’ and the final state to be ‘ $a$ ’.

This paper omits or sketches some of the proofs; full details can be found in [13].

## II. SETTING AND MAIN THEOREM

Although we will ultimately fix the initial state, we start by considering a strictly stationary process,  $(X_j, Y_j, S_j)_{j \in \mathbb{Z}}$ . Here,  $X_j$  is binary,  $Y_j \in \mathcal{Y}$ , and  $S_j \in \mathcal{S}$ , with  $\mathcal{Y}$  and  $\mathcal{S}$  finite alphabets. We call  $S_j$  the state at time  $j$ . The conditional distribution of the process is  $P_{X_j, Y_j, S_j | S_{j-1}}$ , independent of  $j$  by stationarity. The distribution has a Markov property: conditioned on  $S_{j-1}$ , the random variables  $X_k, Y_k, S_k$  are independent of  $X_l, Y_l, S_{l-1}$  for any  $l < j \leq k$ .

The state sequence  $S_j$  is a finite-state irreducible Markov (FIM) process. By the Perron-Frobenius theorem [14, Theorem 8.4.4 and Corollary 8.1.30], it indeed has a unique stationary

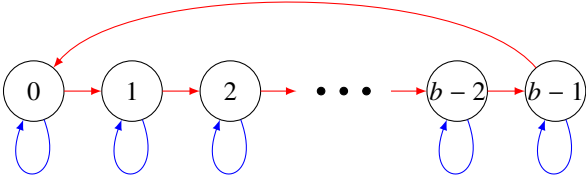


Fig. 3. Markov chain for producing sequences whose weight modulo  $b$  is constrained to some integer  $0 \leq a < b$ . Blue and red arrows are labelled '0' and '1', respectively. All edge probabilities are  $1/2$ . The chain is aperiodic. To construct the sequences, we constrain the initial state to '0' and the final state to 'a'.

distribution  $\pi$ , which is positive. That is, for any state  $s \in \mathcal{S}$ ,  $\pi(s) > 0$ . We denote the period of the state sequence by  $\mathbf{p}$ . That is, we can partition  $\mathcal{S}$  into  $\mathbf{p}$  classes, which we call *phases*. The phase of  $s \in \mathcal{S}$  is denoted  $\phi(s)$ , an integer between 0 and  $\mathbf{p}-1$ . This partition is such that  $\mathbb{P}(S_{j+1} = s' | S_j = s)$  is positive only if  $\phi(s') \equiv \phi(s) + 1 \pmod{\mathbf{p}}$ . For example, in Figure 1, each horizontal layer corresponds to a different phase.

The conditional entropy, Bhattacharyya, and total variation parameters are key to proving polarization theorems. For a binary random variable  $U$ , general random variables  $W, Q$ , and an event  $A$ ,

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

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

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

The entropy rate of our process, excluding the states, is

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

We also denote

$$\mathcal{H}_X = \lim_{N \rightarrow \infty} \frac{1}{N} H(X_1^N). \quad (2)$$

These limits exist, see [4, Section II].

Following is our main theorem. By the Honda-Yamamoto scheme [15], it implies that a polar coding scheme with rate approaching  $\mathcal{H}_X - \mathcal{H}_{X|Y}$  and vanishing error probability exists, if we condition on either the initial state or the initial state and the set of final states.

**Theorem 1.** *Let  $(X_j, Y_j, S_j)_{j \in \mathbb{Z}}$  be a FIM process, where  $(S_j)_{j \in \mathbb{Z}}$  has period  $\mathbf{p}$ . For  $N = 2^n$ , denote by  $U_1^N$  the polar transform of  $X_1^N$ , and fix  $0 < \beta < 1/2$ . Fix  $0 \leq \varphi < \mathbf{p}$ , and a non-empty set  $\Psi_0 \subseteq \mathcal{S}$  such that all states  $s_0 \in \Psi_0$  have phase  $\phi(s_0) = \varphi$ . Furthermore, let  $\Psi_N$  be a non-empty subset of  $\mathcal{S}$  such that all states  $s_N \in \Psi_N$  have phase  $\phi(s_N) = \varphi + N \bmod \mathbf{p}$ . Denote the event  $A_N$  as*

$$A_N \triangleq \{S_0 \in \Psi_0 \text{ and } S_N \in \Psi_N\}.$$

Then,

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

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : K(U_i | U_1^{i-1}, A_N) < 2^{-N^\beta} \right\} \right| = \mathcal{H}_X,$$

We note that the encoding and decoding complexity of our coding scheme is  $O(|\mathcal{S}|^3 N \log N)$ , utilizing successive-cancellation trellis decoding [16], [17] and the Honda-Yamamoto scheme [15]. The only difference is that rather than

marginalizing  $S_0, S_N$  over all states in  $|\mathcal{S}|$ , we marginalize  $S_0$  only over  $\Psi_0$  and  $S_N$  only over  $\Psi_N$ .

Throughout this paper, we assume the setting of Theorem 1. We denote by  $U_1^N, V_1^N$  the polar transforms of  $X_1^N$  and  $X_{N+1}^{2N}$ , respectively. We further denote  $Q_i = (U_1^{i-1}, Y_1^N)$  and  $R_i = (V_1^{i-1}, Y_{N+1}^{2N})$ , for  $1 \leq i \leq N$ .

Our proof of Theorem 1 will follow by showing slow and then fast polarization. We factor the period  $\mathbf{p}$  into

$$\mathbf{p} = \mathbf{d} \cdot \mathbf{q}, \quad (3)$$

where  $\mathbf{q}$  is odd and  $\mathbf{d}$  is a power of 2. In essence, we show that both slow and fast polarization occur if we fix the phase modulo  $\mathbf{d}$  of the initial state. Our proofs are extensions of the ideas presented in [1], [4]–[6], [18], while also taking into account the above.

For  $0 \leq \Delta < \mathbf{d}$ , define

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

We denote the event

$$D(\Delta) \triangleq \{S_0 \in \mathcal{S}(\Delta)\} = \{\phi(S_0) \equiv \Delta \pmod{\mathbf{d}}\}.$$

Since  $N = 2^n$  and  $\mathbf{d}$  are both powers of 2, we have

$$D(\Delta) = \{S_N \in \mathcal{S}(\Delta)\}, \quad \text{for } N \geq \mathbf{d}. \quad (4)$$

Observe that by stationarity, we have for  $0 \leq \Delta \leq \mathbf{d}$

$$\mathbb{P}(D(\Delta)) = 1/\mathbf{d}. \quad (5)$$

For  $N = 2^n \geq \mathbf{d}$  denote

$$\mathcal{S}_N^2(\Delta) = \{(s_0, s_N) \in \mathcal{S}^2 : s_0 \in \mathcal{S}(\Delta) \text{ and } \phi(s_N) - \phi(s_0) \equiv N \pmod{\mathbf{p}}\}, \quad (6)$$

and

$$\mathcal{S}_N^3(\Delta) = \{(s_0, s_N, s_{2N}) \in \mathcal{S}^3 : (s_0, s_N) \in \mathcal{S}_N^2(\Delta) \text{ and } (s_N, s_{2N}) \in \mathcal{S}_N^2(\Delta)\}. \quad (7)$$

Observe that for  $N = 2^n \geq \mathbf{d}$ ,

$$D(\Delta) \text{ holds} \Leftrightarrow \{S_0 \in \mathcal{S}(\Delta)\} \Leftrightarrow \{S_N \in \mathcal{S}(\Delta)\} \Leftrightarrow \{S_{2N} \in \mathcal{S}(\Delta)\} \\ \Leftrightarrow \{(S_0, S_N) \in \mathcal{S}_N^2(\Delta)\} \Leftrightarrow \{(S_0, S_N, S_{2N}) \in \mathcal{S}_N^3(\Delta)\}.$$

The following definition and the observation and lemma that follow will be of use in the sequel.

**Definition 1.** Denote  $f(N) \simeq g(N)$  if  $f(N) - g(N)$  can be upper and lower bounded by expressions independent of  $N$ . It is easily shown that  $\simeq$  is a transitive relation.

Observe that if  $f(N) \simeq g(N)$  and the limit  $\lim_{N \rightarrow \infty} f(N)/N$  exists, then  $\lim_{N \rightarrow \infty} g(N)/N$  exists, and the limits coincide.

**Lemma 2.** If  $V, Q$ , and  $W$  are random variables,  $A$  is an event, and the support of  $W$  is finite, then

$$H(V, W|Q, A) \simeq H(V|Q, A) \simeq H(V|Q, W, A), \quad (8)$$

*Proof sketch:* This is a consequence of the chain rule. ■

Finally, as a shorthand, for random variables  $X, Y$  we denote  $P_{X|Y}(x|y) = \mathbb{P}(X = x | Y = y)$ . The extension for multiple random variables is immediate.

### III. PROOF OF SLOW POLARIZATION

The proof of slow polarization comprises two steps: showing a convergence to a limiting random variable and then showing that this random variable is either 0 or 1, with probability 1.

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

$$\hat{H}_n(\Delta) = H(U_i|Q_i, S_0, S_N, D(\Delta)), \quad (9)$$

$$\hat{H}_n^-(\Delta) = H(U_i + V_i|Q_i, R_i, S_0, S_{2N}, D(\Delta)). \quad (10)$$

$$H_n(\Delta) = H(U_i|Q_i, D(\Delta)). \quad (11)$$

**Lemma 3.** Fix  $0 \leq \Delta < \mathbf{d}$ . Consider the random process

$$J_n = 1 + \langle B_0, B_1, \dots, B_n \rangle_2 = 1 + \sum_{j=0}^{n-1} B_j 2^{n-j},$$

where the  $B_j$  are i.i.d. Bernoulli  $1/2$  random variables. Then, the random processes  $(\hat{H}_n(\Delta))_{n=1}^\infty$  and  $(H_n(\Delta))_{n=1}^\infty$  where  $i = J_n$  converge a.s., in  $L_1$ , and in probability to limiting random variables  $\hat{H}_\infty(\Delta) \in [0, 1]$  and  $H_\infty(\Delta) \in [0, 1]$ , respectively.

*Proof sketch:* Take  $n_0$  large enough such that  $2^{n_0} \geq \mathbf{d}$ . The proof follows by showing that the processes  $(\hat{H}_n(\Delta))_{n=n_0}^\infty$  and  $(H_n(\Delta))_{n=n_0}^\infty$  are a bounded sub-martingale and a bounded a super-martingale, respectively, with respect to  $(J_n)_{n=1}^\infty$ , see [19, Theorems 7.3.1 and 14.2.1 and Proposition 5.2.3]. ■

For  $N > 0$ , denote

$$\mathcal{S}_N^3 = \{(s_0, s_N, s_{2N}) \in \mathcal{S}^3 : \phi(s_N) - \phi(s_0) \equiv \phi(s_{2N}) - \phi(s_N) \equiv N \pmod{\mathbf{p}}\}. \quad (12)$$

Further denote, for fixed  $N$  clear from the context,

$$\pi(s_0, s_N, s_{2N}) \triangleq \mathbb{P}(S_0 = s_0, S_N = s_N, S_{2N} = s_{2N}). \quad (13)$$

**Lemma 4.** There exists  $N_0$  and  $\mu > 0$  such that for all  $N \geq N_0$  and all  $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3$  we have  $\pi(s_0, s_N, s_{2N}) > \mu$ .

For a given  $0 \leq \Delta < \mathbf{d}$ ,  $N = 2^n \geq \mathbf{d}$ , and  $1 \leq i \leq N$ , we follow [6, sec. VI.B] and define for  $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ ,

$$\alpha(s_0, s_N, s_{2N}) \triangleq H(U_i + V_i|Q_i, R_i, S_0 = s_0, S_N = s_N, S_{2N} = s_{2N}) \quad (14)$$

and

$$\beta(s_0, s_N, s_{2N}) \triangleq \frac{\gamma(s_0, s_N) + \gamma(s_N, s_{2N})}{2}, \quad (15)$$

where

$$\gamma(s_0, s_N) \triangleq H(U_i|Q_i, S_0 = s_0, S_N = s_N). \quad (16)$$

By stationarity,  $\gamma(s_N, s_{2N}) = H(V_i|R_i, S_N = s_N, S_{2N} = s_{2N})$ .

The following is the analog of [6, Lemma 16] for our setting.

**Lemma 5.** Let  $N = 2^n \geq \max\{N_0, \mathbf{d}\}$ , for  $N_0$  as in Lemma 4. For  $0 \leq \Delta < \mathbf{d}$  and  $1 \leq i \leq N$  fixed

$$\hat{H}_n^-(\Delta) \geq \mathbf{d} \cdot \sum_{(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)} \pi(s_0, s_N, s_{2N}) \cdot \alpha(s_0, s_N, s_{2N}), \quad (17)$$

and

$$\hat{H}_n(\Delta) = \mathbf{d} \cdot \sum_{(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)} \pi(s_0, s_N, s_{2N}) \cdot \beta(s_0, s_N, s_{2N}). \quad (18)$$

Furthermore, for all  $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$ ,

$$\alpha(s_0, s_N, s_{2N}) \geq \beta(s_0, s_N, s_{2N}). \quad (19)$$

Recall from (3) the factorization  $\mathbf{p} = \mathbf{d} \cdot \mathbf{q}$ , where  $\mathbf{d}$  is a power of 2 and  $\mathbf{q}$  is odd, this is the key for proving the periodic analog of [6, Lemma 17], below.

**Lemma 6.** For every  $0 < \epsilon < 1$  there exists  $\Theta = \Theta(\epsilon) > 0$ , for which the following holds. Let  $N = 2^n \geq \max\{N_0, \mathbf{d}\}$ , where the Euler totient of  $\mathbf{q}$  divides  $n$ , and  $N_0$  is as promised in Lemma 4. Fix  $0 \leq \Delta < \mathbf{d}$  and  $1 \leq i \leq N$ . Then, if  $\epsilon \leq \hat{H}_n(\Delta) \leq 1 - \epsilon$ , there exist  $(s_0, s_N, s_{2N}) \in \mathcal{S}_N^3(\Delta)$  such that

$$\alpha(s_0, s_N, s_{2N}) > \beta(s_0, s_N, s_{2N}) + \Theta. \quad (20)$$

**Corollary 7.** Fix  $0 < \epsilon < 1$ . There exists  $\tau(\epsilon) > 0$  such that the following holds. If  $N = 2^n$  is as in Lemma 6,  $0 \leq \Delta < \mathbf{d}$ ,  $1 \leq i \leq N$ , and  $\epsilon \leq \hat{H}_n(\Delta) \leq 1 - \epsilon$ , then

$$\hat{H}_n^-(\Delta) - \hat{H}_n(\Delta) > \tau(\epsilon).$$

*Proof:* Take  $\tau(\epsilon) = \mu \cdot \mathbf{d} \cdot \Theta(\epsilon)$ , where  $\mu$  is as promised in Lemma 4 and  $\Theta(\epsilon)$  is as promised in Lemma 6. ■

Following is an adaptation of [20, Theorem 1] to our case; its proof relies on Corollary 7.

**Lemma 8.** The random variable  $\hat{H}_\infty(\Delta)$  is a  $\{0, 1\}$  random variable with probability 1.

The following lemma states that fixing the initial phase does not change the entropy rate.

**Lemma 9.** For  $0 \leq \varphi < \mathbf{p}$ , we have

$$\lim_{N \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N) = \lim_{N \rightarrow \infty} \frac{1}{N} H(X_1^N | Y_1^N, \phi(S_0) = \varphi).$$

*Proof:* By (8), we have  $H(X_1^N | Y_1^N) \simeq H(X_1^N | Y_1^N, \phi(S_0))$ , by taking  $A$  as the always true event. Thus, our aim is to show that for any  $0 \leq \varphi < \mathbf{p}$ ,

$$H(X_1^N | Y_1^N, \phi(S_0)) \simeq H(X_1^N | Y_1^N, \phi(S_0) = \varphi).$$

By stationarity, we have  $\mathbb{P}(\phi(S_0) = -\varphi' \pmod{\mathbf{p}}) = 1/\mathbf{p}$  for any  $0 \leq \varphi' < \mathbf{p}$ . Thus,

$$H(X_1^N | Y_1^N, \phi(S_0)) = \sum_{\varphi'=0}^{\mathbf{p}-1} \frac{1}{\mathbf{p}} H(X_1^N | Y_1^N, \phi(S_0) = -\varphi' \pmod{\mathbf{p}}). \quad (21)$$

Recall that  $\varphi$  is fixed. For a given  $0 \leq \varphi' \leq \mathbf{p}$ , denote  $\psi = \varphi' + \varphi$ . Note that  $\psi \geq 0$ . We have

$$\begin{aligned} H(X_1^N | Y_1^N, \phi(S_0) \equiv -\varphi' \pmod{\mathbf{p}}) & \stackrel{(a)}{\simeq} H(X_1^N | Y_1^N, S_\psi, S_N, \phi(S_0) \equiv -\varphi' \pmod{\mathbf{p}}) \\ & = H(X_1^N | Y_1^N, S_\psi, S_N, \phi(S_\psi) = \varphi) \\ & \stackrel{(b)}{=} H(X_1^N | Y_1^{N+\psi}, S_\psi, S_N, \phi(S_\psi) = \varphi) \\ & \stackrel{(c)}{\simeq} H(X_1^{N+\psi} | Y_1^{N+\psi}, S_\psi, S_N, \phi(S_\psi) = \varphi) \\ & \stackrel{(d)}{\simeq} H(X_{\psi+1}^{N+\psi} | Y_1^{N+\psi}, S_\psi, S_N, \phi(S_\psi) = \varphi) \\ & \stackrel{(e)}{=} H(X_{\psi+1}^{N+\psi} | Y_{\psi+1}^{N+\psi}, S_\psi, S_N, \phi(S_\psi) = \varphi) \\ & \stackrel{(f)}{\simeq} H(X_{\psi+1}^{N+\psi} | Y_{\psi+1}^{N+\psi}, \phi(S_\psi) = \varphi) \\ & \stackrel{(g)}{=} H(X_1^N | Y_1^N, \phi(S_0) = \varphi), \end{aligned}$$

where (a) is by the RHS of (8) since the number of states is finite; (b) is by the Markov property; (c) is by the LHS of (8) since we have added a finite number  $\psi$  of binary random

variables; (d) is again by the LHS of (8), now removing a finite number  $\psi$  of binary random variables; (e) is by the Markov property; (f) is by the RHS of (8); and (g) is by stationarity.

We have shown that  $H(X_1^N|Y_1^N, \phi(S_0) = -\varphi' \bmod \mathfrak{p}) \simeq H(X_1^N|Y_1^N, \phi(S_0) = \varphi)$ . By (21),  $H(X_1^N|Y_1^N, \phi(S_0)) \simeq H(X_1^N|Y_1^N, \phi(S_0) = \varphi)$ , completing the proof. ■

The following proposition establishes slow polarization. It is in a similar vein to [6, Theorem 20]

**Proposition 10.** *For  $0 \leq \Delta < \mathfrak{d}$ ,  $0 < \epsilon < 1$ , and  $N = 2^n$ , the following holds:*

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : H(U_i|U_1^{i-1}, Y_1^N, D(\Delta)) < \epsilon\} \right| \quad (22a)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : H(U_i|U_1^{i-1}, Y_1^N, S_0, S_N, D(\Delta)) < \epsilon\} \right| \quad (22b)$$

$$= 1 - \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N|Y_1^N, S_0, S_N, D(\Delta)) \quad (22c)$$

$$= 1 - \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N|Y_1^N, D(\Delta)) \quad (22d)$$

$$= 1 - \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N|Y_1^N) \quad (22e)$$

and

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : H(U_i|U_1^{i-1}, Y_1^N, D(\Delta)) > 1 - \epsilon\} \right| \quad (23a)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : H(U_i|U_1^{i-1}, Y_1^N, S_0, S_N, D(\Delta)) > 1 - \epsilon\} \right| \quad (23b)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N|Y_1^N, S_0, S_N, D(\Delta)) \quad (23c)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N|Y_1^N, D(\Delta)) \quad (23d)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{N} H(X_1^N|Y_1^N). \quad (23e)$$

#### IV. PROOF OF FAST POLARIZATION

To prove fast polarization, we first define  $M(\Delta)$  for all  $0 \leq \Delta < \mathfrak{d}$ ,

$$M(\Delta) = \frac{1}{\mathfrak{d} \cdot \min\{\pi_s : s \in \mathcal{S}(\Delta)\}}. \quad (24)$$

Recall that for any  $s$ , we have by irreducibility and stationarity that  $\pi_s > 0$ , and hence  $M(\Delta)$  is well defined (the denominator is positive). The utility of  $M(\Delta)$  is seen in the next lemma, which allows us to bound the probability of two dependent events by their marginal probabilities.

**Lemma 11.** *Fix  $0 \leq \Delta < \mathfrak{d}$  and  $N = 2^n \geq \mathfrak{d}$ . Let  $A, B \subseteq \mathcal{X}^N \times \mathcal{Y}^N$ . Then,*

$$\begin{aligned} & \mathbb{P} \left( (X_1^N, Y_1^N) \in A \quad \text{and} \quad (X_{N+1}^{2N}, Y_{N+1}^{2N}) \in B \middle| D(\Delta) \right) \\ & \leq M(\Delta) \cdot \mathbb{P} \left( (X_1^N, Y_1^N) \in A \middle| D(\Delta) \right) \\ & \quad \cdot \mathbb{P} \left( (X_{N+1}^{2N}, Y_{N+1}^{2N}) \in B \middle| D(\Delta) \right). \end{aligned} \quad (25)$$

Recall the definitions of  $U_i, V_i, Q_i, R_i$  from Section II. For a given  $0 \leq \Delta < \mathfrak{d}$ ,  $N = 2^n$ , and  $1 \leq i \leq N$ , denote

$$Z_n(\Delta) = Z(U_i|Q_i, D(\Delta))$$

$$Z_n^-(\Delta) = Z(U_i + V_i|Q_i, R_i, D(\Delta))$$

$$Z_n^+(\Delta) = Z(V_i|U_i + V_i, Q_i, R_i, D(\Delta))$$

and

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

$$\hat{K}_n^-(\Delta) = K(U_i + V_i|Q_i, R_i, S_0, S_{2N}, D(\Delta))$$

$$\hat{K}_n^+(\Delta) = K(V_i|U_i + V_i, Q_i, R_i, S_0, S_{2N}, D(\Delta)).$$

**Lemma 12.** *Fix  $0 \leq \Delta < \mathfrak{d}$ ,  $N = 2^n \geq \mathfrak{d}$ , and  $1 \leq i \leq N$ . Then,  $Z_n^-(\Delta) \leq 2 \cdot M(\Delta) \cdot Z_n(\Delta)$  and  $Z_n^+(\Delta) \leq M(\Delta) \cdot (Z_n(\Delta))^2$ .*

*Proof sketch:* This is an extension of [4, Section VI] for our scenario. ■

**Lemma 13.** *Fix  $0 \leq \Delta < \mathfrak{d}$ ,  $N = 2^n \geq \mathfrak{d}$ , and  $1 \leq i \leq N$ . Then,  $\hat{K}_n^-(\Delta) \leq \mathfrak{d} \cdot M(\Delta) \cdot (\hat{K}_n(\Delta))^2$  and  $\hat{K}_n^+(\Delta) \leq 2 \cdot \hat{K}_n(\Delta)$ .*

*Proof sketch:* This is an extension of [5, Proposition 12] to our scenario. ■

The following proposition establishes fast polarization. Note that this is not yet Theorem 1, since that requires conditioning on a finer event than  $D(\Delta)$ .

**Proposition 14.** *Fix  $0 < \beta < 1/2$  and  $0 \leq \Delta < \mathfrak{d}$ . Then, for  $N = 2^n$ ,*

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : Z(U_i|Q_i, D(\Delta)) < 2^{-N^\beta}\} \right| = 1 - \mathcal{H}_{X|Y}, \quad (26)$$

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : K(U_i|Q_i, S_0, S_N, D(\Delta)) < 2^{-N^\beta}\} \right| = \mathcal{H}_{X|Y}. \quad (27)$$

*Proof:* We prove fast polarization using [21, Proposition 49]. We first concentrate on (26). By Lemma 12, the process  $Z_n(\Delta)$  satisfies [21, Equation 167], with  $\kappa = 2M(\Delta)$ . This also holds if we offset our process to start at some  $n'$  instead of 0. As a shorthand, we write  $Z_n$  in place of  $Z_n(\Delta)$  in the sequel.

Fix  $\delta > 0$ . Thus, [21, Proposition 49] implies that there exist  $\eta > 0$  and  $n_0$  such that for  $\beta' = (\beta + 1/2)/2$ ,

$$\mathbb{P} \left( Z_{n+n'} \leq 2^{-2^{n\beta'}} \text{ for all } n \geq n_0 \middle| Z_{n'} \leq \eta \right) \geq 1 - \delta/2.$$

We now show that we can choose  $n'$  such that

$$\mathbb{P}(Z_{n'} \leq \eta) > 1 - \mathcal{H}_{X|Y} - \delta/2. \quad (28)$$

This will imply that

$$\mathbb{P} \left( Z_{n+n'} \leq 2^{-2^{n\beta'}} \text{ for all } n \geq n_0, Z_{n'} \leq \eta \right) > 1 - \mathcal{H}_{X|Y} - \delta.$$

Hence,

$$\mathbb{P} \left( Z_{n+n'} \leq 2^{-2^{n\beta'}} \text{ for all } n \geq n_0 \right) > 1 - \mathcal{H}_{X|Y} - \delta.$$

This implies that

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \{i : Z(U_i|Q_i, D(\Delta)) < 2^{-N^\beta}\} \right| \geq 1 - \mathcal{H}_{X|Y} \quad (29)$$

since  $\beta' > \beta$  and  $\delta > 0$  is arbitrary. All that remains to prove (26), is to show that the above “ $\geq$ ” is in fact an equality. We will come back to this point later.

To prove (28), we call upon Proposition 10 with  $\epsilon = \sqrt{\eta}$ . By, (22a), (22e), and (1),

$$\lim_{n \rightarrow \infty} \mathbb{P}(H_n(\Delta) < \sqrt{\eta}) = 1 - \mathcal{H}_{X|Y}.$$

Thus, there exists  $n'$  such that

$$\mathbb{P}(H_{n'}(\Delta) < \sqrt{\eta}) = 1 - \mathcal{H}_{X|Y} - \delta/2.$$

By [5, Lemma 1],  $H_{n'}(\Delta) < \sqrt{\eta}$  implies  $Z_{n'} < \eta$ , which establishes (28).

We now concentrate on (27). By Lemma 13, the process  $\hat{K}_n(\Delta)$  satisfies [21, Equation 167], with  $\kappa = \max\{\mathbf{d}M(\Delta), 2\}$ . Thus, by a similar reasoning as above we obtain

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : \hat{K}(U_i|Q_i, S_0, S_N, D(\Delta)) < 2^{-N^\beta} \right\} \right| \geq \mathcal{H}_{X|Y}. \quad (30)$$

To complete the proof, we now show that the weak inequalities in (29) and (30) are in fact equalities. To see this, first note by [5, Lemma 2] that  $Z(U_i|Q_i, S_0, S_N, D(\Delta)) \leq Z(U_i|Q_i, D(\Delta))$ . Hence, (29) implies that

$$\lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : Z(U_i|Q_i, S_0, S_N, D(\Delta)) < 2^{-N^\beta} \right\} \right| \geq 1 - \mathcal{H}_{X|Y}, \quad (31)$$

and a strict inequality in (29) implies a strict inequality in (31). Now, assume to the contrary a strict inequality in either (29) or (30), or both. This implies a strict inequality in either (31) or (30), or both. Thus, for all  $N$  large enough, there must exist an index  $0 \leq i < N$ , such that

$$\begin{aligned} Z(U_i|Q_i, S_0, S_N, D(\Delta)) &< 2^{-N^\beta}, \\ K(U_i|Q_i, S_0, S_N, D(\Delta)) &< 2^{-N^\beta}. \end{aligned}$$

This cannot hold, since  $K + Z \geq 1$ , by [5, Lemma 1]. ■

## V. PROOF OF THEOREM 1

The following technical lemma will be used in our proof of Theorem 1.

**Lemma 15.** *Let  $U$  be a binary random variable;  $W, Q$  general random variables; and  $A_1, A_2, \dots, A_\ell$  mutually exclusive events. Denote  $C = A_1 \cup A_2 \cup \dots \cup A_\ell$ . Then,*

$$Z(U|Q, C) \geq \sum_{j=1}^{\ell} \mathbb{P}(A_j|C) Z(U|Q, A_j), \quad (32)$$

$$K(U|Q, C) \leq \sum_{j=1}^{\ell} \mathbb{P}(A_j|C) K(U|Q, A_j), \quad (33)$$

$$H(W|Q, C) \geq \sum_{j=1}^{\ell} \mathbb{P}(A_j|C) H(W|Q, A_j). \quad (34)$$

*Proof of Theorem 1:* Recall the factorization (3),  $\mathbf{p} = \mathbf{d} \cdot \mathbf{q}$ , where  $\mathbf{q}$  is odd and  $\mathbf{d}$  is a power of 2. Recall that  $\varphi$  is the common phase of all the vertices in  $\Psi_0$  and denote  $\Delta = \varphi \bmod \mathbf{d}$ . Next, note that by (6) that for  $N = 2^n \geq \mathbf{d}$  we have for all  $(s_0, s_N) \in \Psi_0 \times \Psi_N$  that  $(s_0, s_N) \in \mathcal{S}_N^2(\Delta)$ .

Proposition 14 with  $\beta' = (\beta + 1/2)/2$  in place of  $\beta$  implies that

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : Z(U_i|U_1^{i-1}, Y_1^N, D(\Delta)) < 2^{-N^\beta} \right\} \right| &= 1 - \mathcal{H}_{X|Y}, \\ \lim_{n \rightarrow \infty} \frac{1}{N} \left| \left\{ i : K(U_i|U_1^{i-1}, S_0, S_N, D(\Delta)) < 2^{-N^\beta} \right\} \right| &= \mathcal{H}_X. \end{aligned}$$

Note that the second equality is obtained by considering the case in which the  $Y$  are constant, and hence nothing is gained by conditioning on them. The proof of Theorem 1 will follow by showing that there is some  $\xi > 0$  independent of  $N$  and  $0 \leq i < N$  such that

$$Z(U_i|U_1^{i-1}, Y_1^N, A) \leq \xi \cdot Z(U_i|U_1^{i-1}, Y_1^N, D(\Delta)) \quad (35)$$

and

$$K(U_i|U_1^{i-1}, A) \leq \xi \cdot K(U_i|U_1^{i-1}, S_0, S_N, D(\Delta)), \quad (36)$$

for  $N = 2^n$  large enough. Indeed, we claim that  $\xi = \frac{1}{\mu \cdot \mathbf{d}}$  suffices for  $N \geq N_0$ , where  $\mu$  and  $N_0$  are as promised by Lemma 4.

For compactness, denote  $\Psi_{0,N} \triangleq \Psi_0 \times \Psi_N$ . To show (35) we apply Lemma 15 with

$$\begin{aligned} C &= \{(S_0, S_N) \in \mathcal{S}_N^2(\Delta)\}, \\ A_1 &= \{(S_0, S_N) \in \Psi_{0,N}\}, \\ A_2 &= \{(S_0, S_N) \in \mathcal{S}_N^2(\Delta) \setminus \Psi_{0,N}\}. \end{aligned}$$

Note that by definition  $C$  and  $A_1$  are simply  $D(\Delta)$  and  $A$ , respectively. Thus,

$$\begin{aligned} Z(U_i|U_1^{i-1}, Y_1^N, D(\Delta)) &\stackrel{(a)}{\geq} \mathbb{P}(A_1|D(\Delta)) Z(U_i|U_1^{i-1}, Y_1^N, A_1) \\ &\quad + \mathbb{P}(A_2|D(\Delta)) Z(U_i|U_1^{i-1}, Y_1^N, A_2) \\ &\stackrel{(b)}{\geq} \mathbb{P}(A|D(\Delta)) Z(U_i|U_1^{i-1}, Y_1^N, A) \\ &= \mathbb{P}((S_0, S_N) \in \Psi_{0,N}|D(\Delta)) \cdot Z(U_i|U_1^{i-1}, Y_1^N, A) \\ &= \frac{\mathbb{P}((S_0, S_N) \in \Psi_{0,N})}{\mathbb{P}(D(\Delta))} Z(U_i|U_1^{i-1}, Y_1^N, A) \\ &\stackrel{(c)}{\geq} \mu \cdot \mathbf{d} \cdot Z(U_i|U_1^{i-1}, Y_1^N, A) \\ &= \xi^{-1} \cdot Z(U_i|U_1^{i-1}, Y_1^N, A) \end{aligned}$$

where (a) is by (32), (b) is since  $A_1 = A$  and probabilities are nonnegative, and (c) is by (5) and Lemma 4. This yields (35).

To show (36), we apply Lemma 15 with

$$\begin{aligned} C &= \{(S_0, S_N) \in \Psi_{0,N}\}, \\ A_{s_0, s_N} &= \{(S_0, S_N) = (s_0, s_N)\}, \end{aligned}$$

where in the above  $(s_0, s_N)$  range over  $\Psi_{0,N}$ . Note that in this case,  $C = A$ , and clearly  $C = \cup_{(s_0, s_N) \in \Psi_{0,N}} A_{s_0, s_N}$ . Thus,

$$\begin{aligned} K(U_i|U_1^{i-1}, A) &= K(U_i|U_1^{i-1}, C) \\ &\stackrel{(a)}{\leq} \sum_{s_0, s_N} \mathbb{P}(A_{s_0, s_N}|C) K(U_i|U_1^{i-1}, S_0 = s_0, S_N = s_N) \\ &\stackrel{(b)}{=} \sum_{s_0, s_N} \frac{\mathbb{P}(A_{s_0, s_N})}{\mathbb{P}(C)} K(U_i|U_1^{i-1}, S_0 = s_0, S_N = s_N) \\ &\stackrel{(c)}{=} \sum_{s_0, s_N} \frac{\mathbb{P}(A_{s_0, s_N}, D(\Delta))}{\mathbb{P}(C)} K(U_i|U_1^{i-1}, S_0 = s_0, S_N = s_N) \\ &= \sum_{s_0, s_N} \frac{\mathbb{P}(A_{s_0, s_N}|D(\Delta))}{\mathbb{P}(D(\Delta))^{-1} \mathbb{P}(C)} K(U_i|U_1^{i-1}, S_0 = s_0, S_N = s_N) \\ &\stackrel{(d)}{\leq} \frac{1}{\mu \cdot \mathbf{d}} \sum_{s_0, s_N} \mathbb{P}(A_{s_0, s_N}|D(\Delta)) K(U_i|U_1^{i-1}, S_0 = s_0, S_N = s_N), \\ &= \xi \cdot K(U_i|U_1^{i-1}, S_0, S_N, D(\Delta)), \end{aligned}$$

where (a) is by (33), (b) is since  $A_{s_0, s_N} \subseteq C$ , (c) is since  $A_{s_0, s_N} \subseteq D(\Delta)$ , and (d) is by (5) and Lemma 4. This yields (36), completing the proof. ■

## REFERENCES

- [1] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.
- [2] —, "Source polarization," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2010)*, Austin, Texas, 2010, pp. 899–903.

- [3] E. Şaçoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," *arXiv:0908.0302v1*, 2009.
- [4] E. Şaçoğlu and I. Tal, "Polar coding for processes with memory," *IEEE Trans. Inform. Theory*, vol. 65, no. 4, pp. 1994–2003, April 2019.
- [5] B. Shuval and I. Tal, "Fast polarization for processes with memory," *IEEE Trans. Inform. Theory*, vol. 65, no. 4, pp. 2004–2020, April 2019.
- [6] I. Tal, H. D. Pfister, A. Fazeli, and A. Vardy, "Polar codes for the deletion channel: weak and strong polarization," *IEEE Trans. Inform. Theory*, vol. 68, no. 4, pp. 2239–2265, April 2022.
- [7] H. D. Pfister and I. Tal, "Polar codes for channels with insertions, deletions, and substitutions," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2021)*, Melbourne, Victoria, Australia, 2021, pp. 2554–2559.
- [8] D. Arava and I. Tal, "Stronger polarization in the deletion channel," in *Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2023)*, Taipei, Taiwan, 2023, pp. 1711–1716.
- [9] H. Mahdaviifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inform. Theory*, vol. 57, pp. 6428–6443, 2011.
- [10] H. Mahdaviifar, "Polar coding for non-stationary channels," *IEEE Trans. Inform. Theory*, vol. 66, pp. 6920–6938, 2020.
- [11] E. Hof and S. Shamai, "Secrecy-achieving polar-coding for binary-input memoryless symmetric wire-tap channels," *arXiv:1005.2759v2*, 2010.
- [12] E. Hof, I. Sason, S. Shamai (Shitz), and C. Tian, "Capacity-achieving polar codes for arbitrarily permuted parallel channels," *IEEE Trans. Inform. Theory*, vol. 59, March 2013.
- [13] B. Shuval and I. Tal, "Constant weight polar codes through periodic markov processes," *arXiv:2501.12379*, 2025.
- [14] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, UK: Cambridge University Press, 1985.
- [15] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric channels," *IEEE Trans. Inform. Theory*, vol. 59, no. 12, pp. 7829–7838, December 2012.
- [16] R. Wang, J. Honda, H. Yamamoto, R. Liu, and Y. Hou, "Construction of polar codes for channels with memory," in *Proc. IEEE Inform. Theory Workshop (ITW'2015)*, Jeju Island, Korea, 2015, pp. 187–191.
- [17] J. Honda and H. Yamamoto, "Variable-to-fixed length homophonic coding with a modified shannon-fano-elias code," *arXiv:1607.06914v1*, 2016.
- [18] E. Şaçoğlu, "Polarization and polar codes," in *Found. and Trends in Commun. and Inform. Theory*, vol. 8, no. 4, 2012, pp. 259–381.
- [19] J. S. Rosenthal, *A first look at rigorous probability theory*. New Jersey, London, Singapore, Beijing, Shanghai, Hong Kong, Taipei, Chennai: World Scientific, 2006.
- [20] E. Şaçoğlu, "Polar coding theorems for discrete systems," Ph.D. dissertation, Ecole Polytechnique Fédérale de Lausanne, 2011.
- [21] B. Shuval and I. Tal, "Universal polarization for processes with memory," *Accepted for publication in IEEE Trans. Inform. Theory*, 2025, available online at <https://ieeexplore.ieee.org/document/10836796>.