Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes

Rémi A. Chou[1] and Matthieu R. Bloch[2]

***Abstract*— We show how to replace some of the randomized decisions in the encoding and decoding of polar codes by deterministic decisions. Specifically, we prove that random decisions on low-entropy bits may be replaced by an argmax decision without any loss of performance. We illustrate the usefulness of this result in the case of polar coding for the Wyner-Ziv problem and for channel coding.**

I. Introduction

Although polar codes possess low-complexity encoders and decoders, their operation often requires the use of many bits of shared randomness [1]. In the following, we show how to further simplify their implementation by using *deterministic* decisions in place of the *random* decisions for the low-entropy bits in the encoding and decoding. Intuitively, the random choice of low-entropy bits is heavily biased so that a deterministic decision, e.g., an argmax rule, should have little impact on their performance. In fact, Arıkan already proved this intuition correct for lossless source coding [2]. However, as further discussed in the next section, the proof technique does not directly extend to more advanced settings.

The remainder of the paper is organized as follows. Section II sets the notation for the paper and reformulates Arıkan's result for lossless source coding. Our main technical contribution is Lemma 2 in Section III, which develops a general proof technique for studying the argmax decision for low-entropy bits in polar coding schemes, Section III and Section IV apply this result to Wyner-Ziv coding and channel coding, respectively. Section V concludes the paper with a discussion of the significance of the results.

II. Argmax decision for lossless source coding

In the following, we consider a binary alphabet $\mathcal{X} \triangleq \{0,1\}$ and a countable alphabet $\mathcal{Y}$. For $n \in \mathbb{N}$, we let $G_n \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes n}$ be the source polarization transform defined in [2]. We also define $N \triangleq 2^n$ and for $\beta < 1/2$, $\delta_N \triangleq 2^{-N^\beta}$.

For two distributions p_X, $p_{X'}$, over the same finite alphabet, we note

$$\mathbb{V}(p_X, p_{X'}) \triangleq \sum_x |p_X(x) - p_{X'}(x)|$$

the variational distance between p_X and $p_{X'}$. We note $\mathbb{D}(\cdot||\cdot)$ the divergence between two distributions. For two joint distributions p_{XY} and q_{XY} over the same finite alphabets, we denote the conditional divergence w.r.t. p_X [3], by

$$\mathbb{D}(p_{Y|X}||q_{Y|X}|p_X) \triangleq \sum_{x,y} p_{YX}(y,x) \log \frac{p_{Y|X}(y|x)}{q_{Y|X}(y|x)}.$$

We denote the indicator function by $\mathbb{1}\{\omega\}$, which is equal to 1 if the predicate ω is true and 0 otherwise.

We define the integer interval $[\![a,b]\!]$ as the set of integers between $\lfloor a \rfloor$ and $\lceil b \rceil$. We indicate the length of vector with superscript; for instance, X^N is a vector with N component. For any set $\mathcal{A} \subset [\![1,N]\!]$, we denote by $X^N[\mathcal{A}]$ the components of X^N whose indices are in $\mathcal{A}$. We also define the constant $\gamma \triangleq \sqrt{2\log 2}$.

Consider a Discrete Memoryless Source (DMS) $(\mathcal{X} \times \mathcal{Y}, q_{XY})$. Lossless source coding with side information consists in forming a compressed version M of X^N, such that a decoder is able to reconstruct X^N from (Y^N, M) with vanishing error probability in the limit of large N.

Define $U^N \triangleq X^N G_n$ whose probability distribution is denoted by q_{U^N} and the set

$$\mathcal{H}_{X|Y} \triangleq \left\{ i \in [\![1,N]\!] : H(U_i | U^{i-1} Y^N) > \delta_N \right\}.$$

Let $\widetilde{U}^N$ be defined by $\widetilde{p}_{U^N} \triangleq \prod_{i=1}^N \widetilde{p}_{U_j|U^{j-1}}$, with

$$\widetilde{p}_{U_j|U^{j-1}}(\widetilde{u}_j|\widetilde{u}^{j-1}) \triangleq \begin{cases} \mathbb{1}\{\widetilde{u}_j = U_j\} & \text{if } j \in \mathcal{H}_{X|Y} \\ \mathbb{1}\{\widetilde{u}_j = u^*\} & \text{if } j \in \mathcal{H}_{X|Y}^c \end{cases}, \quad (1)$$

where $u^* \triangleq \operatorname{argmax}_u q_{U_j|Y^N U^{j-1}}(u|Y^N \widetilde{u}^{j-1})$.

Encoding and decoding are performed as follows.

- **Encoding**: Form U^N from X^N and return $U^N[\mathcal{H}_{X|Y}]$.
- **Decoding**: From $(U^N[\mathcal{H}_{X|Y}], Y^N)$ form $\widetilde{U}^N$ as in (1).

In other words, $\widetilde{U}^N$ is constructed from the "high-entropy" bits $U^N[\mathcal{H}_{X|Y}]$ and by deterministically choosing the remaining "low-entropy" bits $U^N[\mathcal{H}_{X|Y}^c]$ with an argmax decision.

Theorem 1 (Adapted from [2]): Assume that U^N and $\widetilde{U}^N$ are drawn from q_{U^N} and $\widetilde{p}_{U^N}$. Then, the encoding rate is asymptotically optimal, i.e.,

$$\lim_{N\to\infty} |\mathcal{H}_{X|Y}|/N = H(X|Y).$$

With high probability, U^N and $\widetilde{U}^N$ are identical, i.e.,

$$\mathbb{P}[\widetilde{U}^N \neq U^N] \leqslant N\delta_N.$$

This work was supported in part by NSF grants CCF-1320304 and ANR 13-BS03-0008.

[1] Rémi A. Chou is with with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332–0250 and with GT-CNRS UMI 2958, Metz, France remi.chou@gatech.edu

[2] Matthieu R. Bloch is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332–0250 and with GT-CNRS UMI 2958, Metz, France matthieu.bloch@ece.gatech.edu

The proof technique used in [2], [4] relies on Bhattacharyya parameters. Specifically, it exploits the fact that $\widetilde{U}^N[\mathcal{H}_{X|Y}]$ is distributed according to q, based on which the set $\mathcal{H}_{X|Y}$ is defined. Unfortunately, this technique does not seem to extend directly to more advanced settings, specifically those for which the encoder uses a random variable whose distribution only *approximates* the original distribution q, as is the case in Sections III, IV.

Remark 1: Define the set

$$\mathcal{V}_{X|Y} \triangleq \left\{ i \in [\![1, N]\!] : H(U_i|U^{i-1}Y^N) > 1 - \delta_N \right\}.$$

Although $\mathcal{V}_{X|Y} \subset \mathcal{H}_{X|Y}$ and $|\mathcal{V}_{X|Y} \backslash \mathcal{H}_{X|Y}| = o(N)$ by [5, Lemma 1], the decoder will fail if it only has access to $(U^N[\mathcal{V}_{X|Y}], Y^N)$ instead of $(U^N[\mathcal{H}_{X|Y}], Y^N)$. Indeed, if the decoder succeeds then, X^N can be lossessly compressed, and its compressed version $U^N[\mathcal{V}_{X|Y}]$ is nearly uniform in variational distance (see [5] for a proof), which is impossible by [6].

III. Argmax decision for Wyner-Ziv coding

Wyner-Ziv coding for a DMS $(\mathcal{X} \times \mathcal{Y}, q_{XY})$ consists in compressing X^N into a message M, such that a decoder is able to reconstruct X^N within a given distortion D from Y^N and M in the limit of large N. The smallest required message rate is known and completely characterized by the following result.

Theorem 2 ([7]): Consider a DMS $(\mathcal{X} \times \mathcal{Y}, q_{XY})$, a reconstruction alphabet $\mathcal{V}$, and a distortion measure $d : \mathcal{X} \times \mathcal{V} \to \mathbb{R}^+$. The rate-distortion function for Wyner-Ziv coding is given by

$$R(D) = \min_{q_{V|X}, f \colon \mathbb{E}[d(X, f(V,Y))] \leqslant D} I(X; V|Y).$$

We note that a Wyner-Ziv polar coding scheme for binary symmetric and additive sources has already been proposed in [8], for which the symmetry assumption removes the need for common randomness. Polar coding schemes for lossy source coding have also been developed in [1], [8] assuming encoder and decoder share common randomness. We develop next a polar coding scheme that results in significant savings of common randomness.

A. Proposed coding scheme

Consider a DMS $(\mathcal{X} \times \mathcal{Y} \times \mathcal{V}, q_{XYV})$ such that $V - X - Y$ forms a Markov chain and $(q_{V|X}, f)$ achieves $R(D)$ defined in Theorem 2. Define $U^N \triangleq V^N G_n$, as well as the sets

$$\begin{aligned} \mathcal{H}_V &\triangleq \left\{ i \in [\![1, N]\!] : H(U_i|U^{i-1}) > \delta_N \right\}, \\ \mathcal{H}_{V|Y} &\triangleq \left\{ i \in [\![1, N]\!] : H(U_i|U^{i-1}Y^N) > \delta_N \right\}, \\ \mathcal{H}_{V|X} &\triangleq \left\{ i \in [\![1, N]\!] : H(U_i|U^{i-1}X^N) > \delta_N \right\}, \\ \mathcal{V}_{V|X} &\triangleq \left\{ i \in [\![1, N]\!] : H(U_i|U^{i-1}X^N) > 1 - \delta_N \right\}. \end{aligned}$$

Assume that encoder and decoder share a sequence C^* of $|\mathcal{V}_{V|X}|$ uniform bits. We show later that C^* may be reused over several encoding blocks so that the rate of shared randomness vanishes with the blocklength. Our proposed scheme for Wyner-Ziv coding is then the following.

Encoding. From X^N and C^*, form $\widetilde{U}^N$ defined by the joint distribution $\widetilde{p}_{U^N X^N} \triangleq \left(\prod_{i=1}^{N} \widetilde{p}_{U_j|U^{j-1}X^N} \right) q_{X^N}$ with

$$\widetilde{p}_{U_j|U^{j-1}X^N}(u_j|u^{j-1}x^N) \triangleq \begin{cases} q_{U_j|U^{j-1}X^N}(u_j|u^{j-1}x^N) & \text{if } j \in \mathcal{H}_V \backslash \mathcal{V}_{V|X} \\ \mathbb{1}\{u_j = C_j^*\} & \text{if } j \in \mathcal{V}_{V|X} \\ \mathbb{1}\{u_j = \operatorname*{argmax}_u q_{U_j|U^{j-1}}(u|u^{j-1})\} & \text{if } j \in \mathcal{H}_V^c, \end{cases} \tag{2}$$

where the components of C^* have been indexed by the set of indices $\mathcal{V}_{V|X}$.
Return $\widetilde{U}^N[\mathcal{H}_{V|Y} \backslash \mathcal{V}_{V|X}]$.

Decoding. Form an estimate $\widehat{U}^N$ of $\widetilde{U}^N$ from $(\widetilde{U}^N[\mathcal{H}_{V|Y} \backslash \mathcal{V}_{V|X}], C^*, Y^N) = (\widetilde{U}^N[\mathcal{H}_{V|Y}], Y^N)$ using the successive cancellation decoder for lossless source coding described in Section II.

Note that Theorem 1 does not guarantee decoding success because $\widetilde{U}^N[\mathcal{H}_{V|Y}]$ does not necessarily have the same distribution as $U^N[\mathcal{H}_{V|Y}]$. Consequently, the properties of $\mathcal{H}_{V|Y}$ that hold for U^N do not necessarily hold for $\widetilde{U}^N$.

B. Scheme analysis and result

Consider the random variable $\overline{U}^N$ that would be obtained in place of $\widetilde{U}^N$ when using randomized encoding in place of the argmax decision. Specifically, $\overline{U}^N$ is defined by $\overline{p}_{U^N X^N} \triangleq \left(\prod_{i=1}^{N} \overline{p}_{U_j|U^{j-1}X^N} \right) q_{X^N}$ with

$$\overline{p}_{U_j|U^{j-1}X^N}(u_j|u^{j-1}x^N) \triangleq \begin{cases} q_{U_j|U^{j-1}X^N}(u_j|u^{j-1}x^N) & \text{if } j \in \mathcal{H}_V \backslash \mathcal{V}_{V|X} \\ \mathbb{1}\{u_j = C_j^*\} & \text{if } j \in \mathcal{V}_{V|X} \\ q_{U_j|U^{j-1}}(u_j|u^{j-1}) & \text{if } j \in \mathcal{H}_V^c \end{cases} \tag{3}$$

Define $\overline{V}^N \triangleq \overline{U}^N G_n$.

Lemma 1: The distribution $\overline{p}_{V^N X^N}$ is nearly indistinguishable from the distribution $q_{V^N X^N}$, in the sense that

$$\mathbb{V}(q_{V^N X^N}, \overline{p}_{V^N X^N}) \leqslant \delta_N^{(1)},$$

where $\delta_N^{(1)} \triangleq \gamma \sqrt{N \delta_N}$.

Proof: We have

$$\begin{aligned} &\mathbb{D}(q_{V^N X^N} || \overline{p}_{V^N X^N}) \\ &\overset{(a)}{=} \mathbb{D}(q_{U^N X^N} || \overline{p}_{U^N X^N}) \\ &\overset{(b)}{=} \mathbb{D}(q_{U^N|X^N} || \overline{p}_{U^N|X^N} | q_{X^N}) \\ &\overset{(c)}{=} \sum_{j=1}^{N} \mathbb{D}(q_{U_j|U^{j-1}X^N} || \overline{p}_{U_j|U^{j-1}X^N} | q_{U^{j-1}X^N}) \end{aligned}$$

$$
\begin{aligned}
&\overset{(d)}{=} \sum_{j \in \mathcal{H}_V^c \cup \mathcal{V}_{V|X}} \mathbb{D}(q_{U_j|U^{j-1}X^N} || \overline{p}_{U_j|U^{j-1}X^N} | q_{U^{j-1}X^N}) \\
&\overset{(e)}{=} \sum_{j \in \mathcal{V}_{V|X}} (1 - H(U_j|U^{j-1}X^N)) \\
&\qquad + \sum_{j \in \mathcal{H}_V^c} (H(U_j|U^{j-1}) - H(U_j|U^{j-1}X^N)) \\
&\leqslant |\mathcal{V}_{V|X}|\delta_N + |\mathcal{H}_V^c|\delta_N \\
&\leqslant N\delta_N,
\end{aligned}
$$

where (a) holds by invertibility of G_n, (b) and (c) hold by the chain rule for divergence [3], (d) and (e) hold by (3). The result follows by Pinsker's inequality. ■

Lemma 2: Let $\widetilde{U}^N$ and $\overline{U}^N$ be drawn from $\widetilde{p}_{U^N}$ and $\overline{p}_{U^N}$, defined in (2) and (3), respectively, and let $\widetilde{V}^N \triangleq \widetilde{U}^N G_n$. Then, $\widetilde{p}_{X^N V^N}$ is asymptotically close to $q_{X^N V^N}$ and $\overline{p}_{X^N V^N}$, in the sense that

$$
\begin{aligned}
\mathbb{V}(\widetilde{p}_{X^N V^N}, \overline{p}_{X^N V^N}) &\leqslant \delta_N^{(2)}, \\
\mathbb{V}(\widetilde{p}_{X^N V^N}, q_{X^N V^N}) &\leqslant \delta_N^{(1)} + \delta_N^{(2)},
\end{aligned}
$$

with $\delta_N^{(2)} \triangleq N\sqrt{\delta_N + 2\delta_N^{(1)}(N - \log \delta_N^{(1)})}$, and $\delta_N^{(1)}$ as in Lemma 1.

Proof: Define a coupling $p_{\overline{X}^N \overline{V}^N \widetilde{X}^N \widetilde{V}^N}$ for $(\overline{X}^N, \overline{V}^N)$ and $(\widetilde{X}^N, \widetilde{V}^N)$ such that $\overline{U}^N[\mathcal{H}_V] = \widetilde{U}^N[\mathcal{H}_V]$ and $\overline{X}^N = X^N = \widetilde{X}^N$. Then, we have

$$
\begin{aligned}
&\mathbb{V}\left(\overline{p}_{U^N X^N}, \widetilde{p}_{U^N X^N}\right) \\
&\quad \overset{(a)}{\leqslant} \mathbb{P}\left[(\overline{U}^N, \overline{X}^N) \neq (\widetilde{U}^N, \widetilde{X}^N)\right] \\
&\quad \overset{(b)}{=} \mathbb{P}\left[\overline{U}^N \neq \widetilde{U}^N\right] \\
&\quad = \mathbb{P}\left[\cup_{i=1}^N \{\overline{U}_i \neq \widetilde{U}_i\}\right] \\
&\quad \leqslant \sum_{i=1}^N \mathbb{P}\left[\overline{U}_i \neq \widetilde{U}_i | \overline{U}^{i-1} = \widetilde{U}^{i-1}\right] \\
&\quad \overset{(c)}{=} \sum_{i \in \mathcal{H}_V^c} \mathbb{P}\left[\overline{U}_i \neq \widetilde{U}_i | \overline{U}^{i-1} = \widetilde{U}^{i-1}\right] \\
&\quad = \mathbb{E}_{\overline{U}^{i-1}}\left[\sum_{i \in \mathcal{H}_V^c} \mathbb{P}\left[\overline{U}_i \neq \widetilde{U}_i | \overline{U}^{i-1} = \widetilde{U}^{i-1}\right]\right] \\
&\quad = \mathbb{E}_{\overline{U}^{i-1}}\left[\sum_{i \in \mathcal{H}_V^c} \left(1 - \sum_i q_{U_i|U^{i-1}}(u_i|\overline{U}^{i-1})\right.\right. \\
&\qquad\qquad \left.\left. \times \mathbb{1}\{u_i = \arg\max_u q_{U_i|U^{i-1}}(u|\overline{U}^{i-1})\}\right)\right] \\
&\quad \overset{(d)}{=} \mathbb{E}_{\overline{U}^{i-1}}\left[\sum_{i \in \mathcal{H}_V^c} \left(1 - q_{U_i|U^{i-1}}(u_i^*|\overline{U}^{i-1})\right)\right] \\
&\quad = \sum_{i \in \mathcal{H}_V^c} \mathbb{E}_{\overline{U}^{i-1}}\left[1 - q_{U_i|U^{i-1}}(u_i^*|\overline{U}^{i-1})\right] \qquad (4)
\end{aligned}
$$

where (a) follows from the coupling Lemma, (b) holds by definition of the coupling p, (c) holds since $\overline{U}^N[\mathcal{H}_V] = \widetilde{U}^N[\mathcal{H}_V]$, (d) holds if we define $u_i^* \triangleq \operatorname{argmax}_u q(u|u^{i-1})$.

Next, for $i \in \mathcal{H}_V^c$ and N large enough, we have

$$
\begin{aligned}
&\left|H(U_i|U^{i-1}) - H(U_i|\overline{U}^{i-1})\right| \\
&\overset{(a)}{\leqslant} \left|H(U^{i-1}) - H(\overline{U}^{i-1})\right| + \left|H(U^i) - H(U_i\overline{U}^{i-1})\right| \\
&\overset{(b)}{\leqslant} 2\mathbb{V}(\bar{p}_{U^{i-1}}, q_{U^{i-1}}) \log \frac{2^N}{\mathbb{V}(\bar{p}_{U^{i-1}}, q_{U^{i-1}})} \\
&\overset{(c)}{\leqslant} 2\delta_N^{(1)}(N - \log \delta_N^{(1)}), \qquad (5)
\end{aligned}
$$

where (a) holds by the triangle inequality, (b) follows from [9, Lemma 2.7] and because $\mathbb{V}(q_{U_i|U^{i-1}}\bar{p}_{U^{i-1}}, q_{U^i}) = \mathbb{V}(\bar{p}_{U^{i-1}}, q_{U^{i-1}})$, (c) holds by Lemma 1 because $x \mapsto x \log x$ is decreasing for $x > 0$ small enough.

For any $i \in \mathcal{H}_V^c$, we have

$$
\begin{aligned}
&2\delta_N^{(1)}(N - \log \delta_N^{(1)}) + \delta_N \\
&\overset{(a)}{\geqslant} 2\delta_N^{(1)}(N - \log \delta_N^{(1)}) + H(U_i|U^{i-1}) \\
&\overset{(b)}{\geqslant} H(U_i|\overline{U}^{i-1}) \\
&= \mathbb{E}_{\overline{U}^{i-1}}\left[-q(u_i^*|\overline{U}^{i-1}) \log q(u_i^*|\overline{U}^{i-1})\right. \\
&\qquad \left. -(1 - q(u_i^*|\overline{U}^{i-1})) \log(1 - q(u_i^*|\overline{U}^{i-1}))\right] \\
&\geqslant \mathbb{E}_{\overline{U}^{i-1}}\left[-(1 - q(u_i^*|\overline{U}^{i-1})) \log(1 - q(u_i^*|\overline{U}^{i-1}))\right], \\
&\overset{(c)}{\geqslant} \mathbb{E}_{\overline{U}^{i-1}}\left[(1 - q(u_i^*|\overline{U}^{i-1}))^2\right] \\
&\overset{(d)}{\geqslant} \left(\mathbb{E}_{\overline{U}^{i-1}}\left[(1 - q(u_i^*|\overline{U}^{i-1}))\right]\right)^2, \qquad (6)
\end{aligned}
$$

where (a) holds because $i \in \mathcal{H}_V^c$, (b) holds by (5), (c) holds because $\forall x \in [0, 1/2[, \log(x) < -x$ and $q(u_i^*|u^{i-1}) \geqslant 1/2$, (d) follows by Jensen's inequality.

Finally, combining (4) and (6) we obtain

$$
\begin{aligned}
&\mathbb{V}\left(\overline{p}_{U^N X^N}, \widetilde{p}_{U^N X^N}\right) \\
&\quad \leqslant \sum_{i \in \mathcal{H}_V^c} \sqrt{2\delta_N^{(1)}(N - \log \delta_N^{(1)}) + \delta_N} \\
&\quad \leqslant N\sqrt{2\delta_N^{(1)}(N - \log \delta_N^{(1)}) + \delta_N}. \qquad (7)
\end{aligned}
$$

Also,

$$
\begin{aligned}
&\mathbb{V}(q_{V^N X^N}, \widetilde{p}_{V^N X^N}) \\
&\quad \overset{(a)}{=} \mathbb{V}(q_{U^N X^N}, \widetilde{p}_{U^N X^N}) \\
&\quad \overset{(b)}{\leqslant} \mathbb{V}(q_{U^N X^N}, \overline{p}_{U^N X^N}) + \mathbb{V}(\overline{p}_{U^N X^N}, \widetilde{p}_{U^N X^N}) \\
&\quad \overset{(c)}{\leqslant} \delta_N^{(1)} + \delta_N^{(2)},
\end{aligned}
$$

where (a) holds by invertibility of G_n, (b) holds by the triangle inequality, (c) holds by Lemma 1 and (7). ■

We are now ready to prove that the coding scheme of Section III-A is successful and optimal.

Theorem 3: Assume that $\widetilde{U}^N$ and $\widehat{U}^N$ are obtained from the encoding decoding scheme of Section III-A.

(i) $\widetilde{U}^N$ and $\widehat{U}^N$ are identical with high probability, i.e.,

$$
\mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N] \leqslant \delta_N^{(3)},
$$

where $\delta_N^{(3)} \triangleq \delta_N^{(1)} + \delta_N^{(2)} + N\delta_N$ with $\delta_N^{(1)}$ and $\delta_N^{(2)}$ as in Lemma 1 and Lemma 2.

(ii) The distortion constraint is satisfied, i.e.,

$$\mathbb{E}_{\widetilde{p}}\left[\frac{1}{N}\sum_{i=1}^{N} d(X_i, f(\widehat{V}_i, Y_i)\right] \leqslant D + \delta_N^{(4)},$$

with $\widehat{V}^N \triangleq \widehat{U}^N G_n$ and $\delta_N^{(4)} \triangleq d_{\max}(\delta_N^{(1)} + \delta_N^{(2)} + \delta_N^{(3)})$.

(iii) The encoding rate is optimal, i.e.,

$$\lim_{N\to\infty} \frac{|\mathcal{H}_{V|Y} \backslash \mathcal{V}_{V|X}|}{N} = I(X;V|Y)$$

(iv) Encoder and decoder may reuse the common randomness C^* over k blocks of size N. Hence, the rate of common randomness is $H(V|X)/k$, which vanishes as k goes to infinity.

Proof: We prove the statements in order.

(i): Consider an optimal coupling [8], [10] between $\widetilde{p}_{U^N}$ and q_{U^N} such that $\mathbb{P}[\mathcal{E}] = \mathbb{V}(\widetilde{p}_{U^N}, q_{U^N})$, where $\mathcal{E} \triangleq \{\widetilde{U}^N \neq U^N\}$. We then have

$$\begin{aligned}
&\mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N]\\
&\overset{(a)}{=} \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N|\mathcal{E}]\mathbb{P}[\mathcal{E}] + \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N|\mathcal{E}^c]\mathbb{P}[\mathcal{E}^c]\\
&\leqslant \mathbb{P}[\mathcal{E}] + \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N|\mathcal{E}^c]\\
&\overset{(b)}{=} \mathbb{V}(\widetilde{p}_{U^N}, q_{U^N}) + \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N|\mathcal{E}^c]\\
&\overset{(c)}{\leqslant} \mathbb{V}(\widetilde{p}_{U^N}, q_{U^N}) + N\delta_N\\
&\overset{(d)}{\leqslant} \delta_N^{(1)} + \delta_N^{(2)} + N\delta_N, \qquad (8)
\end{aligned}$$

where (a) holds by the law of total probability, (b) holds by optimal coupling, (c) holds by Theorem 1, (d) holds by Lemma 2.

(ii): First, note that

$$\begin{aligned}
&\mathbb{V}(q_{X^NY^NV^N}, \widetilde{p}_{X^NY^NV^N})\\
&= \mathbb{V}(q_{Y^N|X^N} q_{X^NV^N}, q_{Y^N|X^N}\widetilde{p}_{X^NV^N})\\
&= \mathbb{V}(q_{X^NV^N}, \widetilde{p}_{V^NX^N}) \qquad (9)
\end{aligned}$$

where the first equality holds because $V - X - Y$, $\widetilde{V}^N$ is a function of X^N, $\widetilde{p}_{Y^N|X^N} = q_{Y^N|X^N}$. We then upper-bound the average distortion as follows.

$$\begin{aligned}
&\mathbb{E}_{\widehat{p}}\left[\frac{1}{N}\sum_{i=1}^{N} d(X_i, f(\widehat{V}_i, Y_i)\right]\\
&\leqslant \mathbb{E}_{\widehat{p}}\left[\frac{1}{N}\sum_{i=1}^{N} d(X^N, f(\widehat{V}_i, Y_i)|\widehat{V}^N = \widetilde{V}^N\right] + d_{\max}\mathbb{P}[\widehat{V}^N \neq \widetilde{V}^N]\\
&\overset{(a)}{=} \mathbb{E}_{\widehat{p}}\left[\frac{1}{N}\sum_{i=1}^{N} d(X^N, f(\widehat{V}_i, Y_i)\right] + d_{\max}\mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N]\\
&\leqslant \mathbb{E}_{q}\left[\frac{1}{N}\sum_{i=1}^{N} d(X_i, f(V_i, Y_i)\right]\\
&\qquad + d_{\max}(\mathbb{V}(q_{X^NY^NV^N}, \widetilde{p}_{X^NY^NV^N}) + \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N])\\
&\overset{(b)}{\leqslant} D + d_{\max}(\mathbb{V}(q_{X^NY^NV^N}, \widetilde{p}_{X^NY^NV^N}) + \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N])\\
&\overset{(c)}{=} D + d_{\max}(\mathbb{V}(q_{X^NV^N}, \widetilde{p}_{X^NV^N}) + \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N])\\
&\overset{(d)}{\leqslant} D + d_{\max}(2\delta_N^{(1)} + 2\delta_N^{(2)} + N\delta_N),
\end{aligned}$$

where (a) holds by invertibility of G_n, (b) holds by definition of q, chosen to achieve $R(D)$ in Theorem 2, (c) holds by (9), (d) holds by (8) and Lemma 2.

(iii): We have $\mathcal{V}_{V|X} \subset \mathcal{H}_{V|X} \subset \mathcal{H}_{V|Y}$, where the last inclusion holds because $V - X - Y$. Hence,

$$\begin{aligned}
&\lim_{N\to\infty} |\mathcal{H}_{V|Y} \backslash \mathcal{V}_{V|X}|/N\\
&\qquad = \lim_{N\to\infty} |\mathcal{H}_{V|Y}|/N - \lim_{N\to\infty} |\mathcal{V}_{V|X}|/N\\
&\qquad \overset{(a)}{=} H(V|Y) - H(V|X)\\
&\qquad \overset{(b)}{=} I(X;V|Y),
\end{aligned}$$

where (a) holds by Theorem 1 and [5, Lemma 1], (b) holds because $V - X - Y$.

(iv): Assume that the scheme of Section III-A is repeated over k blocks of size N with the same shared randomness C^*. The overall rate of common randomness is then $|C^*|/Nk$, which vanishes as N and k go to infinity. We now justify that statements $(i) - (iii)$ remain asymptotically valid. Statement (i) becomes

$$\mathbb{P}[\widehat{U}^{kN} \neq \widetilde{U}^{kN}] \leqslant \sum_{i=0}^{k-1} \mathbb{P}[\widehat{U}_{iN+1}^{(i+1)N} \neq \widetilde{U}_{iN+1}^{(i+1)N}] \leqslant k\delta_N^{(3)}.$$

Then, similar to [11], one can show the following lemma.

Lemma 3 (Adapted from [11, Lemma 8]): We have

$$\mathbb{V}(q_{X^{kN}Y^{kN}V^{kN}}, \widetilde{p}_{X^{kN}Y^{kN}V^{kN}}) \leqslant k\delta_N^*,$$

where $\delta_N^* = o(2^{-N^{\alpha}})$, $\alpha < \beta$.

Hence, using Lemma 3 and similar to the proof of (ii), we obtain for k fixed

$$\lim_{N\to\infty} \mathbb{E}_{\widetilde{p}}\left[\frac{1}{kN}\sum_{i=1}^{kN} d(X_i, f(\widehat{V}_i, Y_i)\right] \leqslant D.$$

Finally, note that the encoding rate when using k blocks remains optimal. ■

IV. Argmax decision for channel coding

Polar coding for symmetric channels has been introduced in [4], and has subsequently be extended to asymmetric channel without alphabet extension assuming that encoder and decoder share common randomness [1], or with a chaining technique [12, Section V]. We develop next a polar coding scheme that results in significant savings of common randomness compared to [1] and that also recovers some statements made in [12, Section V] for polar coding.

A. Proposed coding scheme

Consider a discrete memoryless channel $(\mathcal{X}, q_{Y|X}, \mathcal{Y})$ and the probability distribution $q_X \triangleq \underset{p_X}{\operatorname{argmax}}\, I(X;Y)$. Assume that X^N is distributed according to q_{X^N}. Define $U^N \triangleq X^N G_n$, as well as the sets

$$\begin{aligned}\mathcal{V}_X &\triangleq \left\{ i \in [\![1,N]\!] : H(U_i|U^{i-1}) > 1-\delta_N \right\},\\ \mathcal{H}_X &\triangleq \left\{ i \in [\![1,N]\!] : H(U_i|U^{i-1}) > \delta_N \right\},\\ \mathcal{V}_{X|Y} &\triangleq \left\{ i \in [\![1,N]\!] : H(U_i|U^{i-1}Y^N) > 1-\delta_N \right\},\\ \mathcal{H}_{X|Y} &\triangleq \left\{ i \in [\![1,N]\!] : H(U_i|U^{i-1}Y^N) > \delta_N \right\}.\end{aligned}$$

Assume that encoder and decoder share a sequence C^* of $|\mathcal{V}_{X|Y}|$ uniform bits. We show later that C^* may be reused over several encoding blocks so that the rate of shared randomness vanishes with the blocklength. Our proposed scheme for channel coding is then the following.

Encoding. From message M, a sequence of uniformly distributed bits, and C^*, form $\widetilde{U}^N$ defined by the distribution $\widetilde{p}_{U^N} \triangleq \prod_{i=1}^{N} \widetilde{p}_{U_j|U^{j-1}}$ with

$$\widetilde{p}_{U_j|U^{j-1}}(u_j|u^{j-1}) \triangleq \begin{cases} \mathbb{1}\{u_j = M_j\} & \text{if } j \in \mathcal{V}_X \backslash \mathcal{V}_{X|Y} \\ \mathbb{1}\{u_j = C_j^*\} & \text{if } j \in \mathcal{V}_{X|Y} \\ q_{U_j|U^{j-1}}(u|u^{j-1}) & \text{if } j \in \mathcal{V}_X^c \backslash \mathcal{H}_X^c \\ \mathbb{1}\{u_j = \operatorname*{argmax}_u q_{U_j|U^{j-1}}(u|u^{j-1})\} & \text{if } j \in \mathcal{H}_X^c, \end{cases} \tag{10}$$

where the components of C^* and M have been indexed by the set of indices $\mathcal{V}_{X|Y}$ and $\mathcal{V}_X \backslash \mathcal{V}_{X|Y}$, respectively.

Send $\widetilde{X}^N \triangleq \widetilde{U}^N G_n$ over the channel $q_{Y|X}$ and assume that

$$F \triangleq \widetilde{U}^N[\mathcal{H}_{X|Y} \backslash \mathcal{V}_{X|Y}]$$

is available at the decoder[a]

Decoding. Form an estimate $\widehat{U}^N$ of $\widetilde{U}^N$ from $(F, C^*, Y^N) = (\widetilde{U}^N[\mathcal{H}_{V|Y}], Y^N)$ using the successive cancellation decoder for lossless source coding described in Section II.

[a] See Remark 2

Remark 2: Assume that the encoding and decoding process is repeated over k block. The randomness C^* and the vectors F's for the k blocks can be send to the decoder with non-optimal transmission rate by means of a polar code for symmetric channel. Moreover, the rate of this transmission is negligible compared to the overall message rate, as it can be upper-bounded by

$$\begin{aligned}&O\left(\frac{k|\mathcal{H}_{X|Y} \backslash \mathcal{V}_{X|Y}| + |C^*|}{kN}\right)\\ &\leqslant O\left(\frac{|\mathcal{H}_{X|Y}| - |\mathcal{V}_{X|Y}|}{N} + \frac{|V_{X|Y}|}{kN}\right)\\ &\xrightarrow{N\to\infty} O\left(\frac{H(X|Y)}{k}\right)\\ &\xrightarrow{k\to\infty} 0,\end{aligned}$$

where we have used $\mathcal{V}_{X|Y} \subset \mathcal{H}_{X|Y}$, and [5, Lemma 1] and Theorem 1 for the limits.

Remark 3: By analogy with Remark 1, the vector $F \triangleq \widetilde{U}^N[\mathcal{H}_{X|Y} \backslash \mathcal{V}_{X|Y}]$ needs to be known at the decoder. Moreover, we keep a randomized decision rule for the indices in $\mathcal{V}_X^c \backslash \mathcal{H}_X^c$ for the proof of Lemma 5. Note that $|\mathcal{V}_X^c \backslash \mathcal{H}_X^c| = o(N)$ by Remark 1.

B. Scheme analysis and result

Consider the random variable $\overline{U}^N$ that would be obtained in place of $\widetilde{U}^N$ when using randomized encoding in place of the argmax decision. Specifically, $\overline{U}^N$ is defined by $\overline{p}_{U^N} \triangleq \prod_{i=1}^{N} \overline{p}_{U_j|U^{j-1}}$ with

$$\overline{p}_{U_j|U^{j-1}}(u_j|u^{j-1}) \triangleq \begin{cases} \mathbb{1}\{u_j = M_j\} & \text{if } j \in \mathcal{V}_X \backslash \mathcal{V}_{X|Y} \\ \mathbb{1}\{u_j = C_j^*\} & \text{if } j \in \mathcal{V}_{X|Y} \\ q_{U_j|U^{j-1}}(u|u^{j-1}) & \text{if } j \in \mathcal{V}_X^c, \end{cases} \tag{11}$$

where the components of C^* and M have been indexed by the set of indices $\mathcal{V}_{X|Y}$ and $\mathcal{H}_X \backslash \mathcal{V}_{X|Y}$, respectively. Define $\overline{X}^N \triangleq \overline{U}^N G_n$.

Lemma 4: The distribution $\overline{p}_{X^N}$ is nearly indistinguishable from the distribution q_{X^N}, in the sense that

$$\mathbb{V}(q_{X^N}, \overline{p}_{X^N}) \leqslant \delta_N^{(1)} \text{ with } \delta_N^{(1)} \triangleq \gamma\sqrt{N\delta_N}.$$

Proof: We have

$$\begin{aligned}&\mathbb{D}(q_{X^N}||\overline{p}_{X^N})\\ &\overset{(a)}{=} \mathbb{D}(q_{U^N}||\overline{p}_{U^N})\\ &\overset{(b)}{=} \sum_{j=1}^{N} \mathbb{D}(q_{U_j|U^{j-1}}||\overline{p}_{U_j|U^{j-1}}|q_{U^{j-1}})\\ &\overset{(c)}{=} \sum_{j \in \mathcal{V}_X} \mathbb{D}(q_{U_j|U^{j-1}}||\overline{p}_{U_j|U^{j-1}}|q_{U^{j-1}})\\ &\overset{(d)}{=} \sum_{j \in \mathcal{V}_X} (1 - H(U_j|U^{j-1}))\\ &\leqslant |\mathcal{V}_X|\delta_N\\ &\leqslant N\delta_N,\end{aligned}$$

where (a) holds by invertibility of G_n, (b) holds by the chain rule for divergence [3], (c) and (d) hold by (11) and uniformity of C^* and M. The result follows by Pinsker's inequality. ■

We can then reuse the proof of Lemma 2 to obtain the following.

Lemma 5: Let $\widetilde{U}^N$ and $\overline{U}^N$ be drawn from $\widetilde{p}_{U^N}$ and $\overline{p}_{U^N}$, defined in (10) and (11), respectively. Then, $\widetilde{p}_{X^N}$ is asymptotically close to q_{X^N} and $\overline{p}_{X^N}$, in the sense that

$$\begin{aligned}\mathbb{V}(\widetilde{p}_{X^N}, \overline{p}_{X^N}) &\leqslant \delta_N^{(2)},\\ \mathbb{V}(\widetilde{p}_{X^N}, q_{X^N}) &\leqslant \delta_N^{(1)} + \delta_N^{(2)},\end{aligned}$$

with $\delta_N^{(2)} \triangleq N\sqrt{\delta_N + 2\delta_N^{(1)}(N - \log \delta_N^{(1)})}$, and $\delta_N^{(1)}$ as in Lemma 4.

We now prove that the coding scheme of Section IV-A is successful and optimal.

Theorem 4: Assume that $\widetilde{U}^N$ and $\widehat{U}^N$ are obtained from the encoding decoding scheme of Section IV-A.

(i) $\widetilde{U}^N$ and $\widehat{U}^N$ are identical with high probability,, i.e.,

$$\mathbb{P}[\widehat{X}^N \neq \widetilde{X}^N] = \mathbb{P}[\widehat{U}^N \neq \widetilde{U}^N] \leqslant \delta_N^{(3)},$$

where $\delta_N^{(3)} \triangleq \delta_N^{(1)} + \delta_N^{(2)} + N\delta_N$ with $\delta_N^{(1)}$ and $\delta_N^{(2)}$ as in Lemma 4 and Lemma 5.

(ii) The encoding rate is optimal, i.e.,

$$\lim_{N\to\infty} \frac{|\mathcal{V}_X \backslash \mathcal{V}_{X|Y}|}{N} = I(X;Y)$$

(iii) Encoder and decoder may reuse the common randomness C^* over k blocks of size N. Hence, the rate of common randomness is $H(X|Y)/k$ and vanishes as k goes to infinity. Moreover, the additional transmission rate of the vectors F's is negligible compared to the overall message transmission rate.

Proof: The proof of (i) is identical to the one of (i) in Theorem 3. The proof of (ii) follows from [5, Lemma 1] and $\mathcal{V}_X \subset \mathcal{V}_{X|Y}$. Finally, (iii) follows from Remark 2, moreover, Statements (i) and (ii) clearly remain valid. ■

V. Discussion

We conclude the paper with a discussion of the significance of the result. First, note that the benefit of a deterministic decision is twofold: it avoids the sharing of random numbers between the encoder and the decoder, and it removes the need to draw sequences according to specific distributions. In the case of Wyner-Ziv coding, this avoids $|\mathcal{H}_V^c|$ random decisions, which is $O(N)$ and is thus non-negligible; similarly, for channel coding, it avoids $|\mathcal{H}_X^c|$ random decisions. Second, our result also clarifies when one may use an argmax decision in the encoding and decoding of polar codes. While earlier works have used this rule, no formal justification had been provided to the best of our knowledge. However, whether the random choice of the bits C^* in (2) or (10) may be replaced by a deterministic one remains an open question. Finally, we point out that the technique used in Sections III-B and IV-B is general and could be applied to more complicated models, e.g., the wiretap channel [13], without much difficulty.

References

[1] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric models," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7829–7838, 2013.

[2] E. Arikan, "Source Polarization," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2010, pp. 899–903.

[3] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley, 1991.

[4] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[5] R. Chou, M. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[6] M. Hayashi, "Second-Order Asymptotics in Fixed-Length Source Coding and Intrinsic Randomness," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4619–4637, 2008.

[7] A. Wyner and J. Ziv, "The Rate Distortion Function for Source Coding with Side Information at the Decoder," *IEEE Trans. Inf. Theory*, vol. 22(1), pp. 1–10, 1973.

[8] S. Korada and R. Urbanke, "Polar Codes are Optimal for Lossy Source Coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, 2010.

[9] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge Univ Pr, 1981.

[10] D. Aldous, "Random walks on finite groups and rapidly mixing markov chains," in *Séminaire de Probabilités XVII 1981/82*. Springer, 1983, pp. 243–297.

[11] R. Chou, M. Bloch, and J. Kliewer, "Polar coding for empirical and strong coordination via distribution approximation," in *Proc. of IEEE Int. Symp. Inf. Theory*, 2015.

[12] M. Mondelli, S. H. Hassani, and R. Urbanke, "How to achieve the capacity of asymmetric channels," in *Proc. of the Annual Allerton Conf. on Communication Control and Computing*, 2014.

[13] R. Chou and M. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, 2016.