

Polar Codes are Optimal for Lossy Source Coding

Satish Babu Korada and Rüdiger Urbanke

EPFL, Switzerland, Email: {satish.korada,ruediger.urbanke}@epfl.ch

Abstract—We consider lossy source compression of a binary symmetric source with Hamming distortion function. We show that polar codes combined with a low-complexity successive cancellation encoding algorithm achieve the rate-distortion bound. The complexity of both the encoding and the decoding algorithm is $O(N \log(N))$, where N is the blocklength of the code. Our result mirrors Arkan’s capacity achieving polar code construction for channel coding.

I. INTRODUCTION

Lossy source compression is one of the fundamental problems of information theory. Consider a binary symmetric source (BSS) Y . Let $d(\cdot, \cdot)$ denote the Hamming distortion function,

$$d(0, 0) = d(1, 1) = 0, d(0, 1) = 1.$$

It is well known that, in order to compress Y with average distortion D , the rate R at which we describe the source has to be at least $R(D) = 1 - h_2(D)$, where $h_2(\cdot)$ is the binary entropy function [1]. Shannon proved that this rate is sufficient by using a random coding argument (using non-linear codes). It was later shown by Goblick that in fact linear codes are sufficient [2], [3, Section 6.2.3].

Trellis-based quantizers [4] were perhaps the first “practical” solution to source compression. Their encoding complexity is linear in the blocklength of the code (Viterbi algorithm). For any rate strictly larger than $R(D)$ the gap between the expected distortion and the design distortion D vanishes exponentially in the constraint length. However, the complexity of the encoding algorithm scales exponentially with the constraint length.

Given the success of sparse graph codes combined with low-complexity message-passing algorithms for the channel coding problem, it is interesting to investigate the performance of such a combination for lossy source compression.

As a first question, we can ask if the codes themselves are suitable for the task. In this respect, Matsunaga and Yamamoto [5] showed that if the degrees of a low-density parity-check (LDPC) ensemble are chosen as large as $\Theta(\log(N))$, where N is the blocklength, then this ensemble saturates the rate-distortion bound if optimal encoding is employed. Even more promising, Martinian and Wainwright [6] proved that properly chosen MN codes with *bounded* degrees are sufficient to achieve the rate-distortion bound under optimal encoding.

Much less is known about the performance of sparse graph codes under *message-passing* encoding. In [7] the authors consider binary erasure quantization, the source-compression equivalent of the binary erasure channel (BEC) coding problem. They show that LDPC-based quantizers fail

to achieve the rate-distortion bound if the parity-check density is $o(\log(N))$. But properly constructed low-density generator-matrix (LDGM) based quantizers combined with message-passing encoders are optimal. They exploit the close relationship between the channel coding problem and the lossy source compression problem, together with the fact that LDPC codes achieve the capacity of the BEC under message-passing decoding, to prove the latter claim.

Regular LDGM codes were considered in [8]. Using non-rigorous methods from statistical physics it was shown that these codes approach rate-distortion bound for large degrees. It was empirically shown that these codes have good performance under a variant of belief propagation algorithm (reinforced belief propagation). In [9] the authors consider check-regular LDGM codes and show, using non-rigorous methods, that these codes approach the rate-distortion bound for large check degree. Moreover, for any rate strictly larger than $R(D)$, the gap between the achieved distortion and D vanishes exponentially in the check degree. They also observe that belief propagation inspired decimation (BID) algorithms do not perform well in this context. In [10], survey propagation inspired decimation (SID) was proposed as an iterative algorithm for finding the solutions of K-SAT (non-linear constraints) formulae efficiently. Based on this success, the authors in [9] replaced the parity-check nodes with non-linear constraints, and empirically showed that using SID one can achieve a performance close to the rate-distortion bound.

The construction in [7] suggests that those LDGM codes whose duals (LDPC) are optimized for the binary symmetric channel (BSC) might be good candidates for the lossy compression of a BSS using message-passing encoding. In [11] the authors consider such LDGM codes and empirically show that by using SID one can approach very close to the rate-distortion bound. They also mention that even BID works well but that it is not as good as SID. Recently, in [12] it was experimentally shown that using BID it is possible to approach the rate-distortion bound closely. The key to making basic BP work well in this context is to choose the code properly.

The current state-of-the-art code design is thus based on the heuristic approach of designing an LDPC code for a suitably defined channel and then taking its dual LDGM code. Such an approach does not extend to sources other than the BSS. In addition to the heuristic argument, the code design relies on finding capacity achieving codes for channel coding which itself is an open problem.

We show that polar codes combined with a successive cancellation (SC) encoder achieve the rate-distortion bound. This is the first practical coding scheme that provably achieves

the rate-distortion bound. In this paper we concentrate on the case of a BSS with Hamming distortion. As shown in [13, Chapter 3] equivalent results can be derived for more general sources.

II. POLAR CODES

Let $W : \{0, 1\} \rightarrow \mathcal{Y}$ be a binary-input discrete memoryless channel (B-DMC). Let $I(W) \in [0, 1]$ denote the mutual information between the input and output of W with uniform distribution on the inputs, call it the symmetric mutual information. Clearly, if the channel W is symmetric, then $I(W)$ is the capacity of W . Also, let $Z(W) \in [0, 1]$ denote the Bhattacharyya parameter of W , i.e., $Z(W) = \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}$.

In the following, an upper case letter, say U , denotes a random variable and u denotes its realization. Let U_i^j denote the random vector (U_i, \dots, U_j) for $i \leq j$ and let $\bar{U} = U_0^{N-1}$. For any set F , $|F|$ denotes its cardinality and let U_F denote $(U_{i_1}, \dots, U_{i_{|F|}})$, where $\{i_k \in F : i_k \leq i_{k+1}\}$. We use the equivalent notation for their realizations too.

Polar codes, introduced by Arkan in [14], are the first practical codes that provably achieve capacity for arbitrary symmetric B-DMCs with low encoding and decoding complexity. Let $G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. The generator matrix of polar codes is defined through the Kronecker powers of G_2 , denoted by $G_2^{\otimes n}$, (where “ $\otimes n$ ” denotes the n^{th} Kronecker power) as follows.

Definition 1 (Polar Code): The polar code $\mathcal{C}_N(F, u_F)$, defined for any $F \subseteq \{0, \dots, N-1\}$ and $u_F \in \{0, 1\}^{|F|}$, is a linear code given by

$$\mathcal{C}_N(F, u_F) = \{v_0^{N-1} G_2^{\otimes n} : v_F = u_F, v_{F^c} \in \{0, 1\}^{|F^c|}\}.$$

In other words the code $\mathcal{C}_N(F, u_F)$ is constructed by fixing the indices in F to u_F and varying the indices in F^c over all the possible values. Let us refer to the set F as *frozen set* and the indices belonging to it as *frozen indices*. Arkan [14] showed that there exists a choice of (F, u_F) that achieves rates close to $I(W)$ using a low-complexity SC decoding algorithm. The complexity of both the encoding and the SC decoding algorithm is $O(N \log(N))$.

III. SUCCESSIVE CANCELLATION ENCODER

Let $Y \in \mathcal{Y}$ be a $\text{Ber}(\frac{1}{2})$ random variable and let the source be a sequence of i.i.d. realizations of Y . Let P_Y denote the probability distribution of Y , i.e., $P_Y(0) = P_Y(1) = 1$. For the case of the Hamming distortion function, the test channel that achieves the rate-distortion tradeoff for design distortion D is the BSC(D). Let us denote this test channel by W , i.e.,

$$\begin{aligned} W(0|1) &= W(1|0) = D, \\ W(0|0) &= W(1|1) = 1 - D. \end{aligned}$$

Let us use polar codes for the above lossy source coding problem. In order to construct a suitable polar code we need to find the appropriate (F, u_F) . For that purpose let us consider the probability distribution $P_{\bar{U}, \bar{X}, \bar{Y}}$ over the space $\{0, 1\}^N \times$

$\{0, 1\}^N \times \{0, 1\}^N$ defined as

$$P_{\bar{U}, \bar{X}, \bar{Y}}(\bar{u}, \bar{x}, \bar{y}) = \underbrace{\frac{1}{2^N}}_{P_{\bar{U}}(\bar{u})} \underbrace{\mathbb{1}_{\{\bar{x} = \bar{u} G_2^{\otimes n}\}}}_{P_{\bar{X}|\bar{U}}(\bar{x}|\bar{u})} \underbrace{\prod_{i=0}^{N-1} W(y_i | x_i)}_{P_{\bar{Y}|\bar{X}}(\bar{y}|\bar{x})}. \quad (1)$$

Since $G_2^{\otimes n}$ is an invertible matrix, the uniform distribution of \bar{U} over $\{0, 1\}^N$ induces a uniform distribution on \bar{X} . Since $W(y|x) = W(y \oplus 1 | x \oplus 1)$ (symmetry), it follows that the marginal induced by the above distribution over the space \mathcal{Y}^N is also uniform. This is indeed the distribution of the source.

Let \bar{y} denote N i.i.d. realizations of the source Y . Let $\hat{U}(\bar{y}, u_F)$ denote the result of the following SC encoding operation using the code $\mathcal{C}_N(F, u_F)$. Given \bar{y} , for each i in the range 0 till $N-1$:

- (i) If $i \in F$, then set $\hat{u}_i = u_i$.
- (ii) If $i \in F^c$, then compute $P_{U_i | U_0^{i-1}, \bar{Y}}(0 | \hat{u}_0^{i-1}, \bar{y})$ and set

$$\hat{u}_i = \begin{cases} 0 & \text{w.p. } P_{U_i | U_0^{i-1}, \bar{Y}}(0 | \hat{u}_0^{i-1}, \bar{y}), \\ 1 & \text{w.p. } P_{U_i | U_0^{i-1}, \bar{Y}}(1 | \hat{u}_0^{i-1}, \bar{y}). \end{cases} \quad (2)$$

We refer to the decision rule (2) as *randomized rounding*. Randomized rounding as a decision rule is not new. In [15] it was applied in the context of finding solutions of a random k -SAT problem.

Remark 2: When making the decision on bit U_i using the SC encoder, it is natural to choose that value for U_i which maximizes the posterior (MAP rule). Why do we use randomized rounding? In simulations, randomized rounding and the MAP rule perform similarly with a slight performance edge for the MAP rule. But for the purpose of analysis the randomized rounding rule is much more convenient. In fact, it is currently not clear if and how the MAP rule can be analyzed. Note that all of the existing source coding schemes use the MAP rule. This is most likely the main obstacle to their analysis. We believe that by combining randomized rounding with existing schemes like BID it might be possible to analyze the performance of LDGM codes for source coding.

The decoding, or the reconstruction operation, is given by $\bar{x} = \hat{u}_0^{N-1} G_2^{\otimes n}$. The decoder has knowledge of \hat{u}_F (since $\hat{u}_F = u_F$) and hence the encoder needs to convey only the vector $(\hat{U}(\bar{y}, u_F))_{F^c}$ to the decoder. This requires $|F^c|$ bits and hence the rate is $|F^c|/N$. The average distortion incurred by this scheme is given by $\frac{1}{N} \mathbb{E}[d(\bar{Y}, \bar{X})]$, where the expectation is over the source randomness and the randomness involved in the randomized rounding at the encoder.

The encoding (decoding) task for source coding is the same as the decoding (encoding) task for channel coding. As shown in [14], both operations can be implemented with $O(N \log(N))$ complexity.

IV. MAIN RESULT

Theorem 3 (Polar Codes Achieve the Rate-Distortion Bound for the Binary Symmetric Source): Let Y be a BSS and fix the design distortion D , $0 < D < \frac{1}{2}$. For any rate $R > 1 - h_2(D)$ and any $0 < \beta < \frac{1}{2}$, there exists a sequence of

polar codes of length N with rates $R_N < R$ so that under SC encoding using randomized rounding they achieve expected distortion D_N satisfying

$$D_N \leq D + O(2^{-(N^\beta)}).$$

The encoding as well as decoding complexity of these codes is $O(N \log(N))$.

Let us consider how polar codes perform in practice. Recall that the length N of the code is always a power of 2, i.e., $N = 2^n$. Let us construct a polar code to achieve a distortion D . Let W denote the channel $\text{BSC}(D)$ and let $R = R(D) + \epsilon$ for some $\epsilon > 0$.

In order to fully specify the code we need to specify the set F , i.e., the set of frozen components. We proceed as follows. For any B-DMC W , let $W_N^{(i)} : \{0, 1\} \rightarrow \mathcal{Y}^{N-1} \times \{0, 1\}^{i-1}$ denote the channel law

$$\begin{aligned} W_N^{(i)}(\bar{y}, u_0^{i-1} | u_i) &\triangleq P_{\bar{Y}, U_0^{i-1} | U_i}(\bar{y}, u_0^{i-1} | u_i) \\ &= \frac{1}{2^{N-1}} \sum_{u_{i+1}^{N-1}} P_{\bar{Y} | \bar{U}}(\bar{y} | \bar{u}). \end{aligned}$$

First we estimate the $Z(W_N^{(i)})$ s for all $i \in \{0, \dots, N-1\}$ and sort the indices i in decreasing order of $Z(W_N^{(i)})$ s. The set F consists of the first $(1-R)N$ indices, i.e., it consists of the indices corresponding to the $(1-R)N$ largest $Z(W_N^{(i)})$ s.

This is similar to the channel code construction for the $\text{BSC}(D)$ but there is a slight difference. For the case of channel coding we assign all indices i so that $Z(W_N^{(i)})$ is *very* small, i.e., so that lets say $Z(W_N^{(i)}) < \delta$, to the set F^c . Therefore, the set F consists of all those indices i so that $Z(W_N^{(i)}) \geq \delta$. For the source compression, on the other hand, F consists of all those indices i so that $Z(W_N^{(i)}) \geq 1 - \delta$, i.e., of all those indices corresponding to *very* large values of $Z(W_N^{(i)})$.

Putting it differently, in channel coding, the rate R is chosen to be strictly less than $1 - h_2(D)$, whereas in source compression it is chosen so that it is strictly larger than this quantity. Figure 1 shows the performance of the SC encoding algorithm combined with randomized rounding. As asserted by Theorem 3, the points approach the rate-distortion bound as the blocklength increases.

In [16] the performance of polar codes for lossy source compression was already investigated empirically. Note that the construction used in [16] is different from the current construction. There is also a slight difference with respect to the decimation step of the encoding algorithm. In [16] we use MAP estimates instead of randomized rounding. Despite all these differences the performance of both schemes is comparable.

V. THE PROOF

Let $\mathcal{C}_N(F)$ denote the polar code ensemble defined as follows.

Definition 4 (Polar Code Ensemble): The polar code ensemble $\mathcal{C}_N(F)$, defined for any $F \subseteq \{0, \dots, N-1\}$, denotes

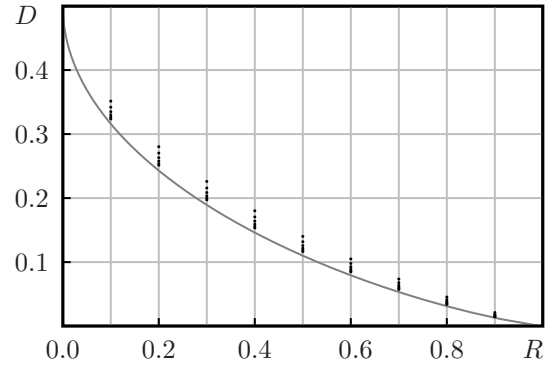


Fig. 1. The rate-distortion performance for the SC encoding algorithm with randomized rounding for $n = 9, 11, 13, 15, 17$ and 19 . As the blocklength increases the points move closer to the rate-distortion bound.

the ensemble

$$\mathcal{C}_N(F) = \{\mathcal{C}_N(F, u_F), \forall u_F \in \{0, 1\}^{|F|}\}.$$

For the proof it is more convenient not to determine the distortion for a fixed choice of u_F but to compute the average distortion over all possible codes belonging to the ensemble $\mathcal{C}_N(F)$ (with a uniform distribution over these choices). Let $D_N(F, u_F)$ denote the resulting average distortion for the code $\mathcal{C}_N(F, u_F)$ and let $D_N(F)$ denote the average of $D_N(F, u_F)$ over all possible codes in the ensemble $\mathcal{C}_N(F)$. We want to show that there exists a set F of cardinality roughly $Nh_2(D)$ and a vector u_F such that $D_N(F, u_F) \approx D$. We accomplish this by showing that there exists a set F of the required cardinality such that $D_N(F) \approx D$. This implies that there exists a choice of u_F for which $D_N(F, u_F) \approx D$. In fact, it can be shown [17] that the distortion *does not depend* on the choice of u_F . A convenient choice is therefore to set u_F to zero.

The encoding function $\hat{U}(\bar{y}, u_F)$ is random. More precisely, in step i of the encoding process, $i \in F^c$, we fix the value of U_i proportional to the posterior (randomized rounding) $P_{U_i | U_0^{i-1}, \bar{Y}}(\hat{u}_i | \hat{u}_0^{i-1}, \bar{y})$. This implies that the probability of picking a vector \hat{u}_0^{N-1} given \bar{y} is equal to

$$\begin{cases} 0, & \hat{u}_F \neq u_F, \\ \prod_{i \in F^c} P_{U_i | U_0^{i-1}, \bar{Y}}(\hat{u}_i | \hat{u}_0^{i-1}, \bar{y}), & \hat{u}_F = u_F. \end{cases}$$

Therefore, the average (over \bar{y} and the randomness of the encoder) distortion $D_N(F, u_F)$ is given by

$$\begin{aligned} D_N(F, u_F) &= \sum_{\bar{y} \in \{0, 1\}^N} \frac{1}{2^N} \sum_{\hat{u}_F \in \{0, 1\}^{|F^c|}} \\ &\quad \prod_{i \in F^c} P(\hat{u}_i | \hat{u}_0^{i-1}, \bar{y}) \frac{1}{N} d(\bar{y}, \hat{u}_0^{N-1} G_2^{\otimes n}), \quad (3) \end{aligned}$$

where $\hat{u}_i = u_i$ for $i \in F$.

The average distortion $D_N(F)$ can then be written as

$$D_N(F) = \sum_{u_F \in \{0, 1\}^{|F|}} \frac{1}{2^{|F|}} D_N(F, u_F)$$

$$\begin{aligned}
&= \sum_{u_F} \frac{1}{2^{|F|}} \sum_{\bar{y}} \frac{1}{2^N} \sum_{u_{F^c}} \prod_{i \in F^c} P(u_i | u_0^{i-1}, \bar{y}) \frac{1}{N} d(\bar{y}, \bar{u} G_2^{\otimes n}) \\
&= \sum_{\bar{y}} \frac{1}{2^N} \sum_{\bar{u}} \frac{1}{2^{|F|}} \prod_{i \in F^c} P(u_i | u_0^{i-1}, \bar{y}) \frac{1}{N} d(\bar{y}, \bar{u} G_2^{\otimes n}).
\end{aligned}$$

Let $Q_{\bar{U}, \bar{Y}}$ denote the distribution defined by $Q_{\bar{Y}}(\bar{y}) = \frac{1}{2^N}$ and $Q_{\bar{U} | \bar{Y}}$ defined by

$$Q(u_i | u_0^{i-1}, \bar{y}) = \begin{cases} \frac{1}{2}, & \text{if } i \in F, \\ P_{U_i | U_0^{i-1}, \bar{Y}}(u_i | u_0^{i-1}, \bar{y}), & \text{if } i \in F^c. \end{cases}$$

Then, $D_N(F) = \frac{1}{N} \mathbb{E}_Q[d(\bar{Y}, \bar{U} G_2^{\otimes n})]$, where $\mathbb{E}_Q[\cdot]$ denotes expectation with respect to the distribution $Q_{\bar{U}, \bar{Y}}$. Similarly, let $\mathbb{E}_P[\cdot]$ denote the expectation with respect to the distribution $P_{\bar{U}, \bar{Y}}$. Recall that $P_{\bar{Y}}(\bar{y}) = \frac{1}{2^N}$ and that we can write $P_{\bar{U} | \bar{Y}}$ in the form

$$P_{\bar{U} | \bar{Y}}(\bar{u} | \bar{y}) = \prod_{i=0}^{N-1} P_{U_i | U_0^{i-1}, \bar{Y}}(u_i | u_0^{i-1}, \bar{y}).$$

If we compare Q to P we see that they have the same structure except for the components $i \in F$. Indeed, in the following lemma we show that the total variation distance between Q and P can be bounded in terms of how much the posteriors $Q_{U_i | U_0^{i-1}, \bar{Y}}$ and $P_{U_i | U_0^{i-1}, \bar{Y}}$ differ for $i \in F$.

Lemma 5 (Bound on the Total Variation Distance): Let F denote the set of frozen indices and let the probability distributions Q and P be as defined above. Then

$$\begin{aligned}
&\sum_{\bar{u}, \bar{y}} |Q(\bar{u}, \bar{y}) - P(\bar{u}, \bar{y})| \\
&\leq 2 \sum_{i \in F} \mathbb{E}_P \left[\left| \frac{1}{2} - P_{U_i | U_0^{i-1}, \bar{Y}}(0 | U_0^{i-1}, \bar{Y}) \right| \right].
\end{aligned}$$

Proof:

$$\begin{aligned}
&\sum_{\bar{u}} |Q(\bar{u} | \bar{y}) - P(\bar{u} | \bar{y})| \\
&= \sum_{\bar{u}} \left| \prod_{i=0}^{N-1} Q(u_i | u_0^{i-1}, \bar{y}) - \prod_{i=0}^{N-1} P(u_i | u_0^{i-1}, \bar{y}) \right| \\
&= \sum_{\bar{u}} \left| \sum_{i=0}^{N-1} \left[(Q(u_i | u_0^{i-1}, \bar{y}) - P(u_i | u_0^{i-1}, \bar{y})) \cdot \right. \right. \\
&\quad \left. \left. \left(\prod_{j=0}^{i-1} P(u_j | u_0^{j-1}, \bar{y}) \right) \left(\prod_{j=i+1}^{N-1} Q(u_j | u_0^{j-1}, \bar{y}) \right) \right] \right|.
\end{aligned}$$

In the last step we have used the following telescoping expansion:

$$A_0^{N-1} - B_0^{N-1} = \sum_{i=0}^{N-1} (A_i - B_i) A_{i+1}^{N-1} B_0^{i-1},$$

where A_k^j denotes here the product $\prod_{i=k}^j A_i$.

Now note that if $i \in F^c$ then $Q(u_i | u_0^{i-1}, \bar{y}) = P(u_i | u_0^{i-1}, \bar{y})$, so that these terms vanish. The above sum therefore reduces to

$$\sum_{\bar{u}} \left| \sum_{i \in F} \underbrace{(Q(u_i | u_0^{i-1}, \bar{y}) - P(u_i | u_0^{i-1}, \bar{y}))}_{\leq \frac{1}{2} - P(u_i | u_0^{i-1}, \bar{y})} \right|.$$

$$\begin{aligned}
&\left(\prod_{j=0}^{i-1} P(u_j | u_0^{j-1}, \bar{y}) \right) \left(\prod_{j=i+1}^{N-1} Q(u_j | u_0^{j-1}, \bar{y}) \right) \Big] \Big| \\
&\leq \sum_{i \in F} \sum_{u_0^i} \left| \frac{1}{2} - P(u_i | u_0^{i-1}, \bar{y}) \right| \prod_{j=0}^{i-1} P(u_j | u_0^{j-1}, \bar{y}) \\
&\leq 2 \sum_{i \in F} \mathbb{E}_{P_{\bar{U} | \bar{Y} = \bar{y}}} \left[\left| \frac{1}{2} - P_{U_i | U_0^{i-1}, \bar{Y}}(0 | U_0^{i-1}, \bar{y}) \right| \right].
\end{aligned}$$

In the last step the summation over u_i gives rise to the factor 2, whereas the summation over u_0^{i-1} gives rise to the expectation.

Note that $Q_{\bar{Y}}(\bar{y}) = P_{\bar{Y}}(\bar{y}) = \frac{1}{2^N}$. The claim follows by taking the expectation over \bar{Y} . ■

Lemma 6 (Distortion under Q versus Distortion under P): Let F be chosen such that for $i \in F$

$$\mathbb{E}_P \left[\left| \frac{1}{2} - P_{U_i | U_0^{i-1}, \bar{Y}}(0 | U_0^{i-1}, \bar{Y}) \right| \right] \leq \delta_N. \quad (4)$$

The average distortion is then bounded by

$$\frac{1}{N} \mathbb{E}_Q[d(\bar{Y}, \bar{U} G_2^{\otimes n})] \leq \frac{1}{N} \mathbb{E}_P[d(\bar{Y}, \bar{U} G_2^{\otimes n})] + |F| 2\delta_N.$$

Proof:

$$\begin{aligned}
&\mathbb{E}_Q[d(\bar{Y}, \bar{U} G_2^{\otimes n})] - \mathbb{E}_P[d(\bar{Y}, \bar{U} G_2^{\otimes n})] \\
&= \sum_{\bar{u}, \bar{y}} (Q(\bar{u}, \bar{y}) - P(\bar{u}, \bar{y})) d(\bar{y}, \bar{u} G_2^{\otimes n}) \\
&\leq N \sum_{\bar{u}, \bar{y}} |Q(\bar{u}, \bar{y}) - P(\bar{u}, \bar{y})| \\
&\stackrel{\text{Lem. 5}}{\leq} 2N \sum_{i \in F} \mathbb{E}_P \left[\left| \frac{1}{2} - P_{U_i | U_0^{i-1}, \bar{Y}}(0 | U_0^{i-1}, \bar{Y}) \right| \right] \\
&\leq |F| 2N \delta_N.
\end{aligned}$$

From Lemma 6 we see that the average (over \bar{y} as well as u_F) distortion is upper bounded by the average distortion with respect to P plus a term which bounds the “distance” between Q and P .

Lemma 7 (Distortion under P):

$$\mathbb{E}_P[d(\bar{Y}, \bar{U} G_2^{\otimes n})] = ND.$$

The proof follows from the fact that $\bar{U} G_2^{\otimes n} = \bar{X}$ and $\Pr(Y_i \neq X_i) = D$. The lemma implies that if we use all the variables $\{U_i\}$ to represent the source word, i.e., F is empty, then the algorithm results in an average distortion D . But the rate of such a code would be 1. Fortunately, the last problem is easily fixed. If we choose F to consist of those variables which are “essentially random,” then there is only a small distortion penalty (namely, $|F| 2\delta_N$) to pay with respect to the previous case. But the rate has been decreased to $1 - |F|/N$.

Lemma 6 shows that the guiding principle for choosing the set F is to include the indices with small δ_N in (4). In the following lemma, we find a sufficient condition for an index to satisfy (4), which is easier to handle.

Lemma 8 ($Z(W_N^{(i)})$ Close to 1 is Good): If $Z(W_N^{(i)}) \geq 1 - 2\delta_N^2$, then

$$\mathbb{E}_P \left[\left| \frac{1}{2} - P_{U_i | U_0^{i-1}, \bar{Y}}(0 | U_0^{i-1}, \bar{Y}) \right| \right] \leq \delta_N.$$

For the proof, please refer to [17]. Intuitively, the above lemma means that if $Z(W_N^{(i)})$ is close to 1, then given the output of $W_N^{(i)}$, which is (Y, U_0^{i-1}) , the input U_i is close to being random, i.e., the posteriors are close to $\frac{1}{2}$.

We are now ready to prove Theorem 3. In order to show that there exists a polar code which achieves the rate-distortion tradeoff, we show that the size of the set F can be made arbitrarily close to $Nh_2(D)$ while keeping the penalty term $|F|2\delta_N$ arbitrarily small.

Proof of Theorem 3: Let $\beta < \frac{1}{2}$ be a constant and let $\delta_N = \frac{1}{2N}2^{-N^\beta}$. Consider a polar code with frozen set F_N ,

$$F_N = \{i \in \{0, \dots, N-1\} : Z(W_N^{(i)}) \geq 1 - 2\delta_N^2\}.$$

For N sufficiently large there exists a $\beta' < \frac{1}{2}$ such that $2\delta_N^2 > 2^{-N^{\beta'}}$. By choosing W to be a BSC(D), and using Theorem 9 and equation (7) we get

$$\lim_{N=2^n, n \rightarrow \infty} \frac{|F_N|}{N} = h_2(D). \quad (5)$$

The above equation implies that for any $\epsilon > 0$ and for N sufficiently large there exists a set F_N such that

$$\frac{|F_N|}{N} \geq h_2(D) - \epsilon.$$

In other words

$$R_N = 1 - \frac{|F_N|}{N} \leq R(D) + \epsilon.$$

Finally, from Lemma 6 we know that

$$D_N(F_N) \leq D + 2|F_N|\delta_N \leq D + O(2^{-(N^\beta)}) \quad (6)$$

for any $0 < \beta < \frac{1}{2}$.

Recall that $D_N(F_N)$ is the average of the distortion over all choices of u_{F_N} . Since the average distortion fulfills (6) it follows that there must be at least one choice of u_{F_N} for which

$$D_N(F_N, u_{F_N}) \leq D + O(2^{-(N^\beta)})$$

for any $0 < \beta < \frac{1}{2}$.

As shown in [14], the complexity of both the encoding and the decoding algorithm is $O(N \log(N))$. ■

APPENDIX

For any B-DMC $W : \{0, 1\} \rightarrow \mathcal{Y}$, the B-DMCs $W^{[i]} : \{0, 1\} \rightarrow \mathcal{Y} \times \mathcal{Y} \times \{0, 1\}^{i-1}$ are defined as follows. Let $W^{[0]}$ denote the channel law

$$W^{[0]}(y_0, y_1 | u_0) = \frac{1}{2} \sum_{u_1} W(y_0 | u_0 \oplus u_1) W(y_1 | u_1),$$

and let $W^{[1]}$ denote the channel law

$$W^{[1]}(y_0, y_1, u_0 | u_1) = \frac{1}{2} W(y_0 | u_0 \oplus u_1) W(y_1 | u_1).$$

Define a random variable W_n through a tree process $\{W_n; n \geq 0\}$ with

$$W_0 = W,$$

$$W_{n+1} = W_n^{[B_{n+1}]},$$

where $\{B_n; n \geq 1\}$ is a sequence of i.i.d. $\text{Ber}(\frac{1}{2})$ random variables. We augment the above process by the process $\{Z_n; n \geq 0\} := \{Z(W_n); n \geq 0\}$. The relevance of this process is that $W_n \in \{W_N^{(i)}\}_{i=0}^{N-1}$ and moreover the symmetric distribution of the random variables B_i implies

$$\Pr(Z_n \in (a, b)) = \frac{|\{i \in \{0, \dots, N-1\} : Z(W_N^{(i)}) \in (a, b)\}|}{N}. \quad (7)$$

As seen in Lemma 8, for lossy source compression, the important quantity is the rate at which the random variable Z_n approaches 1. Using similar techniques as in [18], we can show the following. For the proof please refer to [17].

Theorem 9 (Rate of Z_n Approaching 1): Given a B-DMC W , and any $\beta < \frac{1}{2}$,

$$\lim_{n \rightarrow \infty} \Pr(Z_n \geq 1 - 2^{-2^{n^\beta}}) = 1 - I(W).$$

REFERENCES

- [1] C. E. Shannon, "Coding theorems for a discrete source with a fidelity criterion," *IRE Nat. Conv. Rec.*, pt. 4, vol. 27, pp. 142–163, 1959.
- [2] T. J. Goblick, Jr., "Coding for discrete information source with a distortion measure," Ph.D. dissertation, MIT, 1962.
- [3] T. Berger, *Rate Distortion Theory*. London: Prentice Hall, 1971.
- [4] A. J. Viterbi and J. K. Omura, "Trellis encoding of memoryless discrete-time sources with a fidelity criterion," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 325–332, 1974.
- [5] Y. Matsunaga and H. Yamamoto, "A coding theorem for lossy data compression by LDPC codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 9, pp. 2225–2229, 2003.
- [6] M. J. Wainwright and E. Martinian, "Low-density graph codes that are optimal for source/channel coding and binning," *IEEE Trans. Inform. Theory*, vol. 55, no. 3, pp. 1061–1079, 2009.
- [7] E. Martinian and J. Yedidia, "Iterative quantization using codes on graphs," in *Proc. of the Allerton Conf. on Commun., Control, and Computing*, Monticello, IL, USA, 2003.
- [8] T. Murayama, "Thouless-Anderson-Palmer approach for lossy compression," *J. Phys. Rev. E: Stat. Nonlin. Soft Matter Phys.*, vol. 69, 2004.
- [9] S. Ciliberti, M. Mézard, and R. Zecchina, "Lossy data compression with random gates," *Physical Rev. Lett.*, vol. 95, no. 038701, 2005.
- [10] A. Braunstein, M. Mézard, and R. Zecchina, "Survey propagation: Algorithm for satisfiability," *Random Structures and Algorithms*, vol. 28, pp. 340–373, 2006.
- [11] M. J. Wainwright and E. Maneva, "Lossy source coding via message-passing and decimation over generalized codewords of LDGM codes," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Adelaide, Australia, Sept. 2005, pp. 1493–1497.
- [12] T. Filler and J. Fridrich, "Binary quantization using belief propagation with decimation over factor graphs of LDGM codes," in *Proc. of the Allerton Conf. on Commun., Control, and Computing*, Monticello, IL, USA, 2007.
- [13] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, EPFL, Lausanne, Switzerland, July 2009.
- [14] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *accepted for publication in IEEE Trans. Inform. Theory*, 2009.
- [15] A. Montanari, F. Ricci-Tersenghi, and G. Semerjian, "Solving constraint satisfaction problems through belief propagation-guided decimation," in *Proc. of the Allerton Conf. on Commun., Control, and Computing*, Monticello, USA, Sep 26–Sep 28 2007.
- [16] N. Hussami, S. B. Korada, and R. Urbanke, "Performance of polar codes for channel and source coding," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Seoul, South Korea, July 2009, pp. 1488–1492.
- [17] S. B. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," *submitted to IEEE Trans. Inform. Theory*, 2009.
- [18] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Seoul, South Korea, July 2009, pp. 1493–1495.