Polar Codes are Optimal for Lossy Source Coding

Satish Babu Korada and Rüdiger Urbanke

***Abstract*— We consider lossy source compression of a binary symmetric source using polar codes and the low-complexity successive encoding algorithm. It was recently shown by Arıkan that polar codes achieve the capacity of arbitrary symmetric binary-input discrete memoryless channels under a successive decoding strategy. We show the equivalent result for lossy source compression, i.e., we show that this combination achieves the rate-distortion bound for a binary symmetric source. We further show the optimality of polar codes for various problems including the binary Wyner-Ziv and the binary Gelfand-Pinsker problem.**

I. Introduction

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

$$\mathtt{d}(0,0) = \mathtt{d}(1,1) = 0, \mathtt{d}(0,1) = 1.$$

It is well known that in order to compress Y with average distortion D the rate R has to be at least $R(D) = 1 - h_2(D)$, where $h_2(\cdot)$ is the binary entropy function [1], [2, Theorem 10.3.1]. Shannon's proof of this rate-distortion bound is based on a random coding argument.

It was shown by Goblick that in fact linear codes are sufficient to achieve the rate-distortion bound [3],[4, Section 6.2.3].

Trellis based quantizers [5] 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 also 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 [6] 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, Martininian and Wainwright [7] proved that properly chosen MN codes with *bounded* degrees are sufficient to achieve the rate-distortion bound under optimal encoding.

EPFL, School of Computer, & Communication Sciences, Lausanne, CH-1015, Switzerland, {satish.korada, ruediger.urbanke}@epfl.ch. This work was partially supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322.

Much less is known about the performance of sparse graph codes under *message-passing* encoding. In [8] 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 if the parity check density is $o(\log(N))$ but that 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 [9]. 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 [10] 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 [11], 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 [10] 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 [8] 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 [12] 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 [13] 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. This suggests that in fact the more sophisticated algorithms like SID may not even be necessary.

In [14] the authors consider a different approach. They show that for any fixed $\gamma, \epsilon > 0$ the rate-distortion pair $(R(D) + \gamma, D+\epsilon)$ can be achieved with complexity $C_1(\gamma)\epsilon^{-C_2(\gamma)}N$. Of course, the complexity diverges as γ and ϵ are made smaller. The idea there is to concatenate a small code of rate $R+\gamma$ with expected distortion $D + \epsilon$. The source sequence is then split into blocks of size equal to the code. The concentration with

respect to the blocklength implies that under MAP decoding the probability that the distortion is larger than $D+\epsilon$ vanishes.

Polar codes, introduced by Arıkan in [15], are the first provably capacity achieving codes for arbitrary symmetric binary-input discrete memoryless channels (B-DMC) with low encoding and decoding complexity. These codes are naturally suited for decoding via successive cancellation (SC) [15]. It was pointed out in [15] that an SC decoder can be implemented with $\Theta(N\log(N))$ complexity.

We show that polar codes with an SC encoder are also optimal for lossy source compression. More precisely, we show that for any design distortion $0 < D < \frac{1}{2}$, and any $\delta > 0$ and $0 < \beta < \frac{1}{2}$, there exists a sequence of polar codes of rate at most $R(D)+\delta$ and increasing length N so that their expected distortion is at most $D+O(2^{-(N^\beta)})$. Their encoding as well as decoding complexity is $\Theta(N\log(N))$.

II. Introduction to Polar Codes

Let $W : \{0,1\} \to \mathcal{Y}$ 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 U denotes a random variable and and u denotes its realization. Let $\bar{U}$ denote the random vector $(U_0,\ldots,U_{N-1})$. For any set F, $|F|$ denotes its cardinality. Let $\bar{U}_F$ denote $(U_{i_1},\ldots,U_{i_{|F|}})$ and let $\bar{u}_F$ denote $(u_{i_1},\ldots,u_{i_{|F|}})$, where $\{i_k \in F : i_k \le i_{k+1}\}$. Let U_i^j denote the random vector $(U_i,\ldots,U_j)$ and, similarly, u_i^j denotes $(u_i,\ldots,u_j)$. We use the equivalent notation for other random variables like X or Y. Let $\mathrm{Ber}(p)$ denote a Bernoulli random variable with $\Pr(1) = p$.

The polar code construction is based on the following observation. Let

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{1}$$

Let $A_n : \{0,\ldots,2^n-1\} \to \{0,\ldots,2^n-1\}$ be a permutation defined by the bit-reversal operation in [15]. Apply the transform $A_nG_2^{\otimes n}$ (where "$\otimes n$" denotes the n^{th} Kronecker power) to a block of $N = 2^n$ bits and transmit the output through independent copies of a B-DMC W (see Figure 1). As n grows large, the channels seen by individual bits (suitably defined in [15]) start *polarizing*: they approach either a noiseless channel or a pure-noise channel, where the fraction of channels becoming noiseless is close to the symmetric mutual information $I(W)$.

In what follows, let $H_n = A_nG_2^{\otimes n}$. Consider a random vector $\bar{U}$ that is uniformly distributed over $\{0,1\}^N$. Let $\bar{X} = \bar{U}H_n$, where the multiplication is performed over GF(2). Let $\bar{Y}$ be the result of sending the components of $\bar{X}$ over the channel W. Let $P(\bar{U},\bar{X},\bar{Y})$ denote the induced probability distribution on the set $\{0,1\}^N \times \{0,1\}^N \times \mathcal{Y}^N$. The channel

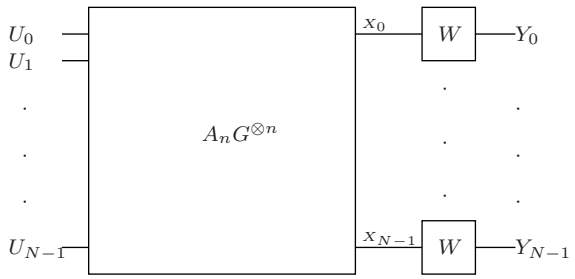

Fig. 1. The transform $A_nG_2^{\otimes n}$ is applied to the information word $\bar{U}$ and the resulting vector $\bar{X}$ is transmitted through the channel W. The received word is $\bar{Y}$.

between $\bar{U}$ and $\bar{Y}$ is defined by the transition probabilities

$$P_{\bar{Y}\,|\,\bar{U}}(\bar{y}\,|\,\bar{u}) = \prod_{i=0}^{N-1} W(y_i\,|\,x_i) = \prod_{i=0}^{N-1} W(y_i\,|\,(\bar{u}H_n)_i).$$

Define $W^{(i)} : \{0,1\} \to \mathcal{Y}^N \times \{0,1\}^{i-1}$ as the channel with input u_i, output (y_0^{N-1}, u_0^{i-1}), and transition probabilities given by

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

Let $Z^{(i)}$ denote the Bhattacharyya parameter of the channel $W^{(i)}$,

$$Z^{(i)} = \sum_{y_0^{N-1}, u_0^{i-1}} \sqrt{W^{(i)}(y_0^{N-1}, u_0^{i-1}\,|\,0)W^{(i)}(y_0^{N-1}, u_0^{i-1}\,|\,1)}. \tag{3}$$

The SC decoder operates as follows: the bits U_i are decoded in the order 0 to $N-1$. The likelihood of U_i is computed using the channel law $W^{(i)}(\bar{y}, \hat{u}_0^{i-1}\,|\,u_i)$, where $\hat{u}_0^{i-1}$ are the estimates of the bits U_0^{i-1} from the previous decoding steps.

In [15] it was shown that the fraction of the channels $W^{(i)}$ that are approximately noiseless approaches $I(W)$. More precisely, it was shown that the $\{Z^{(i)}\}$ satisfy

$$\lim_{n\to\infty} \frac{|\left\{i \in \{0,\ldots,2^n-1\} : Z^{(i)} < 2^{-\frac{5n}{4}}\right\}|}{2^n} = I(W). \tag{4}$$

In [16], the above result was significantly strengthened to

$$\lim_{n\to\infty} \frac{|\left\{i \in \{0,\ldots,2^n-1\} : Z^{(i)} < 2^{-2^{n\beta}}\right\}|}{2^n} = I(W), \tag{5}$$

which is valid for any $0 \le \beta < \frac{1}{2}$.

This suggests to use these noiseless channels (i.e., those channels at position i so that $Z^{(i)} < 2^{-2^{n\beta}}$) for transmitting information while fixing the symbols transmitted through the remaining channels to a value known both to sender as well to the receiver. Following Arıkan, call those components U_i of $\bar{U}$ which are fixed "frozen," (denote this set of positions as F) and the remaining ones "information" bits. If the channel

W is symmetric we can assume without loss of generality that the fixed positions are set to 0. In [15] it was shown that the block error probability of the SC decoder is bounded by $\sum_{i\in F} Z^{(i)}$, which is of order $O(2^{-2^{n\beta}})$ for our choice. Since the fraction of approximately noiseless channels tends to $I(W)$, this scheme achieves the capacity of the underlying symmetric B-DMC W.

In [15] the following alternative interpretation was mentioned; the above procedure can be seen as transmitting a codeword of a code defined through its generator matrix as follows. A polar code of dimension $0 \le k \le 2^n$ is defined by choosing a subset of the rows of H_n as the generator matrix. The choice of the generator vectors is based on the values of $Z^{(i)}$. A polar code is then defined as the set of codewords of the form $\bar{x} = \bar{u}H_n$, where the bits $i \in F$ are fixed to 0. The well known Reed-Muller codes can be considered as special cases of polar codes with a particular rule for the choice of F.

Polar codes with SC decoding have an interesting, and of as yet not fully explored, connection to the recursive decoding of Reed-Muller codes as proposed by Dumer [17]. The Plotkin $(u, u+v)$ construction in Dumer's algorithm plays the role of the channel combining and channel splitting for polar codes. Perhaps the two most important differences are (i) the construction of the code itself (how the frozen vectors are chosen), and (ii) the actual decoding algorithm and the order in which information bits are decoded. A better understanding of this connection might lead to improved decoding algorithms for both constructions.

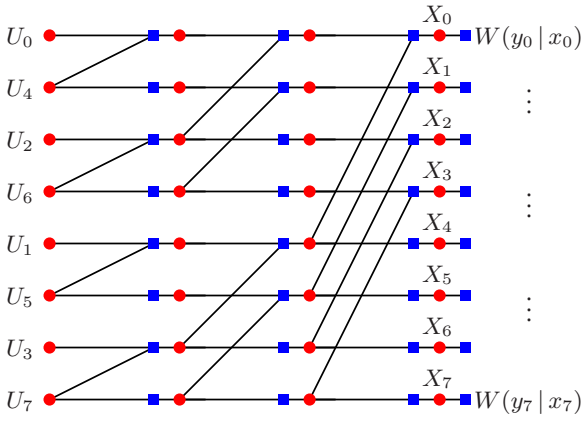

Fig. 2. Factor graph representation used by the SC decoder. $W(y_i \mid x_i)$ is the initial prior of the variable X_i, when y_i is received at the output of a symmetric B-DMC W.

To summarize, the SC decoder operates as follows.

For each i in the range 0 till $N-1$:

(i) If $i \in F$, then set $u_i = 0$.

(ii) If $i \in F^c$, then compute

$$l_i(\bar{y}, u_0^{i-1}) = \frac{W^{(i)}(\bar{y}, u_0^{i-1} \mid u_i = 0)}{W^{(i)}(\bar{y}, u_0^{i-1} \mid u_i = 1)}$$

and set

$$u_i = \begin{cases} 0, & \text{if } l_i > 1, \\ 1, & \text{if } l_i \le 1. \end{cases} \tag{6}$$

As explained in [15] using the factor graph representation shown in Figure 2, the SC decoder can be implemented with complexity $\Theta(N\log(N))$. A similar representation was considered for decoding of Reed-Muller codes by Forney in [18].

A. Decimation and Random Rounding

In the setting of channel coding there is typically one codeword (namely the transmitted one) which has a posterior that is significantly larger than all other codewords. This makes it possible for a greedy message-passing algorithm to successfully move towards this codeword in small steps, using at any given moment "local" information provided by the decoder.

In the case of lossy source compression there are typically many codewords that, if chosen, result in similar distortion. Let us assume that these "candidates" are roughly uniformly spread around the source word to be compressed. It is then clear that a local decoder can easily get "confused," producing locally conflicting information with regards to the "direction" into which one should compress.

A standard way to overcome this problem is to combine the message-passing algorithm with *decimation* steps. This works as follows; first run the iterative algorithm for a fixed number of iterations and subsequently decimate a small fraction of the bits. More precisely, this means that for each bit which we decide to decimate we choose a *value*. We then remove the decimated variable nodes and adjacent edges from the graph. One is hence left with a *smaller* instance of essentially the same problem. The same procedure is then repeated on the reduced graph and this cycle is continued until all variables have been decimated.

One can interpret the SC operation as a kind of decimation where the order of the decimation is fixed in advance $(0, \dots, N-1)$. In fact, the SC decoder can be interpreted as a particular instance of a BID.

When making the decision on bit U_i using the SC decoder, it is natural to choose that value for U_i which maximizes the posterior. Indeed, such a scheme works well in practice for source compression. For the analysis however it is more convenient to use *randomized rounding*. In each step, instead of making the MAP decision we replace (6) with

$$u_i = \begin{cases} 0, & \text{w.p. } \frac{l_i}{1+l_i}, \\ 1, & \text{w.p. } \frac{1}{1+l_i}. \end{cases}$$

In words, we make the decision proportional to the likelihoods. Randomized rounding as a decimation rule is not new. E.g., in [19] it was used to analyze the performance of BID for random K-SAT problems.

For lossy source compression, the SC operation is employed at the encoder side to map the source vector to a codeword. Therefore, from now onwards we refer to this operation as SC *encoding*.

III. Main Result

A. Statement

Theorem 1 (Polar Codes Achieve the Rate-Distortion Bound): 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 $\Theta(N \log(N))$.

B. Simulation Results and Discussion

Let us consider how polar codes behave 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 BSC(D) and let $R = R(D) + \delta$ for some $\delta > 0$.

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

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

For the source compression, on the other hand, F consists of all those indices i so that $Z^{(i)} \geq 1 - \delta$, i.e., of all those indices corresponding to *very* large values of $Z^{(i)}$.

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 3 shows the performance of the SC encoding algorithm combined with randomized rounding. As asserted by Theorem 1, the points approach the rate-distortion bound as the block length increases.

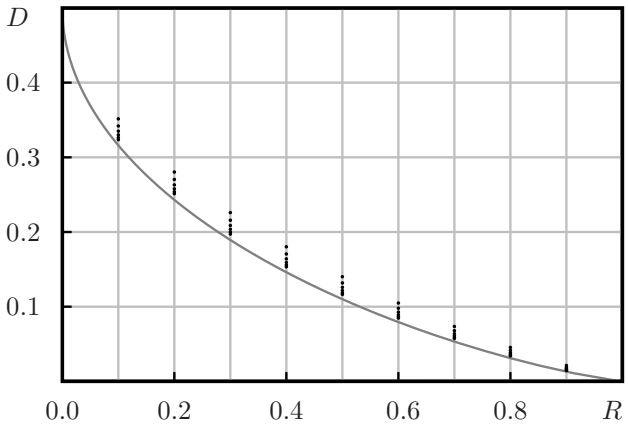

Fig. 3. The rate-distortion performance for the SC encoding algorithm with randomized rounding for $n = 9, 11, 13, 15, 17$ and 19. As the block length increases the points move closer to the rate-distortion bound.

In [20] the performance of polar codes for lossy source compression was already investigated empirically. Note that the construction used in [20] is different from the current construction. Let us recall. Consider a BSC(p), where $p = h_2^{-1}(1 - h_2(D))$. Let the corresponding Bhattacharyya constants be $\tilde{Z}^{(i)}$s. In [20] first a channel code of rate $1 - h_2(p) - \epsilon$ is constructed according to the values $\tilde{Z}^{(i)}$s. Let $\tilde{F}$ be the corresponding frozen set. The set F for the source code is given by

$$F = \{N - 1 - i : i \in \tilde{F}^c\}.$$

The rationale behind this construction is that the resulting source code is the dual of the channel code designed for the BSC(p). The rate of the resulting source code is equal to $h_2(p) + \epsilon = 1 - h_2(D) + \epsilon$. Although this code construction is different, empirically the resulting frozen sets are very similar.

There is also a slight difference with respect to the decimation algorithm. In [20] the decimation step is based on MAP estimates, whereas in the current setting we use randomized rounding.

Despite all these differences the performance of both schemes is comparable.

IV. The Proof

From now on we restrict W to be a BSC(D), i.e.,

$$W(0 \,|\, 1) = W(1 \,|\, 0) = D,$$
$$W(0 \,|\, 0) = W(1 \,|\, 1) = 1 - D.$$

As immediate consequence we have

$$W(y \,|\, x) = W(y \oplus z \,|\, x \oplus z). \tag{7}$$

This extends in a natural way if we consider vectors.

A. The Standard Source Coding Model

Let us describe lossy source compression using polar codes in more detail. We refer to this as the "Standard Model." In the following we assume that we want to compress the source with average distortion D.

Model: Let $\bar{y} = (y_0, \ldots, y_{N-1})$ denote N i.i.d. realizations of the source Y. Let $F \subseteq \{0, \ldots, N-1\}$ and let $\tilde{u}_F \in \{0,1\}^{|F|}$ be a fixed vector. In the sequel we use the shorthand "SM$(F, \tilde{u}_F)$" to denote the Standard Model with frozen set F whose components are fixed to $\tilde{u}_F$. It is defined as follows.

Encoding: Let $f^{\tilde{u}_F} : \{0,1\}^N \to \{0,1\}^{N-|F|}$ denote the *encoding* function. For a given $\bar{y}$ we first compute $\bar{u}$, as described below, where $\bar{u} = (u_0, \ldots, u_{N-1})$. Then $f^{\tilde{u}_F}(\bar{y}) = \bar{u}_{F^c}$.

Given $\bar{y}$, for each i in the range 0 till $N-1$:

(i) Compute

$$l_i(\bar{y}, u_0^{i-1}) \triangleq \frac{W^{(i)}(\bar{y}, u_0^{i-1} \,|\, u_i = 0)}{W^{(i)}(\bar{y}, u_0^{i-1} \,|\, u_i = 1)}.$$

(ii) If $i \in F^c$ then set $u_i = 0$ with probability $\frac{l_i}{1+l_i}$ and equal to 1 otherwise; if $i \in F$ then set $u_i = \tilde{u}_i$.

Decoding: The decoding function $\hat{f}^{\tilde{u}_F} : \{0,1\}^{N-|F|} \to \{0,1\}^N$ maps $\bar{u}_{F^c}$ back to the *reconstruction point* $\bar{x}$ via $\bar{x} = \bar{u} H_n$, where $\bar{u}_F = \tilde{u}_F$.

Distortion: The average distortion incurred by this scheme is given by $\mathbb{E}[\mathrm{d}(\bar{Y}, \bar{X})]$, where the expectation is over the

source randomness and the randomness involved in the randomized rounding at the encoder.

Complexity: The encoding (decoding) task for source coding is the same as the decoding (encoding) task for channel coding. As remarked before, both have complexity $\Theta(N \log N)$.

Remark: Recall that l_i is the posterior of the variable U_i given the observations $\bar{Y}$ as well as $\bar{U}_0^{i-1}$, under the assumption that $\bar{U}$ has uniform prior and that $\bar{Y}$ is the result of transmitting $\bar{U}H_n$ over a BSC(D).

B. Computation of Average Distortion

The encoding function $f^{\tilde{u}_F}$ 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) $P_{U_i \,|\, U_0^{i-1},\bar{Y}}(u_i \,|\, u_0^{i-1}, \bar{y})$. This implies that the probability of picking a vector $\bar{u}$ given $\bar{y}$ is equal to

$$\begin{cases} 0, & \bar{u}_F \neq \tilde{u}_F, \\ \prod_{i \in F^c} P_{U_i \,|\, U_0^{i-1},\bar{Y}}(u_i \,|\, u_0^{i-1}, \bar{y}), & \bar{u}_F = \tilde{u}_F. \end{cases}$$

Therefore, the average (over $\bar{y}$ and the randomness of the encoder) distortion of SM$(F, \tilde{u}_F)$ is given by

$$D_N(F, \tilde{u}_F) = \sum_{\bar{y} \in \{0,1\}^N} \frac{1}{2^N} \sum_{\bar{u}_{F^c} \in \{0,1\}^{|F^c|}} \prod_{i \in F^c} P(u_i \,|\, u_0^{i-1}, \bar{y}) \mathtt{d}(\bar{y}, \bar{u}H_n), \tag{8}$$

where $U_i = \tilde{u}_i$ for $i \in F$.

We want to to show that there exists a set F of cardinality roughly $Nh_2(D)$ and a vector $\tilde{u}_F$ such that $D_N(F, \tilde{u}_F) \approx D$. This will show that polar codes achieve the rate-distortion bound.

For the proof it is more convenient not to determine the distortion for a fixed choice of $\tilde{u}_F$ but to compute the average distortion over all possible choices (with a uniform distribution over these choices). Later, in Section V, we will see that the distortion *does not depend* on the choice of $\tilde{u}_F$. A convenient choice is therefore to set it to zero. This will lead to the desired final result.

Let us therefore start by computing the *average distortion*. Let $D_N(F)$ denote the distortion obtained by averaging $D_N(F, \tilde{u}_F)$ over all $2^{|F|}$ possible values of $\tilde{u}_F$. We will show that $D_N(F)$ is close to D.

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

$$\begin{aligned} D_N(F) &= \sum_{\tilde{u}_F \in \{0,1\}^{|F|}} \frac{1}{2^{|F|}} D_N(F, \tilde{u}_F) \\ &= \sum_{\tilde{u}_F} \frac{1}{2^{|F|}} \sum_{\bar{y}} \frac{1}{2^N} \\ &\quad \sum_{\bar{u}_{F^c}} \prod_{i \in F^c} P(u_i \,|\, u_0^{i-1}, \bar{y}) \mathtt{d}(\bar{y}, \bar{u}H_n) \\ &= \sum_{\bar{y}} \frac{1}{2^N} \sum_{\bar{u}} \frac{1}{2^{|F|}} \prod_{i \in F^c} P(u_i \,|\, u_0^{i-1}, \bar{y}) \mathtt{d}(\bar{y}, \bar{u}H_n). \end{aligned}$$

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

$$Q(u_i \,|\, u_0^{i-1}, \bar{y}) = \begin{cases} \frac{1}{2}, & \text{if } i \in F, \\ P_{U_i \,|\, U_0^{i-1},\bar{Y}}(u_i \,|\, u_0^{i-1}, \bar{y}), & \text{if } i \in F^c. \end{cases} \tag{9}$$

Then,

$$D_N(F) = \mathbb{E}_Q[\mathtt{d}(\bar{Y}, \bar{U}H_n)],$$

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 2 (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

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

Proof:

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

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

$$A_0^{N-1} - B_0^{N-1} = \sum_{i=0}^{N-1} A_0^i B_{i+1}^{N-1} - \sum_{i=0}^{N-1} A_0^{i-1} B_i^{N-1},$$

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

$$\sum_{\bar{u}} \Big| \sum_{i \in F} \Big[\underbrace{\big(Q(u_i \,|\, u_0^{i-1}, \bar{y}) - P(u_i \,|\, u_0^{i-1}, \bar{y}) \big)}_{\leq |\, \frac{1}{2} - P(u_i \,|\, u_0^{i-1}, \bar{y}) \,|} \cdot$$

$$\Big(\prod_{j=0}^{i-1} P(u_j \,|\, u_0^{j-1}, \bar{y})\Big)\Big(\prod_{j=i+1}^{N-1} Q(u_j \,|\, u_0^{j-1}, \bar{y})\Big)\Big]\Big|$$
$$\le \sum_{i\in F}\sum_{\bar{u}_0^i} \Big|\frac{1}{2} - P(u_i \,|\, u_0^{i-1}, \bar{y})\Big| \prod_{j=0}^{i-1} P(u_j \,|\, u_0^{j-1}, \bar{y})$$
$$\le 2\sum_{i\in F} \mathbb{E}_{P_{\bar{U}\,|\,\bar{Y}=\bar{y}}}\left[\Big|\frac{1}{2} - P_{U_i\,|\,U_0^{i-1},\bar{Y}}(0\,|\,U_0^{i-1},\bar{y})\Big|\right].$$

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

$$\mathbb{E}_P\left[\Big|\frac{1}{2} - P_{U_i\,|\,U_0^{i-1},\bar{Y}}(0\,|\,U_0^{i-1},\bar{Y})\Big|\right] \le \delta_N. \qquad (10)$$

The average distortion is then bounded by

$$\frac{1}{N}\mathbb{E}_Q[\mathtt{d}(\bar{Y},\bar{U}H_n)] \le \frac{1}{N}\mathbb{E}_P[\mathtt{d}(\bar{Y},\bar{U}H_n)] + |F|2\delta_N.$$

Proof:

$$\mathbb{E}_Q[\mathtt{d}(\bar{Y},\bar{U}H_n)] - \mathbb{E}_P[\mathtt{d}(\bar{Y},\bar{U}H_n)]$$
$$= \sum_{\bar{u},\bar{y}} \Big(Q(\bar{u},\bar{y}) - P(\bar{u},\bar{y})\Big)\mathtt{d}(\bar{y},\bar{u}H_n)$$
$$\le N\sum_{\bar{u},\bar{y}} \Big|Q(\bar{u},\bar{y}) - P(\bar{u},\bar{y})\Big|$$
$$\overset{\text{Lem. 2}}{\le} 2N\sum_{i\in F}\mathbb{E}_P\left[\Big|\frac{1}{2} - P_{U_i\,|\,U_0^{i-1},\bar{Y}}(0\,|\,U_0^{i-1},\bar{Y})\Big|\right]$$
$$\le |F|2N\delta_N.$$

∎

From Lemma 3 we see that the average (over $\bar{y}$ as well as $\tilde{u}_F$) distortion of the Standard Model is upper bounded by the average distortion with respect to P plus a term which bounds the "distance" between Q and P.

Lemma 4 (Distortion under P):

$$\mathbb{E}_P[\mathtt{d}(\bar{Y},\bar{U}H_n)] = ND.$$

Proof: Let $\bar{X} = \bar{U}H_n$ and write

$$\mathbb{E}_P[\mathtt{d}(\bar{Y},\bar{U}H_n)]$$
$$= \sum_{\bar{u},\bar{y}} P_{\bar{U},\bar{Y}}(\bar{u},\bar{y})\ \mathtt{d}(\bar{y},\bar{u}H_n)$$
$$= \sum_{\bar{y},\bar{u},\bar{x}} P_{\bar{U},\bar{X},\bar{Y}}(\bar{u},\bar{x},\bar{y})\ \mathtt{d}(\bar{y},\bar{u}H_n)$$
$$= \sum_{\bar{y},\bar{u},\bar{x}} P_{\bar{X},\bar{Y}}(\bar{x},\bar{y})\underbrace{P_{\bar{U}\,|\,\bar{X},\bar{Y}}(\bar{u}\,|\,\bar{x},\bar{y})}_{\{0,1\}\text{-valued}}\ \mathtt{d}(\bar{y},\bar{x})$$
$$= \sum_{\bar{y},\bar{x}} P_{\bar{X},\bar{Y}}(\bar{x},\bar{y})\ \mathtt{d}(\bar{y},\bar{x}).$$

Note that the unconditional distribution of $\bar{X}$ as well as $\bar{Y}$ is the uniform one and that the channel between $\bar{X}$ and $\bar{Y}$ is memoryless and identical for each component. Therefore, we can write this expectation as

$$\mathbb{E}_P[\mathtt{d}(\bar{Y},\bar{U}H_n)] = N\sum_{x_0,y_0} P_{X_0,Y_0}(x_0,y_0)\ \mathtt{d}(y_0,x_0)$$
$$\overset{(a)}{=} N\sum_{x_0} P_{X_0}(x_0)\sum_{y_0} W(y_0\,|\,x_0)\ \mathtt{d}(y_0,x_0)$$
$$= NW(0\,|\,1) \overset{(b)}{=} ND.$$

In the above equation, (a) follows from the fact that $P_{Y\,|\,X}(y\,|\,x) = W(y\,|\,x)$, and (b) follows from our assumption that W is a BSC(D). ∎

This 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 3 shows that the guiding principle for choosing the set F is to include the indices with small δ_N in (10). In the following lemma, we find a sufficient condition for an index to satisfy (10), which is easier to handle.

Lemma 5 ($Z^{(i)}$ Close to 1 is Good): If $Z^{(i)} \ge 1 - 2\delta_N^2$, then

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

Proof:

$$\mathbb{E}_P\left[\sqrt{P_{U_i\,|\,U_0^{i-1},\bar{Y}}(0\,|\,U_0^{i-1},\bar{Y})P_{U_i\,|\,U_0^{i-1},\bar{Y}}(1\,|\,U_0^{i-1},\bar{Y})}\right]$$
$$= \sum_{u_0^{i-1},\bar{y}} P_{U_0^{i-1},\bar{Y}}(u_0^{i-1},\bar{y})$$
$$\sqrt{P_{U_i\,|\,U_0^{i-1},\bar{Y}}(0\,|\,u_0^{i-1},\bar{y})P_{U_i\,|\,U_0^{i-1},\bar{Y}}(1\,|\,u_0^{i-1},\bar{y})}$$
$$= \sum_{u_0^{i-1},\bar{y}} \sqrt{P_{U_0^{i-1},U_i,\bar{Y}}(u_0^{i-1},0,\bar{y})P_{U_0^{i-1},U_i,\bar{Y}}(u_0^{i-1},1,\bar{y})}$$
$$= \sum_{u_0^{i-1},\bar{y}} \sqrt{\sum_{u_{i+1}^{N-1}} P_{\bar{U},\bar{Y}}((u_0^{i-1},0,u_{i+1}^{N-1}),\bar{y})}$$
$$\sqrt{\sum_{u_{i+1}^{N-1}} P_{\bar{U},\bar{Y}}((u_0^{i-1},1,u_{i+1}^{N-1}),\bar{y})}$$
$$\overset{(a)}{=} \frac{1}{2^N}\sum_{u_0^{i-1},\bar{y}} \sqrt{\sum_{u_{i+1}^{N-1}} P_{\bar{Y}\,|\,\bar{U}}(\bar{y}\,|\,u_0^{i-1},0,u_{i+1}^{N-1})}$$
$$\sqrt{\sum_{u_{i+1}^{N-1}} P_{\bar{Y}\,|\,\bar{U}}(\bar{y}\,|\,u_0^{i-1},1,u_{i+1}^{N-1})}$$
$$= \frac{1}{2}Z^{(i)}.$$

The equality (a) follows from the fact that $P_{\bar{U}}(\bar{u}) = \frac{1}{2^N}$ for all $\bar{u} \in \{0,1\}^N$.

Assume now that $Z^{(i)} \ge 1 - 2\delta_N^2$. Then

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

Multiplying and dividing the term inside the expectation with

$$\frac{1}{2} + \sqrt{P_{U_i\,|\,U_0^{i-1},\bar{Y}}(0\,|\,u_0^{i-1},\bar{y})P_{U_i\,|\,U_0^{i-1},\bar{Y}}(1\,|\,u_0^{i-1},\bar{y})},$$

and upper bounding this term in the denominator with 1, we get

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

Now, using the equality $\frac{1}{4} - p\bar{p} = (\frac{1}{2} - p)^2$, we get

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

The result now follows by applying the Cauchy-Schwartz inequality. ∎

We are now ready to prove Theorem 1. 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 1:

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,

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

For N sufficiently large there exists a $\beta' < \frac{1}{2}$ such that $2\delta_N^2 > 2^{-N^{\beta'}}$. Theorem 16 and equation (19) imply that

$$\lim_{N=2^n, n\to\infty} \frac{|F_N|}{N} = h_2(D). \tag{11}$$

For any $\epsilon > 0$ this implies that 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 3 we know that

$$D_N(F_N) \leq D + 2|F_N|\delta_N \leq D + O(2^{-(N^\beta)}) \tag{12}$$

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

Recall that $D_N(F_N)$ is the average of the distortion over all choices of $\tilde{u}_F$. Since the average distortion fulfills (12) it follows that there must be at least one choice of $\tilde{u}_{F_N}$ for which

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

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

The complexity of the encoding and decoding algorithms are of the order $\Theta(N\log(N))$ as shown in [15]. ∎

V. Value of Frozen Bits Does Not Matter

In the previous sections we have considered $D_N(F)$, the average distortion if we average over all choices of $\tilde{u}_F$. We will now show a stronger result, namely we will show that *all* choices for $\tilde{u}_F$ lead to the same distortion, i.e., $D_N(F, \tilde{u}_F)$ is independent of $\tilde{u}_F$. This implies that the components belonging to the frozen set F can be set to any value. A convenient choice is to set them to 0. In the following let F be a fixed set. The results here do not dependent on the set F.

Lemma 6 (Gauge Transformation): Consider the Standard Model introduced in the previous section. Let $\bar{y}, \bar{y}' \in \{0,1\}^N$ and let $u_0^{i-1} = {u'}_0^{i-1} \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_0^{i-1}$. Then

$$l_i(\bar{y}, u_0^{i-1}) = \begin{cases} l_i(\bar{y}', {u'}_0^{i-1}), & \text{if } ((\bar{y} \oplus \bar{y}')H_n^{-1})_i = 0, \\ 1/l_i(\bar{y}', {u'}_0^{i-1}), & \text{if } ((\bar{y} \oplus \bar{y}')H_n^{-1})_i = 1. \end{cases}$$

Proof:

$$\begin{aligned}
&l_i(\bar{y}, u_0^{i-1}) \\
&= \frac{W^{(i)}(\bar{y}, u_0^{i-1}\,|\,0)}{W^{(i)}(\bar{y}, u_0^{i-1}\,|\,1)} \\
&= \frac{\sum_{u_{i+1}^{N-1}} P(\bar{y}\,|\,u_0^{i-1}, 0, u_{i+1}^{N-1})}{\sum_{u_{i+1}^{N-1}} P(\bar{y}\,|\,u_0^{i-1}, 1, u_{i+1}^{N-1})} \\
&\overset{(7)}{=} \frac{\sum_{u_{i+1}^{N-1}} P(\bar{y}'\,|\,(u_0^{i-1}, 0, u_{i+1}^{N-1}) \oplus (\bar{y} \oplus \bar{y}')H_n^{-1})}{\sum_{u_{i+1}^{N-1}} P(\bar{y}'\,|\,(u_0^{i-1}, 1, u_{i+1}^{N-1}) \oplus (\bar{y} \oplus \bar{y}')H_n^{-1})} \\
&= \frac{\sum_{u_{i+1}^{N-1}} P(\bar{y}'\,|\,({u'}_0^{i-1}, 0 \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_i, u_{i+1}^{N-1})}{\sum_{u_{i+1}^{N-1}} P(\bar{y}'\,|\,({u'}_0^{i-1}, 1 \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_i, u_{i+1}^{N-1})} \\
&= \frac{W^{(i)}(\bar{y}', {u'}_0^{i-1}\,|\,0 \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_i)}{W^{(i)}(\bar{y}', {u'}_0^{i-1}\,|\,1 \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_i)}.
\end{aligned}$$

The claim follows by considering the two possible values of $((\bar{y} \oplus \bar{y}')H_n^{-1})_i$. ∎

Recall that the decision process involves randomized rounding on the basis of l_i. Consider at first two tuples $(\bar{y}, u_0^{i-1})$ and $(\bar{y}', {u'}_0^{i-1})$ so that their associated l_i values are equal; we have seen in the previous lemma that many such tuples exist. In this case, if both tuples have access to the same source of randomness, we can couple the two instances so that they make the same decision on U_i. An equivalent statement is true in the case when the two tuples have the same reliability $|\log(l_i(\bar{y}, u_0^{i-1}))|$ but different signs. In this case there is a simple coupling that ensures that if for the first tuple the decision is lets say $U_i = 0$ then for the second tuple it is $U_i = 1$ and vice versa. Hence, if in the sequel we compare two instances of "compatible" tuples which have access to the same source of randomness, then we assume exactly this coupling.

Lemma 7 (Symmetry and Distortion): Consider the Standard model introduced in the previous section. Let $\bar{y}, \bar{y}' \in \{0,1\}^N$, $F \subseteq \{0,\dots,N-1\}$, and $\tilde{u}_F, \tilde{u}'_F \in \{0,1\}^{|F|}$. If $\tilde{u}_F = \tilde{u}'_F \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_F$, then under the coupling through a common source of randomness $f^{\tilde{u}_F}(\bar{y}) = f^{\tilde{u}'_F}(\bar{y}') \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_{F^c}$.

Proof: Let $\bar{u}, \bar{u}'$ be the two N dimensional vectors generated within the Standard Model. We use induction. Fix $0 \leq i \leq N-1$. We assume that for $j < i$, $u_j = u'_j \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_j$. This is in particular correct if $i = 0$, which serves as our anchor.

By Lemma 6 we conclude that under our coupling the respective decisions are related as $u_i = u'_i \oplus ((\bar{y} \oplus \bar{y}')H_n^{-1})_i$ if $i \in F^c$. On the other hand, if $i \in F$, then the claim is true by assumption. ∎

Let $\bar{v} \in \{0,1\}^{|F|}$ and let $A(\bar{v}) \subset \{0,1\}^N$ denote the coset

$$A(\bar{v}) = \{\bar{y} : (\bar{y}H_n^{-1})_F = \bar{v}\}.$$

The set of source words $\{0,1\}^N$ can be partitioned as

$$\{0,1\}^N = \cup_{\bar{v}\in\{0,1\}^{|F|}} A(\bar{v}).$$

Note that all the cosets $A(\bar{v})$ have equal size.

The main result of this section is the following lemma. The lemma implies that the distortion of $\mathrm{SM}(F,\tilde{u}_F)$ is independent of $\tilde{u}_F$.

Lemma 8 (Independence of Average Distortion w.r.t. $\tilde{u}_F$): Fix $F \subseteq \{0,\dots,N-1\}$. The average distortion $D_N(F,\tilde{u}_F)$ of the model $\mathrm{SM}(F,\tilde{u}_F)$ is independent of the choice of $\tilde{u}_F \in \{0,1\}^{|F|}$.

Proof: Let $\tilde{u}_F, \tilde{u}'_F \in \{0,1\}^{|F|}$ be two fixed vectors. We will now show that $D_N(F,\tilde{u}_F) = D_N(F,\tilde{u}'_F)$. Let $\bar{y},\bar{y}'$ be two source words such that $\bar{y} \in A(\bar{v})$ and $\bar{y}' \in A(\bar{v}\oplus\tilde{u}_F\oplus\tilde{u}'_F)$, i.e., $\tilde{u}'_F = \tilde{u}_F \oplus ((\bar{y}\oplus\bar{y}')H_n^{-1})_F$. Lemma 7 implies that

$$f^{\tilde{u}'_F}(\bar{y}') = f^{\tilde{u}_F}(\bar{y}) \oplus ((\bar{y}\oplus\bar{y}')H_n^{-1})_{F^c}.$$

This implies that the reconstruction words are related as

$$\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y})) = \hat{f}^{\tilde{u}'_F}(f^{\tilde{u}'_F}(\bar{y}')) \oplus (\bar{y}\oplus\bar{y}')H_n^{-1}.$$

Note that $\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y}))\oplus\bar{y}$ is the quantization error. Therefore

$$\mathtt{d}(\bar{y},\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y}))) = \mathtt{d}(\bar{y}',\hat{f}^{\tilde{u}_F}(f^{\tilde{u}'_F}(\bar{y}'))),$$

which further implies

$$\sum_{\bar{y}\in A(\bar{v})} \mathtt{d}(\bar{y},\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y}))) = \sum_{\bar{y}\in A(\bar{v}\oplus\tilde{u}_F\oplus\tilde{u}'_F)} \mathtt{d}(\bar{y},\hat{f}^{\tilde{u}'_F}(f^{\tilde{u}'_F}(\bar{y}))).$$

Hence, the average distortions satisfy

$$\begin{aligned}
&\sum_{\bar{y}} \frac{1}{2^N}\mathtt{d}(\bar{y},\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y})))\\
&= \sum_{\bar{v}\in\{0,1\}^{|F|}} \frac{1}{2^N} \sum_{\bar{y}\in A(\bar{v})} \mathtt{d}(\bar{y},\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y})))\\
&= \sum_{\bar{v}\in\{0,1\}^{|F|}} \frac{1}{2^N} \sum_{\bar{y}\in A(\bar{v}\oplus\tilde{u}_F\oplus\tilde{u}'_F)} \mathtt{d}(\bar{y},\hat{f}^{\tilde{u}'_F}(f^{\tilde{u}'_F}(\bar{y})))\\
&= \sum_{\bar{v}\in\{0,1\}^{|F|}} \frac{1}{2^N} \sum_{\bar{y}\in A(\bar{v})} \mathtt{d}(\bar{y},\hat{f}^{\tilde{u}'_F}(f^{\tilde{u}'_F}(\bar{y})))\\
&= \sum_{\bar{y}} \frac{1}{2^N}\mathtt{d}(\bar{y},\hat{f}^{\tilde{u}'_F}(f^{\tilde{u}'_F}(\bar{y}))).
\end{aligned}$$

As mentioned before, the functions $f^{\tilde{u}_F}$ and $f^{\tilde{u}'_F}$ are not deterministic and the above equality is valid under the assumption of coupling with a common source of randomness. Averaging over this common randomness, we get $D_N(F,\tilde{u}_F) = D_N(F,\tilde{u}'_F)$. ∎

Let $\mathcal{Q}^{\tilde{u}_F}$ denote the empirical distribution of the quantization noise, i.e.,

$$\mathcal{Q}^{\tilde{u}_F}(\bar{x}) = \mathbb{E}[\mathbb{1}_{\{\bar{Y}\oplus\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{Y}))=\bar{x}\}}],$$

where the expectation is over the randomness involved in the source and randomized rounding. Continuing with the reasoning of the previous lemma, we can indeed show that the distribution $\mathcal{Q}^{\tilde{u}_F}$ is independent of $\tilde{u}_F$. Combining this with Lemma 2, we can bound the distance between $\mathcal{Q}^{\tilde{u}_F}$ and an i.i.d. $\mathrm{Ber}(D)$ noise. This will be useful in settings which involve both channel and source coding, like the Wyner-Ziv problem, where it is necessary to show that the quantization noise is close to a Bernoulli random variable.

Lemma 9 (Distribution of the Quantization Error): Let the frozen set F be

$$F = \{i : Z^{(i)} \geq 1 - 2\delta_N^2\}.$$

Then for $\tilde{u}_F$ fixed,

$$\sum_{\bar{x}} |\mathcal{Q}^{\tilde{u}_F}(\bar{x}) - \prod_i W(x_i\,|\,0)| \leq 2|F|\delta_N.$$

Proof: Recall that $P_{\bar{X}\,|\,\bar{Y}}(\bar{x}\,|\,\bar{y}) = \prod_i W(x_i\,|\,y_i)$. Let $\bar{v}\in\{0,1\}^{|F|}$ be a fixed vector. Consider a vector $\bar{y}\in A(\bar{v})$ and set $\bar{y}' = \bar{0}$. Lemma 7 implies that $f^{\tilde{u}_F}(\bar{y}) = f^{\tilde{u}_F\oplus\bar{v}}(\bar{0}) \oplus (\bar{y}H_n^{-1})_{F^c}$. Therefore,

$$\bar{y}\oplus\hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{y})) = \bar{0}\oplus\hat{f}^{\tilde{u}_F\oplus\bar{v}}(f^{\tilde{u}_F\oplus\bar{v}}(\bar{0})).$$

This implies that all vectors belonging to $A(\bar{v})$ have the same quantization error and this error is equal to the error incurred by the all-zero word when the frozen bits are set to $\tilde{u}_F\oplus\bar{v}$.

Moreover, the uniform distribution of the source induces a uniform distribution on the sets $A(\bar{v})$ where $\bar{v}\in\{0,1\}^{|F|}$. Therefore, the distribution of the quantization error $\mathcal{Q}^{\tilde{u}_F}$ is the same as first picking the coset uniformly at random, i.e., the bits $\tilde{u}_F$, and then generating the error $\bar{x}$ according to $\bar{x} = \hat{f}^{\tilde{u}_F}(f^{\tilde{u}_F}(\bar{0}))$. The distribution of the vector $\bar{u}$ where $\bar{u} = \bar{x}H_n^{-1}$ is indeed the distribution Q defined in (9). Recall that in the distribution $P_{\bar{U},\bar{X},\bar{Y}}$, $\bar{U}$ and $\bar{X}$ are related as $\bar{U} = \bar{X}H_n^{-1}$. Therefore, the distribution induced by $W(\bar{x}\,|\,\bar{y})$ on $\bar{U}$ is $P_{\bar{U}\,|\,\bar{Y}}$. Since multiplication with H_n^{-1} is a one-to-one mapping, the total variation distance can be bounded as

$$\begin{aligned}
\sum_{\bar{x}} |\mathcal{Q}^{\tilde{u}_F}(\bar{x}) - \prod_i W(\bar{x}\,|\,\bar{0})| &= \sum_{\bar{u}} |Q(\bar{u}\,|\,\bar{0}) - P_{\bar{U}\,|\,\bar{Y}}(\bar{u}\,|\,\bar{0})|\\
&\overset{(a)}{\leq} 2|F|\delta_N.
\end{aligned}$$

The inequality (a) follows from Lemma 2 and Lemma 5. ∎

VI. Beyond Source Coding

Polar codes were originally defined in the context of channel coding in [15], where it was shown that they achieve the capacity of symmetric B-DMCs. Now we have seen that polar codes achieve the rate-distortion tradeoff for lossy compression of a BSS. The natural question to ask next is whether these codes are suitable for problems that involve both quantization as well as error correction.

Perhaps the two most prominent examples are the source coding problem with side information (Wyner-Ziv problem [21]) as well as the channel coding problem with side information (Gelfand-Pinsker problem [22]). As discussed in [23], nested linear codes are required to tackle these problems. Polar codes are equipped with such a nested structure and are, hence, natural candidates for these problems. We will show that, by taking advantage of this structure, one can construct polar codes that are optimal in both settings (for the binary versions of these problems). Hence, polar codes provide the first provably optimal low-complexity solution.

In [7] the authors constructed MN codes which have the required nested structure. They show that these codes achieve the optimum performance under MAP decoding. How these codes perform under low complexity message-passing algorithms is still an open problem. Trellis and turbo based codes were considered in [24]–[27] for the Wyner-Ziv problem. It was empirically shown that they achieve good performance with low complexity message-passing algorithms. A similar combination was considered in [28]–[30] for the Gelfand-Pinsker problem. Again, empirical results close to the optimum performance were obtained.

We end this section by applying polar codes to a multi-terminal setup. One such scenario was considered in [20], where it was shown that polar codes are optimal for lossless compression of a correlated binary source (the Slepian-Wolf problem [31]). The result follows by mapping the lossless source compression task to a channel coding problem.

Here we consider another multi-terminal setup known as the one helper problem [32]. This problem involves channel coding at one terminal and source coding at the other. We again show that polar codes achieve optimal performance under low-complexity encoding and decoding algorithms.

A. Binary Wyner-Ziv Problem

Let Y be a BSS and let the decoder have access to a random variable Y'. This random variable is usually called the *side information*. We assume that Y' is correlated to Y as $Y' = Y + Z$, where Z is a Ber(p) random variable. The task of the encoder is to compress the source Y, call the result X, such that a decoder with access to (Y', X) can reconstruct the source to within a distortion D.

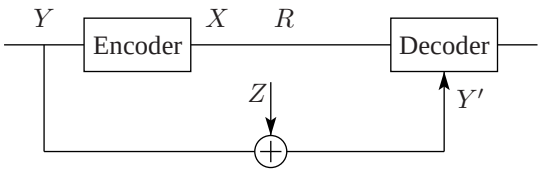

Fig. 4. The side information Y' is available at the decoder. The decoder wants to reconstruct the source Y to within a distortion D given X.

Wyner and Ziv [21] have shown that the rate-distortion curve for this problem is given by

$$l.c.e.\Big\{(R_{\text{WZ}}(D), D), (0, p)\Big\},$$

where $R_{\text{WZ}}(D) = h_2(D * p) - h_2(D)$, $l.c.e.$ denotes the *lower convex envelope*, and $D * p = D(1-p) + p(1-D)$. Here we focus on achieving the rates of the form $R_{\text{WZ}}(D)$. The remaining rates can be achieved by appropriate time-sharing with the pair $(0, p)$.

The proof is based on the following nested code construction. Let $\mathtt{C}_s$ denote the polar code defined by the frozen set F_s with the frozen bits $\bar{u}_{F_s}$ set to 0. Let $\mathtt{C}_c(\bar{v})$ denote the code defined by the frozen set $F_c \supset F_s$ with the frozen bits $\bar{u}_{F_s}$ set to 0 and $\bar{u}_{F_c \setminus F_s} = \bar{v}$. This implies that the code $\mathtt{C}_s$ can be partitioned as $\mathtt{C}_s = \cup_{\bar{v}} \mathtt{C}_c(\bar{v})$.

The code $\mathtt{C}_s$ is designed to be a good source code for distortion D and for each $\bar{v}$ the code $\mathtt{C}_c(\bar{v})$ is designed to be a good channel code for the BSC$(D * p)$.

The encoder compresses the source vector $\bar{Y}$ to a vector $\bar{U}_{F_s^c}$ through the map $\bar{U}_{F_s^c} = f^{\bar{0}}(\bar{Y})$. The reconstruction vector $\bar{X}$ is given by $\bar{X} = \hat{f}^{\bar{0}}(f^{\bar{0}}(\bar{Y}))$. Since the code $\mathtt{C}_s$ is a good source code, the quantization error $\bar{Y} \oplus \bar{X}$ is close to a Ber(D) vector (see Lemma 9). This implies that the vector $\bar{Y}'$ which is available at the decoder is statistically equivalent to the output of a BSC$(D * p)$ when the input is $\bar{X}$. The encoder transmits the vector $\bar{V} = \bar{U}_{F_c \setminus F_s}$ to the decoder. This informs the decoder of the code $\mathtt{C}_c(\bar{V})$ which is used. Since this code $\mathtt{C}_c(\bar{V})$ is designed for the BSC$(D * p)$, the decoder can with high probability determine $\bar{X}$ given $\bar{Y}'$. By construction, $\bar{X}$ represents $\bar{Y}$ with distortion roughly D as desired.

Theorem 10 (Optimality for the Wyner-Ziv Problem): Let Y be a BSS and Y' be a Bernoulli random variable correlated to Y as $Y' = Y \oplus Z$, where $Z \sim$ Ber(p). Fix the *design* distortion D, $0 < D < \frac{1}{2}$. For any rate $R > h_2(D*p) - h_2(D)$ and any $0 < \beta < \frac{1}{2}$, there exists a sequence of nested polar codes of length N with rates $R_N < R$ so that under SC encoding using randomized rounding at the encoder and SC decoding at the decoder, they achieve expected distortion D_N satisfying

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

and the block error probability satisfying

$$P_N^B \leq O(2^{-(N^\beta)}).$$

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

Proof: Let $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$ be some constants. Let $Z^{(i)}(q)$ denote the $Z^{(i)}$s computed with W set to BSC(q). Let $\delta_N = \frac{1}{N} 2^{-(N^\beta)}$. Let F_s and F_c denote the sets

$$F_s = \{i : Z^{(i)}(D) \geq 1 - \delta_N^2\},$$
$$F_c = \{i : Z^{(i)}(D * p) \geq \delta_N\}.$$

Theorem 16 implies that for N sufficiently large

$$\frac{|F_s|}{N} \geq h_2(D) - \frac{\epsilon}{2}.$$

Similarly, Theorem 15 implies that for N sufficiently large

$$\frac{|F_c|}{N} \leq h_2(D * p) + \frac{\epsilon}{2}.$$

The degradation of BSC$(D * p)$ with respect to BSC(D) implies that $F_s \subset F_c$.

The bits F_s are fixed to 0. This is known both to the encoder and the decoder. A source vector $\bar{y}$ is mapped to $\bar{u}_{F_s^c} = f^{\bar{0}}(\bar{y})$ as shown in the Standard Model. Therefore the average distortion D_N is bounded as

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

The encoder transmits the vector $\bar{u}_{F_c \setminus F_s}$ to the decoder. The required rate is

$$R_N = \frac{|F_c| - |F_s|}{N} \leq h_2(D * p) - h_2(p) + \epsilon.$$

It remains to show that at the decoder the block error probability incurred in decoding $\bar{X}$ is $O(2^{-(N^\beta)})$.

Let $\bar{E}$ denote the quantization error, $\bar{E} = \bar{Y} \oplus \bar{X}$. The information available at the decoder ($\bar{Y}'$) can be expressed as,

$$\bar{Y}' = \bar{X} \oplus \bar{E} \oplus \bar{Z}.$$

Consider the code $\mathtt{C}_c(\bar{v})$ for a given $\bar{v}$ and transmission over the BSC$(D * p)$. Let $\mathcal{E} \subseteq \{0,1\}^N$ denote the set of noise vectors of the channel which result in a decoding error under SC decoding. By the equivalent of Lemma 8 for the channel coding case, this set does not depend on $\bar{v}$.

The block error probability of our scheme can then be expressed as

$$P_N^B = \mathbb{E}[\mathbb{1}_{\{\bar{E} \oplus \bar{Z} \in \mathcal{E}\}}].$$

The exact distribution of the quantization error is not known, but Lemma 9 provides a bound on the total variation distance between this distribution and an i.i.d. Ber(D) distribution. Let $\bar{B}$ denote an i.i.d. Ber(D) vector. Let $P_{\bar{E}}$ and $P_{\bar{B}}$ denote the distribution of $\bar{E}$ and $\bar{B}$ respectively. Then

$$\sum_{\bar{e}} |P_{\bar{E}}(\bar{e}) - P_{\bar{B}}(\bar{e})| \leq 2|F_s|\delta_N \leq O(2^{-(N^\beta)}). \tag{13}$$

Let $\Pr(\bar{B}, \bar{E})$ denote the so-called *optimal coupling* between $\bar{E}$ and $\bar{B}$. I.e., a joint distribution of $\bar{E}$ and $\bar{B}$ with marginals equal to $P_{\bar{E}}$ and $P_{\bar{B}}$, and satisfying

$$\Pr(\bar{E} \neq \bar{B}) = \sum_{\bar{e}} |P_{\bar{E}}(\bar{e}) - P_{\bar{B}}(\bar{e})|. \tag{14}$$

It is known [33] that such a coupling exists. Let $\bar{E}$ and $\bar{B}$ be generated according to $\Pr(\cdot, \cdot)$. Then, the block error probability can be expanded as

$$\begin{aligned} P_N^B &= \mathbb{E}[\mathbb{1}_{\{\bar{E} \oplus \bar{Z} \in \mathcal{E}\}} \mathbb{1}_{\{\bar{E} = \bar{B}\}}] + \mathbb{E}[\mathbb{1}_{\{\bar{E} \oplus \bar{Z} \in \mathcal{E}\}} \mathbb{1}_{\{\bar{E} \neq \bar{B}\}}] \\ &\leq \mathbb{E}[\mathbb{1}_{\{\bar{B} \oplus \bar{Z} \in \mathcal{E}\}}] + \mathbb{E}[\mathbb{1}_{\{\bar{E} \neq \bar{B}\}}] \end{aligned}$$

The first term in the sum refers to the block error probability for the BSC$(D * p)$, which can be bounded as

$$\mathbb{E}[\mathbb{1}_{\{\bar{B} \oplus \bar{Z} \in \mathcal{E}\}}] \leq \sum_{i \in F_c} Z^{(i)}(D * p) \leq O(2^{-(N^\beta)}). \tag{15}$$

Using (13), (14) and (15) we get

$$P_N^B \leq O(2^{-(N^\beta)}).$$

■

B. Binary Gelfand-Pinsker Problem

Let S denote a symmetric Bernoulli random variable. Consider a channel with state S given by

$$Y = X \oplus S \oplus Z,$$

where Z is a Ber(p) random variable. The state S is known to the encoder a-causally and not known to the decoder. The output of the encoder is constrained to satisfy $\mathbb{E}[X] \leq D$, i.e., on average the fraction of 1s it can transmit is bounded by D. This is similar to the power constraint in the continuous case. The task of the encoder is to transmit a message M to the decoder with vanishing error probability under the above mentioned input constraint.

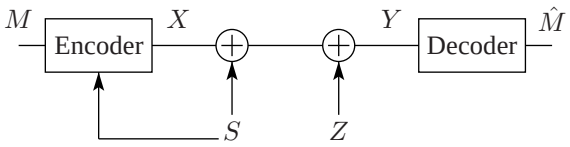

Fig. 5. The state S is known to the encoder in advance. The weight of the input X is constrained to $\mathbb{E}[X] \leq D$.

In [34], it was shown that the achievable rate, weight pairs for this channel are given by

$$u.c.e.\Big\{(R_{\text{GP}}(D), D), (0,0)\Big\},$$

where $R_{\text{GP}}(D) = h_2(D) - h_2(p)$, and $u.c.e$ denotes the upper convex envelope.

Similar to the Wyner-Ziv problem, we need a nested code for this problem. However, they differ in the sense that the role of the channel and source codes are reversed.

Let $\mathtt{C}_c$ denote the polar code defined by the frozen set F_c with frozen bits $\bar{u}_{F_c}$ set to 0. Let $\mathtt{C}_s(\bar{v})$ denote the code defined by the frozen set $F_s \supset F_c$, with the frozen bits $\bar{u}_{F_c}$ set to 0 and $\bar{u}_{F_s \setminus F_c} = \bar{v}$. The code $\mathtt{C}_c$ is designed to be a good channel code for the BSC(p) and the codes $\mathtt{C}_s(\bar{v})$ are designed to be good source codes for distortion D. This implies that the code $\mathtt{C}_c$ can be partitioned into $\mathtt{C}_s(\bar{v})$ for $\bar{v} \in \{0,1\}^{F_s \setminus F_c}$, i.e., $\mathtt{C}_c = \cup_{\bar{v}} \mathtt{C}_s(\bar{v})$.

The frozen bits $\bar{V} = \bar{U}_{F_s \setminus F_c}$ are determined by the message M that is transmitted. The encoder compresses the state vector $\bar{S}$ to a vector $\bar{U}_{F_s^c}$ through the map $\bar{U}_{F_s^c} = f^{\bar{U}_{F_s}}(\bar{S})$. Let $\bar{S}'$ be the reconstruction vector $\bar{S}' = \hat{f}^{\bar{U}_{F_s}}(f^{\bar{U}_{F_s}}(\bar{S}))$. The encoder sends the vector $\bar{X} = \bar{S} \oplus \bar{S}'$ through the channel. Since the codes $\mathtt{C}_s(\bar{V})$ are good source codes, the expected distortion $\frac{1}{N}\mathbb{E}[\mathtt{d}(\bar{S}, \bar{S}')]$ (hence the average weight of $\bar{X}$) is close to D (see Lemma 8). Since the code $\mathtt{C}_c$ is designed for the BSC(p), the decoder will succeed in decoding the codeword $\bar{S} \oplus \bar{X} = \bar{S}'$ (hence the message $\bar{V}$) with high probability.

Here we focus on achieving the rates of the form $R_{\text{GP}}(D)$. The remaining rates can be achieved by appropriate time-sharing with the pair $(0,0)$.

Theorem 11 (Optimality for the Gelfand-Pinsker Problem): Let S be a symmetric Bernoulli random variable. Fix D, $0 < D < \frac{1}{2}$. For any rate $R < h_2(D) - h_2(p)$ and any $0 < \beta < \frac{1}{2}$, there exists a sequence of polar codes of length N so that under SC encoding using randomized rounding at the encoder and SC decoding at the decoder, the achievable rate satisfies

$$R_N > R,$$

with the expected weight of X, D_N, satisfying

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

and the block error probability satisfying

$$P_N^B \leq O(2^{-(N^\beta)}).$$

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

Proof: Let $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$ be some constants. Let $Z^{(i)}(q)$ denote the $Z^{(i)}$s computed with W set to BSC(q). Let $\delta_N = \frac{1}{N}2^{-(N^\beta)}$. Let F_s and F_c denote the sets

$$F_s = \{i : Z^{(i)}(D) \geq 1 - \delta_N^2\}, \tag{16}$$

$$F_c = \{i : Z^{(i)}(p) \geq \delta_N\}. \tag{17}$$

Theorem 16 implies that for N sufficiently large

$$\frac{|F_s|}{N} \geq h_2(D) - \frac{\epsilon}{2}.$$

Similarly, Theorem 15 implies that for N sufficiently large

$$\frac{|F_c|}{N} \leq h_2(p) + \frac{\epsilon}{2}.$$

The degradation of BSC(D) with respect to BSC(p) implies that $F_c \subset F_s$. The vector $\bar{u}_{F_s \setminus F_c}$ is defined by the message that is transmitted. Therefore, the rate of transmission is

$$\frac{|F_s| - |F_c|}{N} \geq h_2(D) - h_2(p) - \epsilon.$$

The vector $\bar{S}$ is compressed using the source code with frozen set F_s. The frozen vector $\bar{u}_{F_s}$ is defined in two stages. The subvector $\bar{u}_{F_c}$ is fixed to 0 and is known to both the transmitter and the receiver. The subvector $\bar{u}_{F_s \setminus F_c}$ is defined by the message being transmitted.

Let $\bar{S}$ be mapped to a reconstruction vector $\bar{S}'$. Lemma 8 implies that the average distortion of the Standard Model is independent of the value of the frozen bits. This implies

$$\mathbb{E}[\bar{S} \oplus \bar{S}'] \leq D + 2|F_s|\delta_N \leq D + O(2^{-(N^\beta)}).$$

Therefore, a transmitter which sends $\bar{X} = \bar{S} \oplus \bar{S}'$ will on average be using $D + O(2^{-(N^\beta)})$ fraction of 1s. The received vector is given by

$$\bar{Y} = \bar{X} \oplus \bar{S} \oplus \bar{Z} = \bar{S}' \oplus \bar{Z}.$$

The vector $\bar{S}'$ is a codeword of $\mathtt{C}_c$, the code designed for the BSC(p) (see (17)). Therefore, the block error probability of the SC decoder in decoding $\bar{S}'$ (and hence $\bar{V}$) is bounded as

$$P_N^B \leq \sum_{i \in F_c^c} Z^{(i)}(p) \leq O(2^{-(N^\beta)}).$$

■

C. Storage in Memory With Defects

Let us briefly discuss another standard problem in the literature that fits within the Gelfand-Pinsker framework but where the state is non-binary. Consider the problem of storing data on a computer memory with defects and noise, explored in [35] and [36]. Each memory cell can be in three possible states, say $\{0, 1, *\}$. The state $S = 0$ (1) means that the value of the cell is stuck at 0 (1) and $S = *$ means that the value of the cell is flipped with probability D. Let the probability distribution of S be

$$\Pr(S = 0) = \Pr(S = 1) = p/2, \quad \Pr(S = *) = 1 - p.$$

The optimal storage capacity when the whole state realization is known in advance only to the encoder is $(1-p)(1-h_2(D))$.

Theorem 12 (Optimality for the Storage Problem): For any rate $R < (1-p)(1-h_2(D))$ and any $0 < \beta < \frac{1}{2}$, there exists a sequence of polar codes of length N so that under SC encoding using randomized rounding at the encoder and SC decoding at the decoder, the achievable rate satisfies

$$R_N > R,$$

and the block error probability satisfying

$$P_N^B \leq O(2^{-(N^\beta)}).$$

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

The problem can be framed as a Gelfand-Pinsker setup with state $S \in \{0, 1, *\}$. As seen before, the nested construction for such a problem consists of a good source code which partitions into cosets of a good channel code. We still need to define what the corresponding source and coding problems are.

Source Code: The source code is designed to compress the ternary source S to the binary alphabet $\{0, 1\}$ with design distortion D. The distortion function is $\mathtt{d}(0, 1) = 1$, $\mathtt{d}(*, 1) = \mathtt{d}(*, 0) = 0$,. The test channel for this problem is a binary symmetric erasure channel (BSEC) shown in Figure 7. The compression of this source is explained in Section VIII. Let $Z^{(i)}(p, D)$ denote the Bhattacharyya values of BSEC(p, D) defined in Figure 7. The frozen set F_s is defined as

$$F_s = \{i : Z^{(i)}(p, D) \geq 1 - \delta_N^2\}.$$

The rate distortion function for this problem is given by $p(1 - h_2(D))$. Therefore, for sufficiently large N, $|F_s|/N$ can be made arbitrarily close to $1 - p(1 - h_2(D))$.

Channel code: The channel code is designed for BSC(D). The frozen set F_c is defined as

$$F_c = \{i : Z^{(i)}(D) \geq \delta_N\}.$$

Therefore, for sufficiently large N, $|F_c|/N$ can be made arbitrarily close to $h_2(D)$. Degradation of BSEC(p, D) with respect to BSC(D) implies $F_c \subseteq F_s$.

Encoding: The frozen bits $\bar{U}_{F_c}$ is fixed to $\bar{0}$. The vector $\bar{U}_{F_s \setminus F_c}$ is defined by the message to be stored. Therefore, the achievable rate is

$$R_N = \frac{|F_s| - |F_c|}{N} \geq (1-p)(1 - h_2(D)) - \epsilon$$

for any $\epsilon > 0$. Compress the source sequence using the function $f^{\bar{U}_{F_s}}(\bar{S})$ and store the reconstruction vector $\bar{X} = f^{\bar{U}_{F_s}}(f^{\bar{U}_{F_s}}(\bar{S}))$ in the memory. As shown in the Wyner-Ziv setting, the quantization noise is close to Ber(D) for the stuck bits. Therefore, a fraction D of the stuck bits differ from $\bar{X}$.

Decoding: When the decoder reads the memory, the stuck bits are read as it is and the remaining bits are flipped with probability D. This is equivalent to seeing $\bar{X}$ through a channel BSC(D). Since the channel code is defined for BSC(D), the decoding will be successful with high probability and the message $\bar{U}_{F_s \setminus F_c}$ will be recovered.

D. One Helper Problem

Let Y be a BSS and let Y' be correlated to Y as $Y' = Y \oplus Z$, where Z is a Ber(p) random variable. The encoder has access to Y and the helper has access to Y'. The aim of the decoder is to reconstruct Y successfully. As the name suggests, the role of the helper is to assist the decoder in recovering Y. This problem was considered by Wyner in [32].

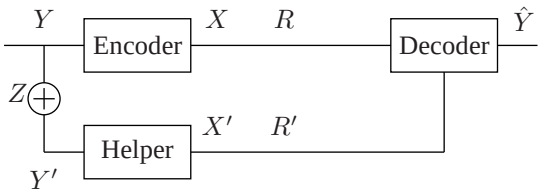

Fig. 6. The helper transmits quantized version of Y'. The decoder uses the information from the helper to decode Y reliably.

Let the rates used by the encoder and the helper be R and R' respectively. Wyner [32] showed that the required rates R, R' must satisfy

$$R > h_2(D * p), \quad R' > 1 - h_2(D),$$

for some $D \in [0, 1/2]$.

Theorem 13 (Optimality for the One Helper Problem): Let Y be a BSS and Y' be a Bernoulli random variable correlated to Y as $Y' = Y \oplus Z$, where $Z \sim$ Ber(p). Fix the *design* distortion D, $0 < D < \frac{1}{2}$. For any rate pair $R > h_2(D * p), R' > 1 - h_2(D)$ and any $0 < \beta < \frac{1}{2}$, there exist sequences of polar codes of length N with rates $R_N < R$ and $R'_N < R'$ so that under syndrome computation at the encoder, SC encoding using randomized rounding at the helper and SC decoding at the decoder, they achieve the block error probability satisfying

$$P_N^B \leq O(2^{-(N^\beta)}).$$

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

For this problem, we require a good channel code at the encoder and a good source code at the helper. We will explain the code construction here. The rest of the proof is similar to the previous setups.

Encoding: The helper quantizes the vector $\bar{Y}'$ to $\bar{X}'$ with a design distortion D. This compression can be achieved with rates arbitrarily close to $1 - h_2(D)$.

The encoder designs a code for the BSC$(D * p)$. Let F denote the frozen set. The encoder computes the syndrome $\bar{U}_F = (\bar{Y} H_n^{-1})_F$ and transmits it to the decoder. The rate involved in such an operation is $R = |F|/N$. Since the fraction $|F|/N$ can be made arbitrarily close to $h_2(D * p)$, the rate R will approach $h_2(D * p)$.

Decoding: The decoder first reconstructs the vector $\bar{X}'$. The remaining task is to decode the codeword $\bar{Y}$ from the observation $\bar{X}'$. As shown in the Wyner-Ziv setting, the quantization noise $\bar{Y} \oplus \bar{X}'$ is very "close" to Ber$(D * p)$. Note that the decoder knows the syndrome $\bar{U}_F = (\bar{Y} H_n^{-1})_F$, where the frozen set F is designed for the BSC$(D * p)$. Therefore, the task of the decoder is to recover the codeword of a code designed for BSC$(D * p)$ when the noise is close to Ber$(D * p)$. Hence the decoder will succeed with high probability.

VII. Complexity Versus Gap

We have seen that polar codes under SC encoding achieve the rate-distortion bound when the blocklength N tends to infinity. It is also well-known that the encoding as well as decoding complexity grows like $\Theta(N \log(N))$. How does the complexity grow as a function of the gap to the rate-distortion bound? This is a much more subtle question.

To see what is involved in being able to answer this question, consider the Bhattacharyya constants $Z^{(i)}$ defined in (3). Let $\tilde{Z}^{(i)}$ denote a re-ordering of these values in an increasing order, i.e., $\tilde{Z}^{(i)} \leq \tilde{Z}^{(i+1)}$, $i = 0, \ldots, N-2$. Define

$$m_N^{(i)} = \sum_{j=0}^{i-1} \tilde{Z}^{(i)},$$
$$M_N^{(i)} = \sum_{j=N-i}^{N-1} \sqrt{2(1 - \tilde{Z}^{(i)})}.$$

For the binary erasure channel there is a simple recursion to compute the $\{Z^{(i)}\}$ as shown in [15]. For general channels the computation of these constants is more involved but the basic principle is the same.

For the channel coding problem we then get an upper bound on the block error probability P_N^B as a function the rate R of the form

$$(P_N^B, R) = (m_N^{(i)}, \frac{i}{N}).$$

On the other hand, for the source coding problem, we get an upper bound on the distortion D_N as a function of the rate of the form

$$(D_N, R) = (D + M_N^{(i)}, \frac{i}{N}).$$

Now, if we knew the distribution of $Z^{(i)}$s it would allow us to determine the rate-distortion performance achievable for this coding scheme for any given length. The complexity per bit is always $\Theta(\log N)$.

Unfortunately, the computation of the quantities $m_N^{(i)}$ and $M_N^{(i)}$ is likely to be a challenging problem. Therefore, we ask a simpler question that we can answer with the estimates we currently have about the $\{Z^{(i)}\}$.

Let $R = R(D) + \delta$, where $\delta > 0$. How does the complexity per bit scale with respect to the gap between the actual (expected) distortion D_N and the design distortion D? Let us answer this question for the various low-complexity schemes that have been proposed to date.

Trellis Codes: In [5] it was shown that, using trellis codes and Viterbi decoding, the average distortion scales like $D + O(2^{-KE(R)})$, where $E(R) > 0$ for $\delta > 0$ and K is the constraint length. The complexity of the decoding algorithm is $\Theta(2^K N)$. Therefore, the complexity per bit in terms of the gap is given by $O(2^{(\log \frac{1}{g})})$.

Low Density Codes: In [37] it was shown that under optimum encoding the gap is $O(\sqrt{K} 2^{-K\Delta})$, for some $\Delta > 0$, where K is the average degree of the parity check node.

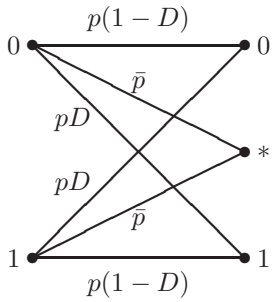

Fig. 7. The test channel for the binary erasure source.

Assuming that using BID we can achieve this distortion, the complexity is given by $\Theta(2^K N)$. Therefore, the complexity per bit in terms of the gap is given by $O(2^{(\log \frac{1}{g})})$.

Polar Codes: For polar codes, the complexity is $\Theta(N \log N)$ and the gap is $O(2^{-(N^\beta)})$ for any $\beta < \frac{1}{2}$. Therefore, the complexity per bit in terms of the gap is $O(\frac{1}{\beta} \log \log \frac{1}{g})$. This is considerably lower than for the two previous schemes.

VIII. Discussion and Future Work

We have considered the lossy source coding problem for the BSS and the Hamming distortion. The reconstruction alphabet in this case is also binary and the test channel "W" is a BSC.

Consider the slightly more general scenario of a q-ary source with a binary *reconstruction* alphabet. Assume further that the test channel, call it W, is such that the marginal induced by the source distribution on the reconstruction alphabet is uniform.

Example 14 (Binary Erasure Source): Let the source alphabet be $\{0, 1, *\}$. Let S denote the source variable with distribution

$$\Pr(S = 1) = \Pr(S = 0) = p/2, \quad \Pr(S = *) = 1 - p.$$

Let the distortion function be

$$\mathtt{d}(0, *) = \mathtt{d}(1, *) = 0, \;\; \mathtt{d}(0, 1) = 1. \tag{18}$$

For a design distortion D, the test channel $W : \{0, 1\} \to \{0, 1, *\}$ is shown in Figure 7. Note that the distribution induced on the input of the channel is uniform.

For this setup one can obtain results mirroring Theorem 1. More precisely, one can show that the optimum rate-distortion tradeoff can again be achieved by polar codes together with SC encoding and randomized-rounding. The proof is analogous to the proof of Theorem 1. The only change in the proof consists of replacing the BSC(D) with the appropriate test channel W. This is the source coding equivalent of Arıkan's channel coding result [15], where it was shown that polar codes achieve the symmetric mutual information $I(W)$ for any B-DMC.

A further important generalization is the compression of *non-symmetric* sources. Let us explain the involved issues by means of the channel coding problem. Consider an asymmetric B-DMC, e.g., the Z-channel. Due to the asymmetry, the capacity-achieving input distribution is in general not the uniform one. To be concrete, assume that it is $(p(0) = \frac{1}{3}, p(1) = \frac{2}{3})$. This causes problems for any scheme which employs linear codes, since linear codes induce uniform marginals. To get around this problem, "augment" the channel to a q-ary input channel by duplicating some of the inputs. For our running example, Figure 8 shows the ternary channel which results when duplicating the input "1." Note that the capacity-

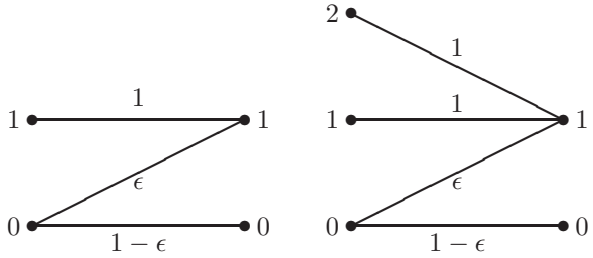

Fig. 8. The Z-channel and its corresponding augmented channel with ternary input alphabet.

achieving input distribution for this ternary-input channel is the uniform one. Assume that we can construct a ternary polar code which achieves the symmetric mutual information of this new channel. (For binary-input channels it was shown by Arıkan [15] that one can achieve the symmetric mutual information and there is good reason to believe that an equivalent result holds for q-ary input channels.) Then this gives rise to a capacity-achieving coding scheme for the original binary Z-channel by mapping the ternary set $\{0, 1, 2\}$ into the binary set $\{0, 1\}$ in the following way; $\{1, 2\} \mapsto 1$ and $0 \mapsto 0$.

More generally, by augmenting the input alphabet and constructing a code for the extended alphabet, we can achieve rates arbitrarily close to the capacity of a q-ary DMC, assuming only that we know how to achieve the symmetric mutual information.

A similar remark applies to the setting of source coding. By extending the reconstruction alphabet if necessary and by using only test channels that induce a uniform distribution on this extended alphabet one can achieve a rate-distortion performance arbitrarily close to the Shannon bound, assuming only that for the uniform case we can get arbitrarily close.

The previous discussion shows that perhaps the most important generalization is the construction of polar codes for both source and channel coding for the setting of q-ary alphabets.

In Section VI we have considered some scenarios beyond basic source coding. E.g., we considered binary versions of the Wyner-Ziv problem as well as the Gelfand-Pinsker problem. This list is by no means exhaustive.

One possible further generalization is to have source codes with a faster convergence speed. In [38] it was shown that, by considering larger matrices (instead of G_2), it is possible to obtain better exponents for the block error probability of the channel coding problem. Such a generalization for source coding would result in better exponents in the convergence of the average distortion to the design distortion.

Acknowledgment

We would like to thank Eren Şaşoğlu and Emre Telatar for useful discussions during the development of this paper. In particular, we would like to thank Emre for his help in proving Lemma 17.

APPENDIX

The proof of (4) and (5) is based on the following approach. For any channel $W : \mathcal{X} \to \mathcal{Y}$ the channels $W^{[i]} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Y} \times U_0^{i-1}$ 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. random variables defined on a probability space $(\Omega, \mathcal{F}, \mu)$, and where B_n is a symmetric Bernoulli random variable. Defining $\mathcal{F}_0 = \{\emptyset, \Omega\}$ and $\mathcal{F}_n = \sigma(B_1, \ldots, B_n)$ for $n \geq 1$, 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 $W_n \in \{W^{(i)}\}_{i=0}^{2^n-1}$ and moreover the symmetric distribution of the random variables B_i implies

$$\Pr(Z_n \in (a, b)) = \frac{|\{i \in \{0, \ldots, 2^n - 1\} : Z^{(i)} \in (a, b)\}|}{2^n}. \tag{19}$$

In [15] it was shown that

$$\lim_{n \to \infty} \Pr(Z_n < 2^{-5n/4}) = I(W).$$

which implies (4). In [16] the polynomial decay (in terms of $N = 2^n$) was improved to exponential decay as stated below.

Theorem 15 (Rate of Z_n Approaching 0 [16]): Given a B-DMC W, and any $\beta < \frac{1}{2}$,

$$\lim_{n \to \infty} \Pr(Z_n \leq 2^{-2^{n\beta}}) = I(W).$$

Of course, this implies (5). For lossy source compression, the important quantity is the rate at which the random variable Z_n approaches 1 (as compared to 0). Let us now show the result mirroring Theorem 15 for this case, using similar techniques as in [16].

Theorem 16 (Rate of Z_n Approaching 1): Given a B-DMC W, and any $\beta < \frac{1}{2}$,

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

Proof: Using Lemma 17 the random variable Z_{n+1} can be bounded as,

$$Z_{n+1} \geq \sqrt{2Z_n^2 - Z_n^4} \text{ w.p. } \frac{1}{2},$$
$$Z_{n+1} = Z_n^2 \text{ w.p. } \frac{1}{2}.$$

Then, with probability $\frac{1}{2}$, $Z_{n+1}^2 \geq 1 - (1 - Z_n^2)^2$. This implies that $1 - Z_{n+1}^2 \leq (1 - Z_n^2)^2$. Similarly, with probability $\frac{1}{2}$,

$$1 - Z_{n+1}^2 = 1 - Z_n^4 \leq 2(1 - Z_n^2).$$

Let X_n denote $X_n = 1 - Z_n^2$. Then $\{X_n : n \geq 0\}$ satisfies

$$X_{n+1} \leq X_n^2 \text{ w.p. } \frac{1}{2},$$
$$X_{n+1} \leq 2X_n \text{ w.p. } \frac{1}{2}.$$

By adapting the proof of [16], we can show that for any $\beta < \frac{1}{2}$,

$$\lim_{n \to \infty} \Pr(X_n \leq 2^{-2^{n\beta}}) = 1 - I(W).$$

Using the relation $X_n = 1 - Z_n^2 \geq 1 - Z_n$, we get

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

■

Lemma 17 (Lower Bound on Z): Let W_1 and W_2 be two B-DMCs and let X_1 and X_2 be their inputs with a uniform prior. Let $Y_1 \in \mathcal{Y}_1$ and $Y_2 \in \mathcal{Y}_2$ denote the outputs. Let W denote the channel between $X = X_1 \oplus X_2$ and the output (Y_1, Y_2), i.e.,

$$W(y_1, y_2 \,|\, x) = \frac{1}{2} \sum_{u} W_1(y_1 \,|\, x \oplus u) W_2(y_2 \,|\, u).$$

Then

$$Z(W) \geq \sqrt{Z(W_1)^2 + Z(W_2)^2 - Z(W_1)^2 Z(W_2)^2}.$$

Proof: Let $Z = Z(W)$ and $Z_i = Z(W_i)$. Z can be expanded as follows.

$$\begin{aligned}
Z &= \sum_{y_1, y_2} \sqrt{W(y_1, y_2 \,|\, 0) W(y_1, y_2 \,|\, 1)} \\
&= \frac{1}{2} \sum_{y_1, y_2} \Big[W_1(y_1 \,|\, 0) W_2(y_2 \,|\, 0) W_1(y_1 \,|\, 0) W_2(y_2 \,|\, 1) \\
&\quad + W_1(y_1 \,|\, 0) W_2(y_2 \,|\, 0) W_1(y_1 \,|\, 1) W_2(y_2 \,|\, 0) \\
&\quad + W_1(y_1 \,|\, 1) W_2(y_2 \,|\, 1) W_1(y_1 \,|\, 0) W_2(y_2 \,|\, 1) \\
&\quad + W_1(y_1 \,|\, 1) W_2(y_2 \,|\, 1) W_1(y_1 \,|\, 1) W_2(y_2 \,|\, 0) \Big]^{\frac{1}{2}} \\
&= \frac{Z_1 Z_2}{2} \sum_{y_1, y_2} P_1(y_1) P_2(y_2) \\
&\quad \sqrt{\frac{W_1(y_1 \,|\, 0)}{W_1(y_1 \,|\, 1)} + \frac{W_1(y_1 \,|\, 1)}{W_1(y_1 \,|\, 0)} + \frac{W_2(y_2 \,|\, 0)}{W_2(y_2 \,|\, 1)} + \frac{W_2(y_2 \,|\, 1)}{W_2(y_2 \,|\, 0)}}
\end{aligned}$$

where $P_i(y_i)$ denotes

$$P_i(y_i) = \frac{\sqrt{W_i(y_i \,|\, 0) W_i(y_i \,|\, 1)}}{Z_i}.$$

Note that P_i is a probability distribution over $\mathcal{Y}_i$. Let $\mathbb{E}_i$ denote the expectation with respect to P_i and let

$$A_i(y) \triangleq \sqrt{\frac{W_i(y \,|\, 0)}{W_i(y \,|\, 1)}} + \sqrt{\frac{W_i(y \,|\, 1)}{W_i(y \,|\, 0)}}.$$

Then Z can be expressed as

$$Z = \frac{Z_1 Z_2}{2} \mathbb{E}_{1,2} \left[\sqrt{\left(A_1(Y_1)\right)^2 + \left(A_2(Y_2)\right)^2 - 4} \right].$$

The arithmetic-mean geometric-mean inequality implies that $A_i(y) \geq 2$. Therefore, for any $y_i \in \mathcal{Y}_i$, $A_i(y_i)^2 - 4 \geq 0$. Note that the function $f(x) = \sqrt{x^2 + a}$ is convex for

$a \geq 0$. Applying Jensen's inequality first with respect to the expectation $\mathbb{E}_1$ and then with respect to $\mathbb{E}_2$, we get

$$\begin{aligned} Z &\geq \frac{Z_1 Z_2}{2} \mathbb{E}_2 \left[\sqrt{\left(\mathbb{E}_1 \left[A_1(Y_1)\right]\right)^2 + \left(A_2(Y_2)\right)^2 - 4} \right] \\ &\geq \frac{Z_1 Z_2}{2} \sqrt{\left(\mathbb{E}_1 \left[A_1(Y_1)\right]\right)^2 + \left(\mathbb{E}_2 \left[A_2(Y_2)\right]\right)^2 - 4}. \end{aligned}$$

The claim follows by substituting $\mathbb{E}_i[A_i(Y_i)] = \frac{2}{Z_i}$. ■

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. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[3] T. J. Goblick, Jr., "Coding for discrete information source with a distortion measure," Ph.D. dissertation, MIT, 1962.

[4] T. Berger, *Rate Distortion Theory*. London: Prentice Hall, 1971.

[5] A. J. Viterbi and J. K. Omura, "Trellis encoding of memoryless disctre-time sources with a fidelity criterion," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 325–332, 1974.

[6] 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.

[7] M. J. Wainwright and E. Martinian, "Low-density graph codes that are optimal for source/channel coding and binning," *IEEE Trans. Inform. Theory*, 2009.

[8] 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.

[9] T. Murayama, "Thouless-anderson-palmer approach for lossy compression," *J. Phys. Rev. E: Stat. Nonlin. Soft Matter Phys.*, vol. 69, 2004.

[10] S. Ciliberti, M. Mézard, and R. Zecchina, "Lossy data compression with random gates," *Physical Rev. Lett.*, vol. 95, no. 038701, 2005.

[11] A. Braunstein, M. Mézard, and R. Zecchina, "Survey propagation: algorithm for satisfiability," e-print: cs.CC//0212002.

[12] 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.

[13] 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.

[14] A. Gupta, S. Verdú, and T. Weissman, "Rate-distortion in near-linear time," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Toronto, Canada, July 6 - July 11 2008, pp. 847–851.

[15] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *submitted to IEEE Trans. Inform. Theory*, 2008.

[16] E. Arıkan and E. Telatar, "On the rate of channel polarization," July 2008, available from "http://arxiv.org/pdf/0807.3917".

[17] I. Dumer, "Recursive decoding and its performance for low-rate reed-muller codes," *IEEE Transactions on Information Theory*, vol. 50, no. 5, pp. 811–823, 2004.

[18] G. D. Forney, Jr., "Codes on graphs: Normal realizations," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 520–548, Feb. 2001.

[19] 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.

[20] N. Hussami, S. B. Korada, and R. Urbanke, "Polar codes for channel and source coding," in *sumitted to ISIT*, 2009.

[21] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, 1976.

[22] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problemy Peredachi Informatsii*, vol. 9(1), pp. 19–31, 1983.

[23] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1250–1216, 2002.

[24] J. Chou, S. S. Pradhan, and K. Ramachandran, "Turbo and trellis-based constructions for source coding with side information," in *Data Compression Conference*, Mar. 2003.

[25] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (discus): design and construction," *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 626–643, 2003.

[26] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Nested convolutional/turbo codes for the binary wyner-ziv problem," in *Proceedings of the International Conference on Image Processing*, Sept. 2003, pp. 601–604.

[27] Y. Yang, V. Stankovic, Z. Xiong, and W. Zhao, "On multiterminal source code design," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2278–2302, 2008.

[28] J. Chou, S. S. Pradhan, and K. Ramachandran, "Turbo coded trellis-based constructions for data embedding: Channel coding with side information," in *Proceedings of the Asilomar Conference*, Nov. 2001, pp. 305–309.

[29] U. Erez and S. ten Brink, "A close-to-capacity dirty paper coding scheme," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3417–3432, 2005.

[30] Y. Sun, A. D. Liveris, V. Stankovic, and Z. Xiong, "Near-capacity dirty-paper code designs based on tcq and ira codes," in *Proc. of the IEEE Int. Symposium on Inform. Theory*, Sept. 2005, pp. 184–188.

[31] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[32] A. D. Wyner, "A theorem on the entropy of certain binary sequences and applications: Part II," *IEEE Trans. Inform. Theory*, vol. 19, no. 6, pp. 772–777, Nov. 1973.

[33] D. Aldous and J. A. Fill, *Reversible Markov chains and random walks on graphs*. Available at www.stat.berkeley.edu/users/aldous/book.html.

[34] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1159–1180, 2003.

[35] C. Heegard and A. A. E. Gamal, "On the capacity of computer memory with defects," *IEEE Transactions on Information Theory*, vol. 29, no. 5, pp. 731–739, 1983.

[36] B. S. Tsybakov, "Defect and error correction," *Problemy Peredachi Informatsii*, vol. 11, pp. 21–30, Jul.-Sep. 1975.

[37] S. Ciliberti and M. Mézard, "The theoretical capacity of the parity source coder," *Journal of Statistical Mechanics:Theory and Experiment*, vol. 1, no. 10003, 2005.

[38] S. B. Korada, E. Şaşoğlu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, and constructions," *submitted to IEEE Trans. Inform. Theory*, 2009.