

Achieving Marton's Region for Broadcast Channels Using Polar Codes

Marco Mondelli, S. Hamed Hassani, Igal Sason, and Rüdiger Urbanke

Abstract

This paper presents polar coding schemes for the 2-user discrete memoryless broadcast channel (DM-BC) which achieve Marton's region with both common and private messages. This is the best achievable rate region known to date, and it is tight for all classes of 2-user DM-BCs whose capacity regions are known. To accomplish this task, we first construct polar codes for both the superposition as well as the binning strategy. By combining these two schemes, we obtain Marton's region with private messages only. Finally, we show how to handle the case of common information. The proposed coding schemes possess the usual advantages of polar codes, i.e., they have low encoding and decoding complexity and a super-polynomial decay rate of the error probability.

We follow the lead of Goela, Abbe, and Gastpar, who recently introduced polar codes emulating the superposition and binning schemes. In order to align the polar indices, for both schemes, their solution involves some degradedness constraints that are assumed to hold between the auxiliary random variables and the channel outputs. To remove these constraints, we consider the transmission of k blocks and employ a chaining construction that guarantees the proper alignment of the polarized indices. The techniques described in this work are quite general, and they can be adopted to many other multi-terminal scenarios whenever there polar indices need to be aligned.

Keywords

Binning, broadcast channel, Marton's region, Marton-Gelfand-Pinsker (MGP) region, polar codes, polarization alignment, superposition coding.

I. INTRODUCTION

Polar codes, introduced by Arikan in [1], have been demonstrated to achieve the capacity of any memoryless binary-input output-symmetric channel with encoding and decoding complexity $\Theta(n \log n)$, where n is the block length of the code, and a block error probability decaying like $O(2^{-n^\beta})$, for any $\beta \in (0, 1/2)$, under successive cancellation decoding [2]. A refined analysis of the block error probability of polar codes leads in [3] to rate-dependent upper and lower bounds.

The original point-to-point communication scheme has been extended, amongst others, to lossless and lossy source coding [4], [5] and to various multi-terminal scenarios, such as the Gelfand-Pinsker, Wyner-Ziv, and Slepian-Wolf problems [6], [7], multiple-access channels [8]–[12], broadcast channels [13]–[15], interference channels [16], [17], degraded relay channels [18], [19], wiretap channels [19]–[23], bidirectional broadcast channels with common and confidential messages [24], write once memories (WOMs) [25], arbitrarily permuted parallel channels [26], and multiple description coding [27].

Goela, Abbe, and Gastpar recently introduced polar coding schemes for the m -user deterministic broadcast channel [13], [15], and for the noisy discrete memoryless broadcast channel (DM-BC) [14], [15]. For the second scenario, they considered two fundamental transmission strategies: *superposition coding*, in the version proposed by Bergmans [28], and *binning* [29]. In order to guarantee a proper alignment of the polar indices, in both the superposition and binning schemes, their solution involves some degradedness constraints that are assumed to hold between the auxiliary random variables and the channel outputs. It is noted that two superposition coding schemes were proposed by Bergmans [28] and Cover [30], and they both achieve the capacity region of the degraded broadcast channel.

M. Mondelli and R. Urbanke are with the School of Computer and Communication Sciences, EPFL, CH-1015 Lausanne, Switzerland (e-mails: {marco.mondelli, ruediger.urbanke}@epfl.ch).

S. H. Hassani is with the Computer Science Department, ETH Zürich, Switzerland (e-mail: hamed@inf.ethz.ch).

I. Sason is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Haifa 32000, Israel (e-mail: sason@ee.technion.ac.il).

The paper was presented in part at the *48th Annual Conference on Information Sciences and Systems (CISS 2014)*, Princeton, New Jersey, USA, March 2014, and at the *2014 IEEE International Symposium on Information Theory (ISIT 2014)*, Honolulu, Hawaii, USA, July 2014.

However, it has recently been proven that under MAP decoding, Cover’s strategy always achieves a rate region at least as large as Bergmans’, and this dominance can sometimes be strict [31].

In this paper we extend the schemes of [15], and we show how to achieve Marton’s region with both common and private messages. The original work by Marton [29] covers the case with only private messages, and the introduction of common information is due to Gelfand and Pinsker [32]. Hence, we will refer to this region as the Marton-Gelfand-Pinsker (MGP) region (this follows the terminology used, e.g., in [33]–[35]). This rate region is tight for all classes of DM-BCs with known capacity region, and it forms the best inner bound known to date for a 2-user DM-BC [36]–[38]. Note that it also includes Cover’s superposition region.

The crucial point consists in removing the degradedness conditions on auxiliary random variables and channel outputs¹, in order to achieve any rate pair inside the region defined by Bergmans’ superposition strategy and by the binning strategy. The ideas which make it possible to lift the constraints come from recent progress in constructing *universal* polar codes, which are capable of achieving the compound capacity of the whole class of memoryless binary-input output-symmetric channels [40], [41]. In short, first we describe polar codes for the superposition and binning strategies. Then, by combining these two techniques, we achieve Marton’s rate region with private messages only. Finally, by describing how to transmit common information, we achieve the whole MGP region.

The current exposition is limited to the case of binary auxiliary random variables and, only for Bergmans’ superposition coding scheme, also to binary inputs. However, there is no fundamental difficulty in extending the work to the q -ary case (see [12], [42]–[45]). The proposed schemes possess the standard properties of polar codes with respect to encoding and decoding, which can be performed with complexity $\Theta(n \log n)$, as well as with respect to the scaling of the block error probability as a function of the block length, which decays like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

The rest of the paper is organized as follows. Section II reviews the information-theoretic achievable rate regions for DM-BCs and the rate regions that can be obtained by the polarization-based code constructions proposed in [15], call them the AGG constructions. It proceeds by comparing Bergmans’ superposition scheme [28] with the AGG superposition region in [15], which serves for motivating this work. Furthermore, alternative characterizations of superposition, binning, and Marton’s regions are presented in Section II for simplifying the description of our novel polar coding schemes in this work. Section III reviews two “polar primitives” that form the basis of the AGG constructions and of our extensions: polar schemes for lossless compression, with and without side information, and for transmission over binary asymmetric channels. Sections IV and V describe our polar coding schemes that achieve the superposition and binning regions, respectively. Section VI first shows polar codes for the achievability of Marton’s region with only private messages and, then, also for the MGP region with both common and private messages. Section VII concludes this paper with some final thoughts.

II. ACHIEVABLE RATE REGIONS

A. Information-Theoretic Schemes

Let us start by considering the rate region that is achievable by Bergmans’ superposition scheme [36, Theorem 5.1], which provides the capacity region of degraded DM-BCs.

Theorem 1 (Superposition Region): Consider the transmission over a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel, and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let V be an auxiliary random variable. Then, for any joint distribution $p_{V, X}$ s.t. $V - X - (Y_1, Y_2)$ forms a Markov chain, a rate pair (R_1, R_2) is achievable if

$$\begin{aligned} R_1 &< I(X; Y_1 | V), \\ R_2 &< I(V; Y_2), \\ R_1 + R_2 &< I(X; Y_1). \end{aligned} \tag{1}$$

Note that the above only describes a subset of the region actually achievable by superposition coding. We get a second subset by swapping the roles of the two users, i.e., by swapping the indices 1 and 2. The actual achievable region is obtained by the convex hull of the closure of the union of these two subsets.

The rate region which is achievable by the binning strategy is described in the following [36, Theorem 8.3]:

¹Note that, in general, such kind of extra conditions make the achievable rate region strictly smaller, see [39].

Theorem 2 (Binning Region): Consider the transmission over a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel, and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let V_1 and V_2 denote auxiliary random variables. Then, for any joint distribution p_{V_1, V_2} and for any deterministic function ϕ s.t. $X = \phi(V_1, V_2)$, a rate pair (R_1, R_2) is achievable if

$$\begin{aligned} R_1 &< I(V_1; Y_1), \\ R_2 &< I(V_2; Y_2), \\ R_1 + R_2 &< I(V_1; Y_1) + I(V_2; Y_2) - I(V_1; V_2). \end{aligned} \quad (2)$$

Note that the achievable rate region does not become larger by considering general distributions $p_{X|V_1, V_2}$, i.e., there is no loss of generality in restricting X to be a deterministic function of (V_1, V_2) (see [36, Remark 8.4]). Furthermore, for deterministic DM-BCs, the choice $V_1 = Y_1$ and $V_2 = Y_2$ in (2) provides their capacity region (see, e.g., [37, Example 7.1]).

The rate region in (2) can be enlarged by combining binning with superposition coding. This leads to Marton's region for a 2-user DM-BC where only private messages are available (see [29, Theorem 2] and [36, Proposition 8.1]).

Theorem 3 (Marton's Region): Consider the transmission over a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel, and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let $V, V_1,$ and V_2 denote auxiliary random variables. Then, for any joint distribution p_{V, V_1, V_2} and for any deterministic function ϕ s.t. $X = \phi(V, V_1, V_2)$, a rate pair (R_1, R_2) is achievable if

$$\begin{aligned} R_1 &< I(V, V_1; Y_1), \\ R_2 &< I(V, V_2; Y_2), \\ R_1 + R_2 &< I(V, V_1; Y_1) + I(V_2; Y_2 | V) - I(V_1; V_2 | V), \\ R_1 + R_2 &< I(V, V_2; Y_2) + I(V_1; Y_1 | V) - I(V_1; V_2 | V). \end{aligned} \quad (3)$$

Note that the binning region (2) is a special case of Marton's region (3) where the random variable V is set to be a constant. As for the binning region in Theorem 2, there is no loss of generality in restricting X to be a deterministic function of (V, V_1, V_2) .

In a more general set-up, the users can transmit also common information. The generalization of Theorem 3 to the case with a common message results in the MGP region. We denote by R_0 the rate associated to the common message, and R_1, R_2 continue to indicate the private rates of the first and the second user, respectively. Then, under the hypotheses of Theorem 3, a rate triple (R_0, R_1, R_2) is achievable if

$$\begin{aligned} R_0 &< \min\{I(V; Y_1), I(V; Y_2)\}, \\ R_0 + R_1 &< I(V, V_1; Y_1), \\ R_0 + R_2 &< I(V, V_2; Y_2), \\ R_0 + R_1 + R_2 &< I(V, V_1; Y_1) + I(V_2; Y_2 | V) - I(V_1; V_2 | V), \\ R_0 + R_1 + R_2 &< I(V, V_2; Y_2) + I(V_1; Y_1 | V) - I(V_1; V_2 | V). \end{aligned} \quad (4)$$

An equivalent form of this region was derived by Liang [33]–[35] (see also Theorem 8.4 and Remark 8.6 in [36]). Note that the MGP region (4) is specialized to Marton's region (3) when $R_0 = 0$ (i.e., if only private messages exist). The evaluation of Marton's region in (3) and the MGP region in (4) for DM-BCs has been recently studied in [46]–[48], proving also their optimality for some interesting and non-trivial models of BCs in [49], [50].

B. Polar AGG Constructions

Let us now compare the results of Theorems 1 and 2 with the superposition and binning regions that are achievable by the polarization-based AGG constructions in [15]. We write $p \succ q$ to denote that the channel q is stochastically degraded with respect to the channel p .

Theorem 4 (AGG Superposition Region): Consider the transmission over a 2-user DM-BC $p_{Y_1, Y_2 | X}$ with a binary input alphabet, where X denotes the input to the channel, and Y_1, Y_2 denote the outputs at the first and second

receiver, respectively. Let V be an auxiliary binary random variable and assume that $p_{Y_1|V} \succ p_{Y_2|V}$. Then, for any joint distribution $p_{V,X}$ s.t. $V - X - (Y_1, Y_2)$ forms a Markov chain and for any rate pair (R_1, R_2) s.t.

$$\begin{aligned} R_1 &< I(X; Y_1 | V), \\ R_2 &< I(V; Y_2), \end{aligned} \tag{5}$$

there exists a sequence of polar codes with an increasing block length n that achieves this rate pair with encoding and decoding complexity $\Theta(n \log n)$, and with a block error probability that decays like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

Theorem 5 (AGG Binning Region): Consider the transmission over a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel, and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let V_1 and V_2 denote auxiliary binary random variables and assume that $p_{Y_2|V_2} \succ p_{V_1|V_2}$. Then, for any joint distribution p_{V_1, V_2} , for any deterministic function ϕ s.t. $X = \phi(V_1, V_2)$, and for any rate pair (R_1, R_2) s.t.

$$\begin{aligned} R_1 &< I(V_1; Y_1), \\ R_2 &< I(V_2; Y_2) - I(V_1; V_2), \end{aligned} \tag{6}$$

there exists a sequence of polar codes with an increasing block length n that achieves this rate pair with encoding and decoding complexity $\Theta(n \log n)$, and with a block error probability that decays like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

The rate regions (5) and (6) describe a subset of the regions actually achievable with polar codes by superposition coding and binning, respectively. However, in some cases it is not possible to achieve the second subset, since, by swapping the indices 1 and 2, we might not be able to fulfill the required degradation assumptions.

C. Comparison of Superposition Regions

As a motivation, before proceeding with the new code constructions and proofs, let us consider a specific transmission scenario and compare the information-theoretic superposition region (1) and the AGG superposition region (5) where the latter requires the degradedness assumption $p_{Y_1|V} \succ p_{Y_2|V}$.

In the following, let the channel between X and Y_1 be a binary symmetric channel with crossover probability p , namely, a BSC(p), and the channel between X and Y_2 be a binary erasure channel with erasure probability ϵ , namely, a BEC(ϵ). Let us recall a few known results for this specific model (see [36, Example 5.4]).

- 1) For any choice of the parameters $p \in (0, 1/2)$ and $\epsilon \in (0, 1)$, the capacity region of this DM-BC is achieved using superposition coding.
- 2) For $0 < \epsilon < 2p$, Y_1 is a stochastically degraded version of Y_2 .
- 3) For $4p(1-p) < \epsilon \leq h_2(p)$, Y_2 is more capable than Y_1 , i.e. $I(X; Y_2) \geq I(X; Y_1)$ for all distributions p_X , where $h_2(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ denotes the binary entropy function.

Let \mathcal{V} and \mathcal{X} denote the alphabets of the auxiliary random variable V and of the input X , respectively. Then, if the DM-BC is stochastically degraded or more capable, the auxiliary random variables satisfy the cardinality bound $|\mathcal{V}| \leq |\mathcal{X}|$ [51]. Consequently, for such a set of parameters, we can restrict our analysis to binary auxiliary random variables without any loss of generality. Furthermore, one can assume that the channel from V to X is a BSC, and that the binary random variable X is symmetric [52, Lemma 7].

First, pick $p = 0.11$ and $\epsilon = 0.2$. In this case, the DM-BC is stochastically degraded and, as can be seen in Figure 1(a), the two regions (1) and (5) coincide despite of the presence of the extra degradedness assumption. In addition, these two regions are non-trivial in the sense that they improve upon the simple time-sharing scheme in which one user remains silent and the other employs a point-to-point capacity achieving code. Then, pick $p = 0.11$ and $\epsilon = 0.4$. In the latter case, the DM-BC is more capable and, as can be seen in Figure 1(b), the information-theoretic region (1) strictly improves upon the AGG region (5) that coincides with a trivial time-sharing.

D. Equivalent Description of Achievable Regions

When describing our new polar coding schemes, we will show how to achieve certain rate pairs. The following propositions state that the achievability of these rate pairs is equivalent to the achievability of the whole rate regions described in Theorems 1–3.

Proposition 1 (Equivalent Superposition Region): In order to show the achievability of all points in the region (1), it suffices to describe a sequence of codes with an increasing block length n that achieves each of the rate pairs

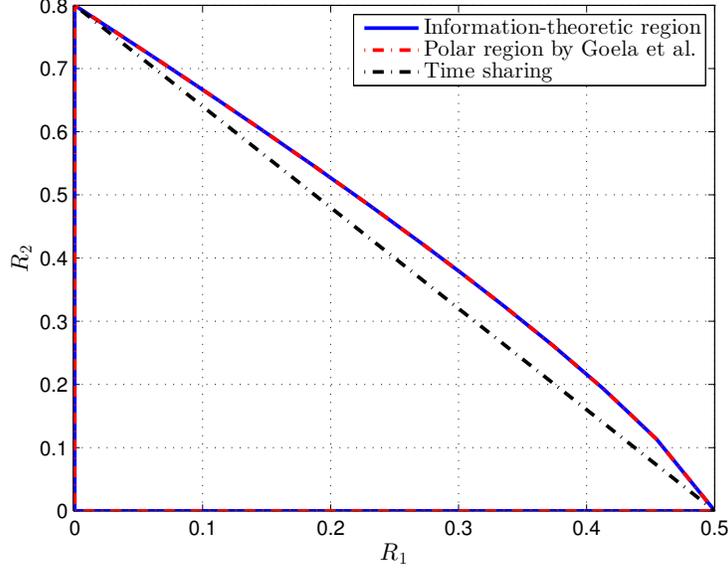
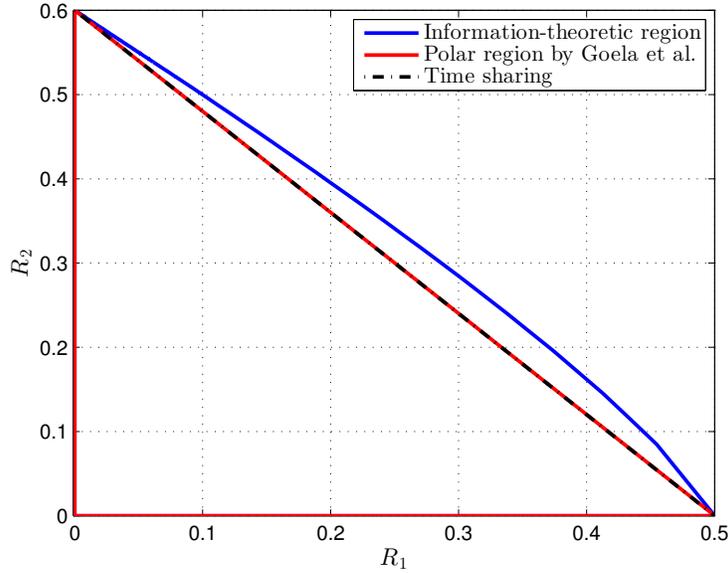
(a) $\epsilon = 0.2$ (b) $\epsilon = 0.4$

Figure 1. Comparison of superposition regions when the channel from X to Y_1 is a BSC(0.11) and the channel from X to Y_2 is a BEC(ϵ). When $\epsilon = 0.2$, the information-theoretic region (in blue) coincides with the AGG region (in red) and they are both strictly larger than the time-sharing line (in black). When $\epsilon = 0.4$, the information-theoretic region is strictly larger than the AGG region which reduces to the time-sharing line.

- $(R_1, R_2) = (I(X; Y_1 | V), \min(I(V; Y_1), I(V; Y_2)))$,
- $(R_1, R_2) = (I(X; Y_1) - I(V; Y_2), I(V; Y_2))$, provided that $I(V; Y_1) < I(V; Y_2) < I(X; Y_1)$,

with a block error probability that decays to zero as $n \rightarrow \infty$.

Proof: Assume that $I(V; Y_2) \leq I(V; Y_1)$. Since $V - X - Y_1$ forms a Markov chain, by the chain rule, the first two inequalities in (1) imply that $R_1 + R_2 < I(X; Y_1 | V) + I(V; Y_2) \leq I(X; Y_1 | V) + I(V; Y_1) = I(V, X; Y_1) = I(X; Y_1)$. Hence, the region (1) is a rectangle and it suffices to achieve the corner point $(I(X; Y_1 | V), I(V; Y_2))$.

Now, suppose that $I(V; Y_1) < I(V; Y_2)$. Let us separate this case into the following two sub-cases:

1) If $I(X; Y_1) > I(V; Y_2)$, the region (1) is a pentagon with the corner points

$$(I(X; Y_1) - I(V; Y_2), I(V; Y_2)), \quad (I(X; Y_1 | V), I(V; Y_1)).$$

The reason for the first corner point is that $I(V; Y_1 | X) = 0$, so, if $R_2 = I(V; Y_2)$, the satisfiability of the equality $R_1 + R_2 = I(X; Y_1)$ yields that

$$R_1 = I(X; Y_1) - I(V; Y_2) = I(V, X; Y_1) - I(V; Y_2) < I(V, X; Y_1) - I(V; Y_1) = I(X; Y_1 | V).$$

The reason for the second corner point is that $R_1 = I(X; Y_1 | V)$, $R_2 = I(V; Y_1) < I(V; Y_2)$, and

$$R_1 + R_2 = I(VX; Y_1) = I(V; Y_1 | X) + I(X; Y_1) = I(X; Y_1).$$

2) Otherwise, if $I(X; Y_1) \leq I(V; Y_2)$, the region (1) is a right trapezoid with corner points $(I(X; Y_1 | V), I(V; Y_1))$ and $(0, I(X; Y_1))$. Since $V - X - Y_2$ forms a Markov chain, then, by the data processing theorem and the last condition, it follows that $I(X; Y_1) \leq I(V; Y_2) \leq I(X; Y_2)$. Hence, the second corner point $(0, I(X; Y_1))$ is dominated by the point achievable when the first user is kept silent and the second user adopts a point-to-point code, taken from a sequence of codes with an increasing block length n , rate close to $I(X; Y_2)$, and block error probability that decays to zero (for example, a sequence of polar codes with an increasing block length). ■

Proposition 2 (Equivalent Binning Region): In order to show the achievability of all points in the region (2), it suffices to describe a sequence of codes with an increasing block length n that achieves the rate pair

$$(R_1, R_2) = (I(V_1; Y_1), I(V_2; Y_2) - I(V_1; V_2)),$$

assuming that $I(V_1; V_2) \leq I(V_2; Y_2)$, with a block error probability that decays to zero as $n \rightarrow \infty$.

Proof: Assume that $I(V_1; V_2) \leq \min(I(V_1; Y_1), I(V_2; Y_2))$. Then, the region (2) is a pentagon with corner points

$$(I(V_1; Y_1), I(V_2; Y_2) - I(V_1; V_2)), \quad (I(V_1; Y_1) - I(V_1; V_2), I(V_2; Y_2)).$$

Since the region (2) and the above condition are not affected by swapping the indices 1 and 2, it suffices to achieve the first corner point. In order to obtain the other corner point, one simply exchanges the roles of the two users.

Next, suppose that $I(V_2; Y_2) \leq I(V_1; V_2) < I(V_1; Y_1)$. Then, the region (2) is a right trapezoid with corner points

$$(I(V_1; Y_1) - I(V_1; V_2), I(V_2; Y_2)), \quad (I(V_1; Y_1) + I(V_2; Y_2) - I(V_1; V_2), 0).$$

Since $I(V_1; Y_1) + I(V_2; Y_2) - I(V_1; V_2) \leq I(V_1; Y_1)$ and $I(V_1; Y_1) \leq I(X; Y_1)$ (this follows from the data processing theorem for the Markov chain $V_1 - X - Y_1$), the last rate pair is dominated by the achievable point $(R_1, R_2) = (I(X; Y_1), 0)$ which refers to a point-to-point communication at rate $I(X; Y_1)$ for the first user, with a block error probability that decays to zero as $n \rightarrow \infty$, while the second user is kept silent.

The case where $I(V_1; Y_1) \leq I(V_1; V_2) < I(V_2; Y_2)$ is solved by swapping the indices of the two users, and by referring to the previous case.

Finally, assume that $I(V_1; V_2) \geq \max(I(V_1; Y_1), I(V_2; Y_2))$. Then, the region (2) is a triangle with corner points that are achievable by letting one user remain silent, while the other user performs a point-to-point reliable communication. ■

Remark: The rate $R_2 = I(V_2; Y_2) - I(V_1; V_2)$ in Proposition 2 is identical to the Gelfand-Pinsker rate if one considers the sequence $V_1^{1:n}$ to be known *non-causally* at the encoder. This suggests a design of an encoder which consists of two encoders: one for $v_1^{1:n}$, and the second for $v_2^{1:n}$ based on the Gelfand-Pinsker coding; in the second encoder, the sequence $v_1^{1:n}$ is provided as side information. The reader is referred to the encoding scheme in [37, Figure 7.3] while the indices 1 and 2 need to be switched.

Proposition 3 (Equivalent Marton's Region): In order to show the achievability of all points in the region (3), it suffices to describe a sequence of codes with an increasing block length n that achieves each of the rate pairs

$$\begin{aligned} (R_1, R_2) &= (I(V, V_1; Y_1), I(V_2; Y_2 | V) - I(V_1; V_2 | V)), \\ (R_1, R_2) &= (I(V, V_1; Y_1) - I(V_1; V_2 | V) - I(V; Y_2), I(V, V_2; Y_2)), \end{aligned} \tag{7}$$

assuming that $I(V; Y_1) \leq I(V; Y_2)$, with a block error probability that decays to zero as $n \rightarrow \infty$.

Proof: Since the region (3) is not affected by swapping the indices 1 and 2, we can assume without loss of generality that $I(V; Y_1) \leq I(V; Y_2)$. Then,

$$\begin{aligned} I(V, V_1; Y_1) + I(V_2; Y_2 | V) &= I(V; Y_1) + I(V_1; Y_1 | V) + I(V_2; Y_2 | V) \\ &\leq I(V; Y_2) + I(V_1; Y_1 | V) + I(V_2; Y_2 | V) = I(V, V_2; Y_2) + I(V_1; Y_1 | V), \end{aligned}$$

which means that the fourth inequality in (3) does not restrict the rate region under the above assumption.

Now, we can follow the same procedure outlined in the proof of Propositions 1 and 2. Suppose that

$$\begin{aligned} I(V_2; Y_2 | V) - I(V_1; V_2 | V) &> 0, \\ I(V, V_1; Y_1) - I(V_1; V_2 | V) - I(V; Y_2) &> 0. \end{aligned} \tag{8}$$

Then, the rate region (3) is a pentagon with the corner points in (7).

If one of the inequalities in (8) is satisfied and the other is violated, then the region (3) is a right trapezoid with one corner point given by (7) and the other corner point which is achievable by letting one user remain silent, while the other uses a point-to-point reliable scheme. If both inequalities in (8) are violated, then the region (3) is a triangle with corner points that are achievable with point-to-point coding schemes. ■

III. POLAR CODING PRIMITIVES

The AGG constructions, as well as our extensions, are based on two polar coding ‘‘primitives’’. Therefore, before discussing the broadcast setting, let us review these basic scenarios.

The first such primitive is the lossless compression, with or without side information. In the polar setting, this problem was first discussed in [6], [53]. In Section III-A, we consider the point of view of source polarization in [4].

The second such primitive is the transmission of polar codes over a general binary-input discrete memoryless channel (a DMC which is either symmetric or asymmetric). The basic problem which one faces here is that linear codes impose a uniform input distribution, while the capacity-achieving input distribution is in general not the uniform one when the DMC is asymmetric (however, in relative terms, the degradation in using the uniform prior for a binary-input DMC is at most 6% [54], [55]). One solution consists of concatenating the linear code with a non-linear pre-mapper [56]. A solution which makes use of the concatenation of two polar codes has been proposed in [57]. However, a more direct polar scheme is implicitly considered in [15], and is independently and explicitly presented in [58]. We will briefly review this last approach in Section III-B.

Notation: In what follows, we assume that n is a power of 2, say $n = 2^m$ for $m \in \mathbb{N}$, and we denote by G_n the polar matrix given by $G_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes m}$, where \otimes denotes the Kronecker product of matrices. The index set $\{1, \dots, n\}$ is abbreviated as $[n]$ and, given a set $\mathcal{A} \subseteq [n]$, we denote by \mathcal{A}^c its complement. We use $X^{i:j}$ as a shorthand for (X^i, \dots, X^j) with $i \leq j$.

A. Lossless Compression

Problem Statement. Consider a binary random variable $X \sim p_X$. Then, given the random vector $X^{1:n} = (X^1, \dots, X^n)$ consisting of n i.i.d. copies of X , the aim is to compress $X^{1:n}$ in a lossless fashion into a binary codeword of size roughly $nH(X)$, which is the entropy of $X^{1:n}$.

Design of the Scheme. Let $U^{1:n} = (U^1, \dots, U^n)$ be defined as

$$U^{1:n} = X^{1:n} G_n. \tag{9}$$

Then, $U^{1:n}$ is a random vector whose components are polarized in the sense that either U^i is approximately uniform and independent of $U^{1:i-1}$, or U^i is approximately a deterministic function of $U^{1:i-1}$. Formally, for $\beta \in (0, 1/2)$, let $\delta_n = 2^{-n^\beta}$ and set

$$\begin{aligned} \mathcal{H}_X &= \{i \in [n]: Z(U^i | U^{1:i-1}) \geq 1 - \delta_n\}, \\ \mathcal{L}_X &= \{i \in [n]: Z(U^i | U^{1:i-1}) \leq \delta_n\}, \end{aligned} \tag{10}$$

where Z denotes the Bhattacharyya parameter. Recall that, given $(T, V) \sim p_{T,V}$, where T is binary and V takes values in an arbitrary discrete alphabet \mathcal{V} , we define

$$Z(T | V) = 2 \sum_{v \in \mathcal{V}} \mathbb{P}_V(v) \sqrt{\mathbb{P}_{T|V}(0|v) \mathbb{P}_{T|V}(1|v)}. \tag{11}$$

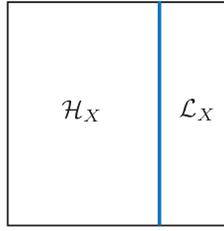


Figure 2. A simple graphical representation of the sets \mathcal{H}_X and \mathcal{L}_X for the lossless compression scheme. The whole square represents $[n]$. The sets \mathcal{H}_X and \mathcal{L}_X almost form a partition of $[n]$ in the sense that the number of indices of $[n]$ which are neither in \mathcal{H}_X nor in \mathcal{L}_X is $o(n)$.

Hence, for $i \in \mathcal{H}_X$, the bit U^i is approximately uniformly distributed and independent of the past $U^{1:i-1}$; also, for $i \in \mathcal{L}_X$, the bit U^i is approximately a deterministic function of $U^{1:i-1}$. Furthermore,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_X| &= H(X), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_X| &= 1 - H(X). \end{aligned} \quad (12)$$

For a graphical representation of this setting, see Figure 2.

Encoding. Given the vector $x^{1:n}$ that we want to compress, the encoder computes $u^{1:n} = x^{1:n} G_n$ and outputs the values of $u^{1:n}$ in the positions $\mathcal{L}_X^c = [n] \setminus \mathcal{L}_X$, i.e., it outputs $\{u^i\}_{i \in \mathcal{L}_X^c}$.

Decoding. The decoder receives $\{u^i\}_{i \in \mathcal{L}_X^c}$ and computes an estimate $\hat{u}^{1:n}$ of $u^{1:n}$ using the rule

$$\hat{u}^i = \begin{cases} u^i, & \text{if } i \in \mathcal{L}_X^c \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U^i | U^{1:i-1}}(u | u^{1:i-1}), & \text{if } i \in \mathcal{L}_X \end{cases} \quad (13)$$

Note that the conditional probabilities $\mathbb{P}_{U^i | U^{1:i-1}}(u | u^{1:i-1})$, for $u \in \{0,1\}$, can be computed recursively with complexity $\Theta(n \log n)$.

Performance. As explained above, for $i \in \mathcal{L}_X$, the bit U^i is almost deterministic given its past $U^{1:i-1}$. Therefore, for $i \in \mathcal{L}_X$, the distribution $\mathbb{P}_{U^i | U^{1:i-1}}(u | u^{1:i-1})$ is highly biased towards the correct value u^i . Indeed, the block error probability P_e , given by

$$P_e = \mathbb{P}(\hat{U}^{1:n} \neq U^{1:n}),$$

can be upper bounded by

$$P_e \leq \sum_{i \in \mathcal{L}_X} Z(U^i | U^{1:i-1}) = O(2^{-n^\beta}), \quad \forall \beta \in (0, 1/2). \quad (14)$$

Addition of Side Information. This is a slight extension of the previous case, and it is also discussed in [4]. Let $(X, Y) \sim p_{X,Y}$ be a pair of random variables, where we think of X as the source to be compressed and of Y as a *side information* about X . Given the vector $(X^{1:n}, Y^{1:n})$ of n independent samples from the distribution $p_{X,Y}$, the problem is to compress $X^{1:n}$ into a codeword of size roughly $nH(X|Y)$, so that the decoder is able to recover the whole vector $X^{1:n}$ by using the codeword and the side information $Y^{1:n}$.

Define $U^{1:n} = X^{1:n} G_n$ and consider the sets

$$\mathcal{H}_{X|Y} = \{i \in [n]: Z(U^i | U^{1:i-1}, Y^{1:n}) \geq 1 - \delta_n\}, \quad (15)$$

representing the positions s.t. U^i is approximately uniformly distributed and independent of $(U^{1:i-1}, Y^{1:n})$, and

$$\mathcal{L}_{X|Y} = \{i \in [n]: Z(U^i | U^{1:i-1}, Y^{1:n}) \leq \delta_n\}, \quad (16)$$

representing the positions s.t. U^i is approximately a deterministic function of $(U^{1:i-1}, Y^{1:n})$ (see Figure 3). Note that lossless compression without side information can be considered as lossless compression with side information \tilde{Y} , where \tilde{Y} is independent of X (say, e.g., that \tilde{Y} is constant). Therefore, \tilde{Y} does not add any information about X and it can be thought as a degraded version of Y . Therefore, the following inclusion relations hold:

$$\begin{aligned} \mathcal{H}_{X|Y} &\subseteq \mathcal{H}_X, \\ \mathcal{L}_X &\subseteq \mathcal{L}_{X|Y}, \end{aligned} \quad (17)$$

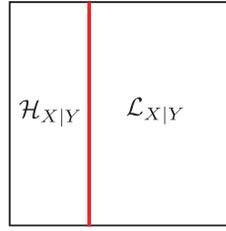


Figure 3. A simple graphical representation of the sets $\mathcal{H}_{X|Y}$ and $\mathcal{L}_{X|Y}$ for the lossless compression scheme with side information. The whole square represents $[n]$. The sets $\mathcal{H}_{X|Y}$ and $\mathcal{L}_{X|Y}$ almost form a partition of $[n]$ in the sense that the number of indices of $[n]$ which are neither in $\mathcal{H}_{X|Y}$ nor in $\mathcal{L}_{X|Y}$ is $o(n)$.

as it is graphically illustrated in Figures 2 and 3. A relationship analogous to (12) holds, namely,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{X|Y}| &= H(X|Y), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{X|Y}| &= 1 - H(X|Y). \end{aligned} \quad (18)$$

Given a realization of $X^{1:n}$, namely $x^{1:n}$, the encoder constructs $u^{1:n} = x^{1:n} G_n$ and outputs $\{u^i\}_{i \in \mathcal{L}_{X|Y}^c}$ as the compressed version of $x^{1:n}$. The decoder, using the side information $y^{1:n}$ and a decoding rule similar to (13), is able to reconstruct $x^{1:n}$ reliably with vanishing block error probability.

B. Transmission over Binary-Input DMCs

Problem Statement. Let W be a DMC with a binary input X and output Y . Fix a distribution p_X for the random variable X . The aim is to transmit over W with a rate close to $I(X; Y)$.

Design of the Scheme. Let $U^{1:n} = X^{1:n} G_n$, where $X^{1:n}$ is a vector of n i.i.d. components drawn according to p_X . Consider the sets \mathcal{H}_X and \mathcal{L}_X defined in (10). From the discussion about lossless compression, we know that, for $i \in \mathcal{H}_X$, the bit U^i is approximately uniformly distributed and independent of $U^{1:i-1}$ and that, for $i \in \mathcal{L}_X$, the bit U^i is approximately a deterministic function of the past $U^{1:i-1}$. Now, assume that the channel output $Y^{1:n}$ is given, and interpret this as side information on $X^{1:n}$. Consider the sets $\mathcal{H}_{X|Y}$ and $\mathcal{L}_{X|Y}$ as defined in (15) and (16), respectively. To recall, for $i \in \mathcal{H}_{X|Y}$, U^i is approximately uniformly distributed and independent of $(U^{1:i-1}, Y^{1:n})$, and, for $i \in \mathcal{L}_{X|Y}$, U^i becomes approximately a deterministic function of $(U^{1:i-1}, Y^{1:n})$.

To construct a polar code for the channel W , we proceed now as follows. We place the information in the positions indexed by $\mathcal{I} = \mathcal{H}_X \cap \mathcal{L}_{X|Y}$ (note that, from (17), $\mathcal{L}_X \subseteq \mathcal{L}_{X|Y}$). Indeed, if $i \in \mathcal{I}$, then U^i is approximately uniformly distributed given $U^{1:i-1}$, since $i \in \mathcal{H}_X$. This implies that U^i is suitable to contain information. Furthermore, U^i is approximately a deterministic function if we are given $U^{1:i-1}$ and $Y^{1:n}$, since $i \in \mathcal{L}_{X|Y}$. This implies that it is also decodable in a successive manner given the channel output. Using (12), (17), (18), and the fact that the number of indices in $[n]$ which are neither in \mathcal{H}_X nor in \mathcal{L}_X is $o(n)$, it follows that

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{X|Y} \setminus \mathcal{L}_X| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{X|Y}| - \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_X| \\ &= H(X) - H(X|Y) \\ &= I(X; Y). \end{aligned} \quad (19)$$

Hence, our requirement on the transmission rate is met.

The remaining positions are frozen. More precisely, they are divided into two subsets, namely $\mathcal{F}_r = \mathcal{H}_X \cap \mathcal{L}_{X|Y}^c$ and $\mathcal{F}_d = \mathcal{H}_X^c$. For $i \in \mathcal{F}_r$, U^i is independent of $U^{1:i-1}$, but cannot be reliably decoded using $Y^{1:n}$. We fill these positions with bits chosen uniformly at random, and this randomness is assumed to be shared between the transmitter

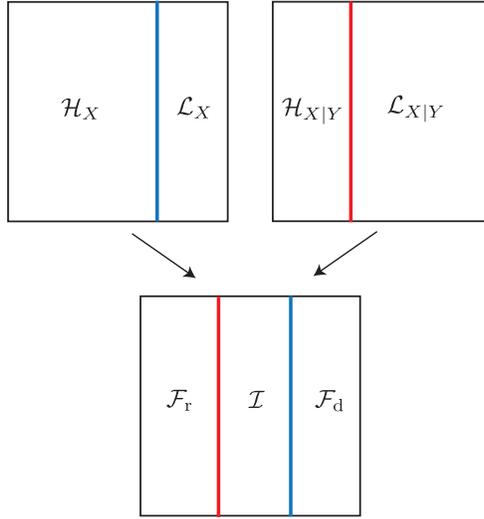


Figure 4. Graphical representation of the sets associated to the channel coding problem. The two images on top represent how the set $[n]$ (the whole square) is partitioned by the source X (top left), and by the source X together with the output Y assumed as a side information (top right). Since $\mathcal{H}_{X|Y} \subseteq \mathcal{H}_X$ and $\mathcal{L}_X \subseteq \mathcal{L}_{X|Y}$, the set of indices $[n]$ can be partitioned into three subsets (bottom image): the information indices $\mathcal{I} = \mathcal{H}_X \cap \mathcal{L}_{X|Y}$; the frozen indices $\mathcal{F}_r = \mathcal{H}_X \cap \mathcal{L}_{X|Y}^c$ filled with binary bits chosen uniformly at random; the frozen indices $\mathcal{F}_d = \mathcal{H}_X^c$ chosen according to a deterministic rule.

and the receiver (i.e., the encoder and the decoder know the values associated to these positions). For $i \in \mathcal{F}_d$, the value of U^i has to be chosen in a particular way. This is true since almost all these positions are in \mathcal{L}_X and, hence, U^i is approximately a deterministic function of $U^{1:i-1}$. The situation is schematically represented in Figure 4.

Encoding. The encoder first places the information bits into $\{u^i\}_{i \in \mathcal{I}}$. Then, $\{u^i\}_{i \in \mathcal{F}_r}$ is filled with a random sequence which is shared between the transmitter and the receiver. Finally, the elements of $\{u^i\}_{i \in \mathcal{F}_d}$ are computed in successive order and, for $i \in \mathcal{F}_d$, u^i is set to the value

$$u^i = \arg \max_{u \in \{0,1\}} \mathbb{P}_{U^i | U^{1:i-1}}(u | u^{1:i-1}).$$

These probabilities can be computed recursively with complexity $\Theta(n \log n)$. Since $G_n = G_n^{(-1)}$, the n -length vector $x^{1:n} = u^{1:n} G_n$ is transmitted over the channel.

Decoding. The decoder receives $y^{1:n}$, and it computes the estimate $\hat{u}^{1:n}$ of $u^{1:n}$ according to the rule

$$\hat{u}^i = \begin{cases} u^i, & \text{if } i \in \mathcal{F}_r \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U^i | U^{1:i-1}}(u | u^{1:i-1}), & \text{if } i \in \mathcal{F}_d \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U^i | U^{1:i-1}, Y^{1:n}}(u | u^{1:i-1}, y^{1:n}), & \text{if } i \in \mathcal{I} \end{cases}, \quad (20)$$

where $\mathbb{P}_{U^i | U^{1:i-1}, Y^{1:n}}(u | u^{1:i-1}, y^{1:n})$ can be computed recursively with complexity $\Theta(n \log n)$.

Performance. The block error probability P_e can be upper bounded by

$$P_e \leq \sum_{i \in \mathcal{I}} Z(U^i | U^{1:i-1}, Y^{1:n}) = O(2^{-n^\beta}), \quad \forall \beta \in (0, 1/2). \quad (21)$$

IV. POLAR CODES FOR SUPERPOSITION REGION

The following theorem provides our main result regarding the achievability of Bergmans' superposition region for DM-BCs with polar codes (compare with Theorem 1).

Theorem 6 (Polar Codes for Superposition Region): Consider a 2-user DM-BC $p_{Y_1, Y_2 | X}$ with a binary input alphabet, where X denotes the input to the channel, and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let V be an auxiliary binary random variable. Then, for any joint distribution $p_{V, X}$ s.t. $V - X - (Y_1, Y_2)$ forms a Markov chain and for any rate pair (R_1, R_2) satisfying the constraints in (1), there exists a sequence of

polar codes with an increasing block length n which achieves this rate pair with encoding and decoding complexity $\Theta(n \log n)$ and a block error probability decaying like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

Problem Statement. Let $(V, X) \sim p_{V,X} = p_V p_{X|V}$. We will show how to transmit over the 2-user DM-BC $p_{Y_1, Y_2|X}$ achieving the rate pair

$$(R_1, R_2) = (I(X; Y_1) - I(V; Y_2), I(V; Y_2)), \quad (22)$$

when $I(V; Y_1) < I(V; Y_2) < I(X; Y_1)$. Once we have accomplished this, we will see that a slight modification of this scheme allows to achieve, in addition, the rate pair

$$(R_1, R_2) = (I(X; Y_1 | V), \min_{l \in \{1, 2\}} I(V; Y_l)). \quad (23)$$

Therefore, by Proposition 1, we can achieve the whole region (1) and Theorem 6 is proved. Note that if polar coding achieves the rate pairs (22) and (23) with complexity $\Theta(n \log n)$ and a block error probability $O(2^{-n^\beta})$, then for any other rate pair in the region (1), there exists a sequence of polar codes with an increasing block length n whose complexity and block error probability have the same asymptotic scalings.

Design of the Scheme. Set $U_2^{1:n} = V^{1:n} G_n$. As in the case of the transmission over a general binary-input DMC with V in place of X and Y_l ($l \in \{1, 2\}$) in place of Y , define the sets \mathcal{H}_V , \mathcal{L}_V , $\mathcal{H}_{V|Y_l}$, and $\mathcal{L}_{V|Y_l}$, analogously to Section III-B, as follows:

$$\begin{aligned} \mathcal{H}_V &= \{i \in [n]: Z(U_2^i | U_2^{1:i-1}) \geq 1 - \delta_n\}, \\ \mathcal{L}_V &= \{i \in [n]: Z(U_2^i | U_2^{1:i-1}) \leq \delta_n\}, \\ \mathcal{H}_{V|Y_l} &= \{i \in [n]: Z(U_2^i | U_2^{1:i-1}, Y_l^{1:n}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{V|Y_l} &= \{i \in [n]: Z(U_2^i | U_2^{1:i-1}, Y_l^{1:n}) \leq \delta_n\}, \end{aligned} \quad (24)$$

which satisfy, for $l \in \{1, 2\}$,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_V| &= H(V), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_V| &= 1 - H(V), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V|Y_l}| &= H(V | Y_l), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V|Y_l}| &= 1 - H(V | Y_l). \end{aligned} \quad (25)$$

Set $U_1^{1:n} = X^{1:n} G_n$. By thinking of V as side information on X and by considering the transmission of X over the memoryless channel with output Y_1 , define also the sets $\mathcal{H}_{X|V}$, $\mathcal{L}_{X|V}$, $\mathcal{H}_{X|V, Y_1}$, and $\mathcal{L}_{X|V, Y_1}$, as follows:

$$\begin{aligned} \mathcal{H}_{X|V} &= \{i \in [n]: Z(U_1^i | U_1^{1:i-1}, V^{1:n}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{X|V} &= \{i \in [n]: Z(U_1^i | U_1^{1:i-1}, V^{1:n}) \leq \delta_n\}, \\ \mathcal{H}_{X|V, Y_1} &= \{i \in [n]: Z(U_1^i | U_1^{1:i-1}, V^{1:n}, Y_1^{1:n}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{X|V, Y_1} &= \{i \in [n]: Z(U_1^i | U_1^{1:i-1}, V^{1:n}, Y_1^{1:n}) \leq \delta_n\}, \end{aligned} \quad (26)$$

which satisfy

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{X|V}| &= H(X | V), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{X|V}| &= 1 - H(X | V), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{X|V, Y_1}| &= H(X | V, Y_1), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{X|V, Y_1}| &= 1 - H(X | V, Y_1). \end{aligned} \quad (27)$$

First, consider only the point-to-point communication problem between the transmitter and the second receiver. As discussed in Section III-B, for this scenario, the correct choice is to place the information bits in those positions of

$U_2^{1:n}$ that are indexed by the set $\mathcal{I}^{(2)} = \mathcal{H}_V \cap \mathcal{L}_{V|Y_2}$. If, in addition, we restrict ourselves to positions in $\mathcal{I}^{(2)}$ which are contained in $\mathcal{I}_v^{(1)} = \mathcal{H}_V \cap \mathcal{L}_{V|Y_1}$, also the first receiver will be able to decode this message. Indeed, recall that in the superposition coding scheme, the first receiver needs to decode the message intended for the second receiver before decoding its own message. Consequently, for sufficiently large n , the first receiver knows the vector $U_2^{1:n}$ with high probability, and, hence, also the vector $V^{1:n} = U_2^{1:n}G_n$ (recall that $G_n^{-1} = G_n$).

Now, consider the point-to-point communication problem between the transmitter and the first receiver, given the side information $V^{1:n}$ (following our discussion, as we let n tend to infinity, the vector $V^{1:n}$ is known to the first receiver with probability that tends to 1). From Section III-B, we know that the information has to be placed in those positions of $U_1^{1:n}$ that are indexed by $\mathcal{I}^{(1)} = \mathcal{H}_{X|V} \cap \mathcal{L}_{X|V,Y_1}$.

The cardinalities of these information sets are given by

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}^{(2)}| &= I(V; Y_2), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}_v^{(1)}| &= I(V; Y_1), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}^{(1)}| &= I(X; Y_1 | V). \end{aligned} \quad (28)$$

Let us now get back to the broadcasting scenario, and see how the previous observations can be used to construct a polar coding scheme. Recall that $X^{1:n}$ is transmitted over the channel, the second receiver only decodes its intended message, but the first receiver decodes both messages.

We start by reviewing the AGG scheme [15]. This scheme achieves the rate pair

$$(R_1, R_2) = (I(X; Y_1 | V), I(V; Y_2)), \quad (29)$$

assuming that $p_{Y_1|V} \succ p_{Y_2|V}$. Under this assumption, we have $\mathcal{L}_{V|Y_2} \subseteq \mathcal{L}_{V|Y_1}$ and therefore $\mathcal{I}^{(2)} \subseteq \mathcal{I}_v^{(1)}$. Consequently, we can in fact use the point-to-point solutions outlined above, i.e., the second user can place his information in $\mathcal{I}^{(2)}$ and decode, and the first user will also be able to decode this message. Furthermore, once the message intended for the second user is known by the first user, the latter can decode his own information which is placed in the positions of $\mathcal{I}^{(1)}$.

Let us now see how to eliminate the restriction imposed by the degradedness condition $p_{Y_1|V} \succ p_{Y_2|V}$. Recall that we want to achieve the rate pair (22) when $I(V; Y_1) < I(V; Y_2) < I(X; Y_1)$. The set of indices of the information bits for the first user is exactly the same as before, namely the positions of $U_1^{1:n}$ indexed by $\mathcal{I}^{(1)}$. The only difficulty lies in designing a coding scheme in which *both* receivers can decode the message intended for the second user.

First of all, observe that we can use all the positions in $\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}$, since they are decodable by both users. Let us define

$$\mathcal{D}^{(2)} = \mathcal{I}^{(2)} \setminus \mathcal{I}_v^{(1)}. \quad (30)$$

If $p_{Y_1|V} \succ p_{Y_2|V}$, as before, then $\mathcal{D}^{(2)} = \emptyset$ (i.e., all the positions decodable by the second user are also decodable by the first user). However, in the general case, where it is no longer assumed that $p_{Y_1|V} \succ p_{Y_2|V}$, the set $\mathcal{D}^{(2)}$ is not empty and those positions cannot be decoded by the first user.

Note that there is a similar set, but with the roles of the two users exchanged, call it $\mathcal{D}^{(1)}$, namely,

$$\mathcal{D}^{(1)} = \mathcal{I}_v^{(1)} \setminus \mathcal{I}^{(2)}. \quad (31)$$

The set $\mathcal{D}^{(1)}$ contains the positions of $U_2^{1:n}$ which are decodable by the first user, but not by the second user. Observe further that $|\mathcal{D}^{(1)}| \leq |\mathcal{D}^{(2)}|$ for sufficiently large n . Indeed, since the equality

$$|A \setminus B| - |B \setminus A| = |A| - |B| \quad (32)$$

holds for any two finite sets A and B , it follows from (28)–(30) that for sufficiently large n

$$\frac{1}{n} (|\mathcal{D}^{(2)}| - |\mathcal{D}^{(1)}|) = \frac{1}{n} (|\mathcal{I}^{(2)}| - |\mathcal{I}_v^{(1)}|) = I(V; Y_2) - I(V; Y_1) + o(1) \geq 0. \quad (33)$$

Assume at first that the two sets are of equal size. The general case will require only a small modification.

Now, the idea is to consider the ‘‘chaining’’ construction introduced in [40] in the context of universal polar codes. Recall that we are only interested in the message intended for the second user, but that both receivers must be able

to decode this message. Our scheme consists in transmitting k polar blocks, and in repeating (“chaining”) some information. More precisely, in block 1 fill the positions indexed by $\mathcal{D}^{(1)}$ with information, but set the bits indexed by $\mathcal{D}^{(2)}$ to a fixed known sequence. In block j ($j \in \{2, \dots, k-1\}$), fill the positions indexed by $\mathcal{D}^{(1)}$ again with information, and repeat the bits which were contained in the positions indexed by $\mathcal{D}^{(1)}$ of block $j-1$ into the positions indexed by $\mathcal{D}^{(2)}$ of block j . In the final block k , put a known sequence in the positions indexed by $\mathcal{D}^{(1)}$, and repeat in the positions indexed by $\mathcal{D}^{(2)}$ the bits in the positions indexed by $\mathcal{D}^{(1)}$ of block $k-1$. The remaining bits are frozen and, as in Section III-B, they are divided into the two subsets $\mathcal{F}_d^{(2)} = \mathcal{H}_V^c$ and $\mathcal{F}_r^{(2)} = \mathcal{H}_V \cap \mathcal{L}_{V|Y_2}^c \subset \mathcal{H}_V$. In the first case, U_2^i is approximately a deterministic function of $U_2^{1:i-1}$, while in the second case U_2^i is approximately independent of $U_2^{1:i-1}$.

Note that we lose some rate, since at the boundary we put a known sequence into some bits which were supposed to contain information. However, this rate loss decays like $1/k$, and by choosing a sufficiently large k , one can achieve a rate that is arbitrarily close to the intended rate.

We claim that in the above construction both users can decode all blocks, but the first receiver has to decode “forward”, starting with block 1 and ending with block k , whereas the second receiver decodes “backwards”, starting with block k and ending with block 1. Let us discuss this procedure in some more detail. Look at the first user and start with block 1. By construction, information is only contained in the positions indexed by $\mathcal{D}^{(1)}$ as well as $\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}$, while the positions indexed by $\mathcal{D}^{(2)}$ are set to known values. Hence, the first user can decode this block. For block j ($j \in \{2, \dots, k-1\}$), the situation is similar: the first user decodes the positions indexed by $\mathcal{D}^{(1)}$ and $\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}$, while the positions in $\mathcal{D}^{(2)}$ contain repeated information, which has been already decoded in the previous block. An analogous analysis applies to block k , in which the positions indexed by $\mathcal{D}^{(1)}$ are also fixed to a known sequence. The second user proceeds exactly in the same fashion, but goes backwards.

To get to the general case, we need to discuss what happens when $|\mathcal{D}^{(1)}| < |\mathcal{D}^{(2)}|$ (due to (33), in general $|\mathcal{D}^{(1)}| \leq |\mathcal{D}^{(2)}|$ for sufficiently large n , but the special case where the two sets are of equal size has been already addressed). In this case, we do not have sufficiently many positions in $\mathcal{D}^{(1)}$ to repeat all the information contained in $\mathcal{D}^{(2)}$. To get around this problem, pick sufficiently many extra positions out of the vector $U_1^{1:n}$ indexed by $\mathcal{I}^{(1)}$, and repeat the extra information there.

In order to specify this scheme, let us introduce some notation for the various sets. Recall that we “chain” the positions in $\mathcal{D}^{(1)}$ with an equal amount of positions in $\mathcal{D}^{(2)}$. It does not matter what subset of $\mathcal{D}^{(2)}$ we pick, but call the chosen subset $\mathcal{R}^{(2)}$. Now, we still have some positions left in $\mathcal{D}^{(2)}$, call them $\mathcal{B}^{(2)}$. More precisely, $\mathcal{B}^{(2)} = \mathcal{D}^{(2)} \setminus \mathcal{R}^{(2)}$. Since $\mathcal{R}^{(2)} \subseteq \mathcal{D}^{(2)}$ and $|\mathcal{R}^{(2)}| = |\mathcal{D}^{(1)}|$, it follows from (33) that

$$\frac{1}{n} |\mathcal{B}^{(2)}| = \frac{1}{n} (|\mathcal{D}^{(2)}| - |\mathcal{R}^{(2)}|) = \frac{1}{n} (|\mathcal{D}^{(2)}| - |\mathcal{D}^{(1)}|) = I(V; Y_2) - I(V; Y_1) + o(1) \geq 0. \quad (34)$$

Let $\mathcal{B}^{(1)}$ be a subset of $\mathcal{I}^{(1)}$ s.t. $|\mathcal{B}^{(1)}| = |\mathcal{B}^{(2)}|$. Again, it does not matter what subset we pick. The existence of such a set $\mathcal{B}^{(1)}$, for sufficiently large n , is ensured by noticing that from (28), (34) and the Markovity of the chain $V - X - Y_1$ we obtain

$$\frac{1}{n} (|\mathcal{I}^{(1)}| - |\mathcal{B}^{(2)}|) = I(X; Y_1 | V) - I(V; Y_2) + I(V; Y_1) + o(1) = I(X; Y_1) - I(V; Y_2) + o(1) \geq 0. \quad (35)$$

Indeed, recall that we need to achieve the rate pair (22) when $I(V; Y_1) < I(V; Y_2) < I(X; Y_1)$.

As explained above, we place in $\mathcal{B}^{(1)}$ the value of those extra bits from $\mathcal{D}^{(2)}$ which will help the first user to decode the message of the second user in the next block. Operationally, we repeat the information contained in the positions indexed by $\mathcal{B}^{(2)}$ into the positions indexed by $\mathcal{B}^{(1)}$ of the previous block. By doing this, the first user pays a rate penalty of $I(V; Y_2) - I(V; Y_1) + o(1)$ compared to his original rate given by $\frac{1}{n} |\mathcal{I}^{(1)}| = I(X; Y_1 | V) + o(1)$.

To summarize, the first user puts information bits at positions $\mathcal{I}^{(1)} \setminus \mathcal{B}^{(1)}$, repeats in $\mathcal{B}^{(1)}$ the information bits in $\mathcal{B}^{(2)}$ for the next block, and freezes the rest. In the last block, the information set is the whole $\mathcal{I}^{(1)}$. The frozen positions are divided into the usual two subsets $\mathcal{F}_r^{(1)} = \mathcal{H}_{X|V} \cap \mathcal{L}_{X|V,Y_1}^c$ and $\mathcal{F}_d^{(1)} = \mathcal{H}_{X|V}^c$, which contain positions s.t. U_1^i is or is not, respectively, approximately independent of $(U_1^{1:i-1}, V^{1:n})$. The situation is schematically represented in Figures 5–7.

Suppose that, by applying the same scheme with $k \rightarrow \infty$, we let $\frac{1}{n} |\mathcal{B}^{(2)}|$ shrink from $I(V; Y_2) - I(V; Y_1) + o(1)$ in (34) to $o(1)$. Then, one obtains the whole line going from the rate pair $(I(X; Y_1) - I(V; Y_2), I(V; Y_2))$ to

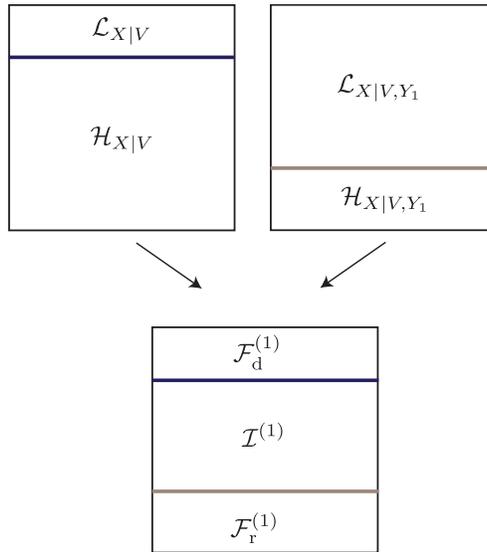


Figure 5. Graphical representation of the sets associated to the first user for the superposition scheme. The set $[n]$ is partitioned into three subsets: the information indices $\mathcal{I}^{(1)}$; the frozen indices $\mathcal{F}_r^{(1)}$ filled with bits chosen uniformly at random; the frozen indices $\mathcal{F}_d^{(1)}$ chosen according to a deterministic rule.

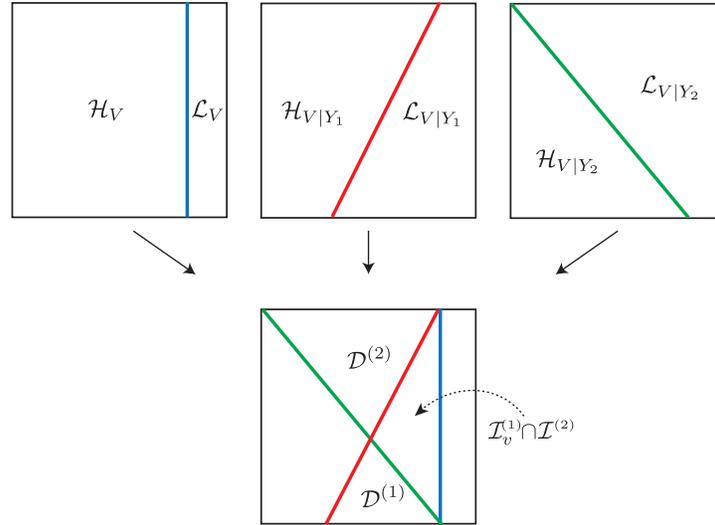


Figure 6. Graphical representation of the sets associated to the second user for the superposition scheme: $\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}$ contains the indices which are decodable by both users; $\mathcal{D}^{(1)} = \mathcal{I}_v^{(1)} \setminus \mathcal{I}^{(2)}$ contains the indices which are decodable by the first user, but not by the second user; $\mathcal{D}^{(2)} = \mathcal{I}^{(2)} \setminus \mathcal{I}_v^{(1)}$ contains the indices which are decodable by the second user, but not by the first user.

$(I(X; Y_1 | V), I(V; Y_1))$ without time-sharing.²

Finally, in order to obtain the rate pair $(I(X; Y_1 | V), I(V; Y_2))$ when $I(V; Y_2) \leq I(V; Y_1)$, it suffices to consider the case where $\mathcal{B}^{(2)} = \emptyset$ and switch the roles of $\mathcal{I}^{(2)}$ and $\mathcal{I}_v^{(1)}$ in the discussion concerning the second user.

Encoding. Let us start from the second user, and encode block by block.

For block 1:

- The information bits are stored in $\{u_2^i\}_{i \in \mathcal{I}_v^{(1)}}$.
- The set $\{u_2^i\}_{i \in \mathcal{F}_r^{(2)}}$ is filled with a random sequence, shared between the transmitter and both receivers.
- For $i \in \mathcal{F}_d^{(2)}$, we set $u_2^i = \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}}(u | u_2^{1:i-1})$.

²The reader will be able to verify this property by relying on (36) and (37); this property is mentioned, however, at this stage as part of the exposition of the polar coding scheme.

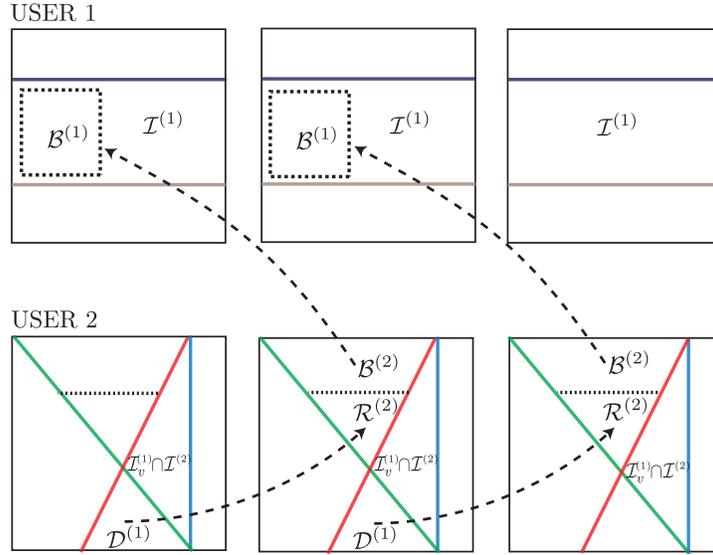


Figure 7. Graphical representation of the repetition construction for the superposition scheme with $k = 3$: the set $\mathcal{D}^{(1)}$ is repeated into the set $\mathcal{R}^{(2)}$ of the following block; the set $\mathcal{B}^{(2)}$ is repeated into the set $\mathcal{B}^{(1)}$ of the previous block (belonging to a different user).

For block j ($j \in \{2, \dots, k-1\}$):

- The information bits are stored in $\{u_2^i\}_{i \in \mathcal{I}_v^{(1)} \cup \mathcal{B}^{(2)}}$.
- $\{u_2^i\}_{i \in \mathcal{R}^{(2)}}$ contains the set $\{u_2^i\}_{i \in \mathcal{D}^{(1)}}$ of block $j-1$.
- The frozen sets $\{u_2^i\}_{i \in \mathcal{F}_r^{(2)}}$ and $\{u_2^i\}_{i \in \mathcal{F}_d^{(2)}}$ are chosen as in block 1.

For block k (the last one):

- The information bits are stored in $\{u_2^i\}_{i \in (\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}) \cup \mathcal{B}^{(2)}}$.
- $\{u_2^i\}_{i \in \mathcal{R}^{(2)}}$ contains the set $\{u_2^i\}_{i \in \mathcal{D}^{(1)}}$ of block $k-1$.
- The frozen bits are computed with the usual rules.

The rate of the second user is given by

$$\begin{aligned} R_2 &= \frac{1}{kn} \left[|\mathcal{I}_v^{(1)}| + (k-2)|\mathcal{I}_v^{(1)} \cup \mathcal{B}^{(2)}| + |(\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}) \cup \mathcal{B}^{(2)}| \right] \\ &= \left(\frac{k-1}{k} \right) I(V; Y_2) + \frac{1}{kn} |\mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}| + o(1), \end{aligned} \quad (36)$$

which, as k tends to infinity, approaches the required rate $I(V; Y_2)$ (the second equality in (36) follows from (28) and (34), and from the fact that the sets $\mathcal{I}_v^{(1)}$ and $\mathcal{B}^{(2)}$ are disjoint). Then, the vector $v^{1:n} = u_2^{1:n} G_n$ is obtained.

The encoder for the first user knows $v^{1:n}$ and proceeds block by block:

- The information bits are stored in $\{u_1^i\}_{i \in \mathcal{I}^{(1)} \setminus \mathcal{B}^{(1)}}$, except for block k , in which the information set is $\{u_1^i\}_{i \in \mathcal{I}^{(1)}}$.
- For block j ($j \in \{1, \dots, k-1\}$), $\{u_1^i\}_{i \in \mathcal{B}^{(1)}}$ contains a copy of the set $\{u_2^i\}_{i \in \mathcal{B}^{(2)}}$ in block $j+1$.
- The frozen set $\{u_1^i\}_{i \in \mathcal{F}_r^{(1)}}$ contains a random sequence shared between the encoder and the first decoder.
- For $i \in \mathcal{F}_d^{(1)}$, we set $u_1^i = \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_1^i | U_1^{1:i-1}, V^{1:n}}(u | u_1^{1:i-1}, v^{1:n})$.

The rate of the first user is given by (see (28) and (35), and recall that $\mathcal{B}^{(1)} \subset \mathcal{I}^{(1)}$ s.t. $|\mathcal{B}^{(1)}| = |\mathcal{B}^{(2)}|$)

$$\begin{aligned} R_1 &= \frac{1}{kn} \left[(k-1)|\mathcal{I}^{(1)} \setminus \mathcal{B}^{(1)}| + |\mathcal{I}^{(1)}| \right] \\ &= I(X; Y_1 | V) - \frac{k-1}{k} (I(V; Y_2) - I(V; Y_1)) + o(1), \end{aligned} \quad (37)$$

which, as k tends to infinity, approaches the required rate $I(X; Y_1) - I(V; Y_2)$. Finally, the vector $x^{1:n} = u_1^{1:n} G_n$ is transmitted over the channel. The encoding complexity per block is $\Theta(n \log n)$.

Decoding. Let us start from the first user, which receives the channel output $y_1^{1:n}$. The decoder acts block by block and reconstructs first $u_2^{1:n}$, computes $v^{1:n} = u_2^{1:n}G_n$, and then decodes $u_1^{1:n}$, thus recovering his own message. For block 1, the decision rule is given by

$$\hat{u}_2^i = \begin{cases} u_2^i, & \text{if } i \in \mathcal{F}_r^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}}(u | u_2^{1:i-1}), & \text{if } i \in \mathcal{F}_d^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, Y_1^{1:n}}(u | u_2^{1:i-1}, y_1^{1:n}), & \text{if } i \in \mathcal{I}_v^{(1)} \end{cases}, \quad (38)$$

and

$$\hat{u}_1^i = \begin{cases} u_1^i, & \text{if } i \in \mathcal{F}_r^{(1)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_1^i | U_1^{1:i-1}, V^{1:n}}(u | u_1^{1:i-1}, v^{1:n}), & \text{if } i \in \mathcal{F}_d^{(1)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_1^i | U_1^{1:i-1}, V^{1:n}, Y_1^{1:n}}(u | u_1^{1:i-1}, v^{1:n}, y_1^{1:n}), & \text{if } i \in \mathcal{I}^{(1)} \end{cases}. \quad (39)$$

For block j ($j \in \{2, \dots, k-1\}$):

- $\{\hat{u}_2^i\}_{i \in \mathcal{B}^{(2)}}$ is deduced from $\{\hat{u}_1^i\}_{i \in \mathcal{B}^{(1)}}$ of block $j-1$.
- $\{\hat{u}_2^i\}_{i \in \mathcal{R}^{(2)}}$ is deduced from $\{\hat{u}_2^i\}_{i \in \mathcal{D}^{(1)}}$ of block $j-1$.
- For the remaining positions of \hat{u}_2^i , the decoding follows the rule in (38).
- The decoding of \hat{u}_1^i proceeds as in (39).

This decoding rule works also for block k , with the only difference that the frozen set $\mathcal{F}_r^{(2)}$ is bigger, and $\hat{u}_2^i = \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, Y_1^{1:n}}(u | u_2^{1:i-1}, y_1^{1:n})$ only for $i \in \mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}$.

Let us consider now the second user, which reconstructs $u_2^{1:n}$ from the channel output $y_2^{1:n}$. As explained before, the decoding goes “backwards”, starting from block k and ending with block 1.

For block k , the decision rule is given by

$$\hat{u}_2^i = \begin{cases} u_2^i, & \text{if } i \in \mathcal{F}_r^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}}(u | u_2^{1:i-1}), & \text{if } i \in \mathcal{F}_d^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, Y_2^{1:n}}(u | u_2^{1:i-1}, y_2^{1:n}), & \text{if } i \in (\mathcal{I}^{(1)} \cap \mathcal{I}^{(2)}) \cup \mathcal{R}^{(2)} \cup \mathcal{B}^{(2)} \end{cases}. \quad (40)$$

For block j ($j \in \{2, \dots, k-1\}$), the decoder recovers $\{u_2^i\}_{i \in \mathcal{D}^{(1)}}$ from $\{u_2^i\}_{i \in \mathcal{R}^{(2)}}$ of block $j+1$; for the remaining positions, the decision rule in (40) is used.

For block 1, the reasoning is the same, except that the information bits are $\{u_2^i\}_{i \in \mathcal{I}_v^{(1)} \cap \mathcal{I}^{(2)}}$, i.e., the information set is smaller. The complexity per block, under successive cancellation decoding, is $\Theta(n \log n)$.

Performance. The block error probability $P_e^{(l)}$ for the l -th user ($l \in \{1, 2\}$) can be upper bounded by

$$\begin{aligned} P_e^{(1)} &\leq k \sum_{i \in \mathcal{I}_v^{(1)}} Z(U_2^i | U_2^{1:i-1}, Y_1^{1:n}) + k \sum_{i \in \mathcal{I}^{(1)}} Z(U_1^i | U_1^{1:i-1}, Y_1^{1:n}) = O(2^{-n^\beta}), \\ P_e^{(2)} &\leq k \sum_{i \in \mathcal{I}^{(2)}} Z(U_2^i | U_2^{1:i-1}, Y_2^{1:n}) = O(2^{-n^\beta}), \quad \forall \beta \in (0, 1/2). \end{aligned} \quad (41)$$

V. POLAR CODES FOR BINNING REGION

The following theorem provides our main result regarding the achievability of the binning region for DM-BCs with polar codes (compare with Theorem 2).

Theorem 7 (Polar Codes for Binning Region): Consider a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel taking values on an arbitrary set \mathcal{X} , and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let V_1 and V_2 denote auxiliary binary random variables. Then, for any joint distribution p_{V_1, V_2} , for any deterministic function $\phi: \{0, 1\}^2 \rightarrow \mathcal{X}$ s.t. $X = \phi(V_1, V_2)$, and for any rate pair (R_1, R_2) satisfying the constraints (2), there exists a sequence of polar codes with an increasing block length n which achieves this rate pair with encoding and decoding complexity $\Theta(n \log n)$ and a block error probability decaying like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

Problem Statement. Let $(V_1, V_2) \sim p_{V_1, V_2} = p_{V_1} p_{V_2 | V_1}$, and let X be a deterministic function ϕ of (V_1, V_2) . The aim is to transmit over the 2-user DM-BC $p_{Y_1, Y_2 | X}$ achieving the rate pair

$$(R_1, R_2) = (I(V_1; Y_1), I(V_2; Y_2) - I(V_1; V_2)), \quad (42)$$

assuming that $I(V_1; V_2) < I(V_2; Y_2)$. Consequently, by Proposition 2, we can achieve the whole region (2) and Theorem 7 is proved. Note that if polar coding achieves the rate pair (42) with complexity $\Theta(n \log n)$ and a block error probability $O(2^{-n^\beta})$, then for any other rate pair in the region (2), there exists a sequence of polar codes with an increasing block length n whose complexity and block error probability have the same asymptotic scalings.

Design of the Scheme. Set $U_1^{1:n} = V_1^{1:n} G_n$ and $U_2^{1:n} = V_2^{1:n} G_n$. As in the case of the transmission over a DMC with V_l in place of X and Y_l in place of Y ($l \in \{1, 2\}$), define the sets \mathcal{H}_{V_l} , \mathcal{L}_{V_l} , $\mathcal{H}_{V_l | Y_l}$, and $\mathcal{L}_{V_l | Y_l}$ for $l \in \{1, 2\}$, similarly to (24) (except of replacing U_2 with U_l and V with V_l), which satisfy

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V_l}| &= H(V_l), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V_l}| &= 1 - H(V_l), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V_l | Y_l}| &= H(V_l | Y_l), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V_l | Y_l}| &= 1 - H(V_l | Y_l). \end{aligned} \quad (43)$$

By thinking of V_1 as a side information for V_2 , we can further define the sets $\mathcal{H}_{V_2 | V_1}$ and $\mathcal{L}_{V_2 | V_1}$, which satisfy

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V_2 | V_1}| &= H(V_2 | V_1), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V_2 | V_1}| &= 1 - H(V_2 | V_1). \end{aligned} \quad (44)$$

First, consider only the point-to-point communication problem between the transmitter and the first receiver. As discussed in Section III-B, for this scenario, the correct choice is to place the information in those positions of $U_1^{1:n}$ that are indexed by the set $\mathcal{I}^{(1)} = \mathcal{H}_{V_1} \cap \mathcal{L}_{V_1 | Y_1}$, which satisfies

$$\lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}^{(1)}| = I(V_1; Y_1). \quad (45)$$

For the point-to-point communication problem between the transmitter and the second receiver, we know from Section III-B that the information has to be placed in those positions of $U_2^{1:n}$ that are indexed by $\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2 | Y_2}$.

Let us get back to the broadcasting scenario and note that, unlike superposition coding, for binning the first user does not decode the message intended for the second user. Consider the following scheme. The first user adopts the point-to-point communication strategy: it ignores the existence of the second user, and it uses $\mathcal{I}^{(1)}$ as an information set. The frozen positions are divided into the two usual subsets $\mathcal{F}_d^{(1)} = \mathcal{H}_{V_1}^c$ and $\mathcal{F}_r^{(1)} = \mathcal{H}_{V_1} \cap \mathcal{L}_{V_1 | Y_1}^c$, which contain positions s.t., respectively, U_1^i can or cannot be approximately inferred from $U_1^{1:i-1}$. On the other hand, the second user does not ignore the existence of the first user by putting his information in $\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2 | Y_2}$. Indeed, V_1 and V_2 are, in general, correlated. Hence, the second user puts his information in $\mathcal{I}^{(2)} = \mathcal{H}_{V_2 | V_1} \cap \mathcal{L}_{V_2 | Y_2}$. If $i \in \mathcal{I}^{(2)}$ then, since $\mathcal{I}^{(2)} \subseteq \mathcal{H}_{V_2 | V_1}$, the bit U_2^i is approximately independent of $(U_2^{1:i-1}, V_1^{1:n})$. This implies that U_2^i is suitable to contain information. Furthermore, since $i \in \mathcal{L}_{V_2 | Y_2}$, the bit U_2^i is approximately a deterministic function of $(U_2^{1:i-1}, Y_2^{1:n})$. This implies that it is also decodable given the channel output $Y_2^{1:n}$. The remaining positions need to be frozen and can be divided into four subsets:

- For $i \in \mathcal{F}_r^{(2)} = \mathcal{H}_{V_2 | V_1} \cap \mathcal{L}_{V_2 | Y_2}^c$, U_2^i is chosen uniformly at random, and this randomness is shared between the transmitter and the second receiver.
- For $i \in \mathcal{F}_d^{(2)} = \mathcal{L}_{V_2}$, U_2^i is approximately a deterministic function of $U_2^{1:i-1}$ and, therefore, its value can be deduced from the past.
- For $i \in \mathcal{F}_{\text{out}}^{(2)} = \mathcal{H}_{V_2 | V_1}^c \cap \mathcal{L}_{V_2}^c \cap \mathcal{L}_{V_2 | Y_2}$, U_2^i is approximately a deterministic function of $(U_2^{1:i-1}, V_1^{1:n})$, but it can be deduced also from the channel output $Y_2^{1:n}$.
- For $i \in \mathcal{F}_{\text{cr}}^{(2)} = \mathcal{H}_{V_2 | V_1}^c \cap \mathcal{L}_{V_2}^c \cap \mathcal{L}_{V_2 | Y_2}^c = \mathcal{H}_{V_2 | V_1}^c \cap \mathcal{L}_{V_2 | Y_2}^c$, U_2^i is approximately a deterministic function of $(U_2^{1:i-1}, V_1^{1:n})$, but it cannot be deduced neither from $U_2^{1:i-1}$ nor from $Y_2^{1:n}$.

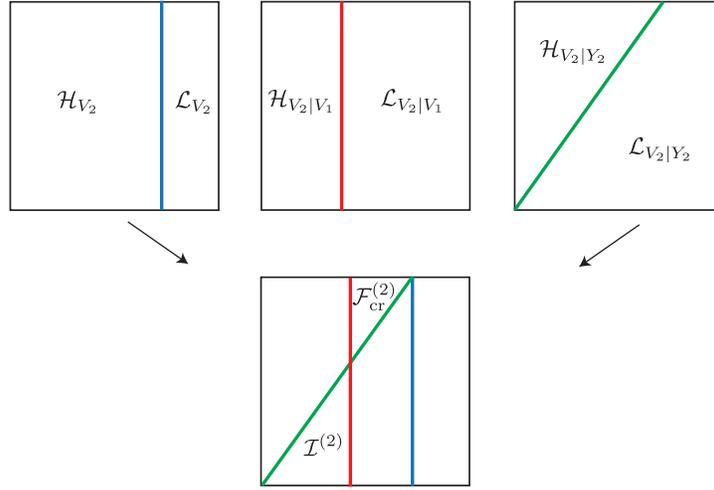


Figure 8. Graphical representation of the sets associated to the second user for the binning scheme: $\mathcal{I}^{(2)}$ contains the information bits; $\mathcal{F}_{\text{cr}}^{(2)}$ contains the frozen positions which are critical in the sense that they cannot be inferred neither from the past $U_2^{1:i-1}$ nor from the channel output $Y_2^{1:n}$.

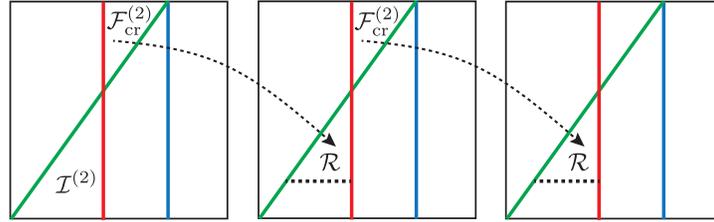


Figure 9. Graphical representation of the repetition construction for the binning scheme with $k = 3$: the set $\mathcal{F}_{\text{cr}}^{(2)}$ is repeated into the set \mathcal{R} of the following block.

The positions belonging to the last set are critical, since, in order to decode them, the receiver needs to know $V_1^{1:n}$. Indeed, recall that the encoding operation is performed jointly by the two users, while the first and the second decoder act separately and cannot exchange any information. The situation is schematically represented in Figure 8.

We start by reviewing the AGG scheme [15]. This scheme achieves the rate pair in (42), assuming that the degradedness relation $p_{Y_2|V_2} \succ p_{V_1|V_2}$ holds. Note that, under this assumption, we have $\mathcal{L}_{V_2|V_1} \subseteq \mathcal{L}_{V_2|Y_2}$. Therefore, $\mathcal{F}_{\text{cr}}^{(2)} \subseteq \mathcal{L}_{V_2|V_1}^c \cap \mathcal{H}_{V_2|V_1}^c$. Since $|\mathcal{L}_{V_2|V_1}^c \cap \mathcal{H}_{V_2|V_1}^c| = o(n)$, it is assumed in [15] that the bits indexed by $\mathcal{L}_{V_2|V_1}^c \cap \mathcal{H}_{V_2|V_1}^c$ are “genie-given” from the encoder to the second decoder. The price to be paid for the transmission of these extra bits is asymptotically negligible. Consequently, the first user places his information in $\mathcal{I}^{(1)}$, the second user places his information in $\mathcal{I}^{(2)}$, and the bits in the positions belonging to $\mathcal{L}_{V_2|V_1}^c \cap \mathcal{H}_{V_2|V_1}^c$ are pre-communicated to the second receiver.

Our goal is to achieve the rate pair (42) without the degradedness condition $p_{Y_2|V_2} \succ p_{V_1|V_2}$. As in the superposition coding scheme, the idea consists in transmitting k polar blocks and in repeating (“chaining”) some bits from one block to the following block. To do so, let \mathcal{R} be a subset of $\mathcal{I}^{(2)}$ s.t. $|\mathcal{R}| = |\mathcal{F}_{\text{cr}}^{(2)}|$. As usual, it does not matter what subset we pick. Since the second user cannot reconstruct the bits at the critical positions $\mathcal{F}_{\text{cr}}^{(2)}$, we use the set \mathcal{R} to store the critical bits of the previous block. This construction is schematically represented in Figure 9.

Let us explain the scheme with some detail. For block 1, we adopt the point-to-point communication strategy: the first user puts his information in $\mathcal{I}^{(1)}$, and the second user in $\mathcal{I}^{(2)}$. For block j ($j \in \{2, \dots, k-1\}$), the first user places again his information in $\mathcal{I}^{(1)}$. The second user puts information in the positions indexed by $\mathcal{I}^{(2)} \setminus \mathcal{R}$ and repeats in \mathcal{R} the bits which were contained in the set $\mathcal{F}_{\text{cr}}^{(2)}$ of block $j-1$. For block k , the second user does not change his strategy, putting information in $\mathcal{I}^{(2)} \setminus \mathcal{R}$ and repeating in \mathcal{R} the bits which were contained in the set $\mathcal{F}_{\text{cr}}^{(2)}$ of block $k-1$. On the other hand, in the last block, the first user does not convey any information and puts in $\mathcal{I}^{(1)}$ a fixed sequence which is shared between the encoder and both decoders. Indeed, for block k , the positions indexed

by $\mathcal{F}_{\text{cr}}^{(2)}$ are not repeated anywhere. Consequently, the only way in which the second decoder can reconstruct the bits in $\mathcal{F}_{\text{cr}}^{(2)}$ consists in knowing a priori the value of $V_1^{1:n}$.

Note that with this scheme, the second user has to decode “backwards”, starting with block k and ending with block 1. In fact, for block k , the second user can compute $V_1^{1:n}$ and, therefore, the critical positions indexed by $\mathcal{F}_{\text{cr}}^{(2)}$ are no longer a problem. Then, for block j ($j \in \{2, \dots, k-1\}$), the second user knows the values of the bits in $\mathcal{F}_{\text{cr}}^{(2)}$ from the decoding of the set \mathcal{R} of block $j+1$.

Suppose now that the second user wants to decode “forward”, i.e., starting with block 1 and ending with block k . Then, the set \mathcal{R} is used to store the critical bits of the following block (instead of those ones of the previous block). In particular, for block k , we adopt the point-to-point communication strategy. For block j ($j \in \{k-1, \dots, 2\}$), the first user places his information in $\mathcal{I}^{(1)}$, the second user places his information in the positions indexed by $\mathcal{I}^{(2)} \setminus \mathcal{R}$ and repeats in \mathcal{R} the bits which were contained in the set $\mathcal{F}_{\text{cr}}^{(2)}$ of block $j+1$. For block 1, the second user does not change his strategy, and the first user puts in $\mathcal{I}^{(1)}$ a shared fixed sequence. Note that in this case the encoding needs to be performed “backwards”.

Encoding. Let us start from the first user.

For block j ($j \in \{1, \dots, k-1\}$):

- The information bits are stored in $\{u_1^i\}_{i \in \mathcal{I}^{(1)}}$.
- The set $\{u_1^i\}_{i \in \mathcal{F}_r^{(1)}}$ is filled with a random sequence, which is shared between the transmitter and the first receiver.
- For $i \in \mathcal{F}_d^{(1)}$, we set $u_1^i = \arg \max_{u \in \{0,1\}} \mathbb{P}(U_1^i = u | U_1^{1:i-1} = u_1^{1:i-1})$.

For block k :

- The user conveys no information, and $\{u_1^i\}_{i \in \mathcal{I}^{(1)}}$ contains a fixed sequence known to the second decoder.
- The frozen bits are chosen according to the usual rules with the only difference that the sequence $\{u_1^i\}_{i \in \mathcal{F}_r^{(1)}}$ is shared also with the second decoder.

The rate of communication of the first user is given by (see (45))

$$R_1 = \left(\frac{k-1}{kn} \right) |\mathcal{I}^{(1)}| = \left(\frac{k-1}{k} \right) I(V_1; Y_1) + o(1), \quad (46)$$

where, by choosing a large value of k , the rate R_1 approaches $I(V_1; Y_1)$. Then, the vector $v_1^{1:n} = u_1^{1:n} G_n$ is obtained.

Let us now move to the second user.

For block 1:

- The information bits are stored in $\{u_2^i\}_{i \in \mathcal{I}^{(2)}}$.
- For $i \in \mathcal{F}_r^{(2)}$, u_2^i is chosen uniformly at random, and its value is supposed to be known to the second decoder.
- For $i \in \mathcal{F}_d^{(2)}$, u_2^i is set to $\arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}}(u | u_2^{1:i-1})$
- For $i \in \mathcal{F}_{\text{out}}^{(2)} \cup \mathcal{F}_{\text{cr}}^{(2)}$, u_2^i is set to $\arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, V_1^{1:n}}(u | u_2^{1:i-1}, v_1^{1:n})$.

Observe that the encoder has an access to $v_1^{1:n}$ and, therefore, it can compute the probabilities above.

For block j ($j \in \{2, \dots, k\}$):

- The information bits are placed into $\{u_2^i\}_{i \in \mathcal{I}^{(2)} \setminus \mathcal{R}}$.
- The set $\{u_2^i\}_{i \in \mathcal{R}}$ contains a copy of the set $\{u_2^i\}_{i \in \mathcal{F}_{\text{cr}}^{(2)}}$ of block $j-1$.
- The frozen bits are chosen as in block 1.

In order to compute the rate achievable by the second user, first observe that

$$\begin{aligned} \frac{1}{n} (|\mathcal{I}^{(2)}| - |\mathcal{R}|) &\stackrel{(a)}{=} \frac{1}{n} \left(|\mathcal{H}_{V_2|V_1} \cap \mathcal{L}_{V_2|Y_2}| - |\mathcal{H}_{V_2|V_1}^c \cap \mathcal{L}_{V_2}^c \cap \mathcal{L}_{V_2|Y_2}^c| \right) \\ &\stackrel{(b)}{=} \frac{1}{n} \left(|(\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2|Y_2}) \setminus (\mathcal{H}_{V_2} \cap \mathcal{H}_{V_2|V_1}^c)| - |(\mathcal{H}_{V_2} \cap \mathcal{H}_{V_2|V_1}^c) \setminus (\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2|Y_2})| \right) + o(1) \\ &\stackrel{(c)}{=} \frac{1}{n} \left(|\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2|Y_2}| - |\mathcal{H}_{V_2} \cap \mathcal{H}_{V_2|V_1}^c| \right) + o(1) \\ &\stackrel{(d)}{=} \frac{1}{n} \left(|\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2|Y_2}| - |\mathcal{H}_{V_2} \cap \mathcal{L}_{V_2|V_1}| \right) + o(1) \\ &\stackrel{(e)}{=} \frac{1}{n} \left(|\mathcal{L}_{V_2|Y_2} \setminus \mathcal{L}_{V_2}| - |\mathcal{L}_{V_2|V_1} \setminus \mathcal{L}_{V_2}| \right) + o(1) \\ &\stackrel{(f)}{=} I(V_2; Y_2) - I(V_1; V_2) + o(1), \end{aligned} \quad (47)$$

where equality (a) holds since $|\mathcal{R}| = |\mathcal{F}_{\text{cr}}^{(2)}|$, equality (b) follows from $\mathcal{H}_{V_2|V_1} \subseteq \mathcal{H}_{V_2}$ and $|[n] \setminus (\mathcal{H}_{V_2} \cup \mathcal{L}_{V_2})| = o(n)$, equality (c) follows from the identity in (32) for arbitrary finite sets, equality (d) holds since $|[n] \setminus (\mathcal{H}_{V_2|V_1} \cup \mathcal{L}_{V_2|V_1})| = o(n)$, equality (e) holds since $|[n] \setminus (\mathcal{H}_{V_2} \cup \mathcal{L}_{V_2})| = o(n)$, and equality (f) follows from the second and fourth equalities in (43), as well as from the second equality in (44). Consequently,

$$R_2 = \frac{1}{nk} |\mathcal{R}| + I(V_2; Y_2) - I(V_1; V_2) + o(1), \quad (48)$$

which, as k tends to infinity, approaches the required rate. Then, the vector $v_2^{1:n} = u_2^{1:n} G_n$ is obtained and, finally, the vector $x^{1:n} = \phi(v_1^{1:n}, v_2^{1:n})$ is transmitted over the channel. The encoding complexity per block is $\Theta(n \log n)$.

Decoding. Let us start from the first user, which reconstructs $u_1^{1:n}$ from the channel output $y_1^{1:n}$. For each block, the decision rule is given by

$$\hat{u}_1^i = \begin{cases} u_1^i, & \text{if } i \in \mathcal{F}_r^{(1)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_1^i | U_1^{1:i-1}}(u | u_1^{1:i-1}), & \text{if } i \in \mathcal{F}_d^{(1)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_1^i | U_1^{1:i-1}, Y_1^{1:n}}(u | u_1^{1:i-1}, y_1^{1:n}), & \text{if } i \in \mathcal{I}^{(1)} \end{cases}. \quad (49)$$

The second user reconstructs $u_2^{1:n}$ from the channel output $y_2^{1:n}$. As explained before, the decoding goes “backwards”, starting from block k and ending with block 1. For block k , the second decoder knows $v_1^{1:n}$. Hence, the decision rule is given by

$$\hat{u}_2^i = \begin{cases} u_2^i & \text{if } i \in \mathcal{F}_r^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}}(u | u_2^{1:i-1}), & \text{if } i \in \mathcal{F}_d^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, V_1^{1:n}}(u | u_2^{1:i-1}, v_1^{1:n}), & \text{if } i \in \mathcal{F}_{\text{out}}^{(2)} \cup \mathcal{F}_{\text{cr}}^{(2)} \\ \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, Y_2^{1:n}}(u | u_2^{1:i-1}, y_2^{1:n}), & \text{if } i \in \mathcal{I}^{(2)} \end{cases}. \quad (50)$$

For block j ($j \in \{2, \dots, k\}$), the decision rule is the same as (50) for $i \notin \mathcal{F}_{\text{out}}^{(2)} \cup \mathcal{F}_{\text{cr}}^{(2)}$. Indeed, $\{u_2^i\}_{i \in \mathcal{F}_{\text{cr}}^{(2)}}$ of block j can be deduced from $\{u_2^i\}_{i \in \mathcal{R}}$ of block $j+1$, and, for $i \in \mathcal{F}_{\text{out}}^{(2)}$, we set $\hat{u}_2^i = \arg \max_{u \in \{0,1\}} \mathbb{P}_{U_2^i | U_2^{1:i-1}, Y_2^{1:n}}(u | u_2^{1:i-1}, y_2^{1:n})$. The complexity per block, under successive cancellation decoding, is $\Theta(n \log n)$.

Performance. The block error probability $P_e^{(l)}$ for the l -th user ($l \in \{1, 2\}$) can be upper bounded by

$$\begin{aligned} P_e^{(1)} &\leq k \sum_{i \in \mathcal{I}^{(1)}} Z(U_1^i | U_1^{1:i-1}, Y_1^{1:n}) = O(2^{-n^\beta}), \\ P_e^{(2)} &\leq k \sum_{i \in \mathcal{L}_{V_2|Y_2}} Z(U_2^i | U_2^{1:i-1}, Y_2^{1:n}) = O(2^{-n^\beta}), \quad \forall \beta \in (0, 1/2). \end{aligned} \quad (51)$$

VI. POLAR CODES FOR MARTON'S REGION

A. Only Private Messages

Consider first the case where only private messages are available. The following theorem provides our main result regarding the achievability with polar codes of Marton's region, which forms the tightest inner bound known to date for a 2-user DM-BC without common information (compare with Theorem 3).

Theorem 8 (Polar Codes for Marton's Region): Consider a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel, taking values on an arbitrary set \mathcal{X} , and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let V, V_1 , and V_2 denote auxiliary binary random variables. Then, for any joint distribution p_{V, V_1, V_2} , for any deterministic function $\phi : \{0, 1\}^3 \rightarrow \mathcal{X}$ s.t. $X = \phi(V, V_1, V_2)$, and for any rate pair (R_1, R_2) satisfying the constraints (3), there exists a sequence of polar codes with an increasing block length n , which achieves this rate pair with encoding and decoding complexity $\Theta(n \log n)$ and a block error probability decaying like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

The proposed coding scheme is a combination of the techniques described in detail in Sections IV and V, and it is outlined below.

Problem Statement. Let $(V, V_1, V_2) \sim p_V p_{V_2|V} p_{V_1|V_2 V}$, and let X be a deterministic function of (V, V_1, V_2) , i.e., $X = \phi(V, V_1, V_2)$. Consider the 2-user DM-BC $p_{Y_1, Y_2|X}$ s.t. $I(V; Y_1) \leq I(V; Y_2)$. The aim is to achieve the rate pair

$$(R_1, R_2) = (I(V, V_1; Y_1) - I(V_1; V_2 | V) - I(V; Y_2), I(V, V_2; Y_2)). \quad (52)$$

Once we have accomplished this, we will see that a slight modification of this scheme allows us to achieve, in addition, the rate pair

$$(R_1, R_2) = (I(V, V_1; Y_1), I(V_2; Y_2 | V) - I(V_1; V_2 | V)). \quad (53)$$

Therefore, by Proposition 3, we can achieve the whole rate region in (3) by using polar codes. Note that if polar coding achieves the rate pairs (52) and (53) with complexity $\Theta(n \log n)$ and a block error probability $O(2^{-n^\beta})$, then for any other rate pair in the region (3), there exists a sequence of polar codes with an increasing block length n whose complexity and block error probability have the same asymptotic scalings.

Sketch of the Scheme. Set $U_0^{1:n} = V^{1:n} G_n$, $U_1^{1:n} = V_1^{1:n} G_n$, and $U_2^{1:n} = V_2^{1:n} G_n$. Then, the idea is that $U_1^{1:n}$ carries the message of the first user, while $U_0^{1:n}$ and $U_2^{1:n}$ carry the message of the second user. The second user will be able to decode only his message, namely, $U_0^{1:n}$ and $U_2^{1:n}$. On the other hand, the first user will decode both his message, namely, $U_1^{1:n}$, and a part of the message of the second user, namely, $U_0^{1:n}$. In a nutshell, the random variable V comes from the superposition coding scheme, because $U_0^{1:n}$ is decodable by both users, but carries information meant only for one of them. The random variables V_1 and V_2 come from the binning scheme, since the first user decodes $U_1^{1:n}$ and the second user decodes $U_2^{1:n}$, i.e., each user decodes only his own information.

Let the sets \mathcal{H}_V , \mathcal{L}_V , $\mathcal{H}_{V|Y_l}$, and $\mathcal{L}_{V|Y_l}$ for $l \in \{1, 2\}$ be defined as in (24), where these subsets of $[n]$ satisfy (25). In analogy to Sections IV and V let us also define the following sets ($l \in \{1, 2\}$):

$$\begin{aligned} \mathcal{H}_{V_l|V} &= \{i \in [n]: Z(U_l^i | U_l^{1:i-1}, U_0^{1:n}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{V_l|V} &= \{i \in [n]: Z(U_l^i | U_l^{1:i-1}, U_0^{1:n}) \leq \delta_n\}, \\ \mathcal{H}_{V_l|V, Y_l} &= \{i \in [n]: Z(U_l^i | U_l^{1:i-1}, U_0^{1:n}, Y_l^{1:n}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{V_l|V, Y_l} &= \{i \in [n]: Z(U_l^i | U_l^{1:i-1}, U_0^{1:n}, Y_l^{1:n}) \leq \delta_n\}, \\ \mathcal{H}_{V_1|V, V_2} &= \{i \in [n]: Z(U_1^i | U_1^{1:i-1}, U_0^{1:n}, U_2^{1:n}) \geq 1 - \delta_n\}, \\ \mathcal{L}_{V_1|V, V_2} &= \{i \in [n]: Z(U_1^i | U_1^{1:i-1}, U_0^{1:n}, U_2^{1:n}) \leq \delta_n\}, \end{aligned} \quad (54)$$

which satisfy

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V_l|V}| &= H(V_l | V), & \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V_l|V}| &= 1 - H(V_l | V), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V_l|V, Y_l}| &= H(V_l | V, Y_l), & \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V_l|V, Y_l}| &= 1 - H(V_l | V, Y_l), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{V_1|V, V_2}| &= H(V_1 | V, V_2), & \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{V_1|V, V_2}| &= 1 - H(V_1 | V, V_2). \end{aligned} \quad (55)$$

First, consider the subsets of positions of $U_0^{1:n}$. The set $\mathcal{I}_{\text{sup}}^{(2)} = \mathcal{H}_V \cap \mathcal{L}_{V|Y_2}$ contains the positions which are decodable by the second user, and the set $\mathcal{I}_v^{(1)} = \mathcal{H}_V \cap \mathcal{L}_{V|Y_1}$ contains the positions which are decodable by the first user. Recall that $U_0^{1:n}$ needs to be decoded by both users, but contains information only for the second user.

Second, consider the subsets of positions of $U_2^{1:n}$. The set $\mathcal{I}_{\text{bin}}^{(2)} = \mathcal{H}_{V_2|V} \cap \mathcal{L}_{V_2|V, Y_2}$ contains the positions which are decodable by the second user. Recall that $U_2^{1:n}$ needs to be decoded only by the second user, and it contains part of his message.

Third, consider the subsets of positions of $U_1^{1:n}$. The set $\mathcal{I}^{(1)} = \mathcal{H}_{V_1|V} \cap \mathcal{L}_{V|Y_2}$ contains the positions which are decodable by the first user. Recall that $U_1^{1:n}$ needs to be decoded by the first user, and it contains only his message. However, the first user cannot decode $U_2^{1:n}$ and, therefore, this user cannot infer $V_2^{1:n}$. Consequently, the positions in the set $\mathcal{F}_{\text{cr}}^{(1)} = \mathcal{H}_{V_1|V, V_2}^c \cap \mathcal{L}_{V_1|V}^c \cap \mathcal{L}_{V_1|V, Y_1}^c$ are critical. Indeed, for $i \in \mathcal{F}_{\text{cr}}^{(1)}$, the bit U_1^i is approximately a deterministic function of $(U_1^{1:i-1}, U_0^{1:n}, U_2^{1:n})$, but it cannot be deduced from $(U_1^{1:i-1}, U_0^{1:n}, Y_1^{1:n})$.

In order to achieve the rate pair (52), k polar blocks are transmitted, and three different ‘‘chaining’’ constructions are used. The first and the second chaining come from superposition coding, and the last one comes from binning.

First, define $\mathcal{D}^{(2)} = \mathcal{I}_{\text{sup}}^{(2)} \setminus \mathcal{I}_v^{(1)}$ and $\mathcal{D}^{(1)} = \mathcal{I}_v^{(1)} \setminus \mathcal{I}_{\text{sup}}^{(2)}$, as in (30) and (31), respectively. The former set contains the positions of $U_0^{1:n}$ which are decodable by the second user but not by the first, while the latter contains the positions

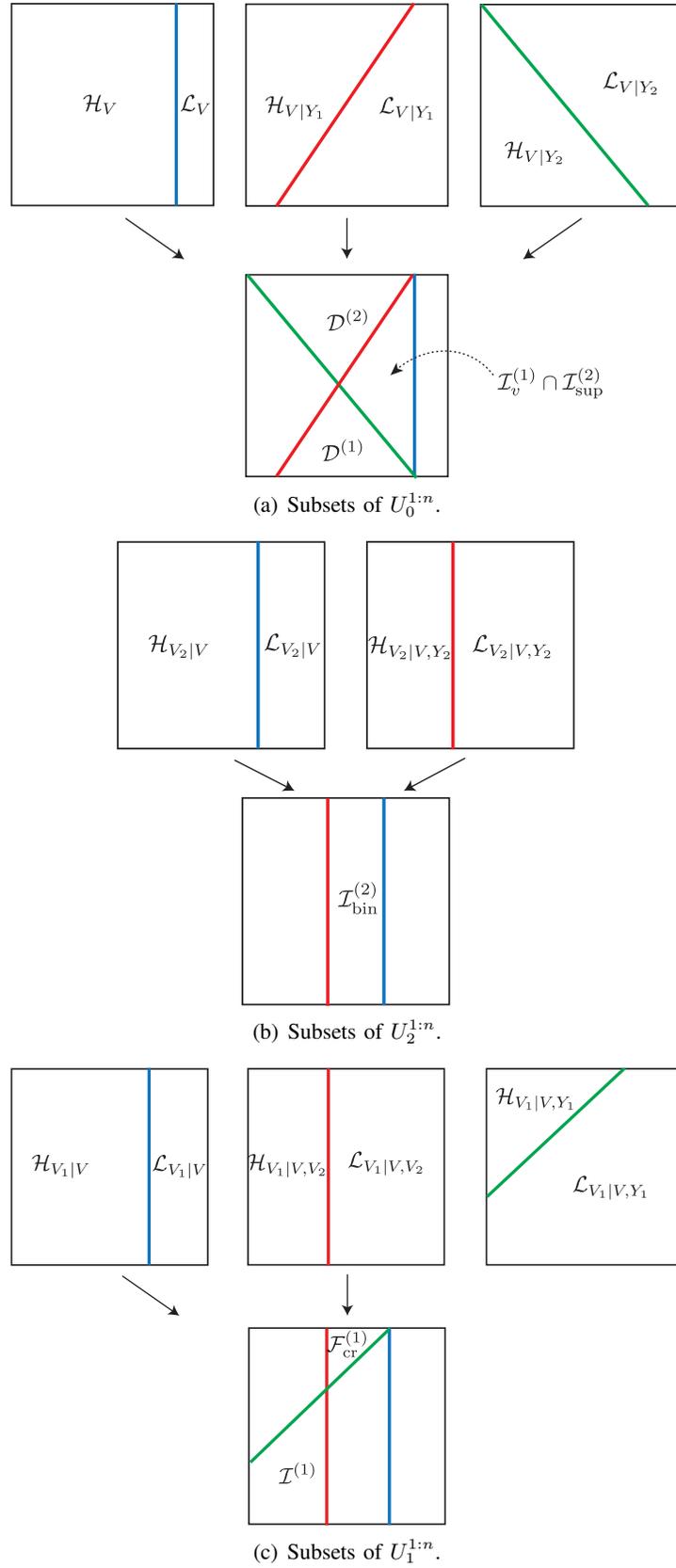


Figure 10. Graphical representation of the sets associated to the three auxiliary random variables in the scheme which achieves Marton's region with only private messages (3).

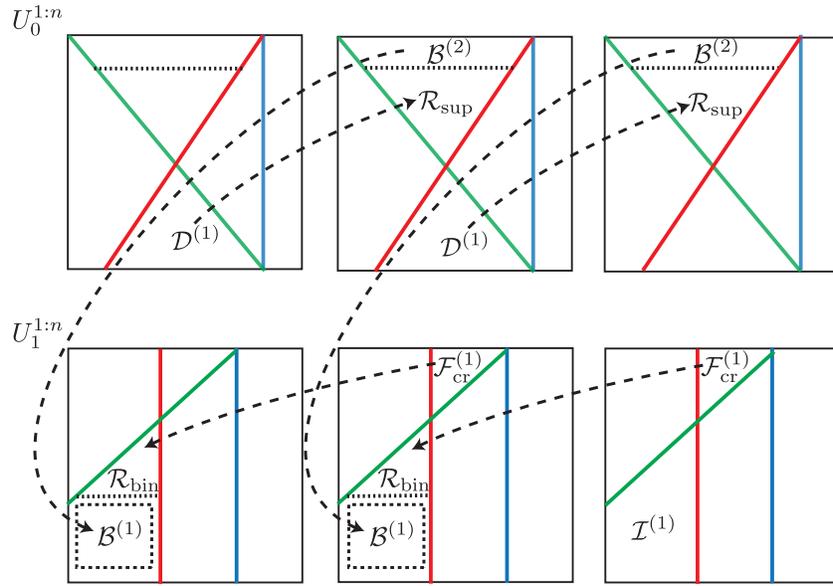


Figure 11. Graphical representation of the repetition constructions for Marton's region with $k = 3$: the set $\mathcal{D}^{(1)}$ is repeated into the set \mathcal{R}_{sup} of the following block; the set $\mathcal{B}^{(2)}$ is repeated into the set $\mathcal{B}^{(1)}$ of the previous block; the set $\mathcal{F}_{\text{cr}}^{(1)}$ is repeated into the set \mathcal{R}_{bin} of the previous block.

of $U_0^{1:n}$ which are decodable by the first user but not by the second. Let \mathcal{R}_{sup} be a subset of $\mathcal{D}^{(2)}$ s.t. $|\mathcal{R}_{\text{sup}}| = |\mathcal{D}^{(1)}|$. In block 1, fill $\mathcal{D}^{(1)}$ with information for the second user, and set the bits indexed by $\mathcal{D}^{(2)}$ to a fixed known sequence. In block j ($j \in \{2, \dots, k-1\}$), fill $\mathcal{D}^{(1)}$ again with information for the second user, and repeat the bits which were contained in the set $\mathcal{D}^{(1)}$ of block $j-1$ into the positions indexed by \mathcal{R}_{sup} of block j . In the final block k , put a known sequence in the positions indexed by $\mathcal{D}^{(1)}$, and repeat in the positions indexed by \mathcal{R}_{sup} the bits which were contained in the set $\mathcal{D}^{(1)}$ of block $k-1$. In all the blocks, fill $\mathcal{I}_v^{(1)} \cap \mathcal{I}_{\text{sup}}^{(2)}$ with information for the second user. In this way, both users will be able to decode a fraction of the bits of $U_0^{1:n}$ that is roughly equal to $I(V; Y_1)$. The bits in these positions contain information for the second user.

Second, define $\mathcal{B}^{(2)} = \mathcal{D}^{(2)} \setminus \mathcal{R}_{\text{sup}}$, and let $\mathcal{B}^{(1)}$ be a subset of $\mathcal{I}^{(1)}$ s.t. $|\mathcal{B}^{(1)}| = |\mathcal{B}^{(2)}|$. Note that $\mathcal{B}^{(2)}$ contains positions of $U_0^{1:n}$, and $\mathcal{B}^{(1)}$ contains positions of $U_1^{1:n}$. For block j ($j \in \{2, \dots, k\}$), we fill $\mathcal{B}^{(2)}$ with information for the second user, and we repeat these bits into the positions indexed by $\mathcal{B}^{(1)}$ of block $j-1$. In this way, both users will be able to decode a fraction of the bits of $U_0^{1:n}$ that is roughly equal to $I(V; Y_2)$ (recall that $I(V; Y_1) \leq I(V; Y_2)$). Again, the bits in these positions contain information for the second user.

Third, let \mathcal{R}_{bin} be a subset of $\mathcal{I}^{(1)}$ s.t. $|\mathcal{R}_{\text{bin}}| = |\mathcal{F}_{\text{cr}}^{(1)}|$. Since the first user cannot reconstruct the bits at the critical positions $\mathcal{F}_{\text{cr}}^{(1)}$, we use the set \mathcal{R}_{bin} to store the critical bits of the following block. For block k , the first user places all his information in $\mathcal{I}^{(1)}$. For block j ($j \in \{1, \dots, k-1\}$), the first user places all his information in $\mathcal{I}^{(1)} \setminus (\mathcal{R}_{\text{bin}} \cup \mathcal{B}^{(1)})$, repeats in \mathcal{R}_{bin} the bits in $\mathcal{F}_{\text{cr}}^{(1)}$ for block $j+1$, and repeats in $\mathcal{B}^{(1)}$ the bits in $\mathcal{B}^{(2)}$ for block $j+1$. The second user puts part of his information in $\mathcal{I}_{\text{bin}}^{(2)}$ (which is a subset of the positions of $U_2^{1:n}$) for all the blocks except for the first, in which $\mathcal{I}_{\text{bin}}^{(2)}$ contains a fixed sequence which is shared between the encoder and both decoders. Indeed, for block 1, the positions indexed by $\mathcal{F}_{\text{cr}}^{(1)}$ are not repeated anywhere, and the only way in which the second decoder can reconstruct those bits consists in knowing a-priori the value of $V_2^{1:n}$. The situation is schematically represented in Figures 10 and 11.

The encoding of $U_0^{1:n}$ is performed "forward", i.e., from block 1 to block k ; the encoding of $U_1^{1:n}$ is performed "backwards", i.e., from block k to block 1; the encoding of $U_2^{1:n}$ can be performed in any order. The first user decodes $U_0^{1:n}$ and $U_1^{1:n}$ "forward"; the second user decodes $U_0^{1:n}$ "backwards" and can decode $U_2^{1:n}$ in any order.

With this polar coding scheme, by letting k tend to infinity, the first user decodes a fraction of the positions of $U_1^{1:n}$ containing his own message, which is given by

$$\begin{aligned} R_1 &= \frac{1}{n}(|\mathcal{I}^{(1)}| - |\mathcal{B}^{(1)}| - |\mathcal{R}_{\text{bin}}|) = I(V_1; Y_1 | V) - I(V_1; V_2 | V) - (I(V; Y_2) - I(V; Y_1)) \\ &= I(V, V_1; Y_1) - I(V_1; V_2 | V) - I(V; Y_2). \end{aligned} \quad (56)$$

The information for the second user is spread between the positions of $U_0^{1:n}$ and the positions of $U_2^{1:n}$ for a total rate, which, as k tends to infinity, is given by

$$R_2 = \frac{1}{n}(|\mathcal{I}_{\text{sup}}^{(2)}| + |\mathcal{I}_{\text{bin}}^{(2)}|) = I(V; Y_2) + I(V_2; Y_2 | V) = I(V, V_2; Y_2). \quad (57)$$

It is possible to achieve the rate pair (53) with a scheme similar to the one described above by swapping the roles of the two users. Since $I(V; Y_1) \leq I(V; Y_2)$, only the first and the third chaining constructions are required. Indeed, the set which has the role of $\mathcal{B}^{(2)}$ is empty in this scenario.

As our schemes consist in the repetition of polar blocks, the encoding and decoding complexity per block is $\Theta(n \log n)$, and the block error probability decays like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

B. Private and Common Messages: MGP Region

Finally, consider the case of a 2-user DM-BC with both common and private messages. Our most general result consists in the construction of polar codes which achieve the MGP region (4).

Theorem 9 (Polar Codes for MGP Region): Consider a 2-user DM-BC $p_{Y_1, Y_2 | X}$, where X denotes the input to the channel, taking values on an arbitrary set \mathcal{X} , and Y_1, Y_2 denote the outputs at the first and second receiver, respectively. Let R_0, R_1 , and R_2 designate the rates of the common message and the two private messages of the two users, respectively. Let V, V_1 , and V_2 denote auxiliary binary random variables. Then, for any joint distribution p_{V, V_1, V_2} , for any deterministic function $\phi: \{0, 1\}^3 \rightarrow \mathcal{X}$ s.t. $X = \phi(V, V_1, V_2)$, and for any rate triple (R_0, R_1, R_2) satisfying the constraints (4), there exists a sequence of polar codes with an increasing block length n which achieves this rate triple with encoding and decoding complexity $\Theta(n \log n)$ and a block error probability decaying like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$.

The polar coding scheme follows the ideas outlined in Section VI-A. Recall that $U_0^{1:n}$ is decoded by both users. Then, we put the common information in the positions of $U_0^{1:n}$ which previously contained private information meant only for one of the users. The common rate is clearly upper bounded by $\min\{I(V; Y_1), I(V; Y_2)\}$. The remaining four inequalities of (4) are equivalent to the conditions in (3) with the only difference that a portion R_0 of the private information for one of the users has been converted into common information. This suffices to achieve the required rate region.

VII. CONCLUSIONS

Extending the work by Goela, Abbe, and Gastpar [15], we have shown how to construct polar codes for the 2-user discrete memoryless broadcast channel (DM-BC) that achieve the superposition and binning regions. By combining these two strategies, we achieve any rate pair inside Marton's region with both common and private messages. This rate region is tight for all classes of broadcast channels with known capacity regions and it is also known as the Marton-Gelfand-Pinsker (MGP) region. The described coding techniques possess the usual advantages of polar codes, i.e., encoding and decoding complexity of $\Theta(n \log n)$ and block error probability decaying like $O(2^{-n^\beta})$ for any $\beta \in (0, 1/2)$, and they can be easily extended to obtain inner bounds for the K -user DM-BC in a low-complexity fashion.

We conclude by remarking that the chaining constructions used to align the polarized indices do not rely on the specific structure of the broadcast channel. Indeed, similar techniques have been considered, independently of this work, in the context of interference networks [17] and, in general, we believe that they can be adapted to the design of polar coding schemes for a variety of multi-user scenarios.

ACKNOWLEDGMENT

We wish to thank the Associate Editor, Henry Pfister, for efficiently handling our manuscript. The work of M. Mondelli, S. H. Hassani and R. Urbanke was supported by grant No. 200020_146832/1 of the Swiss National Science Foundation. The work of I. Sason was supported by the Israeli Science Foundation (ISF), grant number 12/12.

REFERENCES

- [1] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.
- [2] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. of the IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 1493–1495.
- [3] S. H. Hassani, R. Mori, T. Tanaka, and R. Urbanke, "Rate-dependent analysis of the asymptotic behavior of channel polarization," *IEEE Trans. on Information Theory*, vol. 59, no. 4, pp. 2267–2276, April 2013.
- [4] E. Arıkan, "Source polarization," in *Proc. of the IEEE International Symposium on Information Theory*, Austin, Texas, June 2010, pp. 899–903.
- [5] S. B. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. on Information Theory*, vol. 56, no. 4, pp. 1751–1768, April 2010.
- [6] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, EPFL, Lausanne, Switzerland, July 2009.
- [7] E. Arıkan, "Polar coding for the Slepian-Wolf problem based on monotone chain rules," in *Proc. of the IEEE International Symposium on Information Theory*, MIT, Cambridge, USA, July 2012, pp. 571–575.
- [8] E. Abbe and I. E. Telatar, "Polar codes for the m -user multiple access channel," *IEEE Trans. on Information Theory*, vol. 58, no. 8, pp. 5437–5448, August 2012.
- [9] I. Tal, A. Sharov, and A. Vardy, "Constructing polar codes for non-binary alphabets and MACs," in *Proc. of the IEEE International Symposium on Information Theory*, Cambridge, MA, July 2012, pp. 2142–2146.
- [10] E. Şaşıođlu, I. E. Telatar, and E. Yeh, "Polar codes for the two-user binary-input multiple-access channel," in *Proc. of the IEEE Information Theory Workshop*, Cairo, Egypt, January 2010, pp. 1–5.
- [11] H. Mahdaviifar, M. El-Khamy, J. Lee, and I. Kang, "Achieving the uniform rate region of multiple access channels using polar codes," July 2013, [Online]. Available: <http://arxiv.org/pdf/1307.2889v1.pdf>.
- [12] R. Nasser and E. Telatar, "Polar codes for arbitrary DMCs and arbitrary MACs," November 2013, <http://arxiv.org/pdf/1311.3123v1.pdf>.
- [13] N. Goela, E. Abbe, and M. Gastpar, "Polar codes for the deterministic broadcast channel," in *Proc. of the International Zurich Seminar on Communications*, February 2012, pp. 51–54.
- [14] —, "Polar codes for broadcast channels," in *Proc. of the IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 1127–1131.
- [15] —, "Polar codes for broadcast channels," January 2013, [Online]. Available: <http://arxiv.org/pdf/1301.6150v1.pdf>.
- [16] K. Appaiah, O. Koyluoglu, and S. Vishwanath, "Polar alignment for interference networks," in *Proc. of the Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, September 2011, pp. 240–246.
- [17] L. Wang and E. Şaşıođlu, "Polar coding for interference networks," in *Proc. of the IEEE International Symposium on Information Theory*, Honolulu, Hawaii, USA, July 2014, pp. 311–315.
- [18] M. Karzand, "Polar codes for degraded relay channels," in *Proc. Intern. Zurich Seminar on Comm.*, February 2012, pp. 59–62.
- [19] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 8, pp. 752–754, August 2010.
- [20] H. Mahdaviifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. on Information Theory*, vol. 57, no. 10, pp. 6428–6443, October 2011.
- [21] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. on Information Forensics Security*, vol. 7, no. 5, pp. 1472–1483, October 2012.
- [22] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. of the IEEE Information Theory Workshop*, Dublin, Ireland, September 2010, pp. 1–5.
- [23] E. Şaşıođlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. of the IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 1117–1121.
- [24] M. Andersson, R. Schaefer, T. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1901–1908, September 2013.
- [25] D. Burshtein and A. Struatski, "Polar write once memory codes," *IEEE Trans. on Information Theory*, vol. 59, no. 8, pp. 5088–5101, August 2013.
- [26] E. Hof, I. Sason, S. Shamai, and C. Tian, "Capacity-achieving polar codes for arbitrarily-permuted parallel channels," *IEEE Trans. on Information Theory*, vol. 59, no. 3, pp. 1505–1516, March 2013.
- [27] A. G. Sahebi and S. S. Pradhan, "Polar codes for multi-terminal communications," in *Proc. of the IEEE International Symposium on Information Theory*, Honolulu, Hawaii, USA, July 2014, pp. 316–320.
- [28] P. P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. on Information Theory*, vol. 19, no. 2, pp. 197–207, March 1973.
- [29] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. on Information Theory*, vol. 25, no. 3, pp. 306–311, May 1979.
- [30] T. M. Cover, "Broadcast channels," *IEEE Trans. on Information Theory*, vol. 18, no. 1, pp. 2–14, Jan. 1972.
- [31] L. Wang, E. Şaşıođlu, B. Bandemer, and Y.-H. Kim, "A comparison of superposition coding schemes," in *Proc. of the IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 2970 – 2974.

- [32] S. I. Gelfand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Peredachi Inf.*, vol. 16, no. 1, pp. 24–34, 1980.
- [33] Y. Liang, "Multiuser communications with relaying and user cooperation," Ph.D. dissertation, University of Illinois, Urbana-Champaign, Illinois, USA, 2005.
- [34] Y. Liang and G. Kramer, "Rate regions for relay broadcast channels," *IEEE Trans. on Information Theory*, vol. 53, no. 10, pp. 3517–3535, October 2007.
- [35] Y. Liang, G. Kramer, and H. V. Poor, "On the equivalence of two achievable regions for the broadcast channel," *IEEE Trans. on Information Theory*, vol. 57, no. 1, pp. 95 – 100, January 2011.
- [36] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.
- [37] G. Kramer, "Topics in multi-user information theory," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 4-5, pp. 265–444, April 2007.
- [38] Y. Geng, A. Gohari, C. Nair, and Y. Yu, "On Marton's inner bound and its optimality for classes of product broadcast channels," *IEEE Trans. on Information Theory*, vol. 60, no. 1, pp. 22–41, January 2014.
- [39] S. H. Hassani, S. B. Korada, and R. Urbanke, "The compound capacity of polar codes," in *47th Annual Allerton Conference on Communication, Control, and Computing*, October 2009, pp. 16 – 21.
- [40] S. H. Hassani and R. Urbanke, "Universal polar codes," Dec. 2013, [Online]. Available: <http://arxiv.org/pdf/1307.7223v2.pdf>.
- [41] E. Şaşıoğlu and L. Wang, "Universal polarization," in *Proc. of the IEEE International Symposium on Information Theory*, Honolulu, Hawaii, USA, July 2014, pp. 1456–1460.
- [42] E. Şaşıoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," in *Proc. of the IEEE Information Theory Workshop*, Taormina, Sicily, October 2009, pp. 144–148.
- [43] R. Mori and T. Tanaka, "Channel polarization on q -ary discrete memoryless channels by arbitrary kernel," in *Proc. of the IEEE International Symposium on Information Theory*, Austin, Texas, June 2010, pp. 894–898.
- [44] W. Park and A. Barg, "Polar codes for q -ary channels, $q = 2^r$," *IEEE Trans. on Information Theory*, vol. 59, no. 2, pp. 955–969, February 2013.
- [45] A. G. Sahebi and S. S. Pradhan, "Multilevel channel polarization for arbitrary discrete memoryless channels," *IEEE Trans. on Information Theory*, vol. 59, no. 12, pp. 7839–7857, December 2013.
- [46] A. A. Gohari and V. Anantharam, "Evaluation of Marton's inner bound for the general broadcast channel," *IEEE Trans. on Information Theory*, vol. 58, no. 2, pp. 608–619, February 2012.
- [47] Y. Geng, V. Jog, C. Nair, and Z. V. Wang, "An information inequality and evaluation of Marton's inner bound for binary-input broadcast channels," *IEEE Trans. on Information Theory*, vol. 59, no. 7, pp. 4095–4105, July 2013.
- [48] A. Gohari, C. Nair, and V. Anantharam, "Improved cardinality bounds on the auxiliary random variables in Marton's inner bound," in *Proc. of the IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 1272–1276.
- [49] Y. Geng, A. Gohari, C. Nair, and Y. Yu, "On Marton's inner bound and its optimality for classes of product broadcast channels," *IEEE Trans. on Information Theory*, vol. 60, no. 1, pp. 22–41, January 2014.
- [50] Y. Geng and C. Nair, "The capacity region of the two-receiver Gaussian vector broadcast channel with private and common messages," *IEEE Trans. on Information Theory*, vol. 60, no. 4, pp. 2087–2104, April 2014.
- [51] M. Salehi, "Cardinality bounds on auxiliary variables in multiple-user theory via the method of Ahlswede and Korner," Stanford University, Tech. Rep. 33, 1978.
- [52] Y. Geng, C. Nair, S. Shamai, and Z. V. Wang, "On broadcast channels with binary inputs and symmetric outputs," *IEEE Trans. on Information Theory*, vol. 59, no. 11, pp. 6980–6989, November 2013.
- [53] N. Hussami, S. B. Korada, and R. Urbanke, "Performance of polar codes for channel and source coding," in *Proc. of the IEEE International Symposium on Information Theory*, July 2009, pp. 1488–1492.
- [54] E. E. Majani and H. Rumsey, "Two results on binary-input discrete memoryless channels," in *Proc. of the IEEE International Symposium on Information Theory*, Budapest, Hungary, June 1991, p. 104.
- [55] N. Shulman and M. Feder, "The uniform distribution as a uniform prior," *IEEE Trans. on Information Theory*, vol. 50, no. 6, pp. 1356 – 1362, Jun. 2004.
- [56] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
- [57] D. Sutter, J. M. Renes, F. Dupuis, and R. Renner, "Achieving the capacity of any DMC using only polar codes," in *Proc. of the IEEE Information Theory Workshop*, Lausanne, Switzerland, September 2012, pp. 114–118.
- [58] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric models," *IEEE Trans. on Information Theory*, vol. 59, no. 12, pp. 7829–7838, December 2013.