

# Partially-Robust Communications over a Noisy Channel

Tibor Keresztfalvi and Amos Lapidoth,  
Signal and Information Processing Laboratory  
ETH Zurich  
Email: {keresztfalvi, lapidoth}@isi.ee.ethz.ch

**Abstract**—To study the fundamental limits on the joint transmission of data of different levels of sensitivity, we establish the deterministic-code capacity region of a network with one transmitter and two receivers: an “ordinary receiver” and a “robust receiver.” The channel to the ordinary receiver is a given (known) discrete memoryless channel, whereas the channel to the robust receiver is an arbitrarily varying channel. Both receivers are required to decode the “common message” (the more sensitive data), whereas only the ordinary receiver is required to decode the “private message” (the less sensitive data).

## I. INTRODUCTION

Data of two levels of sensitivity are to be jointly transmitted over a noisy channel. Only the sensitive data must be transmitted robustly with respect to the channel law; the less sensitive data need only be decodable when the channel has some nominal law. We model this scenario using the broadcast channel of Figure 1, where the channel from the transmitter to one receiver—the “robust receiver”—is an arbitrarily varying channel (AVC) [1], [2] and to the other receiver—the “ordinary receiver”—has some nominal law  $W(y|x)$ . Both receivers must decode the rate- $R_c$  common message (the sensitive data), and only the ordinary receiver must recover the rate- $R_p$  private message (the less sensitive data). The set of rate pairs  $(R_c, R_p)$  that can be communicated reliably under these requirements is the *capacity region*, which we derive here.

The scenario where one receiver must recover both streams and the other only one, falls under the heading of *degraded message sets*. The capacity region of the broadcast channel with degraded message sets was established by Körner and Marton in [3]. But their model differs from ours because their broadcast channel is fixed and given: there is nothing “varying” about it. The general arbitrarily varying broadcast channel with degraded message sets was studied by Hof and Bross in [4].

Our network can be viewed as an arbitrarily varying broadcast channel (AVBC) of a special kind: one where the channel to one of the receivers is degenerate in the sense of being given and not depending on the state. General AVBCs were studied by Jahn [5] who derived an inner bound on their capacity regions, and our achievability result essentially follows from his. Our converse shows that in our setting the inner bound is tight. More recent results on the AVBC for settings with causal and noncausal side information were obtained by Pereg and Steinberg [6]–[8], see [9] for other related work.

## II. THE MAIN RESULT

A discrete memoryless *state-dependent broadcast channel*  $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{S}, W_{Y,Z|X,S})$  consists of a finite input alphabet  $\mathcal{X}$ , finite output alphabets  $\mathcal{Y}$  and  $\mathcal{Z}$ , a (not necessarily finite) state set  $\mathcal{S}$ , and a collection of transition probability matrices  $W_{Y,Z|X,S}$ . A *semi-AVBC* (SAVBC) is a state-dependent broadcast channel where the conditional law of the output  $Y$  given the input  $x$  and the state  $s$  does not depend on the state. For such a channel, we denote the marginal conditional distributions of the outputs  $Y$  and  $Z$  given the input  $x$  and the state  $s$  by  $W(y|x)$  and  $V_s(z|x)$  respectively:

$$W(y|x) = W_{Y|X,S}(y|x, s), \quad (1a)$$

$$V_s(z|x) = W_{Z|X,S}(z|x, s). \quad (1b)$$

Given a blocklength  $n$ , an input sequence  $\mathbf{x} \in \mathcal{X}^n$ , and a state sequence  $\mathbf{s} \in \mathcal{S}^n$ ,

$$W_{Y^n, Z^n | X^n, S^n}(\mathbf{y}, \mathbf{z} | \mathbf{x}, \mathbf{s}) = \prod_{i=1}^n W_{Y,Z|X,S}(y_i, z_i | x_i, s_i), \quad (2)$$

where  $(\mathbf{y}, \mathbf{z}) \in \mathcal{Y}^n \times \mathcal{Z}^n$ .

We consider the transmission from *degraded message sets*: the encoder sends a *common message*  $m_c$  to both receivers and a *private message*  $m_p$  to the receiver observing  $Y$ . The receiver observing  $Z$  is thus only required to decode the common message.

Given a blocklength  $n$ , a *deterministic code*  $\mathcal{C}$  for the SAVBC consists of a common message set  $\mathcal{M}_c$  with  $2^{nR_c}$  messages, a private message set  $\mathcal{M}_p$  with  $2^{nR_p}$  messages, an encoder mapping

$$f: \mathcal{M}_c \times \mathcal{M}_p \rightarrow \mathcal{X}^n, \quad (3)$$

and decoding mappings

$$\phi_y: \mathcal{Y}^n \rightarrow \mathcal{M}_c \times \mathcal{M}_p \quad (4a)$$

$$\phi_z: \mathcal{Z}^n \rightarrow \mathcal{M}_c. \quad (4b)$$

The message-averaged probability of error of a code  $\mathcal{C}$  given a state sequence  $\mathbf{s} \in \mathcal{S}^n$  is

$$P_{e|\mathbf{s}}^{(n)}(\mathcal{C}) = \frac{1}{|\mathcal{M}_c||\mathcal{M}_p|} \sum_{(m_c, m_p) \in \mathcal{M}_c \times \mathcal{M}_p} \sum_{(\mathbf{y}, \mathbf{z}) \notin \mathcal{D}(m_c, m_p)} W_{Y^n, Z^n | X^n, S^n}(\mathbf{y}, \mathbf{z} | \mathbf{x}, \mathbf{s}), \quad (5)$$

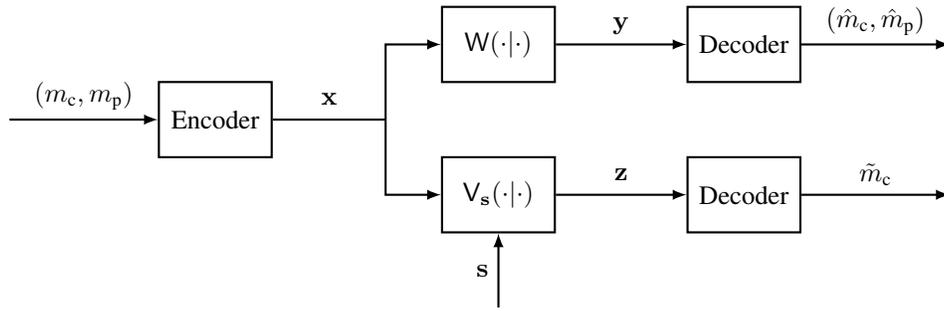


Fig. 1. The semi-arbitrarily-varying broadcast channel (semi-AVBC) with common message  $m_c$ , private message  $m_p$ , and state sequence  $\mathbf{s} \in \mathcal{S}^n$ .

where

$$\mathcal{D}(m_c, m_p) = \{(\mathbf{y}, \mathbf{z}) \in \mathcal{Y}^n \times \mathcal{Z}^n : \phi_y(\mathbf{y}) = (m_c, m_p), \phi_z(\mathbf{z}) = m_c\}. \quad (6)$$

We say that the rate pair  $(R_c, R_p)$  is *achievable with deterministic codes*, if there exists a sequence of codes  $\{\mathcal{C}_n\}$  with rates  $(R_c, R_p)$  such that

$$\lim_{n \rightarrow \infty} \sup_{\mathbf{s} \in \mathcal{S}^n} P_{e|\mathbf{s}}^{(n)}(\mathcal{C}_n) = 0. \quad (7)$$

The *deterministic-code capacity*  $\mathcal{C}_{\text{det}}$  (under the average-probability-of-error criterion) is the closure of the set of rate pairs that are achievable with deterministic codes.

As in [10, Corollary 12.3], it can be shown that the capacity region depends on the states only via the convex-closure of the channels they induce. We shall thus make the following assumption without any loss of generality:

**Assumption:** We assume throughout that  $\{V_s(z|x)\}_{s \in \mathcal{S}}$  is compact<sup>1</sup> and convex in the sense that for every  $0 < \lambda < 1$  and  $s_1, s_2 \in \mathcal{S}$ , there exists a state  $\bar{s} \in \mathcal{S}$  such that

$$V_{\bar{s}}(z|x) = \lambda V_{s_1}(z|x) + (1 - \lambda) V_{s_2}(z|x), \quad (8)$$

for all  $(x, z) \in \mathcal{X} \times \mathcal{Z}$ .

Following [5, Remark IIB2] or using a time-sharing argument we note:

**Remark 1.** *The interior of  $\mathcal{C}_{\text{det}}$  is nonempty if, and only if, the capacity of the channel  $W(y|x)$  to  $Y$  and the capacity (under the average-probability-of-error criterion) of the AVC to  $Z$  are both positive. The latter is positive if, and only if, the AVC is nonsymmetrizable [11], [12].*

We next define the region  $\mathcal{C}_{\text{det}}^{(I)}$  that will turn out to equal the capacity region when the latter is nonempty. It is defined as the closure of the union over all PMFs  $p_{U,X}$  of the set of rate pairs  $(R_c, R_p)$  that satisfy

$$R_c \leq \min_{s \in \mathcal{S}} I(U; Z) \quad (9a)$$

$$R_p \leq I(X; Y|U) \quad (9b)$$

$$R_c + R_p \leq I(X; Y), \quad (9c)$$

<sup>1</sup>If the set  $\{V_s(z|x)\}_{s \in \mathcal{S}}$  is not compact our result still holds, but with infima replacing the minima in the characterizations of the capacity region.

where the mutual informations are computed w.r.t. the joint distribution

$$p_{U,X}(u, x) W(y|x) V_s(z|x), \quad (10)$$

and where  $U$  is an auxiliary chance variable taking values in a finite set  $\mathcal{U}$ . Our main result is the following theorem.

**Theorem 2.** *Under the above assumption, if the interior of the deterministic-code capacity  $\mathcal{C}_{\text{det}}$  of a SAVBC is nonempty, then it equals  $\mathcal{C}_{\text{det}}^{(I)}$ :*

$$\left(\text{interior}(\mathcal{C}_{\text{det}}) \neq \emptyset\right) \implies \left(\mathcal{C}_{\text{det}} = \mathcal{C}_{\text{det}}^{(I)}\right). \quad (11)$$

### III. PROOF OUTLINE OF THE MAIN RESULT

The achievability result—that  $\mathcal{C}_{\text{det}} \neq \emptyset$  implies that every rate pair  $(R_c, R_p)$  satisfying (9) for some  $p_{U,X}$  is achievable—follows directly from Jahn [5, Theorem 2]. We therefore focus on the converse, i.e., on showing that the achievability of a rate pair  $(R_c, R_p)$  implies that it lies in  $\mathcal{C}_{\text{det}}^{(I)}$ . But before proving this, we study  $\mathcal{C}_{\text{det}}^{(I)}$ . The proofs of the following propositions are available in [13].

**Proposition 3.** *The region  $\mathcal{C}_{\text{det}}^{(I)}$  can also be expressed as the closure of the union over all PMFs  $p_{U,X,Q}$  of the set of rate pairs  $(R_c, R_p)$  that satisfy*

$$R_c \leq \min_{s \in \mathcal{S}} I(U; Z|Q) \quad (12a)$$

$$R_p \leq I(X; Y|U, Q) \quad (12b)$$

$$R_c + R_p \leq I(X; Y|Q), \quad (12c)$$

where the mutual informations are computed w.r.t. the joint distribution

$$p_{U,X,Q}(u, x, q) W(y|x) V_s(z|x), \quad (13)$$

and where  $U$  and  $Q$  are auxiliary chance variables taking values in the finite sets  $\mathcal{U}$  and  $\mathcal{Q}$ .

From Proposition 3 we obtain:

**Proposition 4.** *The region  $\mathcal{C}_{\text{det}}^{(I)}$  is a compact convex set containing the rate pairs*

$$\left(\min\{C_{\text{Sh}}(W), \min_{s \in \mathcal{S}} C_{\text{Sh}}(V_s)\}, 0\right) \quad (14a)$$

and

$$(0, C_{\text{Sh}}(W)), \quad (14b)$$

where  $C_{\text{Sh}}(W)$  denotes the Shannon capacity of the channel  $W$ . Moreover,  $\mathcal{C}_{\text{det}}^{(I)}$  is included in the triangle with vertices

$$(0, 0), \quad (C_{\text{Sh}}(W), 0), \quad (0, C_{\text{Sh}}(W)). \quad (15)$$

We next provide one last characterization of  $\mathcal{C}_{\text{det}}^{(I)}$ . To that end, let  $\mathcal{C}_{\text{det}}^{(O)}$  denote the set of rate pairs  $(R_c, R_p)$  that satisfy

$$R_c \leq \min_{s \in \mathcal{S}} I(U; Z|Q) \quad (16a)$$

$$R_p + R_c \leq I(X; Y|U, Q) + \min_{s \in \mathcal{S}} I(U; Z|Q) \quad (16b)$$

$$R_p + R_c \leq I(X; Y|Q), \quad (16c)$$

for some PMF  $p_{U,X,Q}$ , where the mutual informations are computed w.r.t. the joint PMF of (13). The inequalities in the definition of  $\mathcal{C}_{\text{det}}^{(O)}$  thus differ from those in (12) in that we have replaced (12b) with (16b). As it turns out, this replacement does not change the region, and  $\mathcal{C}_{\text{det}}^{(O)} = \mathcal{C}_{\text{det}}^{(I)}$ .

**Proposition 5.** *The region  $\mathcal{C}_{\text{det}}^{(O)}$ , which is defined in (16), is equal to  $\mathcal{C}_{\text{det}}^{(I)}$ :*

$$\mathcal{C}_{\text{det}}^{(O)} = \mathcal{C}_{\text{det}}^{(I)}. \quad (17)$$

The converse is then established by proving that no rate pair outside  $\mathcal{C}_{\text{det}}^{(O)}$  is achievable [13].

#### IV. EXAMPLE

Consider the binary symmetric semi-arbitrarily-varying broadcast channel (BS-SAVBC), where the channel to  $Y$  is a BSC( $p$ ), i.e., a binary symmetric channel (BSC) with crossover probability  $p$ , and the channel to  $Z$  is a BSC with a state-dependent crossover probability between  $p_{\min}$  and  $p_{\max}$ . The state alphabet  $\mathcal{S}$  is the closed interval  $[p_{\min}, p_{\max}]$ , and we identify a state  $s \in \mathcal{S}$  with its corresponding crossover probability  $p_s$ . Thus, when the state is  $s$ , the channel from  $X$  to  $Z$  is a BSC( $p_s$ ). We focus on the case<sup>2</sup>

$$0 \leq p < 1/2 \quad (18)$$

$$0 \leq p_{\min} \leq p_{\max} < 1/2. \quad (19)$$

In this case the capacity of the DMC to  $Y$  and of the AVC to  $Z$  are both positive (c.f. [11], [12]), and therefore (by Remark 1 and Theorem 2) the capacity region of the BS-SAVBC is  $\mathcal{C}_{\text{det}}^{(I)}$ . Evaluating (9) for the joint PMF  $p_{U,X}$  under which

$$U \sim \text{Bernoulli}(1/2) \quad (20a)$$

$$V \sim \text{Bernoulli}(\alpha) \quad (20b)$$

$$X = U + V \pmod{2}, \quad (20c)$$

<sup>2</sup>When  $p$  equals  $1/2$  the capacity from  $X$  to  $Y$  is zero, and if we exclude this case, then—by possibly inverting  $Y$ —we can guarantee that  $p$  be in  $[0, 1/2)$ . Likewise, if the interval  $[p_{\min}, p_{\max}]$  includes  $1/2$ , then the capacity of the AVC from  $X$  to  $Z$  is zero. And if this is excluded, then—again by possibly inverting  $Z$ —we can restrict ourselves to the case where this interval is a subset of  $[0, 1/2)$ .

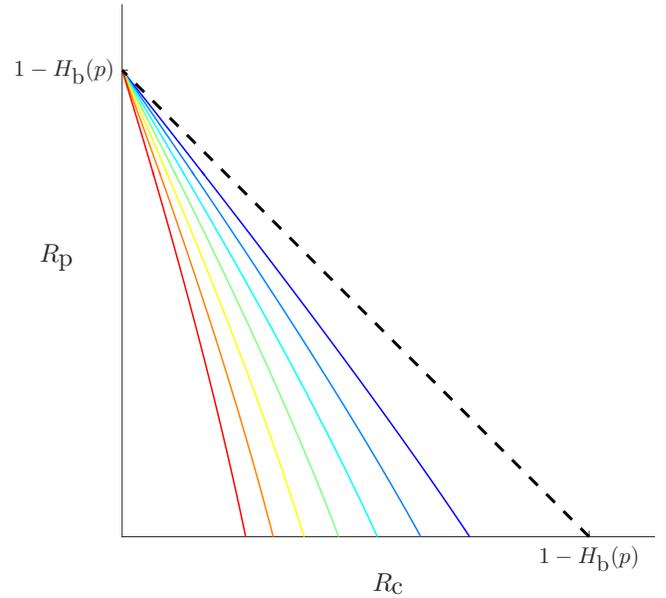


Fig. 2. The boundary of the capacity region of the binary symmetric semi-arbitrarily varying broadcast channel for various values of  $p_{\max} > p$ . The capacity region shrinks (and eventually has an empty interior) as  $p_{\max}$  increases to  $1/2$ . If  $p_{\max} \leq p$ , the capacity region is the triangle defined by the sum-rate constraint  $R_c + R_p \leq 1 - H_b(p)$ .

proves that  $\mathcal{C}_{\text{det}}^{(I)}$  contains all the rate pairs  $(R_c, R_p)$  satisfying

$$R_c \leq \min_{s \in \mathcal{S}} (1 - H_b(\alpha * p_s)) \quad (21a)$$

$$R_p \leq H_b(\alpha * p) - H_b(p) \quad (21b)$$

$$R_c + R_p \leq 1 - H_b(p) \quad (21c)$$

for some  $\alpha \in [0, 1/2]$ . Here  $H_b(\cdot)$  denotes the binary entropy function, and  $\alpha * \delta \triangleq \alpha(1 - \delta) + (1 - \alpha)\delta$ .

For a fixed  $\alpha \in [0, 1/2]$  the mapping  $\delta \mapsto \alpha * \delta$  is nondecreasing on  $(0 < \delta < 1/2)$ , and so is  $H_b(\cdot)$ . Consequently, the minimum on the RHS of (21a) is achieved when  $p_s$  equals  $p_{\max}$ , and (21) simplifies to

$$R_c \leq 1 - H_b(\alpha * p_{\max}) \quad (22a)$$

$$R_p \leq H_b(\alpha * p) - H_b(p) \quad (22b)$$

$$R_c + R_p \leq 1 - H_b(p). \quad (22c)$$

We next show that  $\mathcal{C}_{\text{det}}^{(I)}$  contains no other rate pairs, and that it thus equals the union over all  $\alpha \in [0, 1/2]$  of the polytopes defined by (22). This region is depicted in Figure 2. We do so by fixing the state to be  $p_{\max}$  throughout the block and by then showing that every achievable rate pair  $(R_c, R_p)$  must satisfy (22) for some  $\alpha \in [0, 1/2]$ . To this end, we distinguish between two cases, depending on whether or not  $p$  exceeds  $p_{\max}$ .

But first we note that if  $\alpha \in [0, 1/2]$  then, by the above monotonicity argument, the relation between  $p$  and  $p_{\max}$  trans-

lates to the relation between  $H_b(\alpha * p)$  and  $H_b(\alpha * p_{\max})$  as follows:

$$(p \leq p_{\max}) \iff (H_b(\alpha * p) \leq H_b(\alpha * p_{\max})) \quad (23a)$$

$$(p > p_{\max}) \iff (H_b(\alpha * p) > H_b(\alpha * p_{\max})). \quad (23b)$$

*Case I:  $p \leq p_{\max}$ .*

In this case fixing the state at  $p_{\max}$  results in a stochastically degraded binary-symmetric broadcast channel (BS-BC), where  $Z$  is a stochastically degraded version of  $Y$ . Since Receiver  $Y$  recovers  $(M_c, M_p)$ , and Receiver  $Z$  recovers  $M_c$ , any achievable rate pair  $(R_c, R_p)$  must be in the private-message capacity region of the above BS-BC. The latter is given by the set of rate pairs  $(R_c, R_p)$  that satisfy

$$R_p \leq I(X; Y|U) \quad (24a)$$

$$R_c \leq I(U; Z) \quad (24b)$$

for some PMF  $p_{U,X}$  [14, Theorem 5.2]. For the stochastically degraded BS-BC with the stronger receiver  $Y$  observing the BSC( $p$ ) and the degraded receiver  $Z$  observing the BSC( $p_s$ ), the capacity region (24) simplifies to the set of rate pairs  $(R_c, R_p)$  that satisfy

$$R_p \leq H_b(\alpha * p) - H_b(p) \quad (25a)$$

$$R_c \leq 1 - H_b(\alpha * p_{\max}) \quad (25b)$$

for some  $\alpha \in [0, 1/2]$  [14, Section 5.4.2]. Since these inequalities coincide with (22a) and (22b), it follows that to every rate pair  $(R_c, R_p) \in \mathcal{C}_{\det}^{(I)}$  there corresponds some  $\alpha \in [0, 1/2]$  for which (22a) and (22b) are satisfied. The sum-rate constraint (22c) is satisfied automatically because, in the case at hand, (22a) and (22b) imply (22c). Indeed, adding (22a) and (22b) yields

$$R_c + R_p \leq 1 - H_b(\alpha * p_{\max}) + H_b(\alpha * p) - H_b(p) \quad (26)$$

$$\leq 1 - H_b(p), \quad (27)$$

where the second inequality follows from (23a).

*Case II:  $p > p_{\max}$ .*

In this case fixing the state at  $p_{\max}$  again results in a stochastically degraded BS-BC, but in reverse order: now  $Y$  is a degraded version of  $Z$ . To show that any achievable rate pair  $(R_c, R_p)$  must satisfy (22), we first note that—since it is now the weaker receiver, namely Receiver  $Y$ , that must recover both  $M_c$  and  $M_p$ —the sum-rate  $R_c + R_p$  must not exceed the Shannon capacity of the BSC( $p$ ) from  $X$  to  $Y$

$$R_c + R_p \leq 1 - H_b(p). \quad (28)$$

Every rate pair in  $\mathcal{C}_{\det}^{(I)}$  must thus satisfy (28).

We next show that, to every rate pair  $(R_c, R_p)$  satisfying (28), there corresponds some  $\alpha \in [0, 1/2]$  for which (22) hold. To see why, note that, for the case at hand, for every  $\alpha \in [0, 1/2]$  the pair

$$R_c = 1 - H_b(\alpha * p) \quad (29a)$$

$$R_p = H_b(\alpha * p) - H_b(p) \quad (29b)$$

satisfies (22) (because, by (23b),  $1 - H_b(\alpha * p)$  cannot exceed  $1 - H_b(\alpha * p_{\max})$  and (22a) must therefore hold). As we vary  $\alpha$  from 0 to 1/2, the rate pair (29) traces the line  $R_c + R_p = 1 - H_b(p)$ .

## REFERENCES

- [1] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. on Inform. Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.
- [2] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie Verw. Gebiete*, vol. 44, pp. 159–175, 1978.
- [3] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. on Inform. Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.
- [4] E. Hof and S. I. Bross, "On the deterministic-code capacity of the two-user discrete memoryless arbitrarily varying general broadcast channel with degraded message sets," *IEEE Trans. on Inform. Theory*, vol. 52, no. 11, pp. 5023–5044, 2006.
- [5] J.-H. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. on Inform. Theory*, vol. 27, no. 2, pp. 212–226, 1981.
- [6] U. Pereg and Y. Steinberg, "The arbitrarily varying broadcast channel with degraded message sets with causal side information at the encoder," *arXiv preprint arXiv:1709.04770*, 2017.
- [7] —, "The arbitrarily varying degraded broadcast channel with causal side information at the encoder," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, June 2017, pp. 1033–1037.
- [8] Y. Steinberg, "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information," *IEEE Trans. on Inform. Theory*, vol. 51, no. 8, pp. 2867–2877, 2005.
- [9] R. F. Schaefer and H. Boche, "How much coordination is needed for robust broadcasting over arbitrarily varying bidirectional broadcast channels," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 1872–1877.
- [10] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.
- [11] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Trans. on Inform. Theory*, vol. 34, no. 2, pp. 181–193, March 1988.
- [12] I. Csiszár, "Arbitrarily varying channel with general alphabets and states," *IEEE Trans. on Inform. Theory*, vol. 38, no. 6, pp. 1725–1742, Nov. 1992.
- [13] T. Keresztfalvi and A. Lapidoth, "Semi-robust communications over a broadcast channel," *arXiv preprint arXiv:1711.00657*, 2017.
- [14] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.