Semi-Robust Communications over a Broadcast Channel

Tibor Keresztfalvi and Amos Lapidoth, *Fellow, IEEE*

***Abstract*— 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 better-protected message), whereas only the ordinary receiver is required to decode the private message (the less-protected message). As in the single-user case, under the appropriate compactness and convexity conditions, the capacity region is either empty or else the intersection of the capacity regions of the broadcast channels that the various states induce.**

***Index Terms*— Arbitrarily varying channel, broadcast channel, degraded message set, robust communications, unequal error protection.**

I. Introduction

AS IN Figure 1, two independent data streams—a rate-R_{c} common data stream and a rate-R_{p} private data stream—are to be transmitted over a broadcast channel with two receivers: an "ordinary receiver" and a "robust receiver." The channel to the ordinary receiver, the receiver that is required to recover both streams reliably, is a given (known) discrete memoryless channel (DMC) $\mathsf{W}(y|x)$. The channel to the robust receiver, the receiver that is required to recover only the common stream, is an arbitrarily varying channel (AVC) [1]. The set of rate pairs $(R_{\mathrm{c}}, R_{\mathrm{p}})$ that can be communicated reliably under these requirements is the *capacity region*, which we derive here.

This setting can be used to model a system employing unequal error protection: the common message can be viewed as the "better-protected message," and the private message as the "less-protected message."

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 [2]. But their model differs from ours because their broadcast channel is fixed and given: there is nothing "varying" about it.

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 where studied by Jahn [3] 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. General AVBCs with degraded message sets were studied by Hof and Bross [4].

More recent results on the AVBC for settings with causal and noncausal side information were obtained by Pereg and Steinberg [5]–[8].

Manuscript received December 7, 2017; revised October 5, 2018; accepted February 28, 2019. Date of publication March 12, 2019; date of current version July 12, 2019. This paper was presented in part at the 2018 International Symposium on Information Theory (ISIT).

The authors are with ETH Zurich, 8092 Zurich, Switzerland (e-mail: tibork@isi.ee.ethz.ch; lapidoth@isi.ee.ethz.ch).

Communicated by M. Costa, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2904504

II. The Main Result

A discrete memoryless state-dependent broadcast channel $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{S}, \mathsf{W}_{Y,Z|X,S})$ 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 $\mathsf{W}_{Y,Z|X,S}$. Given an input sequence $\mathbf{x} \in \mathcal{X}^n$ and a state sequence $\mathbf{s} \in \mathcal{S}^n$, the output sequences are distributed according to

$$\mathsf{W}_{Y^n,Z^n|X^n,S^n}(\mathbf{y},\mathbf{z}|\mathbf{x},\mathbf{s}) = \prod_{i=1}^{n} \mathsf{W}_{Y,Z|X,S}(y_i,z_i|x_i,s_i), \tag{1}$$

for all $(\mathbf{y},\mathbf{z}) \in \mathcal{Y}^n \times \mathcal{Z}^n$. 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 $\mathsf{W}(y|x)$ and $\mathsf{V}_s(z|x)$ respectively:

$$\mathsf{W}(y|x) = \mathsf{W}_{Y|X,S}(y|x,s), \tag{2a}$$

$$\mathsf{V}_s(z|x) = \mathsf{W}_{Z|X,S}(z|x,s). \tag{2b}$$

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.

A blocklength-n *deterministic code* $\mathcal{C}$ for the SAVBC consists of a common message set $\mathcal{M}_{\mathrm{c}}$ with $2^{nR_{\mathrm{c}}}$ messages, a private message set $\mathcal{M}_{\mathrm{p}}$ with $2^{nR_{\mathrm{p}}}$ messages, an encoding mapping

$$f\colon \mathcal{M}_{\mathrm{c}} \times \mathcal{M}_{\mathrm{p}} \to \mathcal{X}^n, \tag{3}$$

and decoding mappings

$$\phi_y\colon \mathcal{Y}^n \to \mathcal{M}_{\mathrm{c}} \times \mathcal{M}_{\mathrm{p}} \tag{4a}$$

$$\phi_z\colon \mathcal{Z}^n \to \mathcal{M}_{\mathrm{c}}. \tag{4b}$$

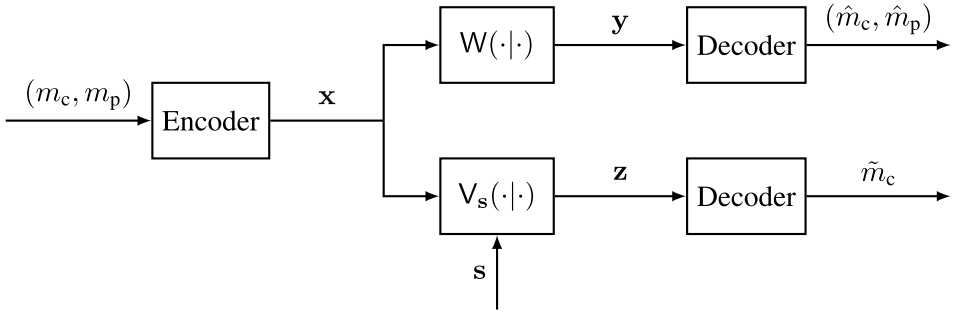

Fig. 1. The semi-arbitrarily-varying broadcast channel with common message m_c, private message m_p, and state sequence $\mathbf{s}$.

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

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

where

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

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

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

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

We do not consider here the capacity under the maximal-probability-of-error criterion, which would have resulted had we replaced the averaging over the messages in (5) with a maximum. Calculating this capacity is an open problem even in the single-user case to which our problem reduces when R_p is zero and the channel W is noiseless.

As in [9, Corollary 12.3], it can be shown that $\mathscr{C}_{\text{det}}$ depends on the states only via the convex-closure of the channels they induce. We thus define the set of channels $\mathcal{V}$ to be the closure of the set of all channels $\mathsf{V}(z|x)$ having the form

$$\mathsf{V}(z|x) = \sum_{s\in\tilde{\mathcal{S}}} P(s)\, \mathsf{V}_s(z|x) \tag{8}$$

where $\tilde{\mathcal{S}}$ is a finite subset of $\mathcal{S}$, and $P(\cdot)$ is a PMF on this subset. The set of channels $\mathcal{V}$ is compact and convex, and we henceforth assume that it equals $\{\mathsf{V}_s(z|x)\}_{s\in\mathcal{S}}$.

Following [3, Remark IIB2], [4], or using a time-sharing argument we note:

Remark 1. *The interior of $\mathscr{C}_{\text{det}}$ is nonempty if, and only if, the capacity of the channel $\mathsf{W}(y|x)$ 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 *[10], [11].*

We next define the region $\mathscr{C}^{(I)}$ that will turn out to equal the capacity region when the latter is not empty. 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

$$R_c \le \min_{\mathsf{V}\in\mathcal{V}} I(U; Z) \tag{9a}$$

$$R_p \le I(X; Y|U) \tag{9b}$$

$$R_c + R_p \le I(X; Y), \tag{9c}$$

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

$$p_{U,X}(u, x)\, \mathsf{W}(y|x)\, \mathsf{V}(z|x), \tag{10}$$

and where U is an auxiliary chance variable taking values in a finite set $\mathcal{U}$.

If there is only a single state and the set of channels $\mathcal{V}$ is hence a singleton $\{\mathsf{V}\}$, our network reduces to the broadcast channel that was solved by Körner and Marton [2], [12, Th. 8.1]. In this case the capacity region coincides with $\mathscr{C}^{(I)}$ (with the minimum being superfluous). We use $\mathcal{C}_{\mathsf{V}}$ to denote the resulting capacity, with the subscript V denoting the channel from X to Z and with the channel W from X to Y being implicit. The intersection

$$\mathcal{C}_{\text{cmp}} = \bigcap_{\mathsf{V}\in\mathcal{V}} \mathcal{C}_{\mathsf{V}} \tag{11}$$

is the capacity region corresponding to the setting where the state sequence is constant and is revealed to the code designer and receiver designer before transmission begins. (This setting is more benign than the compound-channel setting where the state is constant but not revealed to the designers [1].)

In the single-user case, when the family of channels is convex and compact, the AVC capacity (under the average-probability-of-error criterion) is either zero or else equal to the minimum of the capacities of the channels in the family [9, Th. 12.11]. Our main result can be viewed as an extension of this result to the SAVBC.

Theorem 2. *For any SAVBC,*

$$\mathscr{C}^{(I)} = \mathcal{C}_{\text{cmp}}, \tag{12}$$

and if the deterministic-code capacity $\mathscr{C}_{\text{det}}$ of a SAVBC is not empty, then it equals $\mathscr{C}^{(I)}$:

$$\left(\mathscr{C}_{\text{det}} \neq \emptyset\right) \implies \left(\mathscr{C}_{\text{det}} = \mathscr{C}^{(I)}\right). \tag{13}$$

Proof: See Section III. ∎

As noted by Jahn [3, Sec. III-D], if we allow random codes, then the region $\mathscr{C}^{(I)}$ is achievable even when the interior of $\mathscr{C}_{\text{det}}$ is empty. And since $\mathcal{C}_{\text{cmp}}$ is an outer bound on the capacity region even when random codes are allowed we infer:

Corollary 3. *The random-code capacity region of the SAVBC is equal to $\mathscr{C}^{(I)}$.*

III. Proof of the Main Result

The achievability result—that $\mathscr{C}_{\text{det}} \neq \emptyset$ implies that every rate pair $(R_{\text{c}}, R_{\text{p}})$ in $\mathscr{C}^{(I)}$ is achievable—follows from Jahn's work [3, Th. 2]. The converse follows directly from (12) and the inclusion $\mathscr{C}_{\text{det}} \subseteq \mathcal{C}_{\text{cmp}}$, which holds because the probabilities of error must be vanishingly small irrespective of the state sequence and hence, *a fortiori*, when the state sequence is constant. We therefore focus on proving (12).

But first we provide an alternative description for $\mathscr{C}^{(I)}$. To this end we define $\mathscr{C}^{(Q)}$ to be the closure of the union over all PMFs $p_{U,X,Q}$ of the set of rate pairs $(R_{\text{c}}, R_{\text{p}})$ that satisfy

$$R_{\text{c}} \leq \min_{\mathsf{V}\in\mathcal{V}} I(U; Z|Q) \tag{14a}$$

$$R_{\text{p}} \leq I(X; Y|U, Q) \tag{14b}$$

$$R_{\text{c}} + R_{\text{p}} \leq I(X; Y|Q), \tag{14c}$$

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

$$p_{U,X,Q}(u, x, q)\, \mathsf{W}(y|x)\, \mathsf{V}(z|x), \tag{15}$$

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

Proposition 4. *The regions $\mathscr{C}^{(I)}$ and $\mathscr{C}^{(Q)}$ are identical*

$$\mathscr{C}^{(I)} = \mathscr{C}^{(Q)}. \tag{16}$$

Proof: One inclusion is obvious and simply follows by setting Q to be deterministic. We therefore focus on the other, namely, on showing that if there exists some joint PMF $p_{U,X,Q}$ under which the pair $(R_{\text{c}}, R_{\text{p}})$ satisfies (14), then there exists some auxiliary chance variable $\tilde{U}$ and a PMF $p_{\tilde{U},X}$ under which the pair satisfies (9) when we substitute $\tilde{U}$ for U. To this end we choose $\tilde{U} = (U, Q)$ and show that the results of substituting $\tilde{U}$ for U on the right hand side (RHS) of each of the inequalities in (9) is at least as high as the RHS of the corresponding inequality in (14):

$$\begin{aligned}\min_{\mathsf{V}\in\mathcal{V}} I(\tilde{U}; Z) &= \min_{\mathsf{V}\in\mathcal{V}} I(U, Q; Z)\\ &= \min_{\mathsf{V}\in\mathcal{V}} \big\{ I(U; Z|Q) + I(Q; Z) \big\}\\ &\geq \min_{\mathsf{V}\in\mathcal{V}} I(U; Z|Q);\end{aligned}$$

$$I(X; Y|\tilde{U}) = I(X; Y|U, Q);$$

and

$$\begin{aligned}I(X; Y) &= I(X, Q; Y)\\ &= I(Q; Y) + I(X; Y|Q)\\ &\geq I(X; Y|Q),\end{aligned} \tag{17}$$

where (17) follows from the Markovity $Q—\circ—X—\circ—Y$. ■

From Proposition 4 we obtain:

Corollary 5. *The region $\mathscr{C}^{(I)}$ is a compact convex set*

We are now ready to prove (12) and thus conclude the proof of Theorem 2.

Proof that $\mathscr{C}^{(I)} = \mathcal{C}_{\text{cmp}}$: Since $\mathscr{C}^{(I)}$ equals $\mathscr{C}^{(Q)}$ (Proposition 4), it suffices to prove that

$$\mathscr{C}^{(Q)} = \mathcal{C}_{\text{cmp}}. \tag{18}$$

We begin by describing $\mathscr{C}^{(Q)}$ more explicitly by restricting the cardinality of the auxiliary chance variable U to m and then letting m tend to infinity. Let $\mathcal{U}_m$ denote the set $\{1, \ldots, m\}$, and $\mathcal{P}_m$ the set of probability distributions on $\mathcal{U}_m \times \mathcal{X}$. Let $\text{Prob}_0(\mathcal{P}_m)$ denote the set of probability distributions on $\mathcal{P}_m$ of finite support. A generic element $\mu \in \text{Prob}_0(\mathcal{P}_m)$ has the form

$$\mu = \sum_{q=1}^{k} \alpha_q\, \delta_{\nu_{U,X}^{(q)}}, \quad \alpha_q \geq 0, \quad \sum_{q=1}^{k} \alpha_q = 1, \tag{19}$$

where $\delta_{\nu_{U,X}^{(q)}}$ is the PMF on $\mathcal{P}_m$ that is concentrated at $\nu_{U,X}^{(q)}$, so

$$\delta_{\nu_{U,X}^{(q)}}(\nu_{U,X}) = \begin{cases} 1 & \text{if } \nu_{U,X} = \nu_{U,X}^{(q)} \\ 0 & \text{otherwise,} \end{cases} \quad \nu_{U,X} \in \mathcal{P}_m, \tag{20}$$

and

$$\mu(\nu_{U,X}) = \sum_{q=1}^{k} \alpha_q\, \delta_{\nu_{U,X}^{(q)}}(\nu_{U,X}). \tag{21}$$

Define for every $\mathsf{V} \in \mathcal{V}$ and $\nu_{U,X} \in \mathcal{P}_m$

$$I^{(\text{c})}(\mathsf{V}, \nu_{U,X}) = I(U; Z) \tag{22a}$$

$$I^{(\text{p})}(\nu_{U,X}) = I(X; Y|U) \tag{22b}$$

$$I^{(\text{s})}(\nu_{U,X}) = I(X; Y), \tag{22c}$$

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

$$\nu_{U,X}(u, x)\, \mathsf{W}(y|x)\, \mathsf{V}(z|x), \tag{22d}$$

and "c," "p," and "s" are mnemonic for "common," "private," and "sum." For every $\mathsf{V} \in \mathcal{V}$ and every $\mu \in \text{Prob}_0(\mathcal{P}_m)$ of the form (19), define

$$I^{(\text{c})}(\mathsf{V}, \mu) = \sum_{q=1}^{k} \alpha_q\, I^{(\text{c})}(\mathsf{V}, \nu_{U,X}^{(q)}) \tag{23a}$$

$$I^{(\text{p})}(\mu) = \sum_{q=1}^{k} \alpha_q\, I^{(\text{p})}(\nu_{U,X}^{(q)}) \tag{23b}$$

$$I^{(\text{s})}(\mu) = \sum_{q=1}^{k} \alpha_q\, I^{(\text{s})}(\nu_{U,X}^{(q)}). \tag{23c}$$

These correspond to $I(U; Z|Q)$, $I(X, Y|U, Q)$, and $I(X; Y|Q)$ when the channel from X to Z is V; the chance variable Q takes on the value q with probability α_q; and $P_{U,X|Q=q}$ is $\nu_{U,X}^{(q)}$.

Note that neither $I^{(\text{p})}(\mu)$ nor $I^{(\text{s})}(\mu)$ depends on V: they only depend on μ. As to $I^{(\text{c})}(\mathsf{V}, \mu)$, it inherits the following properties from $I^{(\text{c})}(\mathsf{V}, \nu_{U,X})$: For any fixed $\mu \in \text{Prob}_0(\mathcal{P}_m)$, the mapping $\mathsf{V} \mapsto I^{(\text{c})}(\mathsf{V}, \mu)$ is convex and continuous with

a compact domain (namely, $\mathcal{V}$). Moreover, for a fixed $\mathsf{V} \in \mathcal{V}$, the mapping $\mu \mapsto I^{(\mathrm{c})}(\mathsf{V}, \mu)$ is concave.

Minimizing over V, we now define for every $\mu \in \mathrm{Prob}_0(\mathcal{P}_m)$ as above

$$J^{(\mathrm{c})}(\mu) = \min_{\mathsf{V}\in\mathcal{V}} \sum_{q=1}^{k} \alpha_q \, I^{(\mathrm{c})}(\mathsf{V}, \nu_{U,X}^{(q)}) \tag{24a}$$

$$J^{(\mathrm{p})}(\mu) = \sum_{q=1}^{k} \alpha_q \, I^{(\mathrm{p})}(\nu_{U,X}^{(q)}) \tag{24b}$$

$$J^{(\mathrm{s})}(\mu) = \sum_{q=1}^{k} \alpha_q \, I^{(\mathrm{s})}(\nu_{U,X}^{(q)}), \tag{24c}$$

$$\mathbf{J}(\mu) = \big(J^{(\mathrm{c})}(\mu), J^{(\mathrm{p})}(\mu), J^{(\mathrm{s})}(\mu)\big). \tag{24d}$$

(Here $J^{(\mathrm{p})}(\mu) = I^{(\mathrm{p})}(\mu)$ and $J^{(\mathrm{s})}(\mu) = I^{(\mathrm{s})}(\mu)$, but we introduced the new notation for consistency with $J^{(\mathrm{c})}(\mu)$.) Here $J^{(\mathrm{c})}(\mu)$ corresponds to $\min_{\mathsf{V}} I(U; Z|Q)$ for Q as before.

Rather than studying the two-dimensional region in the $(R_\mathrm{c}, R_\mathrm{p})$-plane that the three constraints induce, we prefer to study the three-dimensional set of constraints triples. We thus define

$$\mathcal{J}_m = \bigcup_{\mu\in\mathrm{Prob}_0(\mathcal{P}_m)} \big\{\boldsymbol{\rho} \in \mathbb{R}_+^3 : \mathbf{0} \preceq \boldsymbol{\rho} \preceq \mathbf{J}(\mu)\big\}, \tag{25}$$

where $\mathbb{R}_+$ denotes the nonnegative reals, $\mathbf{0} = (0, 0, 0)$, and for vectors $\mathbf{a} = (a_1, a_2, a_3) \in \mathbb{R}^3$ and $\mathbf{b} = (b_1, b_2, b_3) \in \mathbb{R}^3$ we use $\mathbf{a} \preceq \mathbf{b}$ to indicate that $a_i \le b_i$ for every $i \in \{1, 2, 3\}$. Note that $\mathcal{J}_m$ is convex (because the minimum of a convex combination is lower-bounded by the convex combination of the minima). Also, the sequence $\{\mathcal{J}_m\}$ is monotonically nondecreasing in the sense that $\mathcal{J}_m \subseteq \mathcal{J}_{m+1}$ for every $m \in \mathbb{N}$ (with $\mathbb{N}$ denoting the natural numbers). We define

$$\mathcal{J} = \bigcup_{m\in\mathbb{N}} \mathcal{J}_m \tag{26}$$

and denote its closure $\bar{\mathcal{J}}$.

For every rate pair $(R_\mathrm{c}, R_\mathrm{p}) \in \mathbb{R}_+^2$, define the triple

$$\mathbf{R}(R_\mathrm{c}, R_\mathrm{p}) = \big(R_\mathrm{c},\ R_\mathrm{p},\ R_\mathrm{c} + R_\mathrm{p}\big). \tag{27}$$

The relationship between $\mathscr{C}^{(Q)} \subset \mathbb{R}_+^2$ and $\bar{\mathcal{J}} \subset \mathbb{R}_+^3$ can now be expressed by

$$\Big((R_\mathrm{c}, R_\mathrm{p}) \in \mathscr{C}^{(Q)}\Big) \iff \Big(\mathbf{R}(R_\mathrm{c}, R_\mathrm{p}) \in \bar{\mathcal{J}}\Big). \tag{28}$$

The Körner-Marton region $\mathcal{C}_\mathsf{V} \in \mathbb{R}_+^2$ can also be described in the constraints space. To this end, we let $\mathcal{J}_\mathsf{V} \in \mathbb{R}_+^3$ correspond to $\mathcal{J}$ of (26) for the single-state setting, with the subscript V denoting the channel from X to Z and with the channel W from X to Y being implicit. In this single-state setting it suffices to choose m equal to $|\mathcal{X}| + 1$ and there is no need to take the closure: $\mathcal{J}_\mathsf{V}$ is compact and convex [12, Th. 8.1]. As in (28),

$$\Big((R_\mathrm{c}, R_\mathrm{p}) \in \mathcal{C}_\mathsf{V}\Big) \iff \Big(\mathbf{R}(R_\mathrm{c}, R_\mathrm{p}) \in \mathcal{J}_\mathsf{V}\Big). \tag{29}$$

Similarly, we define

$$\mathcal{J}_\mathrm{cmp} = \bigcap_{\mathsf{V}\in\mathcal{V}} \mathcal{J}_\mathsf{V}, \tag{30}$$

so

$$\Big((R_\mathrm{c}, R_\mathrm{p}) \in \mathcal{C}_\mathrm{cmp}\Big) \iff \Big(\mathbf{R}(R_\mathrm{c}, R_\mathrm{p}) \in \mathcal{J}_\mathrm{cmp}\Big). \tag{31}$$

It follows from (31) and (28) that proving that $\mathscr{C}^{(Q)}$ equals $\mathcal{C}_\mathrm{cmp}$ is equivalent to proving that

$$\bar{\mathcal{J}} = \mathcal{J}_\mathrm{cmp}, \tag{32}$$

which is what we set out to do now. The inclusion

$$\bar{\mathcal{J}} \subseteq \mathcal{J}_\mathrm{cmp} \tag{33}$$

holds because replacing the minimum in (24) with a fixed channel V cannot decrease the result, so $\mathcal{J}_\mathsf{V}$ must contain $\bar{\mathcal{J}}$, and this is true for every $\mathsf{V} \in \mathcal{V}$. The reverse inclusion is trickier.

The set $\bar{\mathcal{J}}$ is compact and convex (because for every $m \in \mathbb{N}$ the set $\mathcal{J}_m$ is convex and $\mathcal{J}_m \subseteq \mathcal{J}_{m+1}$). We shall study it by studying the mapping

$$\boldsymbol{\lambda} \mapsto \max_{\boldsymbol{\rho}\in\bar{\mathcal{J}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho} \rangle \tag{34}$$

for triples $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$. Since $\mathcal{J}_m \subseteq \mathcal{J}_{m+1}$,

$$\max_{\boldsymbol{\rho}\in\bar{\mathcal{J}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho} \rangle = \lim_{m\to\infty} \sup_{\boldsymbol{\rho}\in\mathcal{J}_m} \langle \boldsymbol{\lambda}, \boldsymbol{\rho} \rangle . \tag{35}$$

As we next argue,

$$\sup_{\boldsymbol{\rho}\in\mathcal{J}_m} \langle \boldsymbol{\lambda}, \boldsymbol{\rho} \rangle = \sup_{\boldsymbol{\rho}\in\mathcal{J}_m} \big\langle \boldsymbol{\lambda}^+, \boldsymbol{\rho} \big\rangle \tag{36}$$

$$= \sup_{\mu\in\mathrm{Prob}_0(\mathcal{P}_m)} \big\langle \boldsymbol{\lambda}^+, \mathbf{J}(\mu) \big\rangle, \tag{37}$$

where $\boldsymbol{\lambda}^+ = (\lambda_1^+, \lambda_2^+, \lambda_3^+)$, and we are using the notation

$$\xi^+ = \max\{\xi, 0\}, \quad \xi \in \mathbb{R}. \tag{38}$$

Here (36) holds because the components of all the tuples in $\mathcal{J}_m$ are nonnegative, and because we have included in $\mathcal{J}_m$ all the vectors with $\mathbf{0} \preceq \boldsymbol{\rho} \preceq \mathbf{J}(\mu)$ so that if some λ_i is negative we can restrict ourselves without loss of optimality to tuples $\boldsymbol{\rho}$ whose i-th component is zero; and (37) holds because $\boldsymbol{\lambda}^+$ has nonnegative components so $\big\langle \boldsymbol{\lambda}^+, \mathbf{J}(\mu) \big\rangle$ is at least as large as $\big\langle \boldsymbol{\lambda}^+, \boldsymbol{\rho} \big\rangle$ whenever $\mathbf{0} \preceq \boldsymbol{\rho} \preceq \mathbf{J}(\mu)$.

We next study the supremum on the RHS of (37). We shall need the Minisup Theorem of Nakaido [13, Sec. 7.1.8], which we quote from [11]: Let $f(x, y)$ be defined for $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ are convex subsets of topological vector spaces, and $\mathcal{X}$ is compact. Let $f(x, y)$ be convex and lower semicontinuous in x for every $y \in \mathcal{Y}$ and concave in y for every $x \in \mathcal{X}$. Then there exists an $\bar{x} \in \mathcal{X}$ such that

$$\sup_{y\in\mathcal{Y}} \min_{x\in\mathcal{X}} f(x, y) = \sup_{y\in\mathcal{Y}} f(\bar{x}, y) = \min_{x\in\mathcal{X}} \sup_{y\in\mathcal{Y}} f(x, y). \tag{39}$$

We shall use this theorem with the supremum being over $\mathrm{Prob}_0(\mathcal{P}_m)$ and with the minimum being over $\mathcal{V}$.

Starting from (37),

$$\begin{aligned}
&\sup_{\boldsymbol{\rho}\in\mathcal{J}_m} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle \\
&= \sup_{\mu\in\mathrm{Prob}_0(\mathcal{P}_m)} \Big\{\lambda_1^+ J^{(\mathrm{c})}(\mu) + \lambda_2^+ J^{(\mathrm{p})}(\mu) \\
&\qquad + \lambda_3^+ J^{(\mathrm{s})}(\mu)\Big\} && (40)\\
&= \sup_{\mu\in\mathrm{Prob}_0(\mathcal{P}_m)} \Big\{\lambda_1^+ \Big(\min_{\mathsf{V}\in\mathcal{V}} I^{(\mathrm{c})}(\mathsf{V},\mu)\Big) + \lambda_2^+ I^{(\mathrm{p})}(\mu) \\
&\qquad + \lambda_3^+ I^{(\mathrm{s})}(\mu)\Big\} && (41)\\
&= \sup_{\mu\in\mathrm{Prob}_0(\mathcal{P}_m)} \min_{\mathsf{V}\in\mathcal{V}} \Big\{\lambda_1^+ I^{(\mathrm{c})}(\mathsf{V},\mu) + \lambda_2^+ I^{(\mathrm{p})}(\mu) \\
&\qquad + \lambda_3^+ I^{(\mathrm{s})}(\mu)\Big\} && (42)\\
&= \min_{\mathsf{V}\in\mathcal{V}} \sup_{\mu\in\mathrm{Prob}_0(\mathcal{P}_m)} \Big\{\lambda_1^+ I^{(\mathrm{c})}(\mathsf{V},\mu) + \lambda_2^+ I^{(\mathrm{p})}(\mu) \\
&\qquad + \lambda_3^+ I^{(\mathrm{s})}(\mu)\Big\} && (43)\\
&= \min_{\mathsf{V}\in\mathcal{V}} \max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathsf{V}}} \big\langle \boldsymbol{\lambda}^+, \boldsymbol{\rho}\big\rangle, \quad m \geq |\mathcal{X}| + 1, && (44)
\end{aligned}$$

with the following justification. The second equality (41) holds by the definitions in (24), and the third equality (42) because λ_1^+ is nonnegative and because $I^{(\mathrm{p})}(\mu)$ and $I^{(\mathrm{s})}(\mu)$ do not depend on V. The fourth equality (43) holds by the Minisup Theorem. To justify (44) we note that the supremum on the RHS of (43) corresponds to a situation where the channel V is fixed and we maximize over μ. It is thus similar to the situation we encounter in studying the broadcast channel with degraded message sets [2] [12, Th. 8.1], and the cardinality bounds in the latter show that when $m \geq |\mathcal{X}| + 1$ this supremum is achieved by some deterministic μ, i.e., by a μ whose support is a singleton. It now follows from (44) and (35) that

$$\max_{\boldsymbol{\rho}\in\bar{\mathcal{J}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle = \min_{\mathsf{V}\in\mathcal{V}} \max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathsf{V}}} \big\langle \boldsymbol{\lambda}^+, \boldsymbol{\rho}\big\rangle. \tag{45}$$

We are now ready to conclude the proof that $\bar{\mathcal{J}} = \mathcal{J}_{\mathrm{cmp}}$ and that therefore $\mathscr{C}^{(I)} = \mathcal{C}_{\mathrm{cmp}}$. Being the intersection of compact convex sets, $\mathcal{J}_{\mathrm{cmp}}$ is compact and convex. And since so is $\bar{\mathcal{J}}$, it suffices to prove that for all triples $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$ [14, Th. 11.5]

$$\max_{\boldsymbol{\rho}\in\bar{\mathcal{J}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle = \max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathrm{cmp}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle. \tag{46}$$

Since $\bar{\mathcal{J}} \subseteq \mathcal{J}_{\mathrm{cmp}}$ (33),

$$\max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathrm{cmp}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle \geq \max_{\boldsymbol{\rho}\in\bar{\mathcal{J}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle, \quad \boldsymbol{\lambda} \in \mathbb{R}^3, \tag{47}$$

and it remains to prove the reverse inequality. Since the maximum over an intersection of sets is upper-bounded by the minimum of the maxima over the sets, it follows from (30) that

$$\begin{aligned}
\max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathrm{cmp}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle &\leq \min_{\mathsf{V}\in\mathcal{V}} \max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathsf{V}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle && (48)\\
&= \min_{\mathsf{V}\in\mathcal{V}} \max_{\boldsymbol{\rho}\in\mathcal{J}_{\mathsf{V}}} \big\langle \boldsymbol{\lambda}^+, \boldsymbol{\rho}\big\rangle && (49)\\
&= \max_{\boldsymbol{\rho}\in\bar{\mathcal{J}}} \langle \boldsymbol{\lambda}, \boldsymbol{\rho}\rangle, \quad \boldsymbol{\lambda} \in \mathbb{R}^3, && (50)
\end{aligned}$$

where the second line follows from arguments similar to those leading to (36); and the final equality follows from (45). The combination of (50) and (47) establishes (46) and thus concludes the proof of (32), which implies (18) and hence by Proposition 4 that $\mathscr{C}^{(I)} = \mathcal{C}_{\mathrm{cmp}}$. ■

IV. Computational Considerations

Calculating $\mathscr{C}^{(I)}$ numerically is a bit tricky without a bound on the size of the alphabet $\mathcal{U}$ in which the auxiliary U takes values. Here we propose a workaround. Recalling Proposition 4, it suffices to compute $\mathscr{C}^{(Q)}$, which is in one-to-one correspondence with the compact and convex set $\bar{\mathcal{J}} \subset \mathbb{R}^3_+$. The latter can be characterized using the mapping (34), which is given explicitly in (45). This has some computational advantages, because on the RHS of (45) the inner maximization is for a fixed channel V, so we may limit the cardinality of the auxiliary alphabet $\mathcal{U}$ to [12, Th. 8.1]

$$|\mathcal{U}| \leq \min\big\{|\mathcal{X}|, |\mathcal{Y}| + |\mathcal{Z}|\big\} + 1. \tag{51}$$

Moreover, the RHS of (45) could perhaps be computed using numerical techniques for finding equilibrium points.

V. 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[1]

$$0 \leq p < 1/2 \tag{52}$$

$$0 \leq p_{\min} \leq p_{\max} < 1/2. \tag{53}$$

In this case the capacity of the DMC to Y and of the AVC to Z are both positive (c.f. [10], [11]), and therefore (by Remark 1 and Theorem 2) the capacity region of the BS-SAVBC is $\mathscr{C}^{(I)}$, which is also equal to $\mathcal{C}_{\mathrm{cmp}}$. The BSC($p_{\max}$) is a degraded version of all the channels in $\mathcal{V}$, so $\mathcal{C}_{\mathrm{cmp}}$ is the Körner-Marton region corresponding to $\mathsf{V} = \mathrm{BSC}(p_{\max})$, i.e., $\mathcal{C}_{\mathsf{V}}$.

An inner bound on $\mathcal{C}_{\mathsf{V}}$ can be found by evaluating (9) (with the minimization replaced by choosing the state corresponding to $p_{\max}$) for the joint PMF $p_{U,X}$ under which

$$U \sim \mathrm{Bernoulli}(1/2) \tag{54a}$$

$$V \sim \mathrm{Bernoulli}(\alpha) \tag{54b}$$

$$X = U + V \mod 2. \tag{54c}$$

[1]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 $[0, 1/2)$.

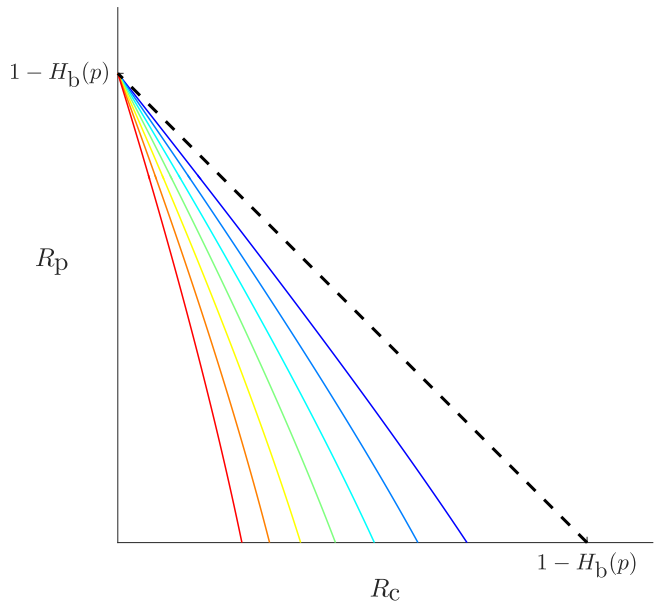

Fig. 2. The boundary of the capacity region of the binary symmetric semi-arbitrarily varying broadcast channel for various values of p, $p_{\max} \in [0, 1/2]$. The dashed line corresponds to the boundary when $p_{\max} \leq p$. As $p_{\max}$ increases from p towards $1/2$ the region shrinks and eventually, when $p_{\max}$ increases to $1/2$, loses its interior.

This proves that $\mathcal{C}_{\mathsf{V}}$ contains all the rate pairs $(R_{\mathrm{c}}, R_{\mathrm{p}})$ satisfying

$$R_{\mathrm{c}} \leq 1 - H_{\mathrm{b}}(\alpha * p_{\max}) \tag{55a}$$

$$R_{\mathrm{p}} \leq H_{\mathrm{b}}(\alpha * p) - H_{\mathrm{b}}(p) \tag{55b}$$

$$R_{\mathrm{c}} + R_{\mathrm{p}} \leq 1 - H_{\mathrm{b}}(p). \tag{55c}$$

Here $H_{\mathrm{b}}(\cdot)$ denotes the binary entropy function, and we introduce the notation $\alpha * \delta \triangleq \alpha(1-\delta) + (1-\alpha)\delta$.

We next show that $\mathcal{C}_{\mathsf{V}}$ contains no other rate pairs, and that it thus equals the union over all $\alpha \in [0, 1/2]$ of the polytopes defined by (55). This region is depicted in Figure 2. We do so by showing that every rate pair $(R_{\mathrm{c}}, R_{\mathrm{p}})$ in $\mathcal{C}_{\mathsf{V}}$ must satisfy (55) for some $\alpha \in [0, 1/2]$. To this end, we distinguish between two cases, depending on whether or not p exceeds $p_{\max}$.

We first note that for a fixed $\alpha \in [0, 1/2)$, the mapping $\delta \mapsto \alpha * \delta$ is monotonically increasing on $(0 < \delta < 1/2)$, and so is $H_{\mathrm{b}}(\cdot)$. Consequently, for such α's, the relation between p and $p_{\max}$ translates to the relation between $H_{\mathrm{b}}(\alpha * p)$ and $H_{\mathrm{b}}(\alpha * p_{\max})$ as follows:

$$\Big(p \leq p_{\max}\Big) \iff \Big(H_{\mathrm{b}}(\alpha * p) \leq H_{\mathrm{b}}(\alpha * p_{\max})\Big) \tag{56a}$$

$$\Big(p > p_{\max}\Big) \iff \Big(H_{\mathrm{b}}(\alpha * p) > H_{\mathrm{b}}(\alpha * p_{\max})\Big). \tag{56b}$$

Case I: $p \leq p_{\max}$.
In this case the broadcast channel corresponding to $\mathsf{V} = \mathrm{BSC}(p_{\max})$ is a stochastically degraded binary-symmetric broadcast channel (BS-BC), where Z is a stochastically degraded version of Y. Since Receiver Y recovers $(M_{\mathrm{c}}, M_{\mathrm{p}})$ and Receiver Z recovers M_{c}, any rate pair $(R_{\mathrm{c}}, R_{\mathrm{p}})$ in $\mathcal{C}_{\mathsf{V}}$ must satisfy

$$R_{\mathrm{p}} \leq I(X; Y|U) \tag{57a}$$

$$R_{\mathrm{c}} \leq I(U; Z) \tag{57b}$$

for some PMF $p_{U,X}$ [12, Th. 5.2]. For the stochastically degraded BS-BC with the stronger receiver Y observing the $\mathrm{BSC}(p)$ and the degraded receiver Z observing the $\mathrm{BSC}(p_s)$, the capacity region (57) simplifies to the set of rate pairs $(R_{\mathrm{c}}, R_{\mathrm{p}})$ that satisfy

$$R_{\mathrm{p}} \leq H_{\mathrm{b}}(\alpha * p) - H_{\mathrm{b}}(p) \tag{58a}$$

$$R_{\mathrm{c}} \leq 1 - H_{\mathrm{b}}(\alpha * p_{\max}) \tag{58b}$$

for some $\alpha \in [0, 1/2]$ [12, Sec. 5.4.2]. Since these inequalities coincide with (55a) and (55b), it follows that to every rate pair $(R_{\mathrm{c}}, R_{\mathrm{p}}) \in \mathcal{C}_{\mathsf{V}}$ there corresponds some $\alpha \in [0, 1/2]$ for which (55a) and (55b) are satisfied. The sum-rate constraint (55c) is satisfied automatically because, in the case at hand, (55a) and (55b) imply (55c). Indeed, adding (55a) and (55b) yields

$$R_{\mathrm{c}} + R_{\mathrm{p}} \leq 1 - H_{\mathrm{b}}(\alpha * p_{\max}) + H_{\mathrm{b}}(\alpha * p) - H_{\mathrm{b}}(p) \tag{59}$$

$$\leq 1 - H_{\mathrm{b}}(p), \tag{60}$$

where the second inequality follows from (56a) for $\alpha \in [0, 1/2)$ and by inspection for $\alpha = 1/2$.
Case II: $p > p_{\max}$.
In this case too the broadcast channel corresponding to $\mathsf{V} = \mathrm{BSC}(p_{\max})$ is a stochastically degraded BS-BC, but the order is reversed: now Y is a degraded version of Z. To show that any achievable rate pair $(R_{\mathrm{c}}, R_{\mathrm{p}})$ must satisfy (55), 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 $R_{\mathrm{c}} + R_{\mathrm{p}}$ must not exceed the Shannon capacity of the $\mathrm{BSC}(p)$ from X to Y

$$R_{\mathrm{c}} + R_{\mathrm{p}} \leq 1 - H_{\mathrm{b}}(p). \tag{61}$$

Every rate pair in $\mathscr{C}^{(I)}$ must thus satisfy (61).

We next show that, to every rate pair $(R_{\mathrm{c}}, R_{\mathrm{p}})$ satisfying (61), there corresponds some $\alpha \in [0, 1/2]$ for which (55) hold. To see why, note that, for the case at hand, for every $\alpha \in [0, 1/2]$ the pair

$$R_{\mathrm{c}} = 1 - H_{\mathrm{b}}(\alpha * p) \tag{62a}$$

$$R_{\mathrm{p}} = H_{\mathrm{b}}(\alpha * p) - H_{\mathrm{b}}(p) \tag{62b}$$

satisfies (55) (because, by (56b), $1 - H_{\mathrm{b}}(\alpha * p)$ cannot exceed $1 - H_{\mathrm{b}}(\alpha * p_{\max})$ and (55a) must therefore hold). As we vary α from 0 to $1/2$, the rate pair (62) traces the line $R_{\mathrm{c}} + R_{\mathrm{p}} = 1 - H_{\mathrm{b}}(p)$.

VI. Summary and Discussion

Motivated by communication scenarios involving unequal error protection, we have studied a special class of arbitrarily varying broadcast channels with degraded message sets, where the channel to the receiver that is required to decode both messages is fixed, and the channel to the receiver that is only required to decode the common message is arbitrarily varying. The private message can be viewed as the "less-well protected message," and the common message as the "better-protected message." Although the capacity region of the general arbitrarily varying broadcast channel is unknown, for our special class we were able to provide a single-letter

characterization of the capacity. Moreover, our results show that our network bears similarity to the single-user AVC where, for convex and compact classes of channels, the AVC capacity is either zero or else equals the minimum of the capacities of the channels in the family.

This raises hopes that other results about the single-user AVC might have counterparts for our class. Of particular interest might be results on cost constraints and noncausal state information at the transmitter. Also of interest might be to solve for the capacity region when the set of channels $\mathcal{V}$ is finite and the state remains constant throughout the transmission. This seems to be an open problem even when $\mathcal{V}$ has only two elements [12, Ch. 8, Open problems].

REFERENCES

[1] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.

[2] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.

[3] J. H. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 2, pp. 212–226, Mar. 1981.

[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. Inf. Theory*, vol. 52, no. 11, pp. 5023–5044, Nov. 2006.

[5] U. Pereg and Y. Steinberg. (2017). "The arbitrarily varying broadcast channel with degraded message sets with causal side information at the encoder." [Online]. Available: https://arxiv.org/abs/1709.04770

[6] U. Pereg and Y. Steinberg, "The arbitrarily varying degraded broadcast channel with causal side information at the encoder," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1033–1037.

[7] Y. Steinberg, "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2867–2877, Aug. 2005.

[8] U. Pereg and Y. Steinberg, "The arbitrarily varying channel under constraints with side information at the encoder," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 861–887, Feb. 2019.

[9] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[10] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.

[11] I. Csiszár, "Arbitrarily varying channels with general alphabets and states," *IEEE Trans. Inform. Theory*, vol. 38, no. 6, pp. 1725–1742, Nov. 1992.

[12] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[13] J.-P. Aubin, *Mathematical Methods of Game and Economic Theory: Revised Edition*. New York, NY, USA: Dover, 2008.

[14] R. T. Rockafellar, *Convex Analysis*. Princeton Univ. Press, 1970.

Tibor Keresztfalvi was born on September 24th, 1991, in Budapest, Hungary. He received his Bachelor of Science (B.Sc.) degree in the field of Electrical Engineering from ETH Zurich, Switzerland, in 2013. He completed his Master of science (M.Sc.) in the field of Electrical Engineering with a focus on Digital Communication at ETH Zurich, in 2015. After that, he joined the Signal and Information Processing Laboratory (ISI) at ETH Zurich, where he pursued a PhD degree in Information Theory, which he acquired in 2018.

His research interests lie in the area of zero-error information theory, and multiterminal information theory.

Amos Lapidoth (S'89–M'95–SM'00–F'04) received the B.A. degree in Mathematics (*summa cum laude*, 1986), the B.Sc. degree in Electrical Engineering (*summa cum laude*, 1986), and the M.Sc. degree in Electrical Engineering (1990) all from the Technion–Israel Institute of Technology. He received the Ph.D. degree in Electrical Engineering from Stanford University in 1995. In the years 1995–1999 he was an Assistant and Associate Professor at the department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, and was the KDD Career Development Associate Professor in Communications and Technology. He is now Professor of Information Theory at the Swiss Federal Institute of Technology (ETH) in Zurich, Switzerland. He served in the years 2003–2004 and 2009 as Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY. Dr. Lapidoth's research interests are in Digital Communications and Information Theory. He is the author of the textbook *A Foundation in Digital Communication*, second edition, published by Cambridge University Press in 2017.