Advances in Mathematics of Communications
Volume 10, No. 2, 2016, 333–354
doi:10.3934/amc.2016009

ARBITRARILY VARYING MULTIPLE ACCESS CHANNELS WITH CONFERENCING ENCODERS: LIST DECODING AND FINITE COORDINATION RESOURCES

Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany

Rafael F. Schaefer

Information Theory and Applications Chair
Technische Universität Berlin
Einsteinufer 25, 10587 Berlin, Germany

(Communicated by Simon Litsyn)

Abstract. Communication over channels that may vary in an arbitrary and unknown manner from channel use to channel use is studied. Such channels fall in the framework of *arbitrarily varying channels (AVCs)*, for which it has been shown that the classical deterministic approaches with pre-specified encoder and decoder fail if the AVC is symmetrizable. However, more sophisticated strategies such as *common randomness (CR)* assisted codes or *list decoding* are capable to resolve the ambiguity induced by symmetrizable AVCs. AVCs further serve as the indispensable basis for modeling adversarial attacks such as jamming in information theoretic security related communication problems. In this paper, we study the *arbitrarily varying multiple access channel (AVMAC) with conferencing encoders*, which models the communication scenario with two cooperating transmitters and one receiver. This can be motivated for example by cooperating base stations or access points in future systems. The capacity region of the AVMAC with conferencing encoders is established and it is shown that list decoding allows for reliable communication also for symmetrizable AVMACs. The list capacity region equals the CR-assisted capacity region for large enough list size. Finally, for fixed probability of decoding error the amount of resources, i.e., CR or list size, is quantified and shown to be finite.

1. Introduction

Communication in practical systems always takes place over noisy channels. To model the influence of the noise, there are different approaches. The most common approach is the concept of *discrete memoryless channels (DMCs)*, where the noisy

2010 *Mathematics Subject Classification:* Primary: 94A15, 62B10; Secondary: 68P30.

Key words and phrases: Arbitrarily varying multiple access channel, conferencing encoders, list decoding, coordination resources, capacity region, derandomization.

The work of Holger Boche was supported in part by the German Research Foundation (DFG) under Grant BO 1734/25-1 and in part by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050. The work of Rafael F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. This work was done while R. F. Schaefer was a Post-Doctoral Research Fellow in the Department of Electrical Engineering, Princeton University. Parts of this work were presented at the 2014 IEEE International Conference on Communications, Sydney, Australia [13].

channel is modeled by a known and fixed stochastic matrix describing the transition probabilities of the transmitted and received symbols.

If the channel, i.e., the stochastic matrix, is unknown and further may vary in an arbitrary and unknown manner from channel use to channel use, the concept of *arbitrarily varying channels (AVCs)* [1, 9, 15] provides a suitable and robust framework for such communication scenarios. AVCs not only capture such effects as unknown varying channel conditions, but also serve as an indispensable model of adversarial attacks such as jamming in information theoretic security related communication scenarios.

It has been shown that DMCs and AVCs have completely different behaviors. Considering the criterion of average decoding error, in terms of capacity it does not matter for DMCs if traditional deterministic codes with pre-specified encoder and decoder are used or more sophisticated strategies such as list codes or random codes. On the other hand, for AVCs this actually has a huge impact on the capacity. In particular, the deterministic approach with pre-specified encoder and decoder fails if the AVC is symmetrizable resulting in zero capacity [1, 15]. Roughly speaking, such a channel can simulate a valid input so that it is impossible for the decoder to decide on the correct one. This necessitates more sophisticated strategies which overcome such channel conditions making reliable communication possible also for symmetrizable AVCs.

If *common randomness (CR)* is available at all users as a coordination resource, then they can use CR-assisted codes allowing for reliable communication over symmetrizable channels [1, 9]. Here, encoder and decoder depend on the particular realization of the common randomness which has to be known at all users prior to the transmission. If such a coordination resource is not available, one is interested in alternatives that do not rely on such assumptions. It has been shown that *list decoding* might help to resolve the ambiguity of codewords caused by symmetrizable channels without the help of coordination resources. The capacity of the single-user AVC under list decoding is studied in [10, 19, 24]. Bounds on the list sizes for the arbitrarily varying multiple access channel (AVMAC) are given in [22]. The broadcast channel with certain receiver side information under list decoding is studied in [25]. Recently, the concept of list decoding attracted attention also for error-correction codes [6, 17, 18].

In this paper, we study the *AVMAC with conferencing encoders* under list decoding. We completely characterize the list capacity region for given list size. It either equals its CR-assisted capacity region or else is zero. This is completely characterized by the concept of *symmetrizability* and the list size at the decoder. In particular, if the list size is large enough, i.e., larger than the symmetrizability of the channel, then a deterministic list code achieves the same performance as a CR-assisted code which requires coordination resources available at all users prior to transmission. In these cases the average probability of error is required to vanish asymptotically and, usually, this results in an amount of common randomness which grows unbounded with increasing block length. Finally, it is shown that for fixed but non-vanishing average probability of error, the amount of such resources needed to achieve the capacity is finite, i.e., in particular independent of the block length.

NOTATION. Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters; $\mathbb{N}$ and $\mathbb{R}_+$ denote the sets of positive integers and non-negative real numbers; $I(A;B) =$

$\sum_{a\in\mathcal{A},b\in\mathcal{B}} P_{AB}(a,b)\log\frac{P_{AB}(a,b)}{P_A(a)P_B(b)}$ and $I(A;B|C)=\sum_{c\in\mathcal{C}} P_C(c)I(A;B|C=c)$ are the (conditional) mutual information between the random variables A and B (conditioned on C); $\mathcal{A}^c$, $|\mathcal{A}|$, and $\mathcal{A}\times\mathcal{B}$ are the complement, cardinality, and Cartesian product of the sets $\mathcal{A}$ and $\mathcal{B}$; $\mathbb{P}\{\cdot\}$ is the probability and $\mathcal{P}(\cdot)$ is the set of all probability distributions; $\mathcal{O}(\cdot)$ is the big-O notation; lhs $\coloneqq$ rhs means the value of the right hand side (rhs) is assigned to the left hand side (lhs), lhs $=:$ rhs is defined accordingly.

2. System model

We consider a multiple access channel with two transmitters X, Y and one receiver Z and denote the finite input and output sets by $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$. Further, we introduce a finite state set $\mathcal{S}$. For every $s\in\mathcal{S}$ we define the multiple access channel by the stochastic matrix

$$W(z|x,y,s)\quad\text{for }(x,y,z)\in\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}.$$

Further, for any probability distribution $q\in\mathcal{P}(\mathcal{S})$, we denote the averaged multiple access channel by

$$\overline{W}_q(z|x,y)\coloneqq\sum_{s\in\mathcal{S}} W(z|x,y,s)q(s). \tag{1}$$

The communication is affected by a channel which may vary in an unknown and arbitrary manner from channel use to channel use. To capture such a behavior, we consider state sequences of length n.

Definition 2.1. For a fixed state sequence $s^n\in\mathcal{S}^n$ of length n and input and output sequences $x^n\in\mathcal{X}^n$, $y^n\in\mathcal{Y}^n$, and $z^n\in\mathcal{Z}^n$, the discrete memoryless *multiple access channel (MAC)* is given by

$$W^n(z^n|x^n,y^n,s^n)\coloneqq\prod_{i=1}^n W(z_i|x_i,y_i,s_i).$$

Collecting all stochastic matrices for all possible state sequences yield the arbitrarily varying multiple access channel.

Definition 2.2. The discrete memoryless *arbitrarily varying multiple access channel (AVMAC)* is the family

$$\mathfrak{W}\coloneqq\left\{W^n(\cdot|\cdot,\cdot,s^n):s^n\in\mathcal{S}^n\right\}.$$

In the classical AVMAC setup, none of the transmitters has any knowledge about the message the other one will transmit and the corresponding capacity region is studied in [5, 20]. Here, we study the case where both transmitters can cooperate in the sense that they can exchange limited information using Willems conferencing [30]. Such information can regard the messages to transmit but is not necessarily restricted to them.

Let $\mathcal{M}_1\coloneqq\{1,\ldots,M_{1,n}\}$ and $\mathcal{M}_2\coloneqq\{1,\ldots,M_{2,n}\}$ be the sets of messages of transmitters 1 and 2, respectively, and further $\mathcal{M}\coloneqq\mathcal{M}_1\times\mathcal{M}_2$. Then Willems conferencing can be described as follows.

Definition 2.3. *Willems conferencing* is an iterative protocol. In the first time slot, each transmitter sends some information to the other one. In the subsequent time slots, they send more information taking the information they received in the previous iterations into account. Such a Willems conference terminates after a fixed

number of iterations I. Then, a pair (c_1, c_2) of functions is determined by functions $c_{i,1}, c_{i,2}, ..., c_{i,I}$, $i = 1, 2$ with

$$c_{i,1} : \mathcal{M}_i \to \mathcal{K}_{i,1} \tag{2}$$

and

$$c_{i,k} : \mathcal{M}_i \times \mathcal{K}_{\bar{i},1} \times ... \times \mathcal{K}_{\bar{i},k-1} \to \mathcal{K}_{i,k}$$

for $k = 2, 3, ..., I$ and $\bar{i} = 2$ if $i = 1$ and $\bar{i} = 1$ if $i = 2$. The number of iterations I may be arbitrary but fixed and also $\mathcal{K}_{i,k}$ can be an arbitrary finite set. Thus, the pair (c_1, c_2) is defined by the concatenation of the individual $c_{i,k}$ as

$$(c_1, c_2) : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{K}_1 \times \mathcal{K}_2 \tag{3}$$

with $\mathcal{K}_1 := \mathcal{K}_{1,1} \times ... \times \mathcal{K}_{1,I}$ and $\mathcal{K}_2 := \mathcal{K}_{2,1} \times ... \times \mathcal{K}_{2,I}$.

If the Willems conferencing is unrestricted, an arbitrary amount of information can be exchanged such that both messages are available at both transmitters turning the AVMAC into a single-user AVC. Due to practical reasons we consider only limited exchange capabilities.

Definition 2.4. Assuming a Willems conference pair $(c_1, c_2) : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{K}_1 \times \mathcal{K}_2$ as given in (3) is used for a code of block length n. Then, the conference (c_1, c_2) has conferencing capacities $C_1, C_2 > 0$ if

$$\frac{1}{n} \log |\mathcal{K}_i| \leq C_i, \quad i = 1, 2.$$

We call this an (n, C_1, C_2)-*Willems conference*, whose definition is independent of the number of iterations I.

3. Code concepts and coordination resources

In general, for AVCs it matters whether deterministic codes or random codes are used. In particular, for symmetrizable channels deterministic codes do not suffice to establish reliable communication. Hence, more sophisticated approaches such as random codes must be used [1, 9, 15].

3.1. Deterministic codes.

The deterministic approach relies on pre-specified encoders and decoder as specified in the following.

Definition 3.1. A *deterministic* $(n, M_{1,n}, M_{2,n}, C_1, C_2)$-*code* $\mathcal{C}$ for the AVMAC $\mathfrak{W}$ is a 5-tuple $(c_1, c_2, f_1, f_2, \phi)$ consisting of an (n, C_1, C_2)-Willems conference

$$(c_1, c_2) : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{K}_1 \times \mathcal{K}_2, \tag{4}$$

encoders at transmitters 1 and 2

$$f_1 : \mathcal{M}_1 \times \mathcal{K}_2 \to \mathcal{X}^n \tag{5a}$$

$$f_2 : \mathcal{M}_2 \times \mathcal{K}_1 \to \mathcal{Y}^n, \tag{5b}$$

and a decoder at the receiver

$$\phi : \mathcal{Z}^n \to \mathcal{M}_1 \times \mathcal{M}_2. \tag{6}$$

Such a code implies the following system

$$\left\{(x_{jk}^n, y_{jk}^n, \mathcal{D}_{jk}) : j \in \mathcal{M}_1, k \in \mathcal{M}_2\right\} \tag{7}$$

with $x_{jk}^n = f_1(j, c_2(j, k))$, $y_{jk}^n = f_2(k, c_1(j, k))$, and disjoint decoding sets $\mathcal{D}_{jk} = \{z^n \in \mathcal{Z}^n : \phi(z^n) = (j, k)\}$.

Then for the deterministic code $\mathcal{C}$, the average probability of decoding error for state sequence $s^n \in \mathcal{S}^n$ is given by

$$\bar{e}_n(s^n|\mathcal{C}) \coloneqq \frac{1}{|\mathcal{M}|} \sum_{(j,k)\in\mathcal{M}} W^n(\mathcal{D}_{jk}^c|x_{jk}^n, y_{jk}^n, s^n).$$

Definition 3.2. A rate pair $(R_1, R_2) \in \mathbb{R}_+^2$ is said to be *deterministically achievable* for the AVMAC $\mathfrak{W}$ with conferencing capacities $C_1, C_2 > 0$ if for any $\delta > 0$ there exists an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_{1,n}, M_{2,n}, C_1, C_2)$-codes $\mathcal{C}$ such that for all $n \geq n(\delta)$ we have

$$\frac{1}{n} \log M_{i,n} \geq R_i - \delta, \qquad i = 1, 2,$$

while

$$\max_{s^n\in\mathcal{S}^n} \bar{e}_n(s^n|\mathcal{C}) =: \lambda_n$$

with $\lambda_n \to 0$ as $n \to \infty$. The *deterministic capacity region* $\mathcal{R}_{\mathrm{det}}(C_1, C_2)$ of the AVMAC $\mathfrak{W}$ with conferencing encoders is the set of all achievable rate pairs.

We further need the concept of symmetrizability which is given in the following definition.

Definition 3.3. An AVMAC $\mathfrak{W}$ is called $(\mathcal{X}, \mathcal{Y})$-*symmetrizable* if there exists a stochastic matrix $\sigma : \mathcal{X} \times \mathcal{Y} \to \mathcal{P}(\mathcal{S})$ such that

$$\sum_{s\in\mathcal{S}} W(z|x, y, s)\sigma(s|x', y') = \sum_{s\in\mathcal{S}} W(z|x', y', s)\sigma(s|x, y)$$

holds for all $x, x' \in \mathcal{X}$, $y, y' \in \mathcal{Y}$, and $z \in \mathcal{Z}$. This means, the channel $\widetilde{W}(z|x, y, x', y') = \sum_{s\in\mathcal{S}} W(z|x, y, s)\sigma(s|x', y')$ is symmetric in (x, y) and (x', y') for all $x, x' \in \mathcal{X}$, $y, y' \in \mathcal{Y}$, and $z \in \mathcal{Z}$.

Remark 1. The capacity region of the classical AVMAC without conferencing encoders depend also on so-called $\mathcal{X}$-symmetrizability and $\mathcal{Y}$-symmetrizability conditions that operate only on one input. While these "marginal" conditions are important for the analysis of the AVMAC without conferencing encoders [16], it has been shown that only $(\mathcal{X}, \mathcal{Y})$-symmetrizability is needed to completely characterize the capacity region of the AVMAC with conferencing encoders.

Let $\mathit{\Pi}$ be the set of all probability distributions $p \in \mathcal{P}(\mathcal{U} \times \mathcal{X} \times \mathcal{Y})$, where $\mathcal{U}$ is a finite (auxiliary) set and p further has the form $p(u, x, y) = P_U(u)P_{X|U}(x|u)P_{Y|U}(y|u)$. We define $\overline{\mathcal{R}}(p, q, C_1, C_2)$ consisting of all $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy

$$\begin{aligned} R_1 &\leq I(X; \overline{Z}_q|Y, U) + C_1 \\ R_2 &\leq I(Y; \overline{Z}_q|X, U) + C_2 \\ R_1 + R_2 &\leq \min\{I(X, Y; \overline{Z}_q), I(X, Y; \overline{Z}_q|U) + C_1 + C_2\} \end{aligned}$$

where $\overline{Z}_q$ is the random variable associated with the output of the averaged channel $\overline{W}_q$, $q \in \mathcal{P}(\mathcal{S})$, cf. (1). Then, we set

$$\overline{\mathcal{R}}(C_1, C_2) \coloneqq \bigcup_{p\in\mathit{\Pi}} \bigcap_{q\in\mathcal{P}(\mathcal{S})} \overline{\mathcal{R}}(p, q, C_1, C_2). \tag{8}$$

With this and the concept of symmetrizability, we are able to characterize the deterministic capacity region.

Theorem 3.4 ([26]). *For the deterministic capacity region $\mathcal{R}_{det}(C_1, C_2)$ of the AVMAC $\mathfrak{W}$ with conferencing capacities $C_1, C_2 > 0$ we have*

$$\mathcal{R}_{det}(C_1, C_2) = \overline{\mathcal{R}}(C_1, C_2)$$

if and only if the AVMAC $\mathfrak{W}$ is non-$(\mathcal{X}, \mathcal{Y})$-symmetrizable. If the AVMAC $\mathfrak{W}$ is $(\mathcal{X}, \mathcal{Y})$-symmetrizable, then

$$\mathcal{R}_{det}(C_1, C_2) = \{(0, 0)\}.$$

Remark 2. In addition, it turns out that a one-shot non-iterative Willems-conference is sufficient to achieve capacity, i.e., (3) consists only of the first conference round (2), cf. Definitions 2.3 and 2.4.

Remark 3. Note that the set $\overline{\mathcal{W}} := \{\overline{W}_q(\cdot|\cdot,\cdot) : q \in \mathcal{P}(\mathcal{S})\}$ of all averaged channels (1) can also be interpreted as a compound channel [8, 31]. Then the region $\overline{\mathcal{R}}(C_1, C_2)$ in (8) is actually the capacity region of the corresponding compound MAC with conferencing encoders [28]. Thus, the deterministic capacity region of the AVMAC with conferencing encoders equals the one of a suitable chosen compound MAC if the the channel is non-$(\mathcal{X}, \mathcal{Y})$-symmetrizable. Moreover, this connection is further deepened by the following technique: the classical approach to prove the CR-assisted capacity of the AVMAC is to take a "good" code for the corresponding compound MAC and to convert this code into a CR-assisted code which is also "good" for the AVMAC. This technique is known as *Ahlswede's robustification technqiue* [2, 3].

3.2. COMMON-RANDOMNESS-ASSISTED CODES. Since such a deterministic code as discussed in Section 3.1 with predetermined encoders and decoder fails if the channel is symmetrizable, one is interested in more sophisticated strategies that work well also in this case. This is where the common-randomness-assisted coding strategies come into play.

If the transmitters and receiver have access to a *common randomness (CR)*, then they can use this resource to coordinate their choice of encoders and decoder. This is modeled by a random variable Γ on $\mathcal{G}_n$. Then, the conference (3), encoders (5), and decoder (6) depend all on the particular realization $\gamma \in \mathcal{G}_n$.

Definition 3.5. A *CR-assisted* $(n, M_{1,n}, M_{2,n}, C_1, C_2, \Gamma)$*-code* $\mathcal{C}_{\mathrm{CR}}$ for the AVMAC $\mathfrak{W}$ is a family

$$\big\{\big(c_1(\gamma), c_2(\gamma), f_1(\gamma), f_2(\gamma), \phi(\gamma)\big) : \gamma \in \mathcal{G}_n\big\}$$

together with a random variable Γ uniformly distributed on $\mathcal{G}_n$.

This means $\mathcal{G}_n$ defines a finite set of deterministic $(n, M_{1,n}, M_{2,n}, C_1, C_2)$-codes as given in Definition 3.1. The number of such codes contained in the CR-assisted code $\mathcal{C}_{\mathrm{CR}}$ is then determined by $|\mathcal{G}_n|$. Thus, each realization $\gamma \in \mathcal{G}_n$ indicates which particular code is selected out of the whole ensemble.

Then for the CR-assisted code $\mathcal{C}_{\mathrm{CR}}$, the average probability of decoding error for state sequence $s^n \in \mathcal{S}^n$ becomes

$$\begin{aligned}\bar{e}_{\mathrm{CR},n}(s^n|\mathcal{C}_{\mathrm{CR}}) :=& \frac{1}{|\mathcal{G}_n|}\sum_{\gamma\in\mathcal{G}_n} \bar{e}_n(s^n|\mathcal{C}(\gamma)) \\ =& \frac{1}{|\mathcal{G}_n|}\sum_{\gamma\in\mathcal{G}_n}\frac{1}{|\mathcal{M}|}\sum_{(j,k)\in\mathcal{M}} W^n\big((\mathcal{D}_{jk}(\gamma))^c|x^n_{jk}(\gamma), y^n_{jk}(\gamma), s^n\big).\end{aligned}$$

Definition 3.6. A rate pair $(R_1, R_2) \in \mathbb{R}_+^2$ is said to be *CR-assisted achievable* for the AVMAC $\mathfrak{W}$ with conferencing capacities $C_1, C_2 > 0$ if for any $\delta > 0$ there exists an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_{1,n}, M_{2,n}, C_1, C_2, \Gamma)$-codes $\mathcal{C}_{\mathrm{CR}}$ such that for all $n \geq n(\delta)$ we have

$$\frac{1}{n} \log M_{i,n} \geq R_i - \delta, \qquad i = 1, 2,$$

while

$$\max_{s^n \in \mathcal{S}^n} \bar{e}_{\mathrm{CR},n}(s^n | \mathcal{C}_{\mathrm{CR}}) =: \lambda_{\mathrm{CR},n}$$

with $\lambda_{\mathrm{CR},n} \to 0$ as $n \to \infty$. The *CR-assisted capacity region* $\mathcal{R}_{\mathrm{CR}}(C_1, C_2)$ of the AVMAC $\mathfrak{W}$ with conferencing encoders is the set of all CR-assisted achievable rate pairs.

Theorem 3.7 ([26])**.** *The CR-assisted capacity region $\mathcal{R}_{CR}(C_1, C_2)$ of the AVMAC $\mathfrak{W}$ with conferencing capacities $C_1, C_2 > 0$ is*

$$\mathcal{R}_{CR}(C_1, C_2) = \overline{\mathcal{R}}(C_1, C_2).$$

Thus, if the channel is non-$(\mathcal{X}, \mathcal{Y})$-symmetrizable, then the CR-assisted capacity equals the deterministic capacity, i.e., $\mathcal{R}_{\mathrm{det}}(C_1, C_2) = \mathcal{R}_{\mathrm{CR}}(C_1, C_2) = \overline{\mathcal{R}}(C_1, C_2)$. This gives the quantity $\mathcal{R}_{\mathrm{CR}}(C_1, C_2)$ an operational meaning in the sense that the capacity region can be described by entropic quantities, cf. (8). If the channel is $(\mathcal{X}, \mathcal{Y})$-symmetrizable, the operational meaning of $\overline{\mathcal{R}}(C_1, C_2)$ is still valid for CR-assisted strategies. However, this is no longer true for deterministic strategies as in this case $\mathcal{R}_{\mathrm{det}}(C_1, C_2) = \{(0, 0)\}$ while $\overline{\mathcal{R}}(C_1, C_2) \neq \{(0, 0)\}$.

One question that arises is how much common randomness $\mathcal{G}_n$ is needed to achieve the capacity as given in Theorem 3.7. In particular, it is important to understand whether the amount of common randomness depends on the block length n and how it scales accordingly. Along with this, an important observation for the analysis of list codes is the following.

Remark 4. We know from [26, Lemma 15] that the amount of common randomness that is needed for achieving the CR-assisted capacity region $\mathcal{R}_{\mathrm{CR}}(C_1, C_2)$ of the AVMAC $\mathfrak{W}$ is quadratic in block length. This means for a transmission of block length n, it is sufficient to use a CR-assisted code which consists of n^2 deterministic codes, i.e., $\mathcal{G}_n := \{1, 2, ..., n^2\}$ and $|\mathcal{G}_n| = n^2$, cf. also Definition 3.5.

4. Capacity region under list decoding

The previous discussion reveals the following dilemma: The traditional deterministic approach with pre-specified encoders and decoder only works for non-symmetrizable channels. And unfortunately, many channels of practical relevance fall in the category of symmetrizable channels resulting in zero capacity [15]. On the other hand, CR-assisted codes allow reliable communication also for such channel conditions. But the drawback of such more sophisticated approaches is the fact that they require a strong coordination between encoders and decoder based on common randomness. In particular, the actual realization has to be perfectly known at all users prior to transmission which might be hard to realize in practice especially for multi-user scenarios.

Thus, one is interested in strategies which work well in the case of symmetrizable channels but which do not rely on such coordination resources as common randomness. It has been shown for the single-user AVC that the concept of list decoding

helps to resolve the ambiguity induced by symmetrizable channels [10, 19] without relying on additional coordination resources. In the following we want to analyze list decoding also for the AVMAC with conferencing encoders.

4.1. LIST CODES. While a deterministic decoder ϕ of Definition 3.1 decides on exactly one message pair $(j,k) \in \mathcal{M}_1 \times \mathcal{M}_2$ based on its received signal $z^n \in \mathcal{Z}^n$, a list decoder with list size L maps the received signal into up to L possible message pairs. The list code is specified as follows.

Definition 4.1. A $(n, M_{1,n}, M_{2,n}, C_1, C_2, L)$-*list code* $\mathcal{C}_{\text{list}}$ with list size L is a deterministic $(n, M_{1,n}, M_{2,n}, C_1, C_2)$-code of Definition 3.1 where the deterministic decoder (6) is replaced by a list decoder

$$\phi : \mathcal{Z}^n \to \mathfrak{P}_L(\mathcal{M}_1 \times \mathcal{M}_2)$$

where $\mathfrak{P}_L(\mathcal{M}_1 \times \mathcal{M}_2)$ is the set of all subsets of $\mathcal{M}_1 \times \mathcal{M}_2$ with cardinality at most L.

Similar to (7), such a code implies the system $\{(x_j^n, y_k^n, \mathcal{D}_{jk}) : j \in \mathcal{M}_1, k \in \mathcal{M}_2\}$ where the decoding sets are given by

$$\mathcal{D}_{jk} = \big\{z^n \in \mathcal{Z}^n : (j,k) \in \phi(z^n)\big\}.$$

In particular, due to the list decoding, the decoding sets need not be disjoint and we have $|\{(j,k) : z^n \in \mathcal{D}_{jk}\}| \le L$ so that $\phi(z^n) = \{(j,k) : z^n \in \mathcal{D}_{jk}\}$.

Then for the list code $\mathcal{C}_{\text{list}}$, the probability of decoding error for message pair $(j,k) \in \mathcal{M}_1 \times \mathcal{M}_2$ and $s^n \in \mathcal{S}^n$ is given by

$$\begin{aligned}\bar{e}_{L,n}\big((j,k), s^n | \mathcal{C}_{\text{list}}\big) &:= W^n(\mathcal{D}_{jk}^c | x_{jk}^n, y_{jk}^n, s^n) \\ &= \sum_{z^n : (j,k) \notin \phi(z^n)} W^n(z^n | x_{jk}^n, y_{jk}^n, s^n)\end{aligned}$$

and the average probability of decoding error for $s^n \in \mathcal{S}^n$ is

$$\bar{e}_{L,n}(s^n | \mathcal{C}_{\text{list}}) = \frac{1}{|\mathcal{M}|} \sum_{(j,k) \in \mathcal{M}} \bar{e}_{L,n}\big((j,k), s^n | \mathcal{C}_{\text{list}}\big).$$

Definition 4.2. A rate pair $(R_1, R_2) \in \mathbb{R}_+^2$ is said to be *list achievable* for the AVMAC $\mathfrak{W}$ with conferencing capacities $C_1, C_2 > 0$ and list size L if for any $\delta > 0$ there exists an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_{1,n}, M_{2,n}, C_1, C_2, L)$-list codes $\mathcal{C}_{\text{list}}$ such that for all $n \ge n(\delta)$ we have

$$\frac{1}{n} \log\Big(\frac{M_{i,n}}{L}\Big) \ge R_i - \delta, \qquad i = 1, 2,$$

while

$$\max_{s^n \in \mathcal{S}^n} \bar{e}_{L,n}(s^n | \mathcal{C}_{\text{list}}) =: \lambda_{L,n}$$

with $\lambda_{L,n} \to 0$ as $n \to \infty$. The *list capacity region* $\mathcal{R}_{\text{list}}(C_1, C_2, L)$ of the AVMAC $\mathfrak{W}$ with conferencing encoders is the set of all list achievable rate pairs.

4.2. SYMMETRIZABILITY. For the analysis of the list capacity region, we need a corresponding extension of the concept of symmetrizability given in Definition 3.3. We follow [10, 19] and introduce a refinement which distinguishes different degrees of symmetry.

We say a channel $\widetilde{W}(z|(x_1,y_1),(x_2,y_2),...,(x_t,y_t))$ with input alphabet $(\mathcal{X}\times\mathcal{Y})^t$ and output alphabet $\mathcal{Z}$ is symmetric if for every permutation π on $\{1,2,...,n\}$ we have $\widetilde{W}(z|(x_1,y_1),(x_2,y_2),...,(x_t,y_t)) = \widetilde{W}(z|(x_{\pi(1)},y_{\pi(1)}),...,(x_{\pi(t)},y_{\pi(t)}))$ for all $(x_1,y_1),...,(x_t,y_t)\in(\mathcal{X}\times\mathcal{Y})$ and $z\in\mathcal{Z}$. This leads to the following definition.

Definition 4.3. For any $t\geq 1$, an AVMAC $\mathfrak{W}$ is t-$(\mathcal{X},\mathcal{Y})$-*symmetrizable* if there exists a stochastic matrix $\sigma:(\mathcal{X}\times\mathcal{Y})^t\to\mathcal{P}(\mathcal{S})$ such that

$$\begin{aligned}&\widetilde{W}\big(z|(x_0,y_0),(x_1,y_1),...,(x_t,y_t)\big)\\ &\qquad:=\sum_{s\in\mathcal{S}}W(z|x_0,y_0,s)\sigma(s|(x_1,y_1),...,(x_t,y_t))\end{aligned}\tag{9}$$

is symmetric in $(x_0,y_0),(x_1,y_1),...,(x_t,y_t)$ for all $(x_0,y_0),(x_1,y_1),...,(x_t,y_t)\in\mathcal{X}\times\mathcal{Y}$ and $z\in\mathcal{Z}$. For convenience, we take all AVMACs to be 0-$(\mathcal{X},\mathcal{Y})$-symmetrizable.

Intuitively, a t-$(\mathcal{X},\mathcal{Y})$-symmetrizable channel can be interpreted as a channel where the state sequence can simulate t replicas of the channel input. In addition, from the definition it follows that if an AVMAC is t-$(\mathcal{X},\mathcal{Y})$-symmetrizable, then it is also t'-$(\mathcal{X},\mathcal{Y})$-symmetrizable for all $0\leq t'\leq t$.

Similarly as for the deterministic approach, the $\mathcal{X}$-symmetrizability and $\mathcal{Y}$-symmetrizability conditions can also be extended to the list case as in (9). But again, the "joint" t-$(\mathcal{X},\mathcal{Y})$-symmetrizability condition suffices to completely characterize the capacity region, cf. also Remark 1.

4.3. LIST CAPACITY REGION. Now we are in the position to characterize the list capacity region of the AVMAC with conferencing encoders.

Theorem 4.4. *For the list capacity region $\mathcal{R}_{list}(C_1,C_2,L)$ for the AVMAC $\mathfrak{W}$ with conferencing capacities $C_1,C_2>0$ and list size L we have*

$$\mathcal{R}_{list}(C_1,C_2,L)=\mathcal{R}_{CR}(C_1,C_2)=\overline{\mathcal{R}}(C_1,C_2)\tag{10}$$

if and only if the AVMAC $\mathfrak{W}$ is non-L-$(\mathcal{X},\mathcal{Y})$-symmetrizable. If the AVMAC $\mathfrak{W}$ is L-$(\mathcal{X},\mathcal{Y})$-symmetrizable, then

$$\mathcal{R}_{list}(C_1,C_2,L)=\{(0,0)\}.\tag{11}$$

Proof. We first prove the second part (11) by contradiction. Therefore, we assume that $\mathcal{R}_{\text{list}}(C_1,C_2,L)\neq\{(0,0)\}$ so that there must be a rate pair $(R,0)$ or $(0,R)$ that is achievable. If the rate is small in the sense it satisfies $R<\min\{C_1,C_2\}$, then the rate pair $(\frac{R}{2},\frac{R}{2})$ is achievable as well. Indeed, if the rate is small enough (i.e. smaller than the conferencing capacities), each transmitter can completely inform the other transmitter about the own message making both messages at both transmitters available.

This allows interpreting both inputs x and y of the AVMAC as a joint input (x,y) so that we obtain a corresponding single-user AVC. Then, the L-$(\mathcal{X},\mathcal{Y})$-symmetrizability becomes the classical L-symmetrizability of the single-user AVC [10, 19]. Moreover, as a result, the communication problem becomes an equivalent single-user AVC list coding problem whose single-user capacity is greater than zero. But we know that if a single-user AVC is L-symmetrizable, then the corresponding

single-user list capacity is zero which contradicts the assumption of non-zero single-user capacity proving (11).

Next we prove the remaining first part (10). We assume $\mathcal{R}_{\mathrm{CR}}(C_1, C_2) \neq \{(0,0)\}$, since otherwise there is nothing to prove. We have to show that if the AVMAC $\mathfrak{W}$ is non-L-$(\mathcal{X}, \mathcal{Y})$-symmetrizable, then using list codes $\mathcal{C}_{\mathrm{list}}$ we achieve the same rates as if we use CR-assisted codes $\mathcal{C}_{\mathrm{CR}}$, cf. (10). This observation already suggests itself to incorporate CR-assisted codes within the list coding as done by the following protocol.

To make use of CR-assisted codes, there is the need of common randomness at transmitters and receiver, cf. Section 3.2. As this coordination resource is not available a priori, we have to create it prior to the transmission of the messages. This has to be done carefully in such a way that we do not "waste" too much communication resources which would result in a loss of rates for the subsequent transmission of the actual messages.

Fortunately, from [26, Lemma 15], cf. also Remark 4, we know that the amount of CR needed for a capacity-achieving CR-assisted code is quadratic in block length. Thus, first transmitter 1 or 2 creates a $\gamma \in \mathcal{G}_n \coloneqq \{1, 2, ..., n^2\}$ uniformly and informs the other transmitter about the particular realization $\gamma \in \mathcal{G}_n$ during the Willems-conference. As for transmission of block length n we need $|\mathcal{G}_n| = n^2$ common randomness, the conference resources spent for informing the other transmitter is of order $\mathcal{O}(\log n)$ so that $n/\mathcal{O}(\log n) \to 0$ as $n \to \infty$. Thus, the resources spent for informing are negligible and do not reduce the available conferencing resources.

After the conference, $\gamma \in \mathcal{G}_n$ is available at both transmitters and it remains to provide the receiver enough information about $\gamma \in \mathcal{G}_n$ to properly select the decoding sets. This is done in a similar fashion by spending a negligible amount of resources. Therefore, prior to the transmission of the actual messages, the transmitters uses a list code $\mathcal{C}_{\mathrm{list}}$ with list size L. Again, as $|\mathcal{G}_n| = n^2$, the channel uses needed for transmission of $\gamma \in \mathcal{G}_n$ is of order $l_n = \mathcal{O}(\log n)$ and therewith negligible. That such a single-user code exists achieving positive rate is guaranteed by the fact that the AVMAC $\mathfrak{W}$ is non-L-$(\mathcal{X}, \mathcal{Y})$-symmetrizable. Concatenated on that list code, we use a CR-assisted code of block length n. This is possible as the particular realization $\gamma \in \mathcal{G}_n$ is available at both transmitters and, further, the receiver has a list of size up to L of possible realizations including the one used by the transmitters.

Having this heuristic outline of the protocol in mind, we present formal definitions and carry out the precise analysis of the decoding error. To transmit the message pair $(j,k) \in \mathcal{M}_1 \times \mathcal{M}_2$ having $\gamma \in \mathcal{G}_n$ available, transmitters 1 and 2 transmit the concatenated codewords

$$x_{jk}^{l_n+n}(\gamma) = \big(x_\gamma^{l_n}, x_{jk}^n(\gamma)\big) \quad \text{and} \quad y_{jk}^{l_n+n}(\gamma) = \big(y_\gamma^{l_n}, y_{jk}^n(\gamma)\big) \tag{12}$$

where $x_\gamma^{l_n}$ and $y_\gamma^{l_n}$ are codewords of a single-user list code to inform the receiver about $\gamma \in \mathcal{G}_n$. As $|\mathcal{G}_n| = n^2$, we have $l_n = \mathcal{O}(\log n)$ so that $l_n/n \to 0$ as $n \to \infty$ which means that there will be no loss in overall rate for transmission of messages $(j,k) \in \mathcal{M}_1 \times \mathcal{M}_2$.

The signal $z^{l_n+n} = (z^{l_n}, z^n) \in \mathcal{Z}^{l_n+n}$ is received and the receiver uses a list decoder with list size L to obtain a list $\{\gamma_1, ..., \gamma_{L'}\}$ with $L' \leq L$, of possible realizations from the first part $z^{l_n} \in \mathcal{Z}^{l_n}$, i.e.,

$$\phi_1(z^{l_n}) = \big\{\gamma : z^{l_n} \in \mathcal{D}_\gamma\big\}.$$

Based on this list, the receiver creates a list decoder for the messages $(j,k) \in \mathcal{M}_1 \times \mathcal{M}_2$ transmitted in the second part $z^n \in \mathcal{Z}^n$, i.e.,

$$\phi_2(z^n) = \big\{(j,k) : \exists\, \gamma \in \phi_1(z^{l_n}) \text{ and } z^n \in \mathcal{D}_{jk}(\gamma)\big\}.$$

Thus, for any $z^{l_n+n} \in \mathcal{Z}^{l_n+n}$ let $\gamma_1, ..., \gamma_{L'} \in \mathcal{G}_n$ with $L' \le L$ the list $\phi_1(z^{l_n}) = \{\gamma_1, ..., \gamma_{L'}\}$, the constructed list decoder

$$\begin{aligned}\phi(z^{l_n+n}) &= \big(\phi_1(z^{l_n}), \phi_2(z^n)\big)\\ &= \big\{(\gamma,j,k) : \gamma \in \{\gamma_1, ..., \gamma_{L'}\} \text{ and } z^n \in \mathcal{D}_{jk}(\gamma)\big\}\end{aligned}$$

defines a valid list decoder with list size not greater than L as required in Definition 4.1.

Next we analyze the decoding error performance. The channel $W(z|x,y,s)$ is non-L-$(\mathcal{X},\mathcal{Y})$-symmetrizable by assumption. Then there exists a (small) rate $R < \min\{C_1, C_2\}$ so that this rate is achievable for the single-user interpretation of this channel with joint input $(x,y) \in \mathcal{X} \times \mathcal{Y}$, cf. also corresponding discussion of the proof of (11) in the beginning. In more detail, let $\lambda_1 \in (0,1)$ arbitrary and set

$$l_n := \frac{2}{R} \log\Big(\frac{n}{L}\Big)$$

(since $R = \frac{1}{l_n}\log(\frac{n^2}{L})$). Then we know from the single-user AVC under list decoding [10, 19] that there exists a $n_1 = n_1(\lambda_1)$ such that for all $n \ge n_1$ there exists a list code

$$\big\{\big((x_\gamma^{l_n}, y_\gamma^{l_n}), \mathcal{D}_\gamma\big) : \gamma \in \{1, ..., n^2\}\big\}$$

of length l_n such that the average probability of error satisfies

$$\frac{1}{n^2} \sum_{\gamma \in \{1,...,n^2\}} W^{l_n}\big(\mathcal{D}_\gamma^c | (x_\gamma^{l_n}, y_\gamma^{l_n}), s^{l_n}\big) \le \lambda_1 \tag{13}$$

for all $s^{l_n} \in \mathcal{S}^{l_n}$.

Next, we want to show that the error probability

$$\begin{aligned}\bar{e}_{L,n}(s^{l_n+n}|\mathcal{C}_{\text{list}}) = \frac{1}{n^2}\frac{1}{|\mathcal{M}|} &\sum_{\gamma \in \{1,...,n^2\}} \sum_{(j,k) \in \mathcal{M}}\\ &\times \sum_{\substack{z^{l_n+n}:\\ (\gamma,j,k) \notin \phi(z^{l_n+n})}} W^{l_n+n}\big(z^{l_n+n} | x_{jk}^{l_n+n}(\gamma), y_{jk}^{l_n+n}(\gamma), s^{l_n+n}\big)\end{aligned} \tag{14}$$

of the final concatenated list code is small as well for all $s^{l_n+n} \in \mathcal{S}^{l_n+n}$, i.e.,

$$\max_{s^{l_n+n} \in \mathcal{S}^{l_n+n}} \bar{e}_{L,n}(s^{l_n+n}|\mathcal{C}_{\text{list}}) \le \lambda. \tag{15}$$

Now, if $(\gamma,j,k) \notin \phi(z^{l_n+n})$, then either a) $\gamma \notin \phi_1(z^{l_n})$ or b) $\gamma \in \phi_1(z^{l_n})$ and we have $z^n \notin \mathcal{D}_{jk}(\gamma_i)$ for all $\gamma_i \in \phi_1(z^{l_n})$. Accordingly, we define the error events

$$\begin{aligned}\mathcal{E}_1(\gamma) &:= \big\{z^{l_n+n} : \gamma \notin \phi_1(z^{l_n})\big\}\\ \mathcal{E}_2(\gamma,j,k) &:= \big\{z^{l_n+n} : \gamma \in \phi_1(z^{l_n}) \text{ and } \forall\, \gamma_i \in \phi_1(z^{l_n}) \text{ we have } z^n \notin \mathcal{D}_{jk}(\gamma_i)\big\}\end{aligned}$$

so that

$$\big\{z^{l_n+n} : (\gamma,j,k) \notin \phi(z^{l_n+n})\big\} \subset \mathcal{E}_1(\gamma) \cup \mathcal{E}_2(\gamma,j,k).$$

With this, the average probability of error in (14) can be bounded from above by

$$\begin{aligned}\bar{e}_{L,n}(s^{l_n+n}|\mathcal{C}_{\text{list}}) \leq \frac{1}{n^2}\frac{1}{|\mathcal{M}|}\sum_{\gamma\in\{1,\dots,n^2\}}\sum_{(j,k)\in\mathcal{M}} \\ \times\Bigg(\sum_{z^{l_n+n}\in\mathcal{E}_1(\gamma)} W^{l_n+n}\big(z^{l_n+n}|x_{jk}^{l_n+n}(\gamma),y_{jk}^{l_n+n}(\gamma),s^{l_n+n}\big) \\ +\sum_{z^{l_n+n}\in\mathcal{E}_2(\gamma,j,k)} W^{l_n+n}\big(z^{l_n+n}|x_{jk}^{l_n+n}(\gamma),y_{jk}^{l_n+n}(\gamma),s^{l_n+n}\big)\Bigg)\end{aligned}$$

where we bound both terms individually. For the first term we observe that

$$\begin{aligned}\sum_{z^{l_n+n}\in\mathcal{E}_1(\gamma)} W^{l_n+n}\big(z^{l_n+n}|x_{jk}^{l_n+n}(\gamma),y_{jk}^{l_n+n}(\gamma),s^{l_n+n}\big) \\ = \sum_{z^{l_n}:\gamma\notin\phi_1(z^{l_n})} W^{l_n}\big(z^{l_n}|x_\gamma^{l_n},y_\gamma^{l_n},s^{l_n}\big)\end{aligned}$$

where the equality follows from the concatenated structure of the codewords (12) and the fact that the error event $\mathcal{E}_1(\gamma)$ only depends on the first part. Thus, by (13) we end up with

$$\begin{aligned}\frac{1}{n^2}\frac{1}{|\mathcal{M}|}\sum_{\gamma\in\{1,\dots,n^2\}}\sum_{(j,k)\in\mathcal{M}}\sum_{z^{l_n}:\gamma\notin\phi_1(z^{l_n})} W^{l_n}\big(z^{l_n}|x_\gamma^{l_n},y_\gamma^{l_n},s^{l_n}\big) \\ = \frac{1}{n^2}\sum_{\gamma\in\{1,\dots,n^2\}} W^{l_n}\big(\mathcal{D}_\gamma^c|x_\gamma^{l_n},y_\gamma^{l_n},s^{l_n}\big) \leq \lambda_1.\end{aligned}$$

For the second event we observe that if $z^{l_n+n}\in\mathcal{E}_2(\gamma,j,k)$, then we have $\gamma\in\phi_1(z^{l_n})$ and $z^n\notin\mathcal{D}_{jk}(\gamma)$ so that

$$\mathcal{E}_2(\gamma,j,k)\subset\big\{z^{l_n+n}:\gamma\in\phi_1(z^{l_n}) \text{ and } z^n\notin\mathcal{D}_{jk}(\gamma)\big\}.$$

With this we obtain for the second term

$$\begin{aligned}\sum_{z^{l_n+n}\in\mathcal{E}_2(\gamma,j,k)} W^{l_n+n}\big(z^{l_n+n}|x_{jk}^{l_n+n}(\gamma),y_{jk}^{l_n+n}(\gamma),s^{l_n+n}\big) \\ \leq \sum_{\substack{z^{l_n+n}:\gamma\in\phi_1(z^{l_n})\\ \text{and } z^n\notin\mathcal{D}_{jk}(\gamma)}} W^{l_n+n}\big(z^{l_n+n}|x_{jk}^{l_n+n}(\gamma),y_{jk}^{l_n+n}(\gamma),s^{l_n+n}\big) \\ \leq \sum_{z^n:z^n\notin\mathcal{D}_{jk}(\gamma)} W^n\big(z^n|x_{jk}^n(\gamma),y_{jk}^n(\gamma),s^n\big) \\ = W^n\big(\mathcal{D}_{jk}^c(\gamma)|x_{jk}^n(\gamma),y_{jk}^n(\gamma),s^n\big)\end{aligned}$$

where the last inequality follows from the concatenated structure of the codewords (12) and the last equality from the definition of the decoding sets of a CR-assisted code. Thus,

$$\frac{1}{n^2}\frac{1}{|\mathcal{M}|}\sum_{\gamma\in\{1,\dots,n^2\}}\sum_{(j,k)\in\mathcal{M}} W^n\big(\mathcal{D}_{jk}^c(\gamma)|x_{jk}^n(\gamma),y_{jk}^n(\gamma),s^n\big)\leq\lambda_1$$

since it is a "good" CR-assisted code according to Definition 3.5. Since $\lambda_1\in(0,1)$ is arbitrary, we can choose λ_1 such that it satisfies $2\lambda_1<\lambda$ which proves (15). Since the rate pair (R_1,R_2) in the CR-assisted code was arbitrary, the achievability is shown so that $\mathcal{R}_{\text{list}}(C_1,C_2,L)\supseteq\mathcal{R}_{\text{CR}}(C_1,C_2)$.

The converse, i.e., $\mathcal{R}_{\text{list}}(C_1, C_2, L) \subseteq \mathcal{R}_{\text{CR}}(C_1, C_2)$, follows immediately by observing that $\mathcal{R}_{\text{CR}}(C_1, C_2)$ remains the same for list decoding similarly as for the single-user AVC [10, 19] or the AVMAC (without conferencing encoders) [22]. □

5. Finite resources

The previous considerations and in particular from [26] we know that for any rate pair $(R_1, R_2) \in \mathcal{R}_{\text{CR}}(C_1, C_2)$ there exists a CR-assisted $(n, M_{1,n}, M_{2,n}, C_1, C_2, \Gamma)$-code $\mathcal{C}_{\text{CR}}$ whose average probability goes exponentially fast to zero [26], i.e.,

$$\max_{s^n \in \mathcal{S}^n} \frac{1}{|\mathcal{G}_n|} \sum_{\gamma \in \mathcal{G}_n} \bar{e}_n(s^n | \mathcal{C}(\gamma)) \leq e^{-n\epsilon}. \tag{16}$$

Unfortunately, we know that for this we need common randomness whose amount tends to infinity for increasing block length n, cf. Theorem 3.7, Remark 4, and [26]. Therefore we ask if it is possible to control the amount of needed resources and to achieve the same rates with a fixed amount of CR (i.e. independent of the block length n) when we allow for a fixed but non-vanishing probability of error. This is an interesting and important question insofar as one is interested to know if it is possible to de-randomize such random coding strategies to obtain deterministic codes.

The following result provides an answer to this question. For this purpose, let $\mathcal{R}_{\text{CR}}(\lambda, C_1, C_2)$ denote the CR-assisted region $\mathcal{R}_{\text{CR}}(C_1, C_2)$ where we additionally allow for a non-vanishing probability of error λ.

Theorem 5.1. *Let $\lambda \in (0,1)$ be arbitrary. Then for every $(R_1, R_2) \in \mathcal{R}_{CR}(C_1, C_2)$, there exists a fixed L such that*

$$(R_1, R_2) \in \mathcal{R}_{CR}(\lambda, C_1, C_2)$$

with Γ is defined on $\mathcal{G}_n$ with $|\mathcal{G}_n| = L$.

Proof. Let $\lambda \in (0,1)$ and $\alpha > 0$ be arbitrary but fixed. Then for any $(R_1, R_2) \in \mathcal{R}_{\text{CR}}(C_1, C_2)$ we know from Theorem 3.7 that there is a CR-assisted code $\mathcal{C}_{\text{CR}}$ such that the error probability satisfies (16). Thus, the probability that for finite $|\mathcal{G}_n| = L$ and fixed $s^n \in \mathcal{S}^n$ this is greater than λ is

$$\begin{aligned}\mathbb{P}\Big\{\frac{1}{L}\sum_{i=1}^{L} \bar{e}_n(s^n|\mathcal{C}(i)) \geq \lambda\Big\} &\leq \mathbb{P}\Big\{\exp\big(\alpha \sum_{i=1}^{L} \bar{e}_n(s^n|\mathcal{C}(i))\big) \geq \exp(\alpha\lambda L)\Big\} \\ &\leq \exp(-\alpha\lambda L) \prod_{i=1}^{L} \mathbb{E}\big[\exp\big(\alpha \bar{e}_n(s^n|\mathcal{C}(i))\big)\big].\end{aligned}$$

By the fact that $\bar{e}_n(s^n|\mathcal{C}(i)) \leq 1$ always holds and by standard arguments, cf. also [4], we obtain for the expectation

$$\begin{aligned}\mathbb{E}\big[\exp\big(\alpha \bar{e}_n(s^n|\mathcal{C}(i))\big)\big] &= \mathbb{E}\Big[\sum_{k=0}^{\infty} \frac{\big(\alpha \bar{e}_n(s^n|\mathcal{C}(i))\big)^k}{k!}\Big] \\ &\leq \mathbb{E}\Big[\sum_{k=1}^{\infty} \frac{\alpha^k}{k!} \bar{e}_n(s^n|\mathcal{C}(i)) + 1\Big] \\ &\leq 1 + \Big(\sum_{k=1}^{\infty} \frac{\alpha^k}{k!}\Big) e^{-n\epsilon}\end{aligned}$$

$$\begin{aligned} &= 1 + e^{-n\epsilon}(e^{\alpha} - 1) \\ &< 1 + \exp(-n\epsilon + \alpha) \end{aligned}$$

so that

$$\mathbb{P}\Big\{ \exp\big(\alpha \sum_{i=1}^{L} \bar{e}_n(s^n|\mathcal{C}(i))\big) \geq \exp(\alpha\lambda L) \Big\} \leq \exp(-\alpha\lambda L)\big(1 + \exp(-n\epsilon + \alpha)\big)^L.$$

Now, taking all state sequences $s^n \in \mathcal{S}^n$ into account yields

$$\begin{aligned} &\mathbb{P}\Big\{ \exp\big(\alpha \sum_{i=1}^{L} \bar{e}_n(s^n|\mathcal{C}(i))\big) \geq \exp(\alpha\lambda L) \text{ for some } s^n \in \mathcal{S}^n \Big\} \\ &\quad \leq \exp(-\alpha\lambda L)\big(1 + \exp(-n\epsilon + \alpha)\big)^L \exp(n \ln |\mathcal{S}|) \\ &\quad \leq \exp(-n\epsilon\lambda L + \ln 2L + n \ln |\mathcal{S}|) \\ &\quad = \exp\big(- n\epsilon\lambda\big(L - \big(\tfrac{\ln 2}{n\epsilon\lambda} + \tfrac{\ln |\mathcal{S}|}{\epsilon\lambda}\big)\big)\big) \end{aligned} \tag{17}$$

where the second step follows with the choice $\alpha = n\epsilon$.

Now, if we choose

$$L > \underline{L} := \frac{1}{\epsilon\lambda} \ln |\mathcal{S}|,$$

then the probability that the average probability of error of the constructed code is smaller than the required λ is

$$\mathbb{P}\Big\{ \frac{1}{L} \sum_{i=1}^{L} \bar{e}_n(s^n|\mathcal{C}(i)) < \lambda \text{ for all } s^n \in \mathcal{S}^n \Big\} \underset{n\to\infty}{\longrightarrow} 1$$

exponentially fast as given by (17). □

This establishes a *sufficient condition* on how large the finite amount of resources must be to achieve the whole region $\mathcal{R}_{\mathrm{CR}}(\lambda, C_1, C_2)$ (with non-vanishing probability of error λ).

Corollary 1. *For any $\lambda \in (0,1)$, there exists a CR-assisted $(n, M_{1,n}, M_{2,n}, C_1, C_2, \Gamma)$-code $\mathcal{C}_{CR}$ with $|\mathcal{G}_n| = L$ that achieves all rate pairs $(R_1, R_2) \in \mathcal{R}_{CR}(\lambda, C_1, C_2)$ if*

$$L > \underline{L} = \frac{1}{\epsilon\lambda} \ln |\mathcal{S}|.$$

Next we want to establish also a *necessary* condition on the minimal amount of common randomness.

Theorem 5.2. *Let the AVMAC $\mathfrak{W}$ be $(\mathcal{X}, \mathcal{Y})$-symmetrizable and let $\lambda \in (0,1)$ arbitrary but fixed. Then for every rate pair $(R_1, R_2) \in \mathcal{R}_{CR}(\lambda, C_1, C_2)$ with $R_1, R_2 > 0$, the amount of resources L has to satisfy*

$$L > \frac{1}{2\lambda}.$$

Proof. Let $\lambda \in (0,1)$ be arbitrary but fixed and $(R_1, R_2) \in \mathcal{R}_{\mathrm{CR}}(\lambda, C_1, C_2)$. Let $\tau \in (0, 1/2)$ be arbitrary. Then, for an $(\mathcal{X}, \mathcal{Y})$-symmetrizable AVMAC $\mathfrak{W}$, it holds for all deterministic codes $\mathcal{C}$ that

$$\max_{s^n \in \mathcal{S}^n} \bar{e}_n(s^n|\mathcal{C}) \geq \frac{1}{2} - \frac{1}{|\mathcal{M}|}$$

for rates $(R_1, R_2) \in \mathcal{R}_{\mathrm{CR}}(\lambda, C_1, C_2)$ with $R_1, R_2 > 0$. This can be easily shown by extending the results from [15] and [26].

Now, for $n \geq n_0 = n_0(R_1, R_2)$ sufficiently large, let $\mathcal{C}(i)$, $i \in \{1, ..., L\}$, be L deterministic codes with probability of error not greater than λ. Then there exists an $n_1 = n_1(\tau, R_1, R_2)$ with $|\mathcal{M}| > 1/\tau$ so that for all $n \geq n_1$ we have

$$\begin{aligned}\lambda &\geq \max_{s^n \in \mathcal{S}^n} \frac{1}{L} \sum_{i=1}^{L} \bar{e}_n(s^n | \mathcal{C}(i)) \\ &\geq \max_{s^n \in \mathcal{S}^n} \frac{1}{L} \bar{e}_n(s^n \mathcal{C}(1)) \geq \frac{1}{L}\Big(\frac{1}{2} - \tau\Big).\end{aligned}$$

Thus, we have for all $n \geq \max\{n_0, n_1\}$

$$L \geq \Big(\frac{1}{2} - \tau\Big)\frac{1}{\lambda}. \tag{18}$$

Since (18) holds for all $\tau \in (0, 1/2)$, we get $L > \frac{1}{2\lambda}$ for $\tau \to 0$ which proves the theorem. □

Remark 5. From Theorem 5.1 we know that if $L > \frac{1}{\epsilon\lambda} \ln |\mathcal{S}|$ then there exists CR-assisted codes $\mathcal{C}_{\mathrm{CR}}$ with finite $L = |\mathcal{G}_n|$ that achieves the desired performance for symmetrizable channels. From Theorem 5.2 we further know that $L > \frac{1}{2\lambda}$ is necessary meaning that for $L \leq \frac{1}{2\lambda}$ no $\mathcal{C}_{\mathrm{CR}}$ with finite L is possible. Unfortunately, there is a gap between these two bounds so that it is open to characterize the minimal CR in general. Closing this gap is an interesting open problem as it is closely related to question of de-randomization of randomized strategies.

Remark 6. We want to note that such a CR-assisted code $\{(x_{jk}^n(i), y_{jk}^n(i), \mathcal{D}_{jk}(i)) : i \in \{1, ..., L\}, (j,k) \in \mathcal{M}\}$, cf. (7) and Definition 3.5, can be converted into a deterministic list code

$$\big\{\big(x_{jk}^n(i), y_{jk}^n(i), \mathcal{D}_{jk}(i)\big) : (i,j,k) \in \{1, ..., L\} \times \mathcal{M}\big\}$$

with list size L as constructed in Section 4, cf. also [4] for a corresponding discussion on the single-user case.

The previous discussion presents a way how CR-assisted codes can be used to construct suitable list codes. Due to this construction, the needed list size at the receiver depends on the targeted probability of error. This reveals the following interesting observation. Thereby, the list sizes determined by Theorems 5.1 and 5.2 might be greater than the actually symmetrizability of the channel. Already Ahlswede conjectured in [4] that this might not be optimal. In fact, this list size might also be greater than the resulting list size due the strategy of Theorem 4.4. Thus, a list code solely created by a CR-assisted code as in Remark 6 might not suffice to achieve the optimal performance. Interestingly, on the other hand, the strategy of Theorem 4.4 given by a "bad" list code with arbitrary small rate in combination with a "good" CR-assisted code is optimal in the sense that it achieves the minimal needed list size.

In the following section, we will further analyze this with the help of examples of AVMACs with binary inputs and output.

6. Sub-optimality of list codes created by CR-assisted codes

Here we want to address the question if list codes solely created by CR-assisted codes are "good" codes in terms of list size. It will be shown that even for binary

AVMACs such codes are suboptimal. In fact, for binary AVMACs with conferencing encoders we will show that for every L there is a channel that is L-$(\mathcal{X},\mathcal{Y})$-symmetrizable. On the other hand, for every AVMAC (with finite $\mathcal{S}$) there exists an L such that this channel is non-L-$(\mathcal{X},\mathcal{Y})$-symmetrizable. This implies that list decoders with list size L are sufficient to achieve arbitrary small decoding errors. On the hand, CR-assisted strategies result in list codes where the list size depends on the chosen decoding error λ. Thus, list codes solely created by CR-assisted codes are suboptimal which confirms the conjecture given by Ahlswede and Cai in [4] for AVMACs with conferencing encoders.

6.1. GENERAL AVMACS. Next we show that list codes which are solely created by CR-assisted codes are always suboptimal in terms of list size (if the channel is $(\mathcal{X},\mathcal{Y})$-symmetrizable). For this purpose, we define

$$\overline{R} \coloneqq \min_{q\in\mathcal{P}(\mathcal{S})} \max_{p\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})} I(X,Y;\overline{Z}_q)$$

with X and Y the input random variables according to the distribution $p\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})$ and $\overline{Z}_q$ the output random variable of the averaged channel $\overline{W}_q$, $q\in\mathcal{P}(\mathcal{S})$, cf. (1). Since the mutual information term $I(X,Y;\overline{Z}_q)$ is concave in $p\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})$ and convex in $\overline{W}_q$, $q\in\mathcal{P}(\mathcal{S})$, we have $\overline{R} = \max_{p\in\mathcal{P}(\mathcal{X}\times\mathcal{Y})}\min_{q\in\mathcal{P}(\mathcal{S})} I(X,Y;\overline{Z}_q)$. If $\overline{R}=0$, then the capacity region of the AVMAC with conferencing encoders consists only of the rate point $(0,0)$. We obtain the following result.

Theorem 6.1. *Let $C_1,C_2>0$. If $\overline{R}>0$ and*

$$L > \frac{\ln|\mathcal{S}|}{\overline{R}} \tag{19}$$

with $\mathcal{S}$ finite state set, then $\mathcal{R}_{list}(C_1,C_2,L) = \mathcal{R}_{CR}(C_1,C_2)$, i.e., all CR-assisted rate pairs are list achievable with list size L.

Proof. To prove the desired result we make use of [10]. If (19) is satisfied, then the corresponding single-user AVC with joint input (x,y) is list decodable with list size L. Following the result given in Section 4, based on this we can construct a list code with list size L for the AVMAC with conferencing encoders, which achieves a positive rate for both transmitters. Consequently, the whole region $\mathcal{R}_{\mathrm{CR}}(C_1,C_2)$ is list achievable with list size L. □

Remark 7. The result shows that every AVMAC with finite state set $\mathcal{S}$ is list decodable, for which (19) provides a sufficient condition on the needed list size (which of course depends on the particular AVMAC, i.e., $|\mathcal{S}|$ and $\overline{R}$). Unfortunately, a upper bound on the list size is not known.

Remark 8. Moreover, the result shows that list codes, which are constructed from CR-assisted codes, are never optimal in the sense of list size.

6.2. CLASSES OF BINARY AVMACS. Let $\mathcal{X}$, $\mathcal{Y}$, $\hat{\mathcal{X}}$, $\mathcal{Z}$, and $\mathcal{S}$ be finite input, output, and state sets with $|\mathcal{X}|=|\mathcal{Y}|=|\hat{\mathcal{X}}|=|\mathcal{Z}|=|\mathcal{S}|=2$. Now let

$$g:\mathcal{X}\times\mathcal{Y}\to\hat{\mathcal{X}}$$

be a non-trivial (deterministic) function so that $\mathrm{range}(g)=\hat{\mathcal{X}}=\{0,1\}$, i.e., the function g is not constant. Then

$$\big\{W(z|\hat{x},s)\big\}_{z\in\mathcal{Z},\hat{x}\in\hat{\mathcal{X}},s\in\mathcal{S}} \tag{20}$$

defines an AVC (with binary input, output, and state set $\mathcal{S}=\{0,1\}$).

Definition 6.2. For the AVC defined in (20) let the associated AVMAC be given by

$$W_g(z|x,y,s) \coloneqq W(z|g(x,y),s)$$

for $z \in \mathcal{Z}$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $s \in \mathcal{S}$.

According to Definition 4.3 we say that the AVMAC W_g is L-$(\mathcal{X},\mathcal{Y})$-*symmetrizable* if there exists a channel $\sigma : (\mathcal{X},\mathcal{Y})^L \to \mathcal{P}(\mathcal{S})$ such that

$$\begin{aligned}\widetilde{W}_g\big(z|(x_0,y_0),(x_1,y_1),...,(x_L,y_L)\big)\\ \coloneqq \sum_{s\in\mathcal{S}} W_g(z|x_0,y_0,s)\sigma(s|(x_1,y_1),...,(x_L,y_L))\end{aligned}$$

is a symmetric function. This means for all permutations $\pi : \{1,...,L+1\} \to \{1,...,L+1\}$ we have

$$\begin{aligned}\widetilde{W}_g\big(z|(x_0,y_0),...,(x_L,y_L)\big)\\ = \widetilde{W}_g\big(z|(x_{\pi(0)},y_{\pi(0)},...,(x_{\pi(L)},y_{\pi(L)})\big)\end{aligned}$$

for all $z \in \mathcal{Z}$, $x_l \in \mathcal{X}$, and $y_l \in \mathcal{Y}_l$, $l = 0,1,...,L$.

Accordingly, we define *L-symmetrizability* for the (single-user) AVC $W(z|\hat{x},s)$, cf. (20). With these definitions, we can state the following result.

Theorem 6.3. *Let $g : \mathcal{X}\times\mathcal{Y} \to \hat{\mathcal{X}}$ be an arbitrary but non-trivial function. An associated AVMAC $\{W_g(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ is L-$(\mathcal{X},\mathcal{Y})$-symmetrizable if and only if the (single-user) AVC $\{W(\cdot|\cdot,s)\}_{s\in\mathcal{S}}$ is L-symmetrizable.*

We postpone the proof of the theorem to state some immediate consequences first.

Corollary 2. *Let $C_1, C_2 > 0$ and $g : \mathcal{X}\times\mathcal{Y} \to \hat{\mathcal{X}}$ be an arbitrary but non-trivial function. Then for every associated AVMAC $\{W_g(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ with conferencing encoders, there exists an L such that the AVMAC is list decodable with list size L according to Definition 4.1.*

Proof. The proof follows immediately from Theorem 6.3 and [10, Theorem 3]. □

Corollary 3. *Let $C_1, C_2 > 0$ and $g : \mathcal{X}\times\mathcal{Y} \to \hat{\mathcal{X}}$ be an arbitrary but non-trivial function. Then for every $\hat{L} > 0$ there exists an associated AVMAC $\{W_g(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ with conferencing encoders so that this AVMAC is $\hat{L}$-$(\mathcal{X},\mathcal{Y})$-symmetrizable, i.e., this AVMAC with conferencing encoders is not list decodable with list size $\hat{L}$.*

Proof. The proof follows immediately from Theorem 6.3 and [10, Theorem 3]. □

Remark 9. It follows that every associated AVMAC with conferencing encoders is list decodable, but there is no universal bound on the needed list size even for this class of binary AVMACs.

Remark 10. List codes which are constructed based on CR-assisted codes, cf. Section 5 and especially Remark 6, are never optimal for the class of associated AVMACs with conferencing encoders discussed above. In particular, for every associated AVMAC there exists a list size L such that this channel is list decodable with list size L.

Corollary 4. *Let the function g_1 be given by*

$$g_1(x,y) = x \oplus y \coloneqq x + y \mod 2.$$

Then the AVMAC $\{W_{g_1}(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ is non-$(\mathcal{X},\mathcal{Y})$-symmetrizable, but $\mathcal{X}$-symmetrizable and $\mathcal{Y}$-symmetrizable.

This presents an example, where conferencing encoders yield an explicit gain, cf. also [5, 26].

6.2.1. *Proof of Theorem 6.3.* In the following we present the proof of Theorem 6.3. We start with the "$\Leftarrow$"-direction, i.e., we have to show that if the (single-user) AVC $\{W(\cdot|\cdot,s)\}_{s\in\mathcal{S}}$ is L-symmetrizable, then an associated AVMAC $\{W_g(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ is L-$(\mathcal{X},\mathcal{Y})$-symmetrizable.

Let the AVC $\{W(\cdot|\cdot,s)\}_{s\in\mathcal{S}}$ be L-symmetrizable. Then there exists a channel $\sigma : \hat{\mathcal{X}}^L \to \mathcal{P}(\mathcal{S})$ such that

$$\widetilde{W}(z|\hat{x}_0,\hat{x}_1,...,\hat{x}_L) = \sum_{s\in\mathcal{S}} W(z|\hat{x}_0,s)\sigma(s|\hat{x}_1,...,\hat{x}_L)$$

is a symmetric function in $\hat{x}_0,...,\hat{x}_L$ according to Definition 3.3. Now, let

$$\sigma_g\big(s|(x_1,y_1),...,(x_L,y_L)\big) \coloneqq \sigma\big(s|g(x_1,y_1),...,g(x_L,y_L)\big).$$

With this, we see that for the associated AVMAC that the channel

$$\begin{aligned}&\widetilde{W}_g\big(z|(x_0,y_0),(x_1,y_1),...,(x_L,y_L)\big)\\ &\quad\coloneqq \sum_{s\in\mathcal{S}} W_g\big(z|g(x_0,y_0),s\big)\sigma_g\big(s|(x_1,y_1),...,(x_L,y_L)\big)\end{aligned}$$

is L-$(\mathcal{X},\mathcal{Y})$-symmetrizable which proves the "$\Leftarrow$"-direction.

Now let us turn to the "$\Rightarrow$"-direction, i.e., we have to show that if an associated AVMAC $\{W_g(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ is L-$(\mathcal{X},\mathcal{Y})$-symmetrizable, then the (single-user) AVC $\{W(\cdot|\cdot,s)\}_{s\in\mathcal{S}}$ is L-symmetrizable.

Let the associated AVMAC $\{W_g(\cdot|\cdot,\cdot,s)\}_{s\in\mathcal{S}}$ be L-$(\mathcal{X},\mathcal{Y})$-symmetrizable. Then there exists a channel $\sigma_g : (\mathcal{X}\times\mathcal{Y})^L \to \mathcal{P}(\mathcal{S})$ such that

$$\begin{aligned}&\widetilde{W}_g\big(z|(x_0,y_0),(x_1,y_1),...,(x_L,y_L)\big)\\ &\quad\coloneqq \sum_{s\in\mathcal{S}} W_g(z|x_0,y_0,s)\sigma_g\big(s|(x_1,y_1),...,(x_L,y_L)\big)\end{aligned} \tag{21}$$

is a symmetric function in the pairs $(x_0,y_0),..,(x_L,y_L)$. Now, if the channel σ_g is of the form

$$\sigma_g\big(s|(x_1,y_1),...,(x_L,y_L)\big) = \tilde{\sigma}\big(s|g(x_1,y_1),...,g(x_L,y_L)\big), \tag{22}$$

then the AVC $\{W(\cdot|\cdot,s)\}_{s\in\mathcal{S}}$ would be immediately L-symmetrizable. Then, it would be sufficient to apply the channel $\tilde{\sigma}(s|\hat{x}_1,...,\hat{x}_L)$, $s\in\mathcal{S}$, $\hat{x}_l\in\hat{\mathcal{X}}$, $l=1,2,...,L$. Unfortunately, in general, we cannot assume that σ is of the form given in (22).

Therefore, we will prove the desired result by contradiction. This means we assume that the AVC $\{W(\cdot|\cdot,s)\}_{s\in\mathcal{S}}$ is non-L-symmetrizable so that AVC must be list decodable with list size L.

There exists a non-negative real number $C_* > 0$ such that for every $0 < R < C_*$ and $\lambda\in(0,1)$ there is an $n_0 = n_0(\lambda)$ such that for all $n \geq n_0$ there is a list code

$$\big\{\big(\hat{x}_m^n, \mathcal{D}_m\big) : m \in \{1,...,2^{nR}\}\big\}$$

with average probability of decoding error smaller than λ. Next we exploit the properties of the function $g : \mathcal{X} \times \mathcal{Y} \to \hat{\mathcal{X}}$. Let $m \in \{1, ..., 2^{nR}\}$ be fixed. Then for every $k \in \{1, ..., n\}$ there exists an $x_{m,k}$ with

$$g(x_{m,k}, y_{m,k}) = \hat{x}_{m,k}.$$

In the following we consider

$$\left\{(x_m^n, y_m^n) : m \in \{1, ..., 2^{nR}\}\right\} \tag{23}$$

where $\{x_m^n : m \in \{1, ..., 2^{nR}\}\}$ is the codebook for encoder 1 and $\{y_m^n : m \in \{1, ..., 2^{nR}\}\}$ is the codebook for encoder 2. Now we can use (23) as a prefix code for a CR-assisted code (with non-vanishing probability of error λ) similarly as in Section 4.3.

Accordingly, we proceed as follows: Transmitter 1 chooses an index $m \in \{1, ..., 2^{nR}\}$ for the CR-assisted code and informs the other transmitter about the index during the Willems-conference. Transmitter 1 then chooses $x_m^{n_1} \in \mathcal{X}^{n_1}$ as input and transmitter 2 chooses $y_m^{n_1} \in \mathcal{Y}^{n_1}$ as input. Thereby, n_1 is sufficiently large such that $2^{n_1 R}$ is large enough for the CR-assisted code to satisfy the error criterion λ. Then, the channel can be expressed as

$$\begin{aligned} W_g^{n_1}\left(z^{n_1}|x_m^{n_1}, y_m^{n_1}, s^{n_1}\right) &= W^{n_1}\left(z^{n_1}|g(x_m^{n_1}, y_m^{n_1}), s^{n_1}\right) \\ &= W^{n_1}\left(z^{n_1}|\hat{x}_m^{n_1}, s^{n_1}\right) \end{aligned}$$

where the function g is applied component-wise. Now, the decoder creates a list of size L of indices $m \in \{1, ..., 2^{n_1 R}\}$ with an average probability of error smaller than λ. Subsequently, we use a CR-assisted code according to Section 4.3 and obtain a concatenated code with list size L and average probability of error smaller than 2λ.

The argumentation above is true for all $\lambda \in (0, 1)$ so that the AVMAC $\{W_g(\cdot|\cdot, \cdot, s)\}_{s\in\mathcal{S}}$ with conferencing encoders is list decodable with list size L. But the channel has to be L-$(\mathcal{X}, \mathcal{Y})$-symmetrizable so that this contradicts the assumption, which means that the AVC $\{W(\cdot|\cdot, s)\}_{s\in\mathcal{S}}$ must be L-symmetrizable. This completes the proof of the theorem. □

6.2.2. *Discussion.* In the following we want discuss the relation (22) in more detail. We have seen in the proof of Theorem 6.3 that if the associated channel is L-$(\mathcal{X}, \mathcal{Y})$-symmetrizable, then the "original" AVC must be L-symmetrizable. This means there exists a $\sigma_g : (\mathcal{X} \times \mathcal{Y})^L \to \mathcal{P}(\mathcal{S})$ such that (21) is satisfied. Then, in the set of all possible channels $\{\sigma_g\}$ there must be at least one channel σ_g^* of the form (22). But this σ_g^* can easily be constructed from the corresponding L-symmetrizability condition of the AVC $\{W(\cdot|\cdot, s)\}_{s\in\mathcal{S}}$ according to the first part of the proof of Theorem 6.3.

7. Conclusion and open problems

We studied the AVMAC with conferencing encoders for which we derived the list capacity region. It can be completely characterized using the L-$(\mathcal{X}, \mathcal{Y})$-symmetrizability condition and it is shown that for large enough list size, i.e., larger than the symmetrizability of the channel, the capacity region under list decoding equals the one for highly involved CR-assisted strategies based on coordination resources which have to be available at all users. Thus, a large enough list size allows to overcome the need of coordination resources. Allowing for a small but non-vanishing probability of error, the amount of resources (i.e. common randomness or list size) can be shown to be finite and independent of the block length.

This is in contrast to the approach with vanishing error requiring an increasing and unbounded amount of such resources.

Based on Ahlswede's robustification technique [2, 3] it was shown in [26] that codes for the compound MAC with conferencing encoders can be used to construct CR-assisted codes for the AVMAC. Subsequently, it was shown in [27] that a weaker form of coordination based on correlated sources is sufficient to achieve the same performance as for CR-assisted codes. We followed that line of construction and extended it insofar as we showed that these CR-assisted codes can then be used to obtain list codes. Although this provides a suitable technique to construct list codes for the AVMAC, such list codes will never be optimal in terms list size. To overcome this problem, we presented a two-phase protocol where we connected a "bad" list code of negligible rate with a "good" CR-assisted code to obtain a final concatenated list code that is optimal in terms of list size.

The fact that both transmitters are able to cooperate using their conferencing links further reveals the following note-worthing observations. Investments in infrastructure immediately yield gains in spectral efficiency as an increase in conferencing capacities results in higher transmission rates. Moreover, the ability of conferencing makes the communication more robust as the capacity region is solely characterized by the L-$(\mathcal{X},\mathcal{Y})$-symmetrizability condition while the capacity of the classical AVMAC (without conferencing encoders) depends on its marginal symmetrizability conditions as well.

The problem at hand can be further motivated by cooperating base stations in cellular systems. In fact, a promising approach to increase the spectral efficiency of such cellular systems, especially at the cell edges, is cooperation among neighboring base stations. High-speed backbones such as glass fiber will allow the base stations to exchange information about the channel state or the messages to transmit. First rigorous studies go back to Willems who studied the corresponding multiple access channel with conferencing encoders [30]. Not surprisingly, this is intensively discussed at the moment by the 3GPP LTE-Advanced group.

Another current research development reveals a paradigm shift from an exclusive to a shared use of certain frequency bands. While current systems such as cellular systems operate on exclusive frequency bands, there will be future systems such as sensor or ad-hoc networks which will operate on shared resources in a self-organizing and uncoordinated way. The major issue of this development is that interference will be ubiquitous making it to the limiting factor of future wireless networks. Since there is no way to coordinate such induced interference, there is the need of new concepts.

In particular, in such environments each receiver receives the signal he is interested in but also interfering signals from the other transmitters. As there is no coordination between the different transmitter-receiver pairs, there is no knowledge about the induced interference. Thus, all users have to be prepared for the worst, which is a channel that may vary in an arbitrary and unknown manner from channel use to channel use, which is the concept of *arbitrarily varying channels (AVCs)*.

AVCs are particularly of interest in the context of secure communication. Such channel models allow model not only passive eavesdroppers but also active adversaries and certain classes of attacks such as jamming. Recently, the corresponding *arbitrarily varying wiretap channel (AVWC)* has attracted considerable interest, cf. for example [7, 12, 14, 21, 29, 23]. These studies have revealed interesting phenomena and results. In particular, in [12, 23] it has been shown that super-activation

is possible, i.e., two orthogonal AVWCs each having zero secrecy capacity can be used jointly to allow for secure communication at a positive rate. In [14] it has been shown that the deterministic secrecy capacity is discontinuous, i.e., small changes in the uncertainty set can lead to dramatic losses in performance. On the other hand, the CR-assisted secrecy capacity is continuous [29]. These works reveal the importance of the legitimate link from the transmitter to the designated receiver. For practical applications of these information theoretic security concepts it is important to study the questions of robustness, continuity, and resource allocation also for the multi-user case. Accordingly as a next step, the AVMAC and AVMAC with conferencing encoders must be studied to understand whether its capacity regions are continuous or not. Along this line of research, it is unknown if super-activation is possible for these scenarios or if the corresponding capacity regions are super-additive.

Acknowledgments

H. Boche would like to thank Dr. R. Baumgart, secunet Security Networks Inc., and Dr. R. Plaga, BSI, for motivating and fruitful discussions that lead to these results.

The question in this paper of how conferencing can be used to stabilize the MAC communication goes back to a corresponding problem for quantum communication. There, the corresponding capacity region of the MAC with conferencing encoders was recently shown in [11].

References

[1] R. Ahlswede, Elimination of correlation in random codes for arbitrarily carying channels, *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, **44** (1978), 159–175.

[2] R. Ahlswede, Coloring hypergraphs: A new approach to multi-user source coding–II, *J. Comb. Inform. Syst. Sci.*, **5** (1980), 220–268.

[3] R. Ahlswede, Arbitrarily varying channels with states sequence known to the sender, *IEEE Trans. Inf. Theory*, **32** (1986), 621–629.

[4] R. Ahlswede and N. Cai, Two proofs of Pinsker's conjecture concerning arbitrarily varying channels, *IEEE Trans. Inf. Theory*, **37** (1991), 1647–1649.

[5] R. Ahlswede and N. Cai, Arbitrarily varying multiple-access channels I – Ericson's symmetrizability is adequate, Gubner's conjecture is true, *IEEE Trans. Inf. Theory*, **45** (1999), 742–749.

[6] P. Beelen and K. Brander, Efficient list decoding of a class of algebraic-geometry codes, *Adv. Math. Commun.*, **4** (2010), 485–518.

[7] I. Bjelaković, H. Boche and J. Sommerfeld, Capacity results for arbitrarily varying wiretap channels, in *Information Theory, Combinatorics, and Search Theory*, Springer, 2013, 123–144.

[8] D. Blackwell, L. Breiman and A. J. Thomasian, The capacity of a class of channels, *Ann. Math. Stat.*, **30** (1959), 1229–1241.

[9] D. Blackwell, L. Breiman and A. J. Thomasian, The capacities of certain channel classes under random coding, *Ann. Math. Stat.*, **31** (1960), 558–567.

[10] V. Blinovsky, P. Narayan and M. Pinsker, Capacity of the arbitrarily varying channel under list decoding, *Probl. Pered. Inform.*, **31** (1995), 99–113.

[11] H. Boche and J. Nötzel, The classical-quantum multiple access channel with conferencing encoders and with common messages, *Quantum Inf. Proc.*, **13** (2014), 2595–2617.

[12] H. Boche and R. F. Schaefer, Capacity results and super-activation for wiretap channels with active wiretappers, *IEEE Trans. Inf. Forensics Sec.*, **8** (2013), 1482–1496.

[13] H. Boche and R. F. Schaefer, List decoding for arbitrarily varying multiple access channels with conferencing encoders, in *Proc. IEEE Int. Conf. Commun.*, Sydney, 2014, 1934–1940.

[14] H. Boche, R. F. Schaefer and H. V. Poor, On the continuity of the secrecy capacity of wiretap channels under channel uncertainty, in *Proc. IEEE Int. Conf. Commun.*, London, 2015, 5779–5784.
[15] I. Csiszár and P. Narayan, The capacity of the arbitrarily varying channel revisited: positivity, constraints, *IEEE Trans. Inf. Theory*, **34** (1988), 181–193.
[16] J. A. Gubner, On the deterministic-code capacity of the multiple-access arbitrarily varying channel, *IEEE Trans. Inf. Theory*, **36** (1990), 262–275.
[17] V. Guruswami, Bridging Shannon and Hamming: List error-correction with optimal rate, in *Proc. ICM*, Hyderabad, 2010.
[18] F. Hernando, T. Høholdt and D. Ruano, List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes, *Adv. Math. Commun.*, **6** (2012), 259–272.
[19] B. L. Hughes, The sSmalles list for the arbitrarily varying channel, *IEEE Trans. Inf. Theory*, **43** (1997), 803–815.
[20] J.-H. Jahn, Coding of arbitrarily varying multiuser channels, *IEEE Trans. Inf. Theory*, **27** (1981), 212–226.
[21] E. MolavianJazi, M. Bloch and J. N. Laneman, Arbitrary jamming can preclude secure communication, in *Proc. 47th Ann. Allerton Conf. Commun. Control Comp.*, Urbana-Champaign, 2009, 1069–1075.
[22] S. Nitinawarat, On the deterministic code capacity region of an arbitrarily varying multiple-access channel under list decoding, *IEEE Trans. Inf. Theory*, **59** (2013), 2683–2693.
[23] J. Nötzel, M. Wiese and H. Boche, The arbitrarily varying wiretap channel - secret randomness, stability and super-activation, in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, 2015, 2151–2155.
[24] A. D. Sarwate and M. Gastpar, List-decoding for the arbitrarily varying channel under state constraints, *IEEE Trans. Inf. Theory*, **58** (2012), 1372–1384.
[25] R. F. Schaefer and H. Boche, List decoding for arbitrarily varying broadcast channels with receiver side information, *IEEE Trans. Inf. Theory*, **60** (2014), 4472–4487.
[26] M. Wiese and H. Boche, The arbitrarily varying multiple-access channel with conferencing encoders, *IEEE Trans. Inf. Theory*, **59** (2013), 1405–1416.
[27] M. Wiese and H. Boche, On the weakest resource for coordination in arbitrarily varying multiple access channels with conferencing encoders, *Probl. Inf. Transm.*, **50** (2014), 15–26.
[28] M. Wiese, H. Boche, I. Bjelaković and V. Jungnickel, The compound multiple access channel with partially cooperating encoders, *IEEE Trans. Inf. Theory*, **57** (2011), 3045–3066.
[29] M. Wiese, J. Nötzel and H. Boche, The arbitrarily varying wiretap channel - communication under uncoordinated attacks, in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, 2015, 2146–2150.
[30] F. M. J. Willems, The discrete memoryless multiple access channel with partially cooperating encoders, *IEEE Trans. Inf. Theory*, **29** (1983), 441–445.
[31] J. Wolfowitz, Simultaneous channels, *Arch. Rat. Mech. Anal.*, **4** (1960), 371–386.

Received for publication May 2014.

E-mail address: boche@tum.de
E-mail address: rafael.schaefer@tu-berlin.de