

An Outer Bound to the Admissible Source Region of Broadcast Channels with Arbitrarily Correlated Sources and Channel Variations

Amin Aminzadeh Gohari¹ and Venkat Anantharam¹

¹ Department of Electrical Engineering and Computer Science

University of California, Berkeley

{aminzade, ananth}@eecs.berkeley.edu

Abstract—In this paper we apply the “potential function method” introduced by the authors in [5] and [6] to prove an outer bound on the admissible source region of an arbitrarily varying general broadcast channel with arbitrarily correlated sources. We are not aware of any previous work discussing any interesting outer bounds on the admissible source region of the general broadcast channel either when the sources are allowed to be arbitrarily correlated, the channel is allowed to vary arbitrarily, or both. Specializing by removing the variability of the channel and assuming independent sources, our outer bound reduces to one that is included inside the region defined by Liang, Kramer and Shamai, a recent outer bound on the capacity region of the traditional broadcast channel [12]. We don’t know if the inclusion is strict. The arbitrarily varying channel aspect of our bound is rather superficial; the main interest is in the arbitrarily correlated source part.

I. INTRODUCTION

Broadcast channels form basic building blocks of many wireless system models. A broadcast channel is a single-input, multi-output system whose goal is to model reliable communication of sets of messages from a transmitter to different sets of receivers [1], [2]. In some practical scenarios the channel parameters may be unknown, imprecise, or subject to variations from one symbol transmission to the next one. An arbitrarily varying channel (AVC) models such a discrete memoryless channel. It is assumed that the channel parameters admit no statistical description and any code over this channel must have guaranteed performance under the worst possible choice of the channel parameters. Furthermore, it is known that unlike the point-to-point scenario, in a broadcast channel the separation of the source and channel codings is not necessarily optimal [8]. In this paper we study the limitations of joint source-channel coding strategies across arbitrarily varying broadcast channels.

We consider only two-receiver arbitrarily varying general broadcast channels in this paper. A two-receiver broadcast channel is characterized by the conditional distribution $q(y, z|x)$ where X is the input to the channel and Y and Z are the outputs of the channel at the two receivers. In a general broadcast channel with correlated sources, the transmitter is observing i.i.d. repetitions of two, possibly correlated, random variables L_1 and L_2 . Roughly speaking, the source pair (L_1, L_2) is called admissible if there exists

a strategy for the transmitter to reliably send the i.i.d. repetitions of L_1 to the receiver Y and the i.i.d. repetitions of L_2 to the receiver Z [8]. Let L_0 be a discrete random variable representing the common part between L_1 and L_2 in the following sense: L_0 satisfies $H(L_0|L_1) = H(L_0|L_2) = 0$ and $H(L_0)$ is equal to its maximum possible value. Random variable L_0 would represent the common message that needs to be transmitted to both receivers. For the accuracy of this interpretation, see [3].

An arbitrarily varying general broadcast channel is characterized by the conditional distribution $q(y, z|x, s)$ where X is the input of the transmitter to the channel, S is the state parameter of the channel (that can vary in an arbitrary way throughout the communication) and Y and Z are the outputs of the channel at the two receivers. The transmitter is observing i.i.d. repetitions of two, possibly correlated, random variables L_1 and L_2 . Roughly speaking, the source pair (L_1, L_2) is called admissible if there exists a strategy for the transmitter to reliably send the i.i.d. repetitions of L_1 to the receiver Y and the i.i.d. repetitions of L_2 to the receiver Z no matter how the state of the channel varies over time. The transmitted messages should be recoverable by the receivers with high probability. Depending on the model, either an average probability of error, or a maximal probability of error constraint at the receivers is imposed. Furthermore, sometimes it is assumed that there are common random bits shared between the transmitter and the receivers in the construction of the transmission scheme. Depending on the choice of model, different notions of admissible source region can be defined. In this paper we assume that shared common randomness of arbitrary length is provided to the transmitter and the receivers, and that the receivers are required to find the intended messages under an average probability of error constraint (see section II for a formal definition). Clearly the same outer bounds hold when no such shared common randomness is provided to the transmitter and the receivers (deterministic-code arbitrarily varying general broadcast channels).

The admissible source region of a broadcast channel is not known when the channel parameters are fixed and the sources are independent, except in certain special cases; less is known when the channel parameters vary arbitrarily or

the sources are allowed to be arbitrarily correlated. The best known inner bound for the two receiver general broadcast channel is due to Liang and Kramer [11]; it is not however known whether this bound strictly improves on the earlier inner bounds of Marton [13], [2, p. 391, Problem 10(c)], and Gel'fand and Pinsker [4]. Recently there has been a series of outer bounds on the broadcast channel (with no channel variation and independent source messages) by Nair [14], Liang, Kramer and Shamai [12] and Nair and El Gamal [15]. Each of these bounds is strictly better than the outer bound of Körner-Marton [13]¹, but it is not known whether any of these bounds are strictly better than the rest. In section III, we simplify the bound proposed by Liang, Kramer and Shamai by, in part, removing its redundant inequalities. The best known inner bound for the two receiver general broadcast channel with correlated sources is due to Han and Costa [8]. For arbitrarily varying general broadcast channels (AVGBC), the best known inner bound, as far as we are aware, belongs to Jahn [10]. For the family of degraded message sets², Hof and Bross [9] found a new inner bound on the capacity region of the AVGBC under state and input constraints. We are not aware of any previous work discussing any interesting outer bounds on the admissible source region of the general broadcast channel either when the sources are allowed to be arbitrarily correlated, the channel is allowed to vary arbitrarily, or both. Han and Costa [8] provide an example of a broadcast channel with correlated messages for which the source–channel separation theorem breaks down. This indicates that finding outer bounds on broadcast channels with correlated sources is a more generic problem.

In this paper, we consider the admissible source region of an AVGBC when shared common randomness of arbitrary length is provided to the transmitter and the receivers.³ The admissible source region is defined in terms of the average probability of error over the source; reliable transmission of the sources needs to be achievable uniformly over the channel parameters (which can vary symbol by symbol). We apply the “potential function method” introduced by the authors in [5] and [6] to prove a new outer bound on the admissible source region of arbitrarily varying general broadcast channels. Specializing by removing the variability of the channel and assuming independent sources, our outer bound reduces to one that is included inside the region defined by Liang, Kramer and Shamai [12]. We don't know if the inclusion is strict. The arbitrarily varying channel aspect of our bound is rather superficial; the main interest is in the arbitrarily correlated source part.

A sketch of the “potential function method” is as follows: we consider the set of all joint distributions on products of four finite sets which represent, roughly speaking, the

¹More specifically, Nair and El Gamal show that their bound is strictly better than that of Körner-Marton for a certain binary skew-symmetric channel [15]. The two other bounds are no worse than the Nair and El Gamal bound.

²We do not consider the degraded message set restriction here; for a definition see [9]

³Our outer bound is however also applicable to the scenario in which no shared common randomness is provided to the transmitter and the receivers.

TABLE I
NOTATIONS

Variable	Description
\mathbb{R}	Real numbers.
\mathbb{R}_+	Non-negative real numbers.
$q(y, z x, s)$	The statistical description of an arbitrarily varying broadcast channel.
L_i ($i = 1, 2$) L_0	The message intended for the i^{th} receiver. Satisfies $H(L_0 L_1) = H(L_0 L_2) = 0$. $H(L_0)$ is equal to its maximum possible value.
$\psi_Y, \psi_Z,$ ψ_X, ψ_S	Alphabet sets of $Y, Z,$ X, S .
$\zeta(\cdot)$ $\vartheta_y(\cdot)$ $\vartheta_z(\cdot)$	The encoding function used by the transmitter. The decoding function at the receivers.
E b	The common randomness shared among all the parties; E is uniform on $\{1, 2, \dots, b\}$.
n	Length of the code used.
$\Delta(\cdot)$ \oplus	Down-set (Definition 4); Sum of two sets (Definition 3).
$\Upsilon_{p(x,s,y,z)}$	A set of probability distributions (see Definition 5)

gained knowledge of the two receivers, the knowledge of the transmitter, and the history of broadcast channel parameter choices at some stage of the communication. We then identify properties of a function on such distributions which would need to be satisfied in one step of the communication for it to give rise to an outer bound. For details see lemma 1 or see [5]-[6].

The outline of this paper is as follows. In section II, we introduce the basic notations and definitions used in this paper. In section III, we simplify the Liang, Kramer and Shamai outer bound on the broadcast channel. Section IV contains the description of the new outer bound followed by section V which gives formal proofs for the results.

II. DEFINITIONS AND NOTATION

Throughout this paper we assume that each random variable takes values in a finite set. \mathbb{R} denotes the set of real numbers and \mathbb{R}_+ denotes the set of non-negative reals.

We represent an arbitrarily varying broadcast channel by the conditional distribution $q(y, z|x, s)$ meaning that X is talking, S is the state of the channel, and Y and Z are listening. We assume that X, S, Y, Z, L_1 and L_2 take values from discrete sets $\psi_X, \psi_S, \psi_Y, \psi_Z, \psi_{L_1}$ and ψ_{L_2} respectively. For any natural number n , $(\psi_X)^n, (\psi_S)^n, (\psi_Y)^n, (\psi_Z)^n, (\psi_{L_1})^n$ and $(\psi_{L_2})^n$ denote the n -th product sets of $\psi_X, \psi_S, \psi_Y, \psi_Z, \psi_{L_1}$ and ψ_{L_2} .

Definition 1: [see also [8]] Given the conditional distribution $q(y, z|x, s)$, positive real ϵ and natural numbers n and b , and random variables L_1, L_2 jointly distributed according to $p(l_1, l_2)$, an (n, b, ϵ) code is the set of the following three mappings:

- $\zeta : (\psi_{L_1})^n \times (\psi_{L_2})^n \times \{1, 2, \dots, b\} \longrightarrow (\psi_X)^n,$
- $\vartheta_y : (\psi_Y)^n \times \{1, 2, \dots, b\} \longrightarrow (\psi_{L_1})^n,$
- $\vartheta_z : (\psi_Z)^n \times \{1, 2, \dots, b\} \longrightarrow (\psi_{L_2})^n,$

such that for any joint distribution $p(s_1, s_2, \dots, s_n)$, the following “average distortion” condition is satisfied:

Assume that $X^n = \zeta(L_1^n, L_2^n, E)$ where L_i^n stands for n i.i.d. repetitions of random variable L_i ($i = 1, 2$). Random

variable E stands for a uniform random variable defined on the set $\{1, 2, \dots, b\}$ and independent of (L_1^n, L_2^n) , and represents the common randomness shared among the communicating parties in constructing the transmission scheme. Random variables S^n , Y^n and Z^n are defined according to

$$p(y^n, z^n, x^n, s^n, l_1^n, l_2^n, e) = p(l_1^n, l_2^n, x^n, e) \cdot p(s^n) \prod_{i=1}^n q(y_i, z_i | x_i, s_i).$$

We then have the following constraints:

$$P(\vartheta_y(Y_1, Y_2, \dots, Y_n, E) \neq (L_1)^n) \leq \epsilon, \\ P(\vartheta_z(Z_1, Z_2, \dots, Z_n, E) \neq (L_2)^n) \leq \epsilon.$$

Definition 2: Given the conditional distribution $q(y, z | x, s)$, a pair of random variables (L_1, L_2) is called an *admissible source* if for every positive ϵ and sufficiently large n and b , an (n, b, ϵ) code exists.

The capacity region of the arbitrarily varying general broadcast channel, $C_{BC}(q(y, z | x, s))$, is a subset of triples of non-negative real numbers (R_0, R_1, R_2) for which an admissible source (L_1, L_2) exists such that $L_1 = (L'_0, L'_1)$, $L_2 = (L'_0, L'_2)$ where L'_0 , L'_1 and L'_2 are jointly independent of each other, and where $R_i = H(L'_i)$ (for $i = 0, 1, 2$).

Definition 3: For any natural number c and any two sets of points K and L in \mathbb{R}_+^c , let $K \oplus L$ refer to their Minkowski sum: $K \oplus L = \{v_1 + v_2 : v_1 \in K, v_2 \in L\}$. For any real number r , let $r \times K = \{r \cdot v_1 : v_1 \in K\}$. We also define $\frac{K}{r}$ as the set formed by shrinking K through scaling each point of it by a factor $\frac{1}{r}$.

Definition 4: For any two points \vec{v}_1 and \vec{v}_2 in \mathbb{R}_+^c , we say $\vec{v}_1 \geq \vec{v}_2$ if and only if each coordinate of \vec{v}_1 is greater than or equal to the corresponding coordinate of \vec{v}_2 . For a set $A \in \mathbb{R}_+^c$, the down-set $\Delta(A)$ is defined as: $\Delta(A) = \{\vec{v} \in \mathbb{R}_+^c : \vec{v} \leq \vec{w} \text{ for some } \vec{w} \in A\}$.

Definition 5: For all given finite sets $\psi_X, \psi_S, \psi_Y, \psi_Z$, let $\Gamma_{\psi_X, \psi_S, \psi_Y, \psi_Z}$ be the set of joint distributions $r(w_0, w_1, w_2, u, v, x, s, y, z)$ defined on $\psi_{W_0} \times \psi_{W_1} \times \psi_{W_2} \times \psi_U \times \psi_V \times \psi_X \times \psi_S \times \psi_Y \times \psi_Z$ where ψ_X, ψ_S, ψ_Y and ψ_Z are given, and $\psi_{W_0}, \psi_{W_1}, \psi_{W_2}, \psi_U$ and ψ_V are arbitrary finite sets, and such that the following three properties are satisfied:

- 1) $H(W_0 | W_1 U) = H(W_0 | W_2 V) = 0$;
- 2) X is a deterministic function of (W_0, W_1, W_2, U, V) ;
- 3) The following Markov chain holds: $UVW_0W_1W_2X - X - XSYZ$.

For every given distribution $p(x, s, y, z)$ defined on $\psi_X, \psi_S, \psi_Y, \psi_Z$, let $\Upsilon_{p(x, s, y, z)}$ be the set of joint distributions $r(w_0, w_1, w_2, u, v, x, s, y, z)$ belonging to $\Gamma_{\psi_X, \psi_S, \psi_Y, \psi_Z}$ for which the marginal $r(x, s, y, z)$ is equal to $p(x, s, y, z)$.

III. ANALYSIS OF LIANG, KRAMER AND SHAMAI'S OUTER BOUND

Given the broadcast channel $q(y, z | x)$ (no variation in the channel is assumed here, i.e. $q(y, z | x, s) = q(y, z | x)$ for all s), Liang, Kramer and Shamai define their outer bound on the

capacity region of the general broadcast channel as follows [12]: let $\varrho(q(y, z | x))$ be the union over all joint distributions $p(w_0, w_1, w_2, u, v, x, y, z) = p(w_0, w_1, w_2, u, v, x)q(y, z | x)$ for which W_0, W_1 and W_2 are both mutually independent and uniform and X is a deterministic function of (W_0, W_1, W_2, U, V) , of the region:

$$\left\{ \begin{array}{l} R_0 \geq 0, R_1 \geq 0, R_2 \geq 0; \\ R_0 \leq \min\{I(W_0; Y|U), I(W_0; Z|V)\}; \\ R_1 \leq I(W_1; Y|U); \quad R_2 \leq I(W_2; Z|V); \\ R_0 + R_1 \leq \min(I(W_0W_1; Y|U), I(W_1; Y|W_0UV) \\ \quad + I(W_0U; Z|V)); \\ R_0 + R_2 \leq \min(I(W_0W_2; Z|V), I(W_2; Z|W_0UV) \\ \quad + I(W_0V; Y|U)); \\ R_0 + R_1 + R_2 \leq \min(I(W_1; Y|W_0W_2UV) + I(W_0W_2U; Z|V), \\ \quad I(W_2; Z|W_0W_1UV) + I(W_0W_1V; Y|U), \\ \quad I(W_0VU; Y) + I(W_1; Y|W_0W_2UV) \\ \quad + I(W_2; Z|W_0UV), \\ \quad I(W_0UV; Z) + I(W_2; Z|W_0W_1UV) \\ \quad + I(W_1; Y|W_0UV)). \end{array} \right.$$

Theorem 1: The region $\varrho(q(y, z | x))$ equals $\varrho_1(q(y, z | x))$ defined as follows: let $\varrho_1(q(y, z | x))$ be the region defined as above except that the extra constraint $H(W_0 | W_1 U) = H(W_0 | W_2 V) = 0$ is imposed on W_0, W_1, W_2, U and V and the set of inequalities is simplified by replacing them with the following apparently stronger set of inequalities:

$$\left\{ \begin{array}{l} R_0 \geq 0, R_1 \geq 0, R_2 \geq 0; \\ R_0 \leq \min\{I(W_0; Y|U), I(W_0; Z|V)\}; \\ R_0 + R_1 \leq I(W_1; Y|U); \quad R_0 + R_2 \leq I(W_2; Z|V); \\ R_0 + R_1 \leq I(W_1; Y|W_0UV) + I(W_0U; Z|V); \\ R_0 + R_2 \leq I(W_2; Z|W_0UV) + I(W_0V; Y|U); \\ R_0 + R_1 + R_2 \leq \min(\\ \quad I(W_1; Y|W_0W_2UV) + I(W_2U; Z|V), \\ \quad I(W_2; Z|W_0W_1UV) + I(W_1V; Y|U), \\ \quad I(W_0UV; Y) + I(W_1; Y|W_0W_2UV) \\ \quad + I(W_2; Z|W_0UV), \\ \quad I(W_0UV; Z) + I(W_2; Z|W_0W_1UV) \\ \quad + I(W_1; Y|W_0UV)). \end{array} \right.$$

Remark 1: In order to get the original set of inequalities, replace the inequality $R_0 + R_1 \leq I(W_1; Y|U)$ with two weaker inequalities $R_1 \leq I(W_1; Y|U)$ and $R_0 + R_1 \leq I(W_0W_1; Y|U)$. Similarly, replace $R_0 + R_2 \leq I(W_2; Z|V)$ with $R_2 \leq I(W_2; Z|V)$ and $R_0 + R_2 \leq I(W_0W_2; Z|V)$. Furthermore, weaken the first and second inequality on $R_0 + R_1 + R_2$ by adding respectively terms $I(W_0; Z|W_2UV)$ and $I(W_0; Y|W_1UV)$ to the left hand side of these inequalities.

Theorem 2: The region $\varrho_1(q(y, z | x))$ with or without the constraint on W_0, W_1 and W_2 being mutually independent and uniform is the same.

Remark 2: Relaxation of the constraint on W_0, W_1 and W_2 being mutually independent parallels a similar result by Nair and Zizhou [16]. Nair and El Gamal in [15] had proposed two outer bounds, defined in equation (3.1) and in Theorem 3.1 of [15], and had suspected that one is strictly

tighter than the other. Nair and Zizhou showed that this is not the case.

IV. THE NEW OUTER BOUND

In this section, the main claims of the paper are formally presented as theorem 3, lemmas 1 and 2.

Theorem 3: Given any arbitrarily varying broadcast channel $q(y, z|x, s)$ and an arbitrary admissible source (L_1, L_2) , let L_0 be an arbitrary random variable satisfying $H(L_0|L_1) = H(L_0|L_2) = 0$. Then there exists $p(x)$ such that for any $p(s)$ there exists $p(w_0, w_1, w_2, u, v, x, s, y, z)$ in the set $\Upsilon_{q(y, z|x, s)p(x)p(s)}$ such that the following inequalities are satisfied:

$$\left\{ \begin{array}{l} H(L_0) \leq \min\{I(W_0; Y|U), I(W_0; Z|V)\}; \\ H(L_1) \leq I(W_1; Y|U); \quad H(L_2) \leq I(W_2; Z|V); \\ H(L_1) \leq I(W_1; Y|W_0UV) + I(W_0U; Z|V); \\ H(L_2) \leq I(W_2; Z|W_0UV) + I(W_0V; Y|U); \\ H(L_1L_2) \leq I(W_1; Y|W_0W_2UV) + I(W_2U; Z|V); \\ H(L_1L_2) \leq I(W_2; Z|W_0W_1UV) + I(W_1V; Y|U); \\ H(L_1L_2) \leq \\ \quad I(W_0V; Y|U) + I(W_1; Y|W_0W_2UV) \\ \quad + I(W_2; Z|W_0UV); \\ H(L_1L_2) \leq \\ \quad I(W_0U; Z|V) + I(W_2; Z|W_0W_1UV) \\ \quad + I(W_1; Y|W_0UV). \end{array} \right.$$

Corollary 1: Given any arbitrarily varying broadcast channel $q(y, z|x, s)$, the following region forms an outer bound on the capacity region of the broadcast channel:

$$\zeta(q(y, z|x, s)) =$$

$$\bigcup_{p(x)} \bigcap_{p(s)} \bigcup_{p(w_0, w_1, w_2, u, v, x, s, y, z) \in \Upsilon_{q(y, z|x, s)p(x)p(s)}} \left\{ \begin{array}{l} R_0 \geq 0, R_1 \geq 0, R_2 \geq 0; \\ R_0 \leq \min\{I(W_0; Y|U), I(W_0; Z|V)\}; \\ R_0 + R_1 \leq I(W_1; Y|U); \quad R_0 + R_2 \leq I(W_2; Z|V); \\ R_0 + R_1 \leq I(W_1; Y|W_0UV) + I(W_0U; Z|V); \\ R_0 + R_2 \leq I(W_2; Z|W_0UV) + I(W_0V; Y|U); \\ R_0 + R_1 + R_2 \leq I(W_1; Y|W_0W_2UV) + I(W_2U; Z|V); \\ R_0 + R_1 + R_2 \leq I(W_2; Z|W_0W_1UV) + I(W_1V; Y|U); \\ R_0 + R_1 + R_2 \leq I(W_0V; Y|U) + I(W_1; Y|W_0W_2UV) \\ \quad + I(W_2; Z|W_0UV); \\ R_0 + R_1 + R_2 \leq I(W_0U; Z|V) + I(W_2; Z|W_0W_1UV) \\ \quad + I(W_1; Y|W_0UV). \end{array} \right.$$

where R_0 denotes the common rate, R_1 the private rate to receiver one, and R_2 the private rate to receiver two.

Remark 3: If $q(y, z|x, s) = q(y, z|x)$, the above outer bound reduces to a region that is included inside that of Liang, Kramer and Shamai [12]. To see this weaken the last two inequalities by adding $I(U; Y)$ to the left hand side of the third inequality on $R_0 + R_1 + R_2$, and $I(V; Z)$ to the left hand side of the last inequality on $R_0 + R_1 + R_2$. We don't know if this bound is strictly better than that of [12].

Lemma 1: Let $\varphi(p(y, z, x, s))$ be a function from the set of all probability distributions defined on a product of four finite sets to down-sets in \mathbb{R}_+^c where c is a natural number (this implies that $\varphi(p(y, z, x, s))$ is always

equal to $\Delta(\varphi(p(y, z, x, s)))$). For any conditional distribution $q(y, z|x, s)$, let

$$\phi(q(y, z|x, s)) = \bigcup_{q(x)} \bigcap_{q(s)} \varphi(q(y, z|x, s)q(x)q(s)).$$

Further assume that φ satisfies the following properties for any $p(y, z|x, s)$ and $p(x)$: (please see definition 3 and 4 for the notations used)

- 1) Whenever $p(yy', zz'|x, ss') = p(y, z|x, s) \times p(y', z'|x', s')$, $H(X'|X) = 0$ and $p(y', z'|x', s') = q(y', z'|x', s')$:

$$\begin{aligned} & \varphi(p(yy', zz'|x, ss')p(x)p(s)p(s')) \subseteq \\ & \varphi(p(y, z|x, s)p(x)p(s)) \oplus \\ & \varphi(q(y', z'|x', s')p(x')p(s')). \end{aligned}$$

- 2) Whenever $p(y = z) = 1$ and $H(Y|X) = H(Z|X) = 0$, and in addition $H(X'|X) = 0$, $p(y', z'|x', s') = q(y', z'|x', s')$:

$$\begin{aligned} & \varphi(p(yy', zz'|x, s')p(x)p(s')) \subseteq \\ & \varphi(q(y', z'|x', s')p(x')p(s')) \oplus \\ & \Delta(\underbrace{\{(H(Y), H(Y), \dots, H(Y))\}}_{c \text{ times}}). \end{aligned}$$

- 3) For any channel $q(y, z|x, s)$, input distributions $p_0(x)$ and $p_1(x)$ and $\lambda \in (0, 1)$, there exists $p_\lambda(x)$ such that for any $p(s)$,

$$\begin{aligned} & (1 - \lambda) \times \varphi(q(y, z|x, s)p_0(x)p(s)) \oplus \\ & \lambda \times \varphi(q(y, z|x_1, s)p_1(x)p(s)) \subseteq \\ & \varphi(q(y, z|x, s)p_\lambda(x)p(s)). \end{aligned}$$

Then, for any broadcast channel $q(y, z|x, s)$, arbitrarily correlated random variables L_1 and L_2 , positive ϵ and (n, b, ϵ) code for this broadcast channel, we have (for the definition of multiplication of a set by a real number see definition 3).

$$\begin{aligned} & \bigcap_{p(s_1, s_2, \dots, s_n)} \varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n) \\ & p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n)) \subseteq \quad (1) \\ & n \times \phi(q(y, z|x, s)) \oplus \Delta(\underbrace{\{(\log b, \log b, \dots, \log b)\}}_{c \text{ times}}), \end{aligned}$$

where random variables $(X'_1, X'_2, \dots, X'_n)$, (S_1, S_2, \dots, S_n) , $(Y'_1, Y'_2, \dots, Y'_n)$ and $(Z'_1, Z'_2, \dots, Z'_n)$ respectively represent the inputs by the encoder at the broadcast channel, the adversary's input to the broadcast channel, the outputs at the Y receiver, and the outputs at the Z receiver. E is a uniform random variable of entropy $\log b$, representing the common randomness shared between the transmitter and the receivers in constructing the transmission scheme. Random variables Y'_0 and Z'_0 equal E with probability one. E is independent of (L_1^n, L_2^n) .

Lemma 2: φ as defined below satisfy the properties of lemma 1 with the choice of $c = 10$.

$$\begin{aligned} \varphi(p(y, z, x, s)) = & \bigcup_{p(w_0, w_1, w_2, u, v, x, s, y, z) \in \Upsilon_{p(y, z, x, s)}} \\ \Delta \left(\{ & (I(W_0; Y|U), I(W_0; Z|V), I(W_1; Y|U), I(W_2; Z|V), \right. \\ & I(W_1; Y|W_0UV) + I(W_0U; Z|V), \\ & I(W_2; Z|W_0UV) + I(W_0V; Y|U), \\ & I(W_1; Y|W_0W_2UV) + I(W_0W_2U; Z|V), \\ & I(W_2; Z|W_0W_1UV) + I(W_0W_1V; Y|U), \\ & I(W_0V; Y|U) + I(W_1; Y|W_0W_2UV) + I(W_2; Z|W_0UV), \\ & \left. I(W_0U; Z|V) + I(W_2; Z|W_0W_1UV) + I(W_1; Y|W_0UV) \} \right). \end{aligned}$$

V. PROOFS

Proof: [Proof of Theorem 1] Clearly $\varrho_1(q(y, z|x)) \subseteq \varrho(q(y, z|x))$ because we have replaced the set of inequalities with a stronger one, and have further restricted the set of permissible (W_0, W_1, W_2, U, V) . Below we will show that $\varrho(q(y, z|x)) \subseteq \varrho_1(q(y, z|x))$: Take an arbitrary $(R_0, R_1, R_2) \in \varrho(q(y, z|x))$. Corresponding to (R_0, R_1, R_2) , there exists $p(x)$ and $p(w_0, w_1, w_2, u, v, x, y, z) = p(w_0, w_1, w_2, u, v, x)q(y, z|x)$ for which $\widetilde{W}_0, \widetilde{W}_1$ and \widetilde{W}_2 are both mutually independent and uniform, and X is a deterministic function of (W_0, W_1, W_2, U, V) , such that the inequalities in $\varrho(q(y, z|x))$ are satisfied. We will define an appropriate $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ that would imply that $(R_0, R_1, R_2) \in \varrho_1(q(y, z|x))$ (i.e. the corresponding inequalities for (R_0, R_1, R_2) in $\varrho_1(q(y, z|x))$ would be satisfied with this choice).

Let random variables A_0, A_1, A_2 and A_3 be uniform on the alphabet set of \widetilde{W}_0 (without loss of generality assumed to be $\{1, 2, \dots, M'_0\}$ for some M'_0). Let A_2 and A_3 and $(W_0, W_1, W_2, U, V, X, Y, Z)$ be mutually independent. Random variables A_0 and A_1 are then defined as follows:

$$A_i = 1 + (\widetilde{W}_0 + A_{i+2} \bmod M'_0) \quad i = 0, 1.$$

Let $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ be equal to $(UA_0, VA_1, W_0, W_1A_2, W_2A_3, X, Y, Z)$.

It can be verified that $p(\widetilde{x}) = p(x)$. Furthermore $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ satisfies the required properties (in particular $H(\widetilde{W}_0|\widetilde{W}_1\widetilde{U}) = H(\widetilde{W}_0|\widetilde{W}_2\widetilde{V}) = 0$). One can use $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ in the definition of ϱ_1 to show that $(R_0, R_1, R_2) \in \varrho_1(q(y, z|x))$. More specifically, one can verify the following inequalities:

$$\left\{ \begin{array}{l} R_0 \geq 0, R_1 \geq 0, R_2 \geq 0; \\ R_0 \leq \min\{I(\widetilde{W}_0; \widetilde{Y}|\widetilde{U}), I(\widetilde{W}_0; \widetilde{Z}|\widetilde{V})\}; \\ R_0 + R_1 \leq I(\widetilde{W}_1; \widetilde{Y}|\widetilde{U}); \\ \dots \\ R_0 + R_1 + R_2 \leq I(\widetilde{W}_0\widetilde{U}\widetilde{V}; \widetilde{Z}) + I(\widetilde{W}_2; \widetilde{Z}|\widetilde{W}_0\widetilde{W}_1\widetilde{U}\widetilde{V}) \\ \quad + I(\widetilde{W}_1; \widetilde{Y}|\widetilde{W}_0\widetilde{U}\widetilde{V}). \end{array} \right.$$

For the details, see [7]. \blacksquare

Proof: [Proof of Theorem 2] Take an arbitrary joint distribution

$p(w_0, w_1, w_2, u, v, x, y, z) = p(w_0, w_1, w_2, u, v, x)q(y, z|x)$ for which X is a deterministic function of (W_0, W_1, W_2, U, V) and such that $H(W_0|W_1U) = H(W_0|W_2V) = 0$. We will define $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ that yield the same region of triples of (R_0, R_1, R_2) as in the definition of $\varrho_1(q(y, z|x))$, but furthermore satisfy the additional constraint that $\widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2$ are both mutually independent and uniform.

Let random variables A_0, A_1, A_2 be uniform on the alphabet set of W_0, W_1 and W_2 respectively (without loss of generality assumed to be $\{1, 2, \dots, M'_i\}$ for some M'_i ($i = 0, 1, 2$)). Furthermore assume that A_0, A_1, A_2 and $(W_0, W_1, W_2, U, V, X, Y, Z)$ are mutually independent. Random variables A_3, A_4 and A_5 are then defined as follows:

$$A_{i+3} = 1 + (W_i + A_i \bmod M'_i) \quad i = 0, 1, 2.$$

It can be verified that A_3, A_4, A_5 and $(W_0, W_1, W_2, U, V, X, Y, Z)$ are mutually independent. Let $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ be equal to $(UA_3A_4A_5, VA_3A_4A_5, A_0, A_1, A_2, X, Y, Z)$.

It can be verified that $p(\widetilde{x}) = p(x)$. Furthermore $(\widetilde{U}, \widetilde{V}, \widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{X}, \widetilde{Y}, \widetilde{Z})$ satisfies all the required properties; in particular $\widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2$ are both mutually independent and uniform. For the details, see [7]. \blacksquare

Proof: [Proof of Theorem 3] Take an arbitrary (n, b, ϵ) code. We show that one can find $d_i = O(\epsilon) + O(\frac{h(\epsilon)}{n})$ ($i = 0, 1, 2, \dots, 9$) and $p(x)$ for which for any $p(s)$ there exist $p(w_0, w_1, w_2, u, v, x, s, y, z) \in \Upsilon_{q(y, z|x, s)p(x)p(s)}$ such that

$$\begin{aligned} H(L_0) - d_0 &\leq I(W_0; Y|U); \quad H(L_0) - d_1 \leq I(W_0; Z|V); \\ H(L_1) - d_2 &\leq I(W_1; Y|U); \quad H(L_2) - d_3 \leq I(W_2; Z|V); \\ H(L_1) - d_4 &\leq I(W_1; Y|W_0UV) + I(W_0U; Z|V); \\ \dots \\ H(L_1L_2) - d_9 &\leq I(W_0U; Z|V) + I(W_2; Z|W_0W_1UV) \\ &\quad + I(W_1; Y|W_0UV), \end{aligned}$$

where $O(\nu)$ here and elsewhere stands for a function of ν bounded in absolute value by a constant multiple of ν , where the constant depends only on the alphabet size of L_1 and L_2 ; the function $h(\cdot)$ is the binary entropy function.

Let $L_1^n, L_2^n, E, (X'_1, X'_2, \dots, X'_n), (S_1, S_2, \dots, S_n), (Y'_0, Y'_1, Y'_2, \dots, Y'_n), (Z'_0, Z'_1, Z'_2, \dots, Z'_n)$ be defined as in lemma 1. This implies that $H(X'_i|\widetilde{X}) = 0$ where the random variable \widetilde{X} is defined as $\widetilde{X} = (L_1^n, L_2^n, E)$.

Let φ be defined as in lemma 2. Since according to lemma 2, $\varphi(\cdot)$ satisfies the properties of lemma 1, we have (for the definition of multiplication of a set by a real number see definition 3):

$$\begin{aligned} \bigcap_{p(s_1, s_2, \dots, s_n)} \varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n)) & \quad (2) \\ p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n) & \subseteq \\ n \times \phi(q(y, z|x, s)) \oplus \Delta(\{(\log b, \log b, \dots, \log b)\}). & \end{aligned}$$

The sketch of the rest of the proof is as follows (for the details, see [7]): The decoding rule ensures that the Y -party and the Z -party are able to compute $\widehat{L}_1^n = \vartheta_y((Y'_1, Y'_2, \dots, Y'_n), E)$ and $\widehat{L}_2^n = \vartheta_z((Z'_1, Z'_2, \dots, Z'_n), E)$ such that for any joint distribution $p(s_1, s_2, \dots, s_n)$, random variables \widehat{L}_1^n and \widehat{L}_2^n are respectively equal to L_1^n and L_2^n with probability at least $1 - \epsilon$. It can be shown that

$$\begin{aligned} & \bigcap_{p(s_1, s_2, \dots, s_n)} \varphi(p(e\widehat{L}_1^n, e\widehat{L}_2^n | l_1^n l_2^n e, s_1 s_2 \dots s_n)) \\ & \quad p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n) \subseteq \\ & \bigcap_{p(s_1, s_2, \dots, s_n)} \varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n)) \\ & \quad p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n). \end{aligned} \quad (3)$$

The fact that for any three random variables A, B and C the inequality $I(A; B|C) + H(B'|BC) \geq I(A; B'|C)$ holds can be used in proving the following:

$$\begin{aligned} & \bigcap_{p(s_1, s_2, \dots, s_n)} \varphi(p(eL_1^n, eL_2^n | l_1^n l_2^n e, s_1 s_2 \dots s_n)) \\ & \quad p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n) \subseteq \\ & \bigcap_{p(s_1, s_2, \dots, s_n)} \left(\varphi(p(e\widehat{L}_1^n, e\widehat{L}_2^n | l_1^n l_2^n e, s_1 s_2 \dots s_n)) \right. \\ & \quad \left. p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n) \right) \oplus \Delta(\vec{v}), \end{aligned} \quad (4)$$

where \vec{v} is a vector whose elements are of the form $O(\epsilon) + O(\frac{h(\epsilon)}{n})$. Lastly, for any joint distribution $p(s_1, s_2, \dots, s_n)$, a 9-tuple $(U, V, W_0, W_1, W_2, L_1^n L_2^n E, S_1 S_2 \dots S_n, EL_1^n, EL_2^n)$ inside $\Upsilon_{p(eL_1^n, eL_2^n | l_1^n l_2^n e, s_1 s_2 \dots s_n) p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n)}$ is specified in the following that would imply that the point

$$\begin{aligned} & \left(\log b + nH(L_0), \log b + nH(L_0), \right. \\ & \quad \log b + nH(L_1), \log b + nH(L_2), \\ & \quad \left. \log b + nH(L_1), \dots, \log b + nH(L_1 L_2) \right), \end{aligned} \quad (5)$$

belongs to the set on the left hand side of equation 4. This fact together equations 3 and 2 complete the proof.

The 9-tuple

$$(U, V, W_0, W_1, W_2, L_1^n L_2^n E, S_1 S_2 \dots S_n, EL_1^n, EL_2^n)$$

is taken to be

$$\begin{aligned} & (A_0^n, A_1^n, EL_0^n, EL_1^n A_2^n, EL_2^n A_3^n, \\ & \quad L_1^n L_2^n E, S_1 S_2 \dots S_n, EL_1^n, EL_2^n), \end{aligned}$$

where $(A_0^n, A_1^n, A_2^n, A_3^n)$ is n i.i.d. repetitions of random variables (A_0, A_1, A_2, A_3) defined as follows:

Random variables A_0, A_1, A_2, A_3 are uniformly distributed on the alphabet set of L_0 (without loss of generality assumed to be $\{1, 2, 3, \dots, M_0\}$). Random variables A_2^n, A_3^n are taken to be mutually independent of each other and of

$(E, L_0^n, L_1^n, L_2^n, S_1 S_2 \dots S_n)$. The j^{th} of i.i.d repetitions of random variables A_0 and A_1 are then defined using the j^{th} copy of L_0 as follows:

$$A_{i,j} = 1 + (L_{0,j} + A_{i+2,j} \pmod{M_0}) \quad i = 0, 1.$$

From this definition, it is clear that A_0^n, A_1^n and $(E, L_0^n, L_1^n, L_2^n, S_1 S_2 \dots S_n)$ are mutually independent. Furthermore, $I(A_0^n; L_0^n | A_2^n) = I(A_1^n; L_0^n | A_3^n) = nH(L_0)$.

It can be verified that the 9-tuple satisfies all the required properties and that it implies the correctness of equation 5. \blacksquare

Proof: [Proof of Lemma 1] Using the properties of $\varphi(\cdot)$, for any $p(s_1, s_2, \dots, s_n)$ that factorizes as $p(s_1)p(s_2)\dots p(s_n)$, we can write:

$$\begin{aligned} & \varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n)) \\ & \quad p(l_1^n l_2^n e) p(s_1) p(s_2) \dots p(s_n) \subseteq \\ & \varphi(p(y'_0 \dots y'_{n-1}, z'_0 \dots z'_{n-1} | l_1^n l_2^n e, s_1 s_2 \dots s_{n-1}) \cdot p(l_1^n l_2^n e) \cdot \\ & \quad p(s_1) p(s_2) \dots p(s_{n-1})) \oplus \\ & \quad \varphi(q(y'_n, z'_n | x'_n, s_n) p(x'_n) p(s_n)) \subseteq \\ & \varphi(p(y'_0 \dots y'_{n-2}, z'_0 \dots z'_{n-2} | l_1^n l_2^n e, s_1 s_2 \dots s_{n-2}) \cdot p(l_1^n l_2^n e) \\ & \quad p(s_1) p(s_2) \dots p(s_{n-2})) \oplus \\ & \quad \varphi(q(y'_{n-1}, z'_{n-1} | x'_{n-1}, s_{n-1}) p(x'_{n-1}) p(s_{n-1})) \oplus \\ & \quad \varphi(q(y'_n, z'_n | x'_n, s_n) p(x'_n) p(s_n)) \subseteq \\ & \quad \dots \subseteq \\ & \varphi(p(y'_0 y'_1, z'_0 z'_1 | l_1^n l_2^n e, s_1) p(l_1^n l_2^n e) p(s_1)) \oplus \\ & \quad \varphi(q(y'_2, z'_2 | x'_2, s_2) p(x'_2) p(s_2)) \oplus \dots \\ & \quad \varphi(q(y'_n, z'_n | x'_n, s_n) p(x'_n) p(s_n)) \subseteq \\ & \quad \varphi(q(y'_1, z'_1 | x'_1, s_1) p(x'_1) p(s_1)) \oplus \\ & \quad \varphi(q(y'_2, z'_2 | x'_2, s_2) p(x'_2) p(s_2)) \oplus \dots \\ & \quad \varphi(q(y'_n, z'_n | x'_n, s_n) p(x'_n) p(s_n)) \oplus \\ & \quad \Delta(\{H(E), H(E), \dots, H(E)\}), \end{aligned} \quad (7)$$

where in equation 6 we have used the first property because

$$\begin{aligned} & p(y'_0 y'_1 \dots y'_n, z'_0 z'_1 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n) = \\ & p(y'_0 y'_1 \dots y'_{n-1}, z'_0 z'_1 \dots z'_{n-1} | l_1^n l_2^n e, s_1 s_2 \dots s_{n-1}) \cdot \\ & \quad p(y'_n, z'_n | x'_n, s_n), \end{aligned}$$

and furthermore $p(y'_n, z'_n | x'_n, s_n) = q(y'_n, z'_n | x'_n, s_n)$. In equation 7 we have used the second property.

Take some arbitrary $p(s)$ and assume that $p(s_i) \sim p(s)$ for all i . Using the fact that the conditional distributions $q(y'_i, z'_i | x'_i, s_i)$ for $i = 1, 2, \dots, n$ are all the same, we apply the third property to conclude that

$$\begin{aligned} & \varphi(q(y'_1, z'_1 | x'_1, s_1) p(x'_1) p(s_1)) \oplus \dots \\ & \quad \varphi(q(y'_n, z'_n | x'_n, s_n) p(x'_n) p(s_n)) \oplus \end{aligned}$$

$$\Delta(\{(H(E), H(E), \dots, H(E))\}) \subseteq$$

$$n \times \varphi(q(y, z|x, s)\tilde{p}(x)p(s)) \oplus \Delta(\{(\log b, \log b, \dots, \log b)\}),$$

for some $\tilde{p}(x)$ not depending on $p(s)$. Here $H(E)$ is replaced with its value, $\log b$. One can therefore conclude that whenever $p(s_i) \sim p(s)$,

$$\varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n) p(l_1^n l_2^n e) p(s_1) p(s_2) \dots p(s_n)) \subseteq$$

$$n \times \varphi(q(y, z|x, s)\tilde{p}(x)p(s)) \oplus \Delta(\{(\log b, \log b, \dots, \log b)\}).$$

Now, since restricting the set over which intersection is taken can not cause the intersection shrink, one can write:

$$\begin{aligned} & \bigcap_{p(s_1, s_2, \dots, s_n)} \varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n) \\ & \quad p(l_1^n l_2^n e) p(s_1 s_2 \dots s_n)) \subseteq \\ & \quad \bigcap_{\substack{p(s_1, s_2, \dots, s_n) = p(s_1)p(s_2)\dots p(s_n) \\ p(s_i) \sim p(s) \quad \forall i}} \left(\varphi(p(y'_0 \dots y'_n, z'_0 \dots z'_n | l_1^n l_2^n e, s_1 s_2 \dots s_n) \right. \\ & \quad \left. p(l_1^n l_2^n e) p(s_1) p(s_2) \dots p(s_n)) \right) \subseteq \\ & \quad \bigcap_{p(s)} \left(n \times \varphi(q(y, z|x, s)\tilde{p}(x)p(s)) \oplus \right. \\ & \quad \left. \Delta(\{(\log b, \log b, \dots, \log b)\}) \right) \subseteq \\ & \quad \bigcap_{p(s)} \left(n \times \varphi(q(y, z|x, s)\tilde{p}(x)p(s)) \oplus \right. \\ & \quad \left. \Delta(\{(\log b, \log b, \dots, \log b)\}) \right) \subseteq \quad (8) \\ & \quad n \times \phi(q(y, z|x, s)) \oplus \\ & \quad \Delta(\{(\log b, \log b, \dots, \log b)\}), \end{aligned}$$

where in 8, we have used the fact that $\tilde{p}(x)$ does not depend on $p(s)$. ■

Proof: [Proof of Lemma 2] *Property 1.* Take an arbitrary point \vec{v} inside $\varphi(p(yy', zz'|x, ss')p(x)p(s)p(s'))$. We would like to prove that there exists $\vec{v}_1 \in \varphi(p(y, z|x, s)p(x)p(s))$ and $\vec{v}_2 \in \varphi(q(y', z'|x', s')p(x')p(s'))$ and such that $\vec{v}_1 + \vec{v}_2 \geq \vec{v}$.

Since $\vec{v} \in \varphi(p(yy', zz'|x, ss')p(x)p(s)p(s'))$, there exists some U, V, W_0, W_1, W_2 created from X satisfying $UVW_0W_1W_2X - X - XSS'YY'ZZ'$, $H(W_0|W_1U) = H(W_0|W_2V) = 0$ and X being a deterministic function of (W_0, W_1, W_2, U, V) such that \vec{v} is coordinate by coordinate less than or equal to:

$$\begin{aligned} & \left(I(W_0; YY'|U), I(W_0; ZZ'|V), I(W_1; YY'|U), \right. \\ & \quad \dots \\ & \quad \left. I(W_0U; ZZ'|V) + I(W_2; ZZ'|W_0W_1UV) + \right. \end{aligned}$$

$$\left. I(W_1; YY'|W_0UV) \right).$$

Let $W'_0 = \widetilde{W}_0 = W_0$, $W'_1 = \widetilde{W}_1 = W_1$, $W'_2 = \widetilde{W}_2 = W_2$, $V' = VZ$, $U' = U$, $\widetilde{V} = V$, $\widetilde{U} = UY'$. The following properties hold:

- The Markov chain $U'V'W'_0W'_1W'_2X' - X' - X'S'Y'Z'$ holds. Also, $H(W'_0|W'_1U') = H(W'_0|W'_2V') = 0$ and X' is a deterministic function of $(W'_0, W'_1, W'_2, U', V')$.
- The Markov chain $\widetilde{U}\widetilde{V}\widetilde{W}_0\widetilde{W}_1\widetilde{W}_2X - X - XSYZ$ holds. Also, $H(\widetilde{W}_0|\widetilde{W}_1\widetilde{U}) = H(\widetilde{W}_0|\widetilde{W}_2\widetilde{V}) = 0$ and X is a deterministic function of $(\widetilde{W}_0, \widetilde{W}_1, \widetilde{W}_2, \widetilde{U}, \widetilde{V})$.

We can define points $\vec{v}_1 \in \varphi(p(y, z|x, s)p(x)p(s))$ and $\vec{v}_2 \in \varphi(q(y', z'|x', s')p(x')p(s'))$ using the above auxiliary random variables. It can be verified that $\vec{v}_1 + \vec{v}_2$ is coordinate by coordinate greater than or equal to \vec{v} .

Property 2. We would like to show that for any arbitrary $p(s')$:

$$\begin{aligned} & \varphi(p(yy', zz'|x, s')p(x)p(s')) \subseteq \\ & \varphi(q(y', z'|x', s')p(x')p(s')) \oplus \Delta(\{(H(Y), \dots, H(Y))\}). \end{aligned}$$

Take an arbitrary point inside

$$\varphi(p(yy', zz'|x, s')p(x)p(s')).$$

There exists some U, V, W_0, W_1, W_2 created from X satisfying $UVW_0W_1W_2 - X - S'X - Y'YZZ'$, $H(W_0|W_1U) = H(W_0|W_2V) = 0$ and X being a deterministic function of (W_0, W_1, W_2, U, V) such that the arbitrarily chosen point is coordinatewise dominated by:

$$\begin{aligned} \vec{v} = & \left(I(W_0; YY'|U), I(W_0; ZZ'|V), I(W_1; YY'|U), \right. \\ & \dots \\ & \left. I(W_0U; ZZ'|V) + I(W_2; ZZ'|W_0W_1UV) + \right. \\ & \left. I(W_1; YY'|W_0UV) \right). \end{aligned}$$

Since Y and Z are equal with probability one, one can replace Z with Y whenever it appears in the above mutual information terms. Using the chain rule, one can write the above vector as the summation of \vec{v}_1 and \vec{v}_2 defined as follows:

$$\begin{aligned} \vec{v}_1 = & \left(I(W_0; Y|U), I(W_0; Y|V), I(W_1; Y|U), I(W_2; Y|V), \right. \\ & \left. I(W_1; Y|W_0UV) + I(W_0U; Y|V), \right. \\ & \dots \\ & \left. I(W_0U; Y|V) + I(W_2; Y|W_0W_1UV) + I(W_1; Y|W_0UV) \right); \\ \vec{v}_2 = & \left(I(W_0; Y'|UY), I(W_0; Z'|VY), I(W_1; Y'|UY), \right. \\ & \dots \\ & \left. I(W_0U; Z'|VY) + I(W_2; Z'|W_0W_1UVY) \right. \\ & \left. + I(W_1; Y'|W_0UVY) \right). \end{aligned}$$

It can be verified that $\vec{v}_1 \in \Delta\{(H(Y), H(Y), \dots, H(Y))\}$. We finish the proof by showing that $\vec{v}_2 \in \varphi(q(y', z'|x', s')p(x')p(s'))$.

Let $(\widehat{W}_0, \widehat{W}_1, \widehat{W}_2, \widehat{U}, \widehat{V}, \widehat{X}, \widehat{S}, \widehat{Y}, \widehat{Z})$ be equal to $(W_0, W_1, W_2, UY, VY, X', S', Y', Z')$. It can be shown that X' is a deterministic function of (W_0, W_1, W_2, UY, VY) , $H(\widehat{W}_0|\widehat{W}_1\widehat{U}) = H(\widehat{W}_0|\widehat{W}_2\widehat{V}) = 0$. Furthermore the Markov chain $(UY)(VY)W_0W_1W_2 - X' - S'X' - Y'Z'$ holds (for the details, see [7]). This completes the proof of \vec{v}_2 belonging to $\varphi(q(y', z'|x', s')p(x')p(s'))$.

Property 3. Let $p_\lambda(x) = (1-\lambda) \cdot p_0(x) + \lambda \cdot p_1(x)$. We will show that for any $p(s)$, whenever $\vec{a} = (a_0, a_1, a_2, \dots, a_9) \in \varphi(q(y, z|x, s)p_0(x)p(s))$ and $\vec{b} = (b_0, b_1, b_2, \dots, b_9) \in \varphi(q(y, z|x, s)p_1(x)p(s))$,

$$(1-\lambda)\vec{a} + \lambda\vec{b} \in \varphi(q(y, z|x, s)p_\lambda(x)p(s)).$$

Since \vec{a} is inside $\varphi(q(y, z|x, s)p_0(x)p(s))$, there exists a distribution

$$p(u_a v_a w_{0a} w_{1a} w_{2a} x_a) p(s_a) q(y_a, z_a | x_a, s_a) \in \Upsilon_{p(x_a)p(s_a)q(y_a, z_a | x_a, s_a)},$$

where $p(s_a) \sim p(s)$ and $p(x_a) \sim p_0(x)$ for which the following inequalities are satisfied:

- $a_0 \leq I(W_{0a}; Y_a | U_a)$;
- $a_1 \leq I(W_{0a}, Z_a | V_a)$;
- ...
- $a_9 \leq I(W_{0a} U_a V_a; Z_a) + I(W_{2a}; Z_a | W_{0a} W_{1a} U_a V_a) + I(W_{1a}; Y_a | W_{0a} U_a V_a)$.

A similar statement holds for (b_0, b_1, \dots, b_9) involving random variables $(U_b, V_b, W_{0b}, W_{1b}, W_{2b}, X_b, S_b, Y_b, Z_b)$.

Without loss of generality, one can assume that $(U_a, V_a, W_{0a}, W_{1a}, W_{2a}, X_a, S_a, Y_a, Z_a)$ is independent of $(U_b, V_b, W_{0b}, W_{1b}, W_{2b}, X_b, S_b, Y_b, Z_b)$.

Take a binary random variable T on $\{0, 1\}$ satisfying $p(T = 1) = \lambda$ that is independent of all the above mentioned random variables. Let $(U, V, W_0, W_1, W_2, X, S, Y, Z)$ be equal to

$$(TU_a, TV_a, TW_{0a}, W_{1a}, W_{2a}, X_a, S_a, Y_a, Z_a)$$

if $T = 0$, and be equal to

$$(TU_b, TV_b, TW_{0b}, W_{1b}, W_{2b}, X_b, S_b, Y_b, Z_b)$$

if $T = 1$.

X has the distribution $p_\lambda(x)$ we started with, and S has the distribution $p(s)$ we started with. It can be proved that $p(y, z|x, s) = q(y, z|x, s)$ and that random variables $(U, V, W_0, W_1, W_2, X, S, Y, Z)$ have joint distribution $p(u, v, w_0, w_1, w_2, x)p(s)q(y, z|x, s)$

belonging to $\Upsilon_{q(y, z|x, s)p_\lambda(x)p(s)}$. Furthermore this choice of variables gives us a point in $\varphi(q(y, z|x, s)p_\lambda(x)p(s))$ that coordinatewise dominates $(1-\lambda)\vec{a} + \lambda\vec{b}$. For the details, see [7]. ■

VI. ACKNOWLEDGMENT

The authors would like to thank TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia and United Technologies, for their support of this work. The research was also partially supported by NSF grants CCF-0500023, CCF-0635372, and CNS-0627161.

REFERENCES

- [1] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.
- [2] I. Csiszár and J. Körner, "Information Theory: Coding Theorems for Discrete Memoryless Systems." Budapest, Hungary: Akademiai Kiad, 1981.
- [3] P. Gács and J. Körner, "Common information is much less than mutual information," *Probl. Contr. Inf. Theory*, Vol. 2, pp. 149-162 (1973).
- [4] S. I. Gel'fand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Inf. Transm.*, 16 (1): 1725 (1980).
- [5] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals – Part I: Source model," *Preprint*, Dec. 2007. Available at <http://www.eecs.berkeley.edu/~aminzade/SourceModel.pdf>
- [6] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals – Part II: Channel model," *Preprint*, Dec. 2007. Available at <http://www.eecs.berkeley.edu/~aminzade/ChannelModel.pdf>
- [7] A. A. Gohari and V. Anantharam, "An Outer Bound to the Admissible Source Region of Broadcast Channels with Arbitrarily Correlated Sources and Channel Variations", *in preparation*, 2008.
- [8] Te Han, M. Costa, "Broadcast channels with arbitrarily correlated sources," *IEEE Trans. Inform. Theory* 33(5): 641- 650 (1987)
- [9] E. Hof, Shraga I. Bross: "On the deterministic-code capacity of the two-user discrete memoryless arbitrarily varying general broadcast channel with degraded message sets," *IEEE Trans. Inform. Theory* 52(11): 5023-5044 (2006)
- [10] J. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. Inform. Theory*, 27(2): 212-226 (1981).
- [11] Y. Liang, G. Kramer, "Rate regions for relay broadcast channels," *IEEE Trans. Inform. Theory*, 53(10): 3517-3535 (2007).
- [12] Y. Liang, G. Kramer, and S. Shamai (Shitz), "Capacity outer bounds for broadcast channels," 2008 IEEE Inf. Theory Workshop, Porto, Portugal, pp. 2-4, May 5-9, 2008.
- [13] K Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inform. Theory*, 25(3): 306-311 (1979).
- [14] C. Nair, "An outer bound for 2-receiver discrete memoryless broadcast channels," Available at <http://chandra.ie.cuhk.edu.hk/pub/papers/outerbound.pdf>
- [15] C. Nair and A. A. El Gamal, "An outer bound to the capacity region of the broadcast channel," *IEEE Trans. Inform. Theory*, 53(1): 350-355 (2007).
- [16] C. Nair and V.W. Zizhou, "On the inner and outer bounds for 2-receiver discrete memoryless broadcast channels," *Proceedings of the ITA workshop*, San Diego, 2008.