

Evaluation of Marton's Inner Bound for the General Broadcast Channel

Amin Aminzadeh Gohari
 EECS Department
 University of California
 Berkeley, CA 94720, USA
 Email: aminzade@eecs.berkeley.edu

Venkat Anantharam
 EECS Department
 University of California
 Berkeley, CA 94720, USA
 Email: ananth@eecs.berkeley.edu

Abstract—The best known inner bound on the two-receiver general broadcast channel without a common message is due to Marton [3]. This result was subsequently generalized in [2, p. 391, Problem 10(c)] and [4] to broadcast channels with a common message. However the latter region is not computable (except in certain special cases) as no bounds on the cardinality of its auxiliary random variables exist. Nor is it even clear that the inner bound is a closed set. The main obstacle in proving cardinality bounds is the fact that the Carathéodory theorem, the main known tool for proving cardinality bounds, does not yield a finite cardinality result. Our new tool is based on an identity that relates the second derivative of the Shannon entropy of a discrete random variable (under a certain perturbation) to the corresponding Fisher information. In order to go beyond the traditional Carathéodory type arguments, we identify certain properties that the auxiliary random variables corresponding to the extreme points of the inner bound satisfy. These properties are then used to establish cardinality bounds on the auxiliary random variables of the inner bound, thereby proving the computability of the region, and its closedness.

Although existence of cardinality bounds renders Marton's inner bound computable, it is still hard to evaluate the region. It is however shown that the computation can be significantly simplified if we further assume that Marton's inner bound and the recent outer bound of Nair and El Gamal match at the given particular channel. In order to demonstrate this, we consider a large class of binary input broadcast channels and compute maximum of the sum rate of private messages assuming that the inner and the outer bound match at the given broadcast channel. We also show that the inner and the outer bound do not match for some broadcast channels, thus establishing a conjecture of [15].

I. INTRODUCTION

In this paper, we consider two-receiver general broadcast channels. 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. Let \mathcal{X} , \mathcal{Y} and \mathcal{Z} denote the alphabet set of X , Y and Z respectively. The transmitter wants to send a common message, M_0 , to both the receivers and two private messages M_1 and M_2 to Y and Z respectively. Assume that M_i (for $i = 0, 1, 2$) is a uniform random variable over set \mathcal{M}_i . The transmitter maps the messages into a codeword of length n using an encoding function $\zeta : \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \rightarrow \mathcal{X}^n$, and sends it over the broadcast channel $q(y, z|x)$ in n times steps. The receivers use the decoding functions $\vartheta_y : \mathcal{Y}^n \rightarrow \mathcal{M}_0 \times$

\mathcal{M}_1 and $\vartheta_z : \mathcal{Z}^n \rightarrow \mathcal{M}_0 \times \mathcal{M}_2$ to map their received signals to $(\widehat{M}_0^{(1)}, \widehat{M}_1)$ and $(\widehat{M}_0^{(2)}, \widehat{M}_2)$ respectively. The average probability of error is then taken to be the probability that $(\widehat{M}_0^{(1)}, \widehat{M}_1, \widehat{M}_0^{(2)}, \widehat{M}_2)$ is not equal to (M_0, M_1, M_0, M_2) .

The capacity region of the broadcast channel is defined as the set of all triples (R_0, R_1, R_2) such that for any $\epsilon > 0$, there is some integer n , uniform random variables M_0, M_1, M_2 with alphabet sets $|\mathcal{M}_i| \geq 2^{n(R_i - \epsilon)}$ (for $i = 0, 1, 2$), encoding function ζ , and decoding functions ϑ_y and ϑ_z such that the average probability of error is less than or equal to ϵ .

The capacity region of the broadcast channel is not known except in certain special cases. Several inner bounds to the capacity region are however available. In an early work, Hajek and Pursley derived cardinality bounds for the inner bound of Cover and van der Meulen when X is binary, i.e. $|\mathcal{X}| = 2$, and R_0 is zero [5]. They also showed that X can be taken as a deterministic function of the auxiliary random variables involved. Hajek and Pursley also conjectured certain cardinality bounds on the auxiliary random variables when $|\mathcal{X}|$ is arbitrary but R_0 is equal to zero. For the case of non-zero R_0 , Hajek and Pursley commented that finding cardinality bounds appears to be considerably more difficult. Soon afterwards Marton [3, Theorem 2] proved a new achievable region of triples $(0, R_1, R_2)$ for the broadcast channel. Marton's work was subsequently generalized in [2, p. 391, Problem 10(c)], and Gelfand and Pinsker [4] who established the achievability of the region formed by taking union over random variables U, V, W, X, Y, Z , having the joint distribution $p(u, v, w, x, y, z) = p(u, v, w, x)q(y, z|x)$, of

$$R_0, R_1, R_2 \geq 0;$$

$$R_0 \leq \min(I(W; Y), I(W; Z)); \quad (1)$$

$$R_0 + R_1 \leq I(UW; Y); \quad (2)$$

$$R_0 + R_2 \leq I(VW; Z); \quad (3)$$

$$R_0 + R_1 + R_2 \leq I(U; Y|W) + I(V; Z|W) - I(U; V|W) + \min(I(W; Y), I(W; Z)). \quad (4)$$

Please note that the auxiliaries U, V and W may be discrete or continuous random variables. Following [10], we call this region the Marton-Gelfand-Pinsker region. Recently Liang and Kramer reported an apparently larger inner bound to

the broadcast channel [9], which however turns out to be equivalent to the Marton-Gelfand-Pinsker region [10]. The Marton-Gelfand-Pinsker region therefore remains to be the currently best known inner bound on the general broadcast channel. Liang, Kramer and Poor showed that in order to evaluate the Marton-Gelfand-Pinsker region, it suffices to search over $p(u, v, w, x)$ for which either $I(W; Y) = I(W; Z)$, or $I(W; Y) > I(W; Z) \& V = \text{constant}$, or $I(W; Y) < I(W; Z) \& U = \text{constant}$ holds [10]. This restriction however does not lead to a computable characterization of the region.

Unfortunately Marton-Gelfand-Pinsker's region is not computable (except in certain special cases) as no bounds on the cardinality of its auxiliary random variables exist. A Carathéodory-type argument results in a cardinality bound of $|\mathcal{V}||\mathcal{X}| + 1$ on $|\mathcal{U}|$, and a cardinality bound of $|\mathcal{U}||\mathcal{X}| + 1$ on $|\mathcal{V}|$. This does not lead to fixed cardinality bounds on the auxiliaries U and V . The main result of this paper is to prove that the subset of Marton-Gelfand-Pinsker region defined by imposing extra constraints $|\mathcal{U}| \leq |\mathcal{X}|$, $|\mathcal{V}| \leq |\mathcal{X}|$, $|\mathcal{W}| \leq |\mathcal{X}| + 4$ and $H(X|UVW) = 0$ is identical to the Marton-Gelfand-Pinsker region.

At the heart of our technique lies the following observation: consider an arbitrary set of finite random variables X_1, X_2, \dots, X_n jointly distributed according to $p_0(x_1, x_2, \dots, x_n)$. One can represent a perturbation of this joint distribution by a vector consisting of the first derivative of the individual probabilities $p_0(x_1, x_2, \dots, x_n)$ for all values of x_1, x_2, \dots, x_n . We however suggest the following perturbation that can be represented by a real valued random variable, L , jointly distributed by X_1, X_2, \dots, X_n and satisfying $\mathbb{E}[L] = 0$, $|\mathbb{E}[L|X_1 = x_1, X_2 = x_2, \dots, X_n = x_n]| < \infty$ for all values of x_1, x_2, \dots, x_n :

$$p_\epsilon(\widehat{X}_1 = x_1, \dots, \widehat{X}_n = x_n) = p_0(X_1 = x_1, \dots, X_n = x_n) \cdot (1 + \epsilon \cdot \mathbb{E}[L|X_1 = x_1, \dots, X_n = x_n]),$$

where ϵ is a real number in some interval $(-\bar{\epsilon}_1, \bar{\epsilon}_2)$. Random variable L is a canonical way of representing the direction of perturbation since given any subset of indices $I \subset \{1, 2, 3, \dots, n\}$, one can verify that the following equation for the marginal distribution of random variables \widehat{X}_i for $i \in I$:

$$p_\epsilon(\widehat{X}_{i \in I} = x_{i \in I}) = p_0(X_{i \in I} = x_{i \in I}) \cdot (1 + \epsilon \cdot \mathbb{E}[L|X_{i \in I} = x_{i \in I}]).$$

Furthermore for any set of indices $I \subset \{1, 2, 3, \dots, n\}$, the second derivative of the joint entropy of random variables \widehat{X}_i for $i \in I$ as a function of ϵ is related to the problem of MMSE estimation of L from $X_{i \in I}$:

$$\frac{\partial^2}{\partial \epsilon^2} H(\widehat{X}_{i \in I})|_{\epsilon=0} = -\log e \cdot \mathbb{E}[\mathbb{E}[L|X_{i \in I}]^2].$$

Lemma 1 describes a generic version of the above identity that relates the second derivative of the Shannon entropy of a discrete random variable to the corresponding Fisher information. This identity is to best of our knowledge new.

It is repeatedly invoked in our proofs to compute the second derivative of various expressions.

It is known that the Marton-Gelfand-Pinsker region coincides the best known outer bound for the degraded, less noisy, more capable, and semi-deterministic broadcast channels. Nair and Zizhou showed that the Marton-Gelfand-Pinsker's inner bound and the recent outer bound of Nair and El Gamal are different for a BSSC channel with parameter $\frac{1}{2}$ if the following conjecture holds [15, Conjecture 1]: Given any five random variables U, V, X, Y, Z satisfying $I(UV; YZ|X) = 0$, the inequality $I(U; Y) + I(V; Z) - I(U; V) \leq \max(I(X; Y), I(X; Z))$ holds whenever X, Y and Z are binary random variables and the channel $p(y, z|x)$ is BSSC with parameter $\frac{1}{2}$. In this paper, we provide examples of broadcast channels for which the two bounds do not match. A few days before the submission of this paper, the authors were informed that Nair believes he has proved the existence of a gap for the BSSC channel by establishing the conjecture of [15, Conjecture 1].

The outline of this paper is as follows. In section II, we introduce the basic notations and definitions used in this paper. Section III contains the main results of the paper. Section IV sketches the proofs and discusses the main ideas of the paper at an intuitive level. Formal proofs are provided in [16].

II. DEFINITIONS AND NOTATIONS

Let \mathbb{R} denote the set of real numbers. All the logarithms throughout this paper are in base two, unless stated otherwise. Let $\mathcal{C}(q(y, z|x))$ denote the capacity region of the broadcast channel $q(y, z|x)$. We use $X_{1:k}$ to denote (X_1, X_2, \dots, X_k) ; similarly we use $Y_{1:k}$ and $Z_{1:k}$ to denote (Y_1, Y_2, \dots, Y_k) and (Z_1, Z_2, \dots, Z_k) respectively.

Definition 1: Let $\mathcal{C}_{MGP}(q(y, z|x))$ denote Marton-Gelfand-Pinsker's inner bound on the channel $q(y, z|x)$. $\mathcal{C}_{MGP}(q(y, z|x))$ is defined as the union over random variables U, V, W, X, Y, Z , having the joint distribution $p(u, v, w, x, y, z) = p(u, v, w, x)q(y, z|x)$, of non-negative triples (R_0, R_1, R_2) satisfying equations 1, 2, 3 and 4. Please note that the auxiliaries U, V and W may be discrete or continuous random variables.

Definition 2: The region $\mathcal{C}_{MGP}^{S_u, S_v, S_w}(q(y, z|x))$ is defined as the union over discrete random variables U, V, W, X, Y, Z satisfying the cardinality bounds $|\mathcal{U}| \leq S_u$, $|\mathcal{V}| \leq S_v$ and $|\mathcal{W}| \leq S_w$, and having the joint distribution $p(u, v, w, x, y, z) = p(u, v, w, x)q(y, z|x)$, of non-negative triples (R_0, R_1, R_2) satisfying equations 1, 2, 3 and 4. Note that $\mathcal{C}_{MGP}^{S_u, S_v, S_w}(q(y, z|x)) \subset \mathcal{C}_{MGP}^{S'_u, S'_v, S'_w}(q(y, z|x))$ whenever $S_u \leq S'_u$, $S_v \leq S'_v$ and $S_w \leq S'_w$.

Definition 3: The region $\mathcal{C}(q(y, z|x))$ is defined as the union over discrete random variables U, V, W, X, Y, Z satisfying the cardinality bounds $|\mathcal{U}| \leq |\mathcal{X}|$, $|\mathcal{V}| \leq |\mathcal{X}|$ and $|\mathcal{W}| \leq |\mathcal{X}| + 4$, and having the joint distribution $p(u, v, w, x, y, z) = p(u, v, w, x)q(y, z|x)$ for which $H(X|UVW) = 0$, of non-negative triples (R_0, R_1, R_2) satisfying equations 1, 2, 3 and 4.

Definition 4: Given broadcast channel $q(y, z|x)$, let $\mathcal{C}_{NE}(q(y, z|x))$ denote the union over random variables U, V, W, X, Y, Z , having the joint distribution $p(u, v, w, x, y, z) = p(u)p(v)p(w|u, v)p(x|u, v, w)q(y, z|x)$, of

$$\begin{aligned} R_0, R_1, R_2 &\geq 0; \\ R_0 &\leq \min(I(W; Y), I(W; Z)); \\ R_0 + R_1 &\leq I(UW; Y); \\ R_0 + R_2 &\leq I(VW; Z); \\ R_0 + R_1 + R_2 &\leq I(UW; Y) + I(V; Z|UW); \\ R_0 + R_1 + R_2 &\leq I(VW; Z) + I(U; Y|VW). \end{aligned}$$

$\mathcal{C}_{NE}(q(y, z|x))$ is shown in [11] to be an outer bound to the capacity region of the broadcast channel. Recently there has been a series of outer bounds on the broadcast channel [11][12][13][14]. Among these outer bounds, only the outer bound of Nair and El Gamal [11] is computable as no cardinality bounds are known for the other outer bounds.

Definition 5: Given any finite random variable X , and real valued random variable L where $|\mathbb{E}[L|X = x]| < \infty$ for all $x \in \mathcal{X}$, $H_L(X)$ is defined as

$$H_L(X) = \sum_{x \in \mathcal{X}} p(X = x) \mathbb{E}[L|X = x] \log \frac{1}{p(X = x)}.$$

The motivation for defining $H_L(X)$ will become clear later. Note that $H_L(X)$ is linear in $\mathbb{E}[L|X = x]$ and in L , and can in general become negative. If L is a constant random variable equal to 1, $H_L(X)$ reduces to the Shannon's entropy.

Given finite random variables X and Y , and real valued random variable L where $|\mathbb{E}[L|X = x, Y = y]| < \infty$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $H_L(X|Y)$ and $I_L(X; Y)$ are defined as follows: $H_L(X|Y) = \sum_{y \in \mathcal{Y}} p(Y = y) H_L(X|Y = y)$, where

$$H_L(X|Y = y) =$$

$$\sum_{x \in \mathcal{X}} p(X = x|Y = y) \mathbb{E}[L|X = x, Y = y] \log \frac{1}{p(X = x|Y = y)},$$

and $I_L(X; Y)$ is equal to

$$\sum_{x, y \in (\mathcal{X}, \mathcal{Y})} p(X = x, Y = y) \mathbb{E}[L|X = x, Y = y] \times \log \frac{p(X = x, Y = y)}{p(X = x)p(Y = y)}.$$

It can be verified that $I_L(X; Y) = H_L(X) - H_L(X|Y) = H_L(Y) - H_L(Y|X)$.

III. STATEMENT OF RESULTS

Theorem 1: For any arbitrary broadcast channel $q(y, z|x)$, the closure of $\mathcal{C}_{MGP}(q(y, z|x))$ is equal to $\mathcal{C}(q(y, z|x))$.

Corollary 1: $\mathcal{C}_{MGP}(q(y, z|x))$ is closed since $\mathcal{C}(q(y, z|x))$ is also a subset of $\mathcal{C}_{MGP}(q(y, z|x))$.

Lemma 1: Given any finite random variable X , and real valued random variable L where $|\mathbb{E}[L|X = x]| < \infty$ for all $x \in \mathcal{X}$, and $\mathbb{E}[L] = 0$, let random variable \hat{X} be defined on the same alphabet set as X according to $p_\epsilon(\hat{X} = x) = p_0(X = x) \cdot (1 + \epsilon \cdot \mathbb{E}[L|X = x])$, where ϵ is a real number in the interval $(-\bar{\epsilon}_1, \bar{\epsilon}_2)$. $\bar{\epsilon}_1$ and $\bar{\epsilon}_2$ are positive reals for which

$1 - \bar{\epsilon}_1 \cdot \mathbb{E}[L|X = x] \geq 0$ and $1 + \bar{\epsilon}_2 \cdot \mathbb{E}[L|X = x] \geq 0$ hold for all $x \in \mathcal{X}$. Then

- 1) $H(\hat{X})|_{\epsilon=0} = H(X)$, and $\frac{\partial}{\partial \epsilon} H(\hat{X})|_{\epsilon=0} = H_L(X)$.
- 2) $\forall \epsilon \in (-\bar{\epsilon}_1, \bar{\epsilon}_2)$, $\frac{\partial^2}{\partial \epsilon^2} H(\hat{X}) = -\log e \cdot \mathbb{E}\left[\frac{\mathbb{E}[L|X]^2}{1 + \epsilon \cdot \mathbb{E}[L|X]}\right] = -\log(e) \cdot I(\epsilon)$ where the Fisher Information $I(\epsilon)$ is defined as $I(\epsilon) = \sum_x \left(\frac{\partial}{\partial \epsilon} \log_e(p_\epsilon(\hat{X} = x))\right)^2 p_\epsilon(\hat{X} = x)$. In particular $\frac{\partial^2}{\partial \epsilon^2} H(\hat{X})|_{\epsilon=0} = -\log e \cdot \mathbb{E}[\mathbb{E}[L|X]^2]$.
- 3) $H(\hat{X}) = H(X) + \epsilon H_L(X) - \mathbb{E}[r(\epsilon \cdot \mathbb{E}[L|X])]$ where $r(x) = (1 + x) \log(1 + x)$.

A. On binary input broadcast channels

In this section, we study binary input broadcast channels, that is when $|\mathcal{X}| = 2$. It therefore suffices to consider binary random variables U and V . The cardinality of W would be six and X can be taken to be a deterministic function of (U, V, W) . Still, the region is hard to evaluate. We however demonstrate that the computation can be greatly simplified if we make the extra assumption that $\mathcal{C}_{MGP}(q(y, z|x))$ and the recent outer bound of Nair and El Gamal, $\mathcal{C}_{NE}(q(y, z|x))$, match at the given broadcast channel $q(y, z|x)$. We demonstrate this by computing maximum of the sum rate $R_1 + R_2$ over all triples (R_0, R_1, R_2) in $\mathcal{C}_{MGP}(q(y, z|x))$. For simplicity, we assume that for any $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, $p(Y = y|X = 0)$, $p(Y = y|X = 1)$, $p(Z = z|X = 0)$ and $p(Z = z|X = 1)$ are non-zero. This is a mild assumption since an arbitrarily small perturbation of a broadcast channel would place it in this class.

Theorem 2: Take an arbitrary binary input broadcast channel $q(y, z|x)$ such that for all $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, $q(Y = y|X = 0)$, $q(Y = y|X = 1)$, $q(Z = z|X = 0)$ and $q(Z = z|X = 1)$ are non-zero. Assuming that $\mathcal{C}_{MGP}(q(y, z|x)) = \mathcal{C}_{NE}(q(y, z|x))$, maximum of the sum rate $R_1 + R_2$ over triples (R_0, R_1, R_2) in the Marton-Gelfand-Pinsker's inner bound is equal to the maximum of

$$\min_{\gamma \in [0, 1]} \left(\max_{\substack{p(w|x)q(y, z|x) \\ |W| = 2}} \left\{ \right. \right.$$

$$\left. \left. \gamma I(W; Y) + (1 - \gamma) I(W; Z) + \sum_w p(w) T(p(X = 1|W = w)) \right\} \right)$$

and

$$\max_{\substack{p(u, v)p(x|uv)q(y, z|x) \\ |\mathcal{U}| = |\mathcal{V}| = 2, I(U; V) = 0, H(X|UV) = 0}} I(U; Y) + I(V; Z),$$

where $T(p) = \max\{I(X; Y), I(X; Z)|P(X = 1) = p\}$.

Remark 1: The expression given in equation 2 is always a lower bound on the maximum of the sum rate $R_1 + R_2$ over triples (R_0, R_1, R_2) in the Marton-Gelfand-Pinsker's inner bound whether $\mathcal{C}_{MGP}(q(y, z|x))$ is equal to $\mathcal{C}_{NE}(q(y, z|x))$ or not.

Corollary 2: Take an arbitrary binary input broadcast channel $q(y, z|x)$ such that for all $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, $q(Y = y|X = 0)$, $q(Y = y|X = 1)$, $q(Z = z|X = 0)$ and $q(Z = z|X = 1)$ are non-zero. If the expression of equation 2 turns out to be strictly less than the maximum of the sum

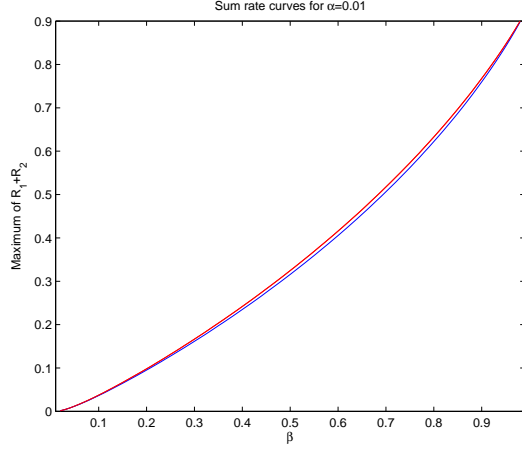


Fig. 1. Red curve (top curve): sum rate for $C_{NE}(q(y, z|x))$; Blue curve (bottom curve): sum rate for $C_{MGP}(q(y, z|x))$ assuming that $C_{NE}(q(y, z|x)) = C_{MGP}(q(y, z|x))$.

rate $R_1 + R_2$ over triples (R_0, R_1, R_2) in $C_{NE}(q(y, z|x))$ (which is given in [15]), it will serve as an evidence for $C_{MGP}(q(y, z|x)) \neq C_{NE}(q(y, z|x))$. The maximum of the sum rate $R_1 + R_2$ over triples (R_0, R_1, R_2) in $C_{NE}(q(y, z|x))$ is known to be (see Bound 4 in [15])

$$\max_{\substack{p(u, v, x)q(y, z|x) \\ |\mathcal{U}| = |\mathcal{V}| = 3, I(U; V|X) = 0}} \min \left(I(U; Y) + I(V; Z), \right. \\ \left. I(U; Y) + I(X; Z|U), I(V; Z) + I(X; Y|V) \right).$$

There are examples for which the expression of equation 2 turns out to be strictly less than the maximum of the sum rate $R_1 + R_2$ over triples (R_0, R_1, R_2) in $C_{NE}(q(y, z|x))$. For instance given any two positive reals α and β in the interval $(0, 1)$, consider the broadcast channel for which $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{Z}| = 2$, $p(Y = 0|X = 0) = \alpha$, $p(Y = 0|X = 1) = \beta$, $p(Z = 0|X = 0) = 1 - \beta$, $p(Z = 0|X = 1) = 1 - \alpha$. Assuming $\alpha = 0.01$, Figure 1 plots maximum of the sum rate for $C_{NE}(q(y, z|x))$, and maximum of the sum rate for $C_{MGP}(q(y, z|x))$ (assuming that $C_{NE}(q(y, z|x)) = C_{MGP}(q(y, z|x))$) as a function of β . Where the two curves do not match, Nair and El Gamal's outer bound and Marton-Gelfand-Pinsker's inner bound can not be equal for the corresponding broadcast channel.

IV. PROOFS

In this section, we sketch the proof of Theorem 1 at an intuitive level. See [16] for the details and formal proofs.

Proof of Theorem 1 begins by showing that the closure of $C_{MGP}(q(y, z|x))$ is equal to the closure of $\bigcup_{S_u, S_v, S_w \geq 0} C_{MGP}^{S_u, S_v, S_w}(q(y, z|x))$. If the auxiliary random variables U, V and W are discrete but not finite, one can truncate these random variables to get finite random variables while preserving the mutual information terms $I(W; Y)$, $I(W; Z)$, $I(UW; Y)$, etc to an arbitrarily high accuracy. If the auxiliaries are continuous, one can quantize them to

get discrete random variables while again preserving the terms $I(W; Y)$, $I(W; Z)$, $I(UW; Y)$, etc to an arbitrarily high accuracy. Next, it is shown that $\mathcal{C}(q(y, z|x))$ is equal to $C_{MGP}^{|\mathcal{X}|, |\mathcal{X}|, |\mathcal{X}|+4}(q(y, z|x))$. We therefore need to show that the closure of $\bigcup_{S_u, S_v, S_w \geq 0} C_{MGP}^{S_u, S_v, S_w}(q(y, z|x))$ is equal to $C_{MGP}^{|\mathcal{X}|, |\mathcal{X}|, |\mathcal{X}|+4}(q(y, z|x))$. The region $C_{MGP}^{|\mathcal{X}|, |\mathcal{X}|, |\mathcal{X}|+4}(q(y, z|x))$ is shown to be a closed set using the fact that the cardinality of the auxiliary random variables are bounded. We therefore need to show that for any arbitrary value of S_u, S_v and S_w , $C_{MGP}^{S_u, S_v, S_w}(q(y, z|x))$ is a subset of $C_{MGP}^{|\mathcal{X}|, |\mathcal{X}|, |\mathcal{X}|+4}(q(y, z|x))$.

The proof of the latter statement is lengthy and is provided in [16]. In order to demonstrate the proof idea, let us consider the problem of finding the supremum of

$$I(U; Y) + I(V; Z) - I(U; V) + \lambda I(U; Y) + \gamma I(V; Z)$$

over all joint distributions $p(uvx)q(y, z|x)$ where the auxiliary random variables U, V satisfy the cardinality bounds of S_u and S_v , and λ and γ are arbitrary non-negative reals. We would like to show that it suffices to take the maximum over random variables U and V with the cardinality bounds of $|\mathcal{X}|$. Although this is a different problem, but its proof conveys the main intuitions.

Since the cardinalities of the U and V are bounded, one can show that the supremum of $I(U; Y) + I(V; Z) - I(U; V) + \lambda I(U; Y) + \gamma I(V; Z)$ is a maximum, and is obtained at some joint distribution $p_0(u, v, x, y, z) = p_0(u, v, x)q(y, z|x)$. Take an arbitrary function $L : \mathcal{U} \times \mathcal{V} \times \mathcal{X} \rightarrow \mathbb{R}$ where $\mathbb{E}[L(U, V, X)] = 0$. Let us then perturb this joint distribution by defining random variables $\hat{U}, \hat{V}, \hat{X}, \hat{Y}$ and \hat{Z} distributed according to

$$p_\epsilon(\hat{U} = u, \hat{V} = v, \hat{X} = x, \hat{Y} = y, \hat{Z} = z) = \\ p_0(U = u, V = v, X = x, Y = y, Z = z) \cdot \\ (1 + \epsilon \cdot \mathbb{E}[L(U, V, X)|U = u, V = v, X = x, Y = y, Z = z]),$$

or equivalently according to

$$p_\epsilon(\hat{U} = u, \hat{V} = v, \hat{X} = x, \hat{Y} = y, \hat{Z} = z) = \\ p_0(U = u, V = v, X = x, Y = y, Z = z)(1 + \epsilon \cdot L(u, v, x)).$$

The parameter ϵ is a real number that can take value in $(-\bar{\epsilon}_1, \bar{\epsilon}_2)$ where $\bar{\epsilon}_1$ and $\bar{\epsilon}_2$ are some positive reals. Since L is a function of U, V and X only, for any value of ϵ , the Markov chain $\hat{U}\hat{V} - \hat{X} - \hat{Y}\hat{Z}$ holds, and $p(\hat{Y} = y, \hat{Z} = z|\hat{X} = x)$ is equal to $q(Y = y, Z = z|X = x)$ for all x, y, z where $q(X = x) > 0$.

The expression $I(\hat{U}; \hat{Y}) + I(\hat{V}; \hat{Z}) - I(\hat{U}; \hat{V}) + \lambda I(\hat{U}; \hat{Y}) + \gamma I(\hat{V}; \hat{Z})$ as a function of ϵ achieves its maximum at $\epsilon = 0$. Therefore its first derivative at $\epsilon = 0$ should be zero, and its second derivative should be less than or equal to zero. In order to compute the second derivative, one can extend the expression as entropy terms and use Lemma 1 to compute the second derivative of each term. In order to simplify the expression let us make the further assumption that $\mathbb{E}[L(U, V, X)|X] = 0$. This implies that the marginal distribution of X is fixed since

$$p_\epsilon(\hat{X} = x) = p_0(X = x) \cdot (1 + \epsilon \cdot \mathbb{E}[L(U, V, X)|X = x]).$$

This further implies that the marginal distributions of Y and Z are also fixed.¹ Having made this assumption, the second derivative of $H(\widehat{Y})$ and $H(\widehat{Z})$ at $\epsilon = 0$ would be equal to zero, the second derivative of $I(\widehat{U}; \widehat{Y})$ at $\epsilon = 0$ will be equal to $-\log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|UY]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|VZ]^2]$, the second derivative of $I(\widehat{V}; \widehat{Z})$ at $\epsilon = 0$ will be equal to $-\log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|VZ]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|UY]^2]$, and the second derivative of $-I(\widehat{U}; \widehat{V})$ at $\epsilon = 0$ will be equal to $+\log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|UY]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|VZ]^2] - \log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|UV]^2]$. Note that the second derivatives of $I(\widehat{U}; \widehat{Y})$ and $I(\widehat{V}; \widehat{Z})$ are always non-negative. Since the second derivative of the expression $I(\widehat{U}; \widehat{Y}) + I(\widehat{V}; \widehat{Z}) - I(\widehat{U}; \widehat{V}) + \lambda I(\widehat{U}; \widehat{Y}) + \gamma I(\widehat{V}; \widehat{Z})$ at $\epsilon = 0$ must be non-positive, the second derivative of $I(\widehat{U}; \widehat{Y}) + I(\widehat{V}; \widehat{Z}) - I(\widehat{U}; \widehat{V})$ must be non-positive at $\epsilon = 0$. The second derivative of the latter expression is equal to $+\log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|UY]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|VZ]^2] - \log e \cdot \mathbb{E}[\mathbb{E}[L(U, V, X)|UV]^2]$. Hence we conclude that for any function $L : \mathcal{U} \times \mathcal{V} \times \mathcal{X} \rightarrow \mathbb{R}$ where $\mathbb{E}[L(U, V, X)|X] = 0$ we must have:

$$\mathbb{E}[\mathbb{E}[L(U, V, X)|UY]^2] + \mathbb{E}[\mathbb{E}[L(U, V, X)|VZ]^2] - \mathbb{E}[\mathbb{E}[L(U, V, X)|UV]^2] \leq 0.$$

Next, take an arbitrary function $L' : \mathcal{U} \rightarrow \mathbb{R}$ where $\mathbb{E}[L'(U)|X] = 0$. Note that

$$\mathbb{E}[\mathbb{E}[L'(U)|UV]^2] = \mathbb{E}[\mathbb{E}[L'(U)|UY]^2] = \mathbb{E}[\mathbb{E}[L'(U)]^2].$$

This implies that $\mathbb{E}[\mathbb{E}[L'(U)|VZ]^2]$ should be non-positive. But this can happen only when $\mathbb{E}[L'(U)|VZ] = 0$. Therefore any arbitrary function $L' : \mathcal{U} \rightarrow \mathbb{R}$ where $\mathbb{E}[L'(U)|X] = 0$ must also satisfy $\mathbb{E}[L'(U)|VZ] = 0$. In other words, any arbitrary direction of perturbation L' that is a function of U and preserves the marginal distribution of X , must also preserve the marginal distribution of VZ .² Note that the direction of direction of perturbation L' being only a function of U implies that

$$p_\epsilon(\widehat{U} = u, \widehat{V} = v, \widehat{X} = x, \widehat{Y} = y, \widehat{Z} = z) = p_\epsilon(\widehat{U} = u)p_0(V = v, X = x, Y = y, Z = z|U = u)$$

In other words, the perturbation only changes the marginal distribution of U , but preserves the conditional distribution of $p_0(V = v, X = x, Y = y, Z = z|U = u)$. The above statement is essentially saying that *any* arbitrary change in the marginal distribution of U that preserves the marginal distribution of X , must also preserve the marginal distribution of VZ .

In order to find a cardinality bound on U in the Carathéodory type arguments, one fixes the conditional distribution of $p_0(V = v, X = x, Y = y, Z = z|U = u)$ and tries to redefine the marginal distribution of U so that the expression at hand does not increase while at the same time few elements of \mathcal{U} get non-zero probability assigned to them. Assuming that

¹The terms $\mathbb{E}[L(U, V, X)|Y] = 0$ and $\mathbb{E}[L(U, V, X)|Z] = 0$ must be zero if $\mathbb{E}[L(U, V, X)|X] = 0$

²Note that $p_\epsilon(\widehat{V} = v, \widehat{Z} = z) = p_0(V = v, Z = z) \cdot (1 + \epsilon \cdot \mathbb{E}[L(U, V, X)|V = v, Z = z]) = p_0(V = v, Z = z)$.

the marginal distribution of X is preserved, the expression $I(U; Y) + I(V; Z) - I(U; V) + \lambda I(U; Y) + \gamma I(V; Z)$ would be equal to a constant plus a linear term in the marginal distribution of U since the terms $I(V; Z)$ and $H(V)$ are preserved. One can then use this property and prove a cardinality bound of $|\mathcal{X}|$ on alphabet set of U using the strengthened Carathéodory theorem of Fenchel and Eggleston. Similarly, one can find a cardinality bound of $|\mathcal{X}|$ on alphabet set of V .

ACKNOWLEDGEMENT

The authors would like to thank the anonymous referees for their comments. The authors also 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] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. IT*, 25 (3): 306-311 (1979).
- [4] S. I. Gelfand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Inf. Transm.*, 16 (1): 17-25 (1980).
- [5] B. E. Hajek and M. B. Pursley, "Evaluation of an achievable rate region for the broadcast channel," *IEEE Trans. IT*, 25 (1): 36-46 (1979).
- [6] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. IT*, 23 (1): 60-64 (1977).
- [7] T. Cover, "An achievable rate region for the broadcast channel," *IEEE Trans. IT*, 21 (4): (399-404) (1975).
- [8] E. C. van der Meulen, "Random coding theorems for the general discrete memoryless broadcast channel," *IEEE Trans. IT*, 21 (2): 180-190 (1975).
- [9] Y. Liang, G. Kramer, "Rate regions for relay broadcast channels," *IEEE Trans. IT*, 53 (10): 3517-3535 (2007).
- [10] Y. Liang, G. Kramer, and H.V. Poor, "Equivalence of two inner bounds on the capacity region of the broadcast channel," 46th Annual Allerton Conf. on Commun., Control and Comp., 1417-1421, (2008).
- [11] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," *IEEE Trans. IT*, 53 (1): 350-355 (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, 2008.
- [13] A. A. Gohari and V. Anantharam, "An Outer Bound to the Admissible Source Region of Broadcast Channels with Arbitrarily Correlated Sources and Channel Variations," 46th Annual Allerton Conf. on Commun., Control and Comp., 301-308 (2008).
- [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 V.W. Zizhou, "On the inner and outer bounds for 2-receiver discrete memoryless broadcast channels," Proceedings of the ITA workshop, San Diego, 2008.
- [16] A. A. Gohari and V. Anantharam, "Evaluation of the Extreme Points of Marton's Inner Bound for the General Broadcast Channel," Available at <http://arxiv.org/abs/0904.4541>