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

Amin Aminzadeh Gohari and Venkat Anantharam
Department of Electrical Engineering and Computer Science
University of California, Berkeley
{aminzade,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 [p. 391, Problem 10(c) 2] 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_1, M_2 and M_3 are mutually independent, and 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 $\zeta : \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}^n$, and sends it over the broadcast channel $q(y, z|x)$ in n times steps. The receivers use the decoding functions $\vartheta_y : \mathcal{Y}^n \to \mathcal{M}_0 \times \mathcal{M}_1$ and $\vartheta_z : \mathcal{Z}^n \to \mathcal{M}_0 \times \mathcal{M}_2$ 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. The best achievable region of triples $(0, R_1, R_2)$ for the broadcast channel is due to Marton [Theorem 2 3]. Marton's work was subsequently generalized in [p. 391, Problem 10(c) 2], 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

$$
\begin{aligned}
R_0, R_1, R_2 &\geq 0; \\
R_0 &\leq \min(I(W;Y), I(W;Z)); && (1) \\
R_0 + R_1 &\leq I(UW;Y); && (2) \\
R_0 + R_2 &\leq I(VW;Z); && (3) \\
R_0 + R_1 + R_2 &\leq I(U;Y|W) + I(V;Z|W) - I(U;V|W) \\
&\quad + \min(I(W;Y), I(W;Z)). && (4)
\end{aligned}
$$

In Marton's original work, the auxiliary random variables U, V and W are finite random variables. We however allow the auxiliary random variables U, V and W to be discrete or continuous random variables to get an apparently larger region. The main result of this paper however implies that this relaxation will not make the region grow. We refer to this region as the Marton's inner bound for the general broadcast channel. Recently Liang and Kramer reported an apparently larger inner bound to the broadcast channel [9], which however turns out to be equivalent to Marton's inner bound [10]. Marton's inner bound 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 Marton's inner bound, it suffices to search over $p(u, v, w, x)$ for which either $I(W;Y) = I(W;Z)$, or $I(W;Y) > I(W;Z)\&V = constant$, or $I(W;Y) < I(W;Z)\&U = constant$ holds [10]. This restriction however does not lead to a computable characterization of the region.

Unfortunately Marton's inner bound is not computable (except in certain special cases) as no bounds on the cardinality of its auxiliary random variables exist. A prior work by Hajek and Pursley derives cardinality bounds for an earlier inner bound of Cover and van der Meulen for the special case of X is binary, and $R_0 = 0$ [5]; Hajek and Pursley showed that X can be taken as a deterministic function of the auxiliary random variables involved, and 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. The inner bound of Cover and van der Meulen was however later improved by Marton. 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 $|\mathcal{V}|$ for Marton's inner bound. This does not lead to fixed cardinality bounds on the auxiliary random variables U and V. The main result of this paper is to prove that the subset of Marton's inner bound 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 Marton's inner bound.

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

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

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

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

Furthermore for any set of indices $I \subset \{1, 2, 3, ..., n\}$, 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 $X_{i\in I}$:

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

Lemma 3 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 Marton's inner bound coincides with the best known outer bound for the degraded, less noisy, more capable, and semi-deterministic broadcast channels. Nair and Zizhou showed that Marton'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 a certain conjecture holds[1]. In this paper, we provide examples of broadcast channels for which the two bounds do not match.

The outline of this paper is as follows. In section II, we introduce the basic notations and definitions we use. Section IV contains the main results of the paper followed by section V which gives formal proofs for the results. Appendices complete the proof of Theorems from section V.

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 $(X_1,X_2,...,X_k)$; similarly we use $Y_{1:k}$ and $Z_{1:k}$ to denote $(Y_1,Y_2,...,Y_k)$ and $(Z_1,Z_2,...,Z_k)$ respectively.

Definition 1: For two vectors $\overrightarrow{v_1}$ and $\overrightarrow{v_2}$ in $\mathbb{R}^d$, we say $\overrightarrow{v_1}\geq\overrightarrow{v_2}$ if and only if each coordinate of $\overrightarrow{v_1}$ is greater than or equal to the corresponding coordinate of $\overrightarrow{v_2}$. For a set $A\subset\mathbb{R}^d$, the down-set $\Delta(A)$ is defined as: $\Delta(A)=\{\overrightarrow{v}\in\mathbb{R}^d:\ \overrightarrow{v}\leq\overrightarrow{w}\text{ for some }\overrightarrow{w}\in A\}$.

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

[1]The conjecture is as follows: [Conjecture 1 15]: Given any five random variables U,V,X,Y,Z satisfying $I(UV;YZ|X)=0$, the inequality $I(U;Y)+I(V;Z)-I(U;V)\leq\max\big(I(X;Y),I(X;Z)\big)$ holds whenever X, Y and Z are binary random variables and the channel $p(y,z|x)$ is BSSC with parameter $\frac{1}{2}$.

Definition 3: Let $\mathcal{C}_{M-I}(q(y,z|x))$ be a subset of $\mathbb{R}^6$ defined as the union of

$$\Delta\big(\big\{\big(I(W;Y), I(W;Z), I(UW;Y), I(VW;Z),$$
$$I(U;Y|W)+I(V;Z|W)-I(U;V|W)+I(W;Y),$$
$$I(U;Y|W)+I(V;Z|W)-I(U;V|W)+I(W;Z)\big)\big\}\big),$$

over random variables U,V,W,X,Y,Z, having the joint distribution $p(u,v,w,x,y,z)=p(u,v,w,x)q(y,z|x)$. Note that the region $\mathcal{C}_{M-I}(q(y,z|x))$ specifies $\mathcal{C}_M(q(y,z|x))$, since given any $p(u,v,w,x,y,z) = p(u,v,w,x)q(y,z|x)$ the corresponding vector in $\mathcal{C}_{M-I}(q(y,z|x))$ is providing the values for the left hand side of the 6 inequalities that define the region $\mathcal{C}_M(q(y,z|x))$. $\mathcal{C}_{M-I}(q(y,z|x))$ is defined as a subset of $\mathbb{R}^6$, and not $\mathbb{R}^6_+$ for technical reasons that will become clear later.

Definition 4: The region $\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$ is defined as the union of non-negative triples (R_0,R_1,R_2) satisfying equations 1, 2, 3 and 4, 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 $p(u,v,w,x,y,z) = p(u,v,w,x)q(y,z|x)$. Note that $\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x)) \subset \mathcal{C}_M^{S'_u,S'_v,S'_w}(q(y,z|x))$ whenever $S_u\leq S'_u$, $S_v\leq S'_v$ and $S_w\leq S'_w$.

The region $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is defined as the union of the six tuple mentioned in Definition 3. Note that the region $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ specifies $\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$, 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 $p(u,v,w,x,y,z)=p(u,v,w,x)q(y,z|x)$.

Definition 5: Let $\mathscr{L}(q(y,z|x))$ be equal to $\mathcal{C}_M^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y,z|x))$, and $\mathscr{L}_I(q(y,z|x))$ be equal to $\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y,z|x))$.

The region $\mathscr{C}(q(y,z|x))$ 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. Please note that the definition of $\mathscr{C}(q(y,z|x))$ differs from that of $\mathscr{L}(q(y,z|x))$ since we have imposed the extra constraint $H(X|UVW)=0$ on the auxiliaries. $\mathscr{C}(q(y,z|x))$ is a *computable* subset of the region $\mathcal{C}_M(q(y,z|x))$. The region $\mathscr{C}_I(q(y,z|x))$ is defined similar to $\mathscr{L}_I(q(y,z|x))$ but by adding the extra constraint $H(X|UVW)=0$ on the auxiliaries.

Definition 6: 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. It was shown in [15] that the following region is an alternative characterization of the set of triples $(0, R_1, R_2)$ in $\mathcal{C}_{NE}(q(y,z|x))$: the union over random variables U, V, X, Y, Z having the joint distribution $p(u,v,x,y,z) = p(u,v,x)q(y,z|x)$, of

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

Definition 7: Given any finite random variable X, and real valued random variable L where $\big|\mathbb{E}[L|X = x]\big| < \infty$ 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 $\big|\mathbb{E}[L|X = x, Y = y]\big| < \infty$ 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

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

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

III. Description of the main technique

In this section, we demonstrate the main idea of the paper. In order to show the essence of the proof while avoiding the unnecessary details, we consider a simpler problem that is different from the problem at hand, although it will be used in the later proofs. In the following discussion, we assume that the reader has read Lemma 3 from Section IV.

Given a broadcast channel $q(y,z|x)$ and an input distribution $p(x)$, 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 $p(uv|x)p(x)q(y,z|x)$ where λ and γ are arbitrary non-negative reals, and auxiliary random variables U, V have alphabet sets satisfying $|\mathcal{U}| \leq S_u$ and $|\mathcal{V}| \leq S_v$ for some natural numbers S_u and S_v. For this problem, we would like to show that it suffices to take the maximum over random variables U and V with the cardinality bounds of $\min(|\mathcal{X}|, S_u)$ and $\min(|\mathcal{X}|, S_v)$. It suffices to prove the following lemma:

Lemma 1: Given an arbitrary broadcast channel $q(y,z|x)$, an arbitrary input distribution $p(x)$, non-negative reals λ and γ, and natural numbers S_u and S_v where $S_u > |\mathcal{X}|$ the following holds:

$$\sup_{UV\rightarrow X\rightarrow YZ; |\mathcal{U}|\leq S_u; |\mathcal{V}|\leq S_v} I(U;Y) + I(V;Z) - I(U;V) + \lambda I(U;Y) + \gamma I(V;Z) =$$
$$I(\widehat{U};\widehat{Y}) + I(\widehat{V};\widehat{Z}) - I(\widehat{U};\widehat{V}) + \lambda I(\widehat{U};\widehat{Y}) + \gamma I(\widehat{V};\widehat{Z}),$$

where random variables $\widehat{U},\widehat{V},\widehat{X},\widehat{Y},\widehat{Z}$ satisfy the following properties: the Markov chain $\widehat{U}\widehat{V}\rightarrow\widehat{X}\rightarrow\widehat{Y}\widehat{Z}$ holds; the joint distribution of $\widehat{X},\widehat{Y},\widehat{Z}$ is the same as the joint distribution of X,Y,Z, and furthermore $|\widehat{\mathcal{U}}| < S_u$, $|\widehat{\mathcal{V}}| \leq S_v$.

Proof. Since the cardinalities of 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[2], and is obtained at some joint distribution $p_0(u,v,x,y,z)=p_0(u,v,x)q(y,z|x)$. If $|\mathcal{U}|<S_u$, one can finish the proof by setting $(\widehat{U},\widehat{V},\widehat{X},\widehat{Y},\widehat{Z})=(U,V,X,Y,Z)$. One can also easily show the existence of appropriate $(\widehat{U},\widehat{V},\widehat{X},\widehat{Y},\widehat{Z})$ if $p(u)=0$ for some $u\in\mathcal{U}$. Therefore assume that $|\mathcal{U}|=S_u$ and $p(u)\neq 0$ for all $u\in\mathcal{U}$. Take an arbitrary non-zero function $L:\mathcal{U}\times\mathcal{V}\times\mathcal{X}\rightarrow\mathbb{R}$ where $\mathbb{E}[L(U,V,X)|X]$=0. Let us then perturb the joint distribution of U,V,X,Y,Z by defining random variables $\widehat{U},\widehat{V},\widehat{X},\widehat{Y}$ and $\widehat{Z}$ distributed according to

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

or equivalently according to

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

The parameter ϵ is a real number that can take value in $[-\overline{\epsilon}_1,\overline{\epsilon}_2]$ where $\overline{\epsilon}_1$ and $\overline{\epsilon}_2$ are some positive reals representing the maximum and minimum values of ϵ, i.e. $\min_{u,v,x}1-\overline{\epsilon}_1\cdot L(u,v,x)=\min_{u,v,x}1+\overline{\epsilon}_2\cdot L(u,v,x)=0$. Since L is a function of U, V and X only, for any value of ϵ, the Markov chain $\widehat{U}\widehat{V}\rightarrow\widehat{X}\rightarrow\widehat{Y}\widehat{Z}$ holds, and $p(\widehat{Y}=y,\widehat{Z}=z|\widehat{X}=x)$ is equal to $q(Y=y,Z=z|X=x)$ for all x,y,z where $p(X=x)>0$. Furthermore $\mathbb{E}[L(U,V,X)|X]=0$ implies that the marginal distribution of X is preserved by this perturbation. This is because

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

This further implies that the marginal distributions of Y and Z are also fixed. [3]

The expression $I(\widehat{U};\widehat{Y})+I(\widehat{V};\widehat{Z})-I(\widehat{U};\widehat{V})+\lambda I(\widehat{U};\widehat{Y})+\gamma I(\widehat{V};\widehat{Z})$ as a function of ϵ achieves its maximum at $\epsilon=0$ (by our assumption). Therefore its first derivative at $\epsilon=0$ should be zero, and

[2]Since the ranges of all the involving random variables are limited and the conditional mutual information function is continuous, the set of admissible joint probability distributions $p(u,v,x,y,z)$ where $I(UV;YZ|X)=0$ and $p(y,z,x)=q(y,z|x)p(x)$ will be a compact set (when viewed as a subset of the Euclidean space). The fact that mutual information function is continuous implies that the union over random variables U,V,X,Y,Z satisfying the cardinality bounds, having the joint distribution $p(u,v,x,y,z)=p(u,v|x)p(x)q(y,z|x)$, of $I(U;Y)+I(V;Z)-I(U;V)+\lambda I(U;Y)+\gamma I(V;Z)$ is a compact set, and thus closed.

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

its second derivative should be less than or equal to zero. Using Lemma 3, one can compute the first derivative and set it to zero, and thereby get the following equation:

$$I_L(U;Y) + I_L(V;Z) - I_L(U;V) + \lambda I_L(U;Y) + \gamma I_L(V;Z) = 0. \tag{5}$$

In order to compute the second derivative, one can expand the expression as entropy terms and use Lemma 3 to compute the second derivative for each term. We can use the assumption that $\mathbb{E}[L(U,V,X)|X] = 0$ (which implies $\mathbb{E}[L(U,V,X)|Y] = 0$ and $\mathbb{E}[L(U,V,X)|Z] = 0$) to simplify the expression. In particular the second derivative of $H(\widehat{Y})$ and $H(\widehat{Z})$ at $\epsilon = 0$ would be equal to zero (as the marginal distributions of Y and Z are preserved under the perturbation), the second derivative of $I(\widehat{U};\widehat{Y})$ at $\epsilon = 0$ will be equal to $-\log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|U]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|UY]^2]$, the second derivative of $I(\widehat{V};\widehat{Z})$ at $\epsilon = 0$ will be equal to $-\log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|V]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|VZ]^2]$, and the second derivative of $-I(\widehat{U};\widehat{V})$ at $\epsilon = 0$ will be equal to $+\log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|U]^2] + \log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|V]^2] - \log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|UV]^2]$. 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 non-zero function $L : \mathcal{U} \times \mathcal{V} \times \mathcal{X} \to \mathbb{R}$ where $\mathbb{E}[L(U,V,X)|X] = 0$ we must have:

$$\mathbb{E}[\mathbb{E}[L(U,V,X)|UY]^2] + \mathbb{E}[\mathbb{E}[L(U,V,X)|VZ]^2] - \mathbb{E}[\mathbb{E}[L(U,V,X)|UV]^2] \leq 0. \tag{6}$$

Next, take an arbitrary non-zero function $L' : \mathcal{U} \to \mathbb{R}$ where $\mathbb{E}[L'(U)|X] = 0$. Since $|\mathcal{U}| = S_u > |\mathcal{X}|$, such a non-zero function L' exists. Note that the 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 $p_0(V = v, X = x, Y = y, Z = z|U = u)$.

Note that

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

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 $L' : \mathcal{U} \to \mathbb{R}$ 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.[4]

We next show that the expression $I(\widehat{U};\widehat{Y})+I(\widehat{V};\widehat{Z})-I(\widehat{U};\widehat{V})+\lambda I(\widehat{U};\widehat{Y})+\gamma I(\widehat{V};\widehat{Z})$ as a function of ϵ is constant.[5] Using the last part of Lemma 3, one can write:

$$I(\widehat{U};\widehat{Y}) = I(U;Y)+\epsilon\cdot I_L(\widehat{U};\widehat{Y}) - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|U]\big)\big] - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|Y]\big)\big] + \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|UY]\big)\big] = I(U;Y)+\epsilon\cdot I_L(\widehat{U};\widehat{Y}) \tag{7}$$

where $r(x)=(1+x)\log(1+x)$. Equation (7) holds because $\mathbb{E}[L|Y]=0$ and $\mathbb{E}[L|U]=\mathbb{E}[L|UY]$. Similarly using the last part of Lemma 3, one can write:

$$I(\widehat{U};\widehat{V}) = I(U;V)+\epsilon\cdot I_L(\widehat{U};\widehat{V}) - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|U]\big)\big] - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|V]\big)\big] + \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|UV]\big)\big] = I(U;V)+\epsilon\cdot I_L(\widehat{U};\widehat{V}) \tag{8}$$

where $r(x)=(1+x)\log(1+x)$. Equation (8) holds because $\mathbb{E}[L|V]=0$ and $\mathbb{E}[L|U]=\mathbb{E}[L|UV]$. One can similarly show that the term $I(\widehat{V};\widehat{Z})$ can be written as $I(V;Z)+\epsilon\cdot I_L(\widehat{V};\widehat{Z})=0$. Therefore the expression $I(\widehat{U};\widehat{Y})+I(\widehat{V};\widehat{Z})-I(\widehat{U};\widehat{V})+\lambda I(\widehat{U};\widehat{Y})+\gamma I(\widehat{V};\widehat{Z})$ as a function of ϵ is equal to

$$I(U;Y)+I(V;Z)-I(U;V)+\lambda I(U;Y)+\gamma I(V;Z)+ \epsilon\cdot\big(I_L(U;Y)+I_L(V;Z)-I_L(U;V)+\lambda I_L(U;Y)+\gamma I_L(V;Z)\big). \tag{9}$$

Equation (5) implies that this expression is equal to $I(U;Y)+I(V;Z)-I(U;V)+\lambda I(U;Y)+\gamma I(V;Z)$.

Therefore the expression $I(\widehat{U};\widehat{Y})+I(\widehat{V};\widehat{Z})-I(\widehat{U};\widehat{V})+\lambda I(\widehat{U};\widehat{Y})+\gamma I(\widehat{V};\widehat{Z})$ as a function of ϵ is constant. Since the function L' is non-zero, setting $\epsilon=-\overline{\epsilon}_1$ or $\epsilon=\overline{\epsilon}_2$ will result in a marginal distribution on $\widehat{U}$ with a smaller support than U since the marginal distribution of U is being perturbed as follows:

$$p_\epsilon(\widehat{U}=u)=p_0(U=u)\cdot\big(1+\epsilon L'(u)\big).$$

This perturbation does not increase the support and would decrease it by at least one when ϵ is at its maximum or minimum, i.e. when $\epsilon=-\overline{\epsilon}_1$ or $\epsilon=\overline{\epsilon}_2$. Therefore one is able to define a random variable with a smaller cardinality as that of U while leaving the value of $I(U;Y)+I(V;Z)-I(U;V)+\lambda I(U;Y)+\gamma I(V;Z)$ unaffected.

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

[5]The authors would like to thank Chandra Nair for suggesting this shortcut to simplify the original proof.

Discussion: Aside from establishing cardinality bounds, the above argument implies that if the maximum of $I(U;Y) + I(V;Z) - I(U;V) + \lambda I(U;Y) + \gamma I(V;Z)$ is obtained at some joint distribution $p_0(u,v,x,y,z) = p_0(u,v,x)q(y,z|x)$, equations 5 and 6 must hold for any non-zero function $L : \mathcal{U} \times \mathcal{V} \times \mathcal{X} \to \mathbb{R}$ where $\mathbb{E}[L(U,V,X)|X] = 0$. The proof used these properties to a limited extent.

IV. Statement of results

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

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

Lemma 2: For any arbitrary natural numbers S_u, S_v and S_w, the following statements hold:

- $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a closed subset of $\mathbb{R}^6$;
- $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a subset of $\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$;
- $\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$ is convex.

Lemma 3: Given any finite random variable X, and real valued random variable L where $\big|\mathbb{E}[L|X = x]\big| < \infty$ for all $x \in \mathcal{X}$, and $\mathbb{E}[L] = 0$, let random variable $\widehat{X}$ be defined on the same alphabet set as X according to $p_\epsilon(\widehat{X} = x) = p_0(X = x) \cdot \big(1 + \epsilon \cdot \mathbb{E}[L|X = x]\big)$, where ϵ is a real number in the interval $[-\overline{\epsilon}_1, \overline{\epsilon}_2]$. $\overline{\epsilon}_1$ and $\overline{\epsilon}_2$ are positive reals for which $\min_x 1 - \overline{\epsilon}_1 \cdot \mathbb{E}[L|X = x] \geq 0$ and $\min_x 1 + \overline{\epsilon}_2 \cdot \mathbb{E}[L|X = x] \geq 0$ hold. Then

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

$\mathcal{C}_M(q(y,z|x))$. 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 $\mathcal{C}_M(q(y,z|x)) = \mathcal{C}_{NE}(q(y,z|x))$, maximum of the sum rate R_1+R_2 over triples (R_0,R_1,R_2) in the Marton's inner bound is equal to

$$\max\Bigg(\min_{\gamma\in[0,1]}\Big(\max_{\substack{p(wx)q(y,z|x)\\ |\mathcal{W}|=2}} \gamma I(W;Y)+(1-\gamma)I(W;Z)+\sum_w p(w)T(p(X=1|W=w))\Big),$$

$$\max_{\substack{p(u,v)p(x|uv)q(y,z|x)\\ |\mathcal{U}|=|\mathcal{V}|=2,\, I(U;V)=0,\, H(X|UV)=0}} I(U;Y)+I(V;Z)\Bigg), \tag{10}$$

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

Remark 1: The expression given in equation 10 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's inner bound whether $\mathcal{C}_M(q(y,z|x))$ 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 10 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 $\mathcal{C}_{NE}(q(y,z|x))$ (which is given in [15]), it will serve as an evidence for $\mathcal{C}_M(q(y,z|x)) \neq \mathcal{C}_{NE}(q(y,z|x))$. The maximum of the sum rate R_1+R_2 over triples (R_0,R_1,R_2) in $\mathcal{C}_{NE}(q(y,z|x))$ is known to be [15]

$$\max_{p(u,v,x)q(y,z|x)} \min\big(I(U;Y)+I(V;Z), I(U;Y)+I(V;Z|U), I(V;Z)+I(U;Y|V)\big),$$

which can be written as (see Bound 4 in [15])

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

There are examples for which the expression of equation 10 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 $\mathcal{C}_{NE}(q(y,z|x))$. 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

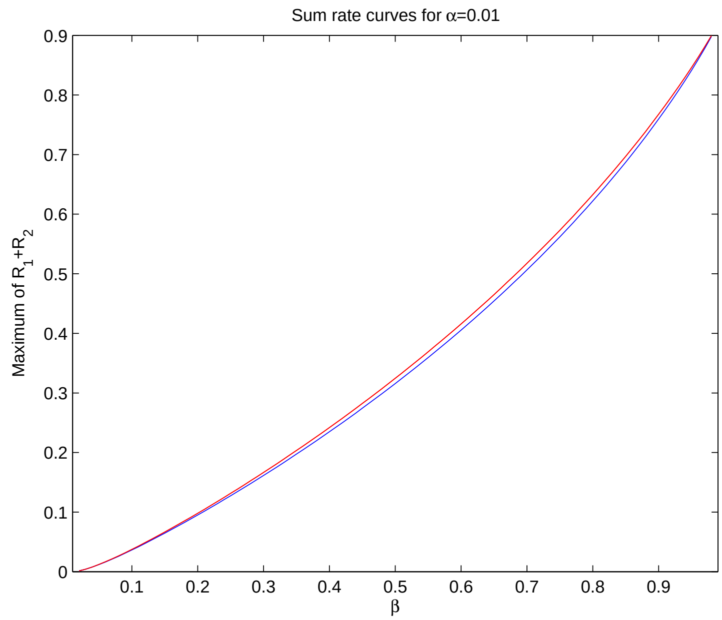

Fig. 1. Red curve (top curve): sum rate for $C_{NE}(q(y,z|x))$; Blue curve (bottom curve): sum rate for $C_M(q(y,z|x))$ assuming that $C_{NE}(q(y,z|x)) = C_M(q(y,z|x))$.

sum rate for $C_M(q(y,z|x))$ (assuming that $C_{NE}(q(y,z|x)) = C_M(q(y,z|x))$) as a function of β. Where the two curves do not match, Nair and El Gamal's outer bound and Marton's inner bound can not be equal for the corresponding broadcast channel.

V. Proofs

Proof of Theorem 1: In appendices B and C, we prove that the closure of $\mathcal{C}_M(q(y,z|x))$ is equal to the closure of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$, and that $\mathscr{C}(q(y,z|x))$ is equal to $\mathscr{L}(q(y,z|x))$. Therefore we need to show that the closure of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$ is equal to $\mathscr{L}(q(y,z|x))$. It suffices to prove that $\mathscr{L}(q(y,z|x))$ is closed, and that for any arbitrary natural numbers S_u, S_v and S_w, $\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x)) \subset \mathscr{L}(q(y,z|x))$. The former can be proven using Lemma 2 according to which the region $\mathscr{L}_I(q(y,z|x))$ is closed.[6] To show the latter, it suffices to prove that $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x)) \subset \mathscr{L}_I(q(y,z|x))$.[7] Lemma 2 shows that the regions $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ and $\mathscr{L}_I(q(y,z|x))$ are closed. Lemma 2 implies that the region $\mathscr{L}_I(q(y,z|x))$ is convex. In order to prove that $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a subset of $\mathscr{L}_I(q(y,z|x))$, it suffices to show that for any supporting hyperplane of $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$, the half-space delimited by the hyperplane which contains $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is contained in the corresponding half-space for $\mathscr{L}_I(q(y,z|x))$.[8]

A supporting hyperplane of $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is identified with constants λ_1, λ_2, ..., λ_6 and the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over triples $(R_1', R_2', ..., R_6')$ in $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$. We must have $\lambda_i \geq 0$ for $i = 1, 2, ..., 6$, since if λ_i is negative, R_i can be made to converge to $-\infty$ causing $\sum_{i=1}^{6}\lambda_i R_i'$ to converge to ∞, and hence not finite. Our goal is therefore to show that for any non-negative values of λ_i ($i = 1, 2, ..., 6$), the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is less than or equal to the corresponding maximum over $\mathscr{L}_I(q(y,z|x))$.

First consider the case where $\lambda_5 = \lambda_6 = 0$. Let $(R_1, R_2, ..., R_6)$ be a point in $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ where the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is obtained. Corresponding to $(R_1, R_2, ..., R_6)$ is at least one joint distribution $p_0(u,v,w,x,y,z) = p_0(u,v,w,x)q(y,z|x)$ on U, V, W, X, Y, Z where $|\mathcal{U}| \leq S_u$, $|\mathcal{V}| \leq S_v$ and $|\mathcal{W}| \leq S_w$, and furthermore the following equalities are satisfied: $R_1 \leq I(W;Y)$, $R_2 \leq I(W;Z)$, $R_3 \leq I(UW;Y)$, ... etc. Maximum of $\sum_{i=1}^{6}\lambda_i R_i' = \sum_{i=1}^{4}\lambda_i R_i'$ over $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ must be then equal to $\lambda_1 \cdot I(W;Y) + \lambda_2 \cdot I(W;Z) + \lambda_3 \cdot I(UW;Y) + \lambda_4 \cdot I(VW;Z)$. Let $\widetilde{U} = \widetilde{V} = X$. Clearly $I(UW;Y) \leq I(\widetilde{U}W;Y)$ and $I(VW;Z) \leq I(\widetilde{V}W;Z)$. Hence the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ would be less than or equal to the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$

[6]The region $\mathscr{L}_I(q(y,z|x))$ determines $\mathscr{L}(q(y,z|x))$. In order to show that the closedness of $\mathscr{L}_I(q(y,z|x))$ implies the closedness of $\mathscr{L}(q(y,z|x))$, take a convergent sequence $(R_{0,i}, R_{1,i}, R_{2,i})$ in $\mathscr{L}(q(y,z|x))$. We would like to show that $(\overline{R_0}, \overline{R_1}, \overline{R_2}) = \lim_{i\to\infty}(R_{0,i}, R_{1,i}, R_{2,i})$ belongs to $\mathscr{L}(q(y,z|x))$. The six-tuple $(R_{0,i}, R_{0,i}, R_{0,i}+R_{1,i}, R_{0,i}+R_{2,i}, R_{0,i}+R_{1,i}+R_{2,i}, R_{0,i}+R_{1,i}+R_{2,i})$ is in $\mathscr{L}_I(q(y,z|x))$. Since $\mathscr{L}_I(q(y,z|x))$ is closed, $\lim_{i\to\infty}(R_{0,i}, R_{0,i}, R_{0,i}+R_{1,i}, R_{0,i}+R_{2,i}, R_{0,i}+R_{1,i}+R_{2,i}, R_{0,i}+R_{1,i}+R_{2,i}) = (\overline{R_0}, \overline{R_0}, \overline{R_0}+\overline{R_1}, \overline{R_0}+\overline{R_2}, \overline{R_0}+\overline{R_1}+\overline{R_2}, \overline{R_0}+\overline{R_1}+\overline{R_2})$ is also in $\mathscr{L}_I(q(y,z|x))$. Thus, $(\overline{R_0}, \overline{R_1}, \overline{R_2}) = \lim_{i\to\infty}(R_{0,i}, R_{1,i}, R_{2,i})$ belongs to $\mathscr{L}(q(y,z|x))$.

[7]This is true because (R_0, R_1, R_2) being in $\mathcal{C}_{M}^{S_u,S_v,S_w}(q(y,z|x))$ implies that $(R_0, R_0, R_0+R_1, R_0+R_2, R_0+R_1+R_2, R_0+R_1+R_2)$ is in $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$. If $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a subset of $\mathscr{L}_I(q(y,z|x))$, the latter point would belong to $\mathscr{L}_I(q(y,z|x))$. Therefore (R_0, R_1, R_2) belongs to $\mathscr{L}(q(y,z|x))$.

[8]This is because the closed convex set $\mathscr{L}_I(q(y,z|x))$ can be expressed as the intersection of its supporting half-spaces, i.e. $(R_1, R_2, ..., R_6) \in \mathscr{L}_I(q(y,z|x))$ if and only if for any λ_1, λ_2, ..., λ_6, $\sum_{i=1}^{6}\lambda_i R_i$ is less than or equal to the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over triples $(R_1', R_2', ..., R_6')$ in $\mathscr{L}_I(q(y,z|x))$. Thus $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a subset of $\mathscr{L}_I(q(y,z|x))$ if and only if the maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over triples $(R_1', R_2', ..., R_6')$ in $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is less than or equal to the same maximum over $\mathscr{L}_I(q(y,z|x))$.

over $\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,S_w}(q(y,z|x))$. The latter is itself less than or equal to the maximum of $\sum_{i=1}^{6}\lambda_i R'_i$ over $\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y,z|x))$ by Lemma 2. This implies the desired result when $\lambda_5=\lambda_6=0$.

Next consider the case when either $\lambda_5>0$ or $\lambda_6>0$, or both: we proceed by proving the following three equations:

$$\max_{(R'_1,\ldots,R'_6)\in\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R'_i \leq \max_{(R'_1,\ldots,R'_6)\in\mathcal{C}_{M-I}^{|\mathcal{X}|,S_v,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R'_i \tag{11}$$

$$\max_{(R'_1,\ldots,R'_6)\in\mathcal{C}_{M-I}^{|\mathcal{X}|,S_v,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R'_i \leq \max_{(R'_1,\ldots,R'_6)\in\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R'_i \tag{12}$$

$$\max_{(R'_1,\ldots,R'_6)\in\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R'_i \leq \max_{(R'_1,\ldots,R'_6)\in\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R'_i \tag{13}$$

The proof for equation 11 is provided in Appendix A. The proof for equation 12 is similar. Equation 13 follows from Lemma 2. ∎

Proof of Theorem 2: Maximum of the sum rate R_1+R_2 over triples (R_0,R_1,R_2) in $\mathcal{C}_M(q(y,z|x))$ is equal to

$$\max_{\substack{p(u,v,w,x)q(y,z|x)\\ |\mathcal{U}|=2,|\mathcal{V}|=2\\ H(X|UVW)=0}} I(U;Y|W)+I(V;Z|W)-I(U;V|W)+\min(I(W;Y),I(W;Z)). \tag{14}$$

The proof consists of two parts: first we show that the above expression is equal to the following expression:

$$\max\Bigg(\max_{p(wx)q(y,z|x)}\min\big(I(W;Y),I(W;Z)\big)+\sum_{w}p(w)T(p(X=1|W=w)),\\ \max_{\substack{p(u,v)p(x|uv)q(y,z|x)\\ |\mathcal{U}|=|\mathcal{V}|=2,\,I(U;V)=0,\,H(X|UV)=0}} I(U;Y)+I(V;Z)\Bigg). \tag{15}$$

Next, we show that the expression of equation 15 is equal to the the expression given in Theorem 2.

The expression of equation 14 is greater than or equal to the expression of equation 15.[9] For the first part of the proof we thus need to prove that the expression of equation 14 is less than or equal to the expression of equation 15. Take the joint distribution $p(u,v,w,x)$ that maximizes the expression of equation 14. Let $\widetilde{U}=(U,W)$ and $\widetilde{V}=(V,W)$. Maximum of the sum rate R_1+R_2 over triples (R_0,R_1,R_2) in

[9]Consider the following special cases: 1) given $W=w$, let $(U,V)=(X,constant)$ if $I(X;Y|W=w)\geq I(X;Z|W=w)$, and $(U,V)=(constant,X)$ otherwise. This would produce the first part of the expression given in Theorem 2. 2) Assume that W is constant, and U is independent of V. This would produce the second part of the expression given in Theorem 2.

$\mathcal{C}_{NE}(q(y,z|x))$ is greater than or equal to $\min\big(I(\widetilde{U};Y)+I(\widetilde{V};Z), I(\widetilde{U};Y)+I(\widetilde{V};Z|\widetilde{U}), I(\widetilde{V};Z)+I(\widetilde{U};Y|\widetilde{V})\big)$ (see Bound 3 in [15]). Since $\mathcal{C}_{NE}(q(y,z|x))=\mathcal{C}_M(q(y,z|x))$, we must have:

$$\min\big(I(UW;Y)+I(VW;Z), I(UW;Y)+I(VW;Z|UW), I(UW;Z)+I(UW;Y|VW)\big)\leq$$

$$I(U;Y|W)+I(V;Z|W)-I(U;V|W)+\min(I(W;Y),I(W;Z)).$$

Or alternatively

$$\min\Bigg(\max(I(W;Y),I(W;Z))+I(U;V|W),$$

$$I(W;Y)-\min(I(W;Y),I(W;Z))+I(U;V|WZ),$$

$$I(W;Z)-\min(I(W;Y),I(W;Z))+I(U;V|WY)\Bigg)\leq 0.$$

Since each expression is also greater than or equal, at least one of the three terms must be equal to zero. Therefore at least one of the following must hold:

1) $I(W;Y)=I(W;Z)=0$ and $I(U;V|W)=0$,
2) $I(U;V|WY)=0$,
3) $I(U;V|WZ)=0$.

If (1) holds, $I(U;Y|W)+I(V;Z|W)-I(U;V|W)+\min(I(W;Y),I(W;Z))$ equals $I(U;Y|W)+I(V;Z|W)$. Suppose $\max_{w:p(w)>0} I(U;Y|W=w)+I(V;Z|W=w)$ occurs at some w^*. Clearly $I(U;Y|W)+I(V;Z|W)\leq I(U;Y|W=w^*)+I(V;Z|W=w^*)$. Let $\widehat{U},\widehat{V},\widehat{X},\widehat{Y}$ and $\widehat{Z}$ be distributed according to $p(u,v,x,y,z|w^*)$. $I(\widehat{U};\widehat{V})=I(U;V|W=w^*)=0$. Therefore $I(U;Y|W)+I(V;Z|W)-I(U;V|W)+\min(I(W;Y),I(W;Z))$ is less than or equal to

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

Next assume (2) or (3) holds, i.e. $I(U;V|WY)=0$ or $I(U;V|WZ)=0$. We show in Appendix D that for any value of w where $p(w)>0$, either $I(U;V|W=w,Y)=0$ or $I(U;V|W=w,Z)=0$ imply that $I(U;Y|W=w)+I(V;Z|W=w)-I(U;V|W=w)\leq T(p(X=1|W=w))$. Therefore $I(U;Y|W)+I(V;Z|W)-I(U;V|W)+\min(I(W;Y),I(W;Z))\leq\min(I(W;Y),I(W;Z))+\sum_w p(w)T(p(X=1|W=w))$. This in turn implies that $I(U;Y|W)+I(V;Z|W)-I(U;V|W)+\min(I(W;Y),I(W;Z))$ is less than or equal to

$$\max_{p(w,x)q(y,z|x)} \min(I(W;Y),I(W;Z))+\sum_w p(w)T(p(X=1|W=w)).$$

This completes the first part of the proof.

Next, we would like to show that the expression of equation 15 is equal to the the expression given in Theorem 2. In order to show this, we prove that

$$\max_{p(w,x)q(y,z|x)} \min(I(W;Y), I(W;Z)) + \sum_{w} p(w)T(p(X=1|W=w)) \tag{16}$$

is equal to

$$\min_{\gamma\in[0,1]} \Big(\max_{\substack{p(wx)q(y,z|x)\\ |\mathcal{W}|=2}} \gamma I(W;Y) + (1-\gamma)I(W;Z) + \sum_{w} p(w)T(p(X=1|W=w))\Big). \tag{17}$$

The expression given in equation 16 can be written as

$$\max_{p(w,x)q(y,z|x)} \min\Big(I(W;Y)+\sum_{w} p(w)T(p(X=1|W=w)), I(W;Z)+\sum_{w} p(w)T(p(X=1|W=w))\Big).$$

Using Proposition 1 of [16], this expression can be expressed as

$$\min_{\gamma\in[0,1]} \Big(\max_{p(wx)q(y,z|x)} \gamma I(W;Y) + (1-\gamma)I(W;Z) + \sum_{w} p(w)T(p(X=1|W=w))\Big).$$

It remains to prove the cardinality bound of two on W. This is done using the strengthened Carathéodory theorem of Fenchel and Eggleston. Take an arbitrary $p(w,x)q(y,z|x)$. The vector $w \to p(W=w)$ belongs to the set of vectors $w \to p(\widetilde{W}=w)$ satisfying the constraints $\sum_w p(\widetilde{W}=w)=1$, $p(\widetilde{W}=w)\geq 0$ and $p(X=1)=\sum_w p(X=1|W=w)p(\widetilde{W}=w)$. The first two constraints ensure that $w \to p(\widetilde{W}=w)$ corresponds to a probability distribution, and the third constraint ensures that one can define random variable $\widetilde{W}$, jointly distributed with X, Y and Z according to $p(\widetilde{w},x)q(y,z|x)$ and further satisfying $p(X=x|\widetilde{W}=w)=p(X=x|W=w)$. Since $w \to p(W=w)$ belongs to the above set, it can be written as the convex combination of some of the extreme points of this set. The expression $\sum_w[-(1-\gamma)H(Z|W=w)-\gamma H(Y|W=w)+T(p(X=1|W=w))]p(\widetilde{W}=w)$ is linear in $p(\widetilde{W}=w)$, therefore this expression for $w \to p(W=w)$ is less than or equal to the corresponding expression for at least one of these extreme points. On the other hand, every extreme point of the set of vectors $w \to p(\widetilde{W}=w)$ satisfying the constraints $\sum_w p(\widetilde{W}=w)=1$, $p(\widetilde{W}=w)\geq 0$ and $p(X=1)=\sum_w p(X=1|W=w)p(\widetilde{W}=w)$ satisfies the property that $p(\widetilde{W}=w)\neq 0$ for at most two values of $w\in\mathcal{W}$. Thus a cardinality bound of two is established. ■

Proof of Lemma 2: We begin by proving that the region $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is closed. Since the ranges of all the involving random variables are limited and the conditional mutual information function is continuous, the set of admissible joint probability distributions $p(u,v,w,x,y,z)$ where $I(UVW;YZ|X)=0$ and $p(y,z|x)=q(y,z|x)$ will be a compact set (when viewed as a subset of the Euclidean space).

The fact that mutual information function is continuous implies that the union over random variables U, V, W, X, Y, Z satisfying the cardinality bounds, having the joint distribution $p(u, v, w, x, y, z) = p(u, v, w, x)q(y, z|x)$, of the six-tuples

$$\Big(I(W;Y), I(W;Z), I(UW;Y), I(VW;Z),$$
$$I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Y),$$
$$I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Z)\Big)$$

is a compact set. Since the down-set of any compact set in $\mathbb{R}^6$ is closed[10], the region $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ must be closed.

Next we prove that $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a subset of $\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$. Take an arbitrary point $(R_1, R_2, ..., R_6)$ in $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$. Corresponding to $(R_1, ..., R_6)$ is at least one joint distribution $p_0(u, v, w, x, y, z) = p_0(u, v, w, x)q(y, z|x)$ on U, V, W, X, Y, Z where $|\mathcal{U}| \leq S_u$, $|\mathcal{V}| \leq S_v$ and $|\mathcal{W}| \leq S_w$, and furthermore the following equations are satisfied: $R_1 \leq I(W;Y)$, $R_2 \leq I(W;Z)$, $R_3 \leq I(UW;Y)$, ... etc. Without loss of generality, assume that $p(W = w) > 0$ for all w. We define $\widetilde{U}$, $\widetilde{V}$ and $\widetilde{W}$ on the same alphabet as U, V and W but will however ensure that $p(\widetilde{W} = w) \neq 0$ for at most $|\mathcal{X}| + 4$ values of w. Random variables $\widetilde{U}$, $\widetilde{V}$ and $\widetilde{W}$ that we will define are jointly distributed with X, Y, Z in a way that

$$\text{The Markov chain } \widetilde{U}\widetilde{V}\widetilde{W}X \to X \to YZ \text{ holds;}$$

$$p(\widetilde{U} = u, \widetilde{V} = v, X = x|\widetilde{W} = w) = p(U = u, V = v, X = x|W = w); \tag{18}$$

$$I(\widetilde{W};Y) = I(W;Y);$$

$$I(\widetilde{W};Z) = I(W;Z);$$

$$I(\widetilde{U};Y|\widetilde{W}) = I(U;Y|W);$$

$$I(\widetilde{V};Z|\widetilde{W}) = I(V;Z|W);$$

$$I(\widetilde{U};\widetilde{V}|\widetilde{W}) \leq I(U;V|W).$$

[10]In order to show this, let $\mathcal{A} \subset \mathbb{R}^6$ be a compact set. Take a convergent sequence of points v_1, v_2, ... in $\Delta(\mathcal{A})$. We would like to show that $\overline{v} = \lim_{i\to\infty} v_i$ is in $\Delta(\mathcal{A})$. Corresponding to v_i is a point w_i in $\mathcal{A}$ where $w_i \geq v_i$. Since $\mathcal{A}$ is compact the sequence w_i has a convergent subsequence, the limit point of which belongs to $\mathcal{A}$. Let $\overline{w}$ denote this limit point. Clearly $\overline{w} \geq \overline{v}$, hence $\overline{v}$ is in $\Delta(\mathcal{A})$.

Please note that proving the existence of random variables $\widetilde{U}$, $\widetilde{V}$ and $\widetilde{W}$ with the above properties implies that the point $(R_1, R_2, ..., R_6)$ belongs to $\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$.

Given that we would like impose the equation $p(\widetilde{U}=u, \widetilde{V}=v, X=x|\widetilde{W}=w) = p(U=u, V=v, X=x|W=w)$, defining the marginal distribution of $p(\widetilde{W}=w)$ would completely characterize the joint distribution $p(\widetilde{U}=u, \widetilde{V}=v, \widetilde{W}=w, X=x)$.

In order to define the elements of the vector $w \mapsto p(\widetilde{W}=w)$, we first identify the properties that this vector needs to satisfy, and then pin down an appropriate vector that has only $|\mathcal{X}|+4$ non-zero elements.

To make sure that the elements of the vector $w \mapsto p(\widetilde{W}=w)$ corresponds to a probability distribution, we impose the following two constraints:

$$p(\widetilde{W}=w) \geq 0 \quad \forall w; \tag{19}$$

$$\sum_w p(\widetilde{W}=w) = 1. \tag{20}$$

Since we require that $p(X=x|\widetilde{W}=w) = p(X=x|W=w)$, $p(\widetilde{W}=w)$ must also satisfy the consistency equation

$$\sum_w p(X=x|W=w)p(W=w) = p(X=x) = \tag{21}$$

$$\sum_w p(X=x|W=w)p(\widetilde{W}=w) \quad \forall x.$$

As long as these three equations hold, the joint distribution of $p(\widetilde{U}=u, \widetilde{V}=v, \widetilde{W}=w, X=x)$ will be well defined. Equation 21 seems to be imposing $|\mathcal{X}|$ equations on $p(\widetilde{W}=w)$. But in fact, one of these equations is a linear combination of the rest and equation 20; thus it is redundant. This is because $\sum_x p(X=x|W=w) = 1$. Therefore the equation 21 imposes $|\mathcal{X}|-1$ constraints on $p(\widetilde{W}=w)$.

Next, in order to enforce $I(\widetilde{W};Y) = I(W;Y)$, we require

$$\sum_w p(\widetilde{W}=w)H(Y|\widetilde{W}=w) = \sum_w p(W=w)H(Y|W=w). \tag{22}$$

Please note that because of equation 18, $H(Y|\widetilde{W}=w) = H(Y|W=w)$. Similarly in order to enforce $I(\widetilde{W};Z) = I(W;Z)$, we require

$$\sum_w p(\widetilde{W}=w)H(Z|\widetilde{W}=w) = \sum_w p(W=w)H(Z|W=w). \tag{23}$$

For $I(\widetilde{U};Y|\widetilde{W}) = I(U;Y|W)$ and $I(\widetilde{V};Z|\widetilde{W}) = I(V;Z|W)$, we require

$$\sum_w p(\widetilde{W}=w)I(\widetilde{U};Y|\widetilde{W}=w) = \sum_w p(W=w)I(U;Y|W=w), \tag{24}$$

and

$$\sum_w p(\widetilde{W}=w)I(\widetilde{V};Z|\widetilde{W}=w)=\sum_w p(W=w)I(V;Z|W=w). \tag{25}$$

Please note that because of equation 18, $I(\widetilde{U};Y|\widetilde{W}=w)=I(U;Y|W=w)$ and $I(\widetilde{V};Z|\widetilde{W}=w)=I(V;Z|W=w)$.

In order to enforce $I(\widetilde{U};\widetilde{V}|\widetilde{W})\leq I(U;V|W)$, we require

$$\sum_w p(\widetilde{W}=w)I(\widetilde{U};\widetilde{V}|\widetilde{W}=w)\leq\sum_w p(W=w)I(U;V|W=w). \tag{26}$$

Because of equation 18, $I(\widetilde{U};\widetilde{V}|\widetilde{W}=w)=I(U;V|W=w)$.

The rest of the proof is based on the technique of Fenchel and Eggleston to strengthen the Carathéodory theorem. The region formed by equations 19, 20, 21, 22, 23, 24 and 25 contains the vector $w\mapsto p(W=w)$. The vector $w\mapsto p(W=w)$ further lies in the half space defined by equation 26. We can write the vector $w\mapsto p(W=w)$ as the convex combination of extreme points of the region formed by equations 19, 20, 22, 23, 24 and 25. Since $w\mapsto p(W=w)$ is in the half space, it must be the case that at least one of these extreme points satisfies equation 26. Any such extreme point can have at most $|\mathcal{X}|+4$ non-negative elements. This is because any extreme point must satisfy with equality at least $|\mathcal{W}|$ of the equations 19, 20, 22, 23, 24 and 25. The number of equations that do not enforce one of the elements of the vector $w\mapsto p(\widetilde{W}=w)$ to zero is $|\mathcal{X}|+4$. Therefore at least $|\mathcal{W}|-|\mathcal{X}|-4$ coordinates of an extreme point must be zero. Hence the number of non-zero elements is at most $|\mathcal{X}|+4$.

It remains to prove that the last part of Lemma 2 is true, i.e. that $\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$ is convex. Since $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is a subset of $\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$, it suffices to show that $\bigcup_{S_w\geq 0}\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ is convex. Take two arbitrary points $(R_1,R_2,...,R_6)$ and $(\widetilde{R_1},\widetilde{R_2},...,\widetilde{R_6})$ in $\bigcup_{S_w\geq 0}\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$. Corresponding to $(R_1,...,R_6)$ and $(\widetilde{R_1},...,\widetilde{R_6})$ are joint distributions $p_0(u,v,w,x,y,z)=p_0(u,v,w,x)q(y,z|x)$ on U,V,W,X,Y,Z, and $p_0(\widetilde{u},\widetilde{v},\widetilde{w},\widetilde{x},\widetilde{y},\widetilde{z})=p_0(\widetilde{u},\widetilde{v},\widetilde{w},\widetilde{x})q(\widetilde{y},\widetilde{z}|\widetilde{x})$ on $\widetilde{U},\widetilde{V},\widetilde{W},\widetilde{X},\widetilde{Y},\widetilde{Z}$, where $|\mathcal{U}|=|\widetilde{\mathcal{U}}|=S_u$, $|\mathcal{V}|=|\widetilde{\mathcal{V}}|=S_v$, and furthermore the following equations are satisfied: $R_1\leq I(W;Y)$, $R_2\leq I(W;Z)$, $R_3\leq I(UW;Y)$, ..., $\widetilde{R_1}\leq I(\widetilde{W};\widetilde{Y})$, $\widetilde{R_2}\leq I(\widetilde{W};\widetilde{Z})$, $\widetilde{R_3}\leq I(\widetilde{U}\widetilde{W};\widetilde{Y})$,...

Without loss of generality we can assume that $(\widetilde{U},\widetilde{V},\widetilde{W},\widetilde{X},\widetilde{Y},\widetilde{Z})$ and (U,V,W,X,Y,Z) are independent. Let Q be a uniform binary random variable independent of all previously defined random variables. Let $(\widehat{U},\widehat{V},\widehat{W},\widehat{X},\widehat{Y},\widehat{Z})$ be equal to (U,V,WQ,X,Y,Z) when $Q=0$, and equal to $(\widetilde{U},\widetilde{V},\widetilde{W}Q,\widetilde{X},\widetilde{Y},\widetilde{Z})$ when $Q=1$. One can verify that $p(\widehat{Y}=y,\widehat{Z}=z|\widehat{X}=x)=q(\widehat{Y}=y,\widehat{Z}=$

$z|\widehat{X}=x)$, $I(\widehat{U}\widehat{V}\widehat{W};\widehat{Y}\widehat{Z}|\widehat{X})=0$, and furthermore

$$I(\widehat{W};\widehat{Y}) \geq \tfrac{1}{2}I(W;Y)+\tfrac{1}{2}I(\widetilde{W};\widetilde{Y})$$
$$I(\widehat{W};\widehat{Z}) \geq \tfrac{1}{2}I(W;Z)+\tfrac{1}{2}I(\widetilde{W};\widetilde{Z})$$
$$I(\widehat{U}\widehat{W};\widehat{Y}) \geq \tfrac{1}{2}I(UW;Y)+\tfrac{1}{2}I(\widetilde{U}\widetilde{W};\widetilde{Y})$$
$$\ldots$$

Hence $(\frac{1}{2}R_1+\frac{1}{2}\widetilde{R_1},\frac{1}{2}R_2+\frac{1}{2}\widetilde{R_2},...,\frac{1}{2}R_6+\frac{1}{2}\widetilde{R_6})$ belongs to $\bigcup_{S_w\geq 0}\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$. Thus $\bigcup_{S_w\geq 0}\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))=\mathcal{C}_{M-I}^{S_u,S_v,|\mathcal{X}|+4}(q(y,z|x))$ is convex. ∎

Proof of Lemma 3: The equation $H(\widehat{X})=H(X)+\epsilon H_L(X)-\mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|X]\big)\big]$ where $r(x)=(1+x)\log(1+x)$ is true because:

$$H(\widehat{X})=-\textstyle\sum_{\widehat{x}}p_\epsilon(\widehat{x})\log p_\epsilon(\widehat{x})$$
$$=-\textstyle\sum_{\widehat{x}}p_0(\widehat{x})\big(1+\epsilon\cdot\mathbb{E}[L|X=\widehat{x}]\big)\cdot\log\Big(p_0(\widehat{x})\cdot\big(1+\epsilon\cdot\mathbb{E}[L|X=\widehat{x}]\big)\Big)$$
$$=-\textstyle\sum_{\widehat{x}}p_0(\widehat{x})\big(1+\epsilon\cdot\mathbb{E}[L|X=\widehat{x}]\big)\cdot\Big[\log\Big(p_0(\widehat{x})\Big)+\log\Big(1+\epsilon\cdot\mathbb{E}[L|X=\widehat{x}]\Big)\Big]$$
$$=H(X)-\epsilon\textstyle\sum_{\widehat{x}}p_0(\widehat{x})\mathbb{E}[L|X=\widehat{x}]\log\Big(p_0(\widehat{x})\Big)-$$
$$\textstyle\sum_{\widehat{x}}p_0(\widehat{x})\big(1+\epsilon\cdot\mathbb{E}[L|X=\widehat{x}]\big)\cdot\log\Big(1+\epsilon\cdot\mathbb{E}[L|X=\widehat{x}]\Big)$$
$$=H(X)+\epsilon H_L(X)-\mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|X]\big)\big].$$

Next, note that $r(0)=0$, $\frac{\partial}{\partial x}r(x)=\log(1+x)+\log(e)$ and $\frac{\partial^2}{\partial x^2}r(x)=\frac{\log(e)}{1+x}$. We have:

$$\frac{\partial}{\partial\epsilon}H(\widehat{X})=H_L(X)-\mathbb{E}\big[\mathbb{E}[L|X]\{\log(1+\epsilon\cdot\mathbb{E}[L|X])+\log e\}\big]=H_L(X)-\mathbb{E}\big[\mathbb{E}[L|X]\log(1+\epsilon\cdot\mathbb{E}[L|X])\big],$$

where at $\epsilon=0$ is equal to $H_L(X)$.

Next, we have:

$$\tfrac{\partial^2}{\partial\epsilon^2}H(\widehat{X})=-\tfrac{\partial}{\partial\epsilon}\mathbb{E}\big[\mathbb{E}[L|X]\log(1+\epsilon\cdot\mathbb{E}[L|X])\big]$$
$$-\mathbb{E}\big[\mathbb{E}[L|X]\tfrac{\mathbb{E}[L|X]}{1+\epsilon\cdot\mathbb{E}[L|X]}\log e\big]=-\log e\cdot\mathbb{E}\big[\tfrac{\mathbb{E}[L|X]^2}{1+\epsilon\cdot\mathbb{E}[L|X]}\big]$$

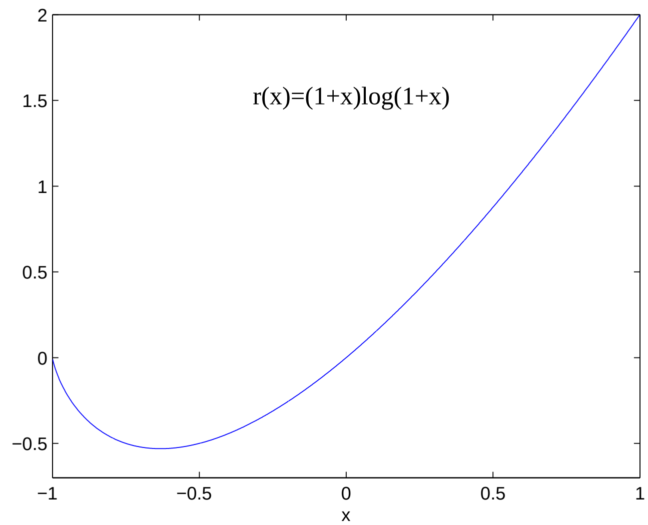

Fig. 2. Plot of the convex function $r(x) = (1 + x)\log(1 + x)$ over the interval $[-1, 1]$. Note that $r(0) = 0$, $\frac{\partial}{\partial x} r(x) = \log(1 + x) + \log(e)$ and $\frac{\partial^2}{\partial x^2} r(x) = \frac{\log(e)}{1+x} > 0$.

On the other hand,

$$I(\epsilon) = \sum_x \left(\frac{\partial}{\partial \epsilon} \log_e(p_\epsilon(\widehat{X} = x)) \right)^2 p_\epsilon(\widehat{X} = x) =$$

$$\sum_x \left(\frac{\partial}{\partial \epsilon} \log_e \left(p_0(X = x) \cdot \big(1 + \epsilon \cdot \mathbb{E}[L|X = x]\big) \right) \right)^2 p_0(X = x) \cdot \big(1 + \epsilon \cdot \mathbb{E}[L|X = x]\big) =$$

$$\sum_x \left(\frac{\partial}{\partial \epsilon} \log_e \big(1 + \epsilon \cdot \mathbb{E}[L|X = x]\big) \right)^2 p_0(X = x) \cdot \big(1 + \epsilon \cdot \mathbb{E}[L|X = x]\big) =$$

$$\sum_x \left(\frac{\mathbb{E}[L|X=x]}{1+\epsilon \cdot \mathbb{E}[L|X=x]} \right)^2 p_0(X = x) \cdot \big(1 + \epsilon \cdot \mathbb{E}[L|X = x]\big) =$$

$$\sum_x \frac{\mathbb{E}[L|X=x]^2}{1+\epsilon \cdot \mathbb{E}[L|X=x]} p_0(X = x) = \mathbb{E}\Big[\frac{\mathbb{E}[L|X]^2}{1+\epsilon \cdot \mathbb{E}[L|X]}\Big].$$

■

Appendix A

In this Appendix we prove equation 11 assuming that $\lambda_5 > 0$ or $\lambda_6 > 0$, or both. Let $(R_1, R_2, ..., R_6)$ be a point in $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y, z|x))$ where the maximum of $\sum_{i=1}^{6} \lambda_i R'_i$ over $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y, z|x))$ is obtained.[11] Corresponding to $(R_1, R_2, ..., R_6)$ is at least one joint distribution $p_0(u, v, w, x, y, z) = p_0(u, v, w, x)q(y, z|x)$

[11]Note that by Lemma 2, $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y, z|x))$ is closed and furthermore $\sum_i \lambda_i R'_i$ is bounded from above when $\lambda_i \geq 0$. Hence maximum of $\sum_i \lambda_i R'_i$ over the region $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y, z|x))$ is well defined.

on U,V,W,X,Y,Z where $|\mathcal{U}|\leq S_u$, $|\mathcal{V}|\leq S_v$ and $|\mathcal{W}|\leq S_w$, and furthermore the following inequalities are satisfied: $R_1\leq I(W;Y)$, $R_2\leq I(W;Z)$, $R_3\leq I(UW;Y)$, ... etc. Maximum of $\sum_{i=1}^{6}\lambda_i R_i'$ over $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ must be then equal to $\lambda_1\cdot I(W;Y)+\lambda_2\cdot I(W;Z)+\lambda_3\cdot I(UW;Y)+\lambda_4\cdot I(VW;Z)+\lambda_5\cdot\big(I(U;Y|W)+I(V;Z|W)-I(U;V|W)+I(W;Y)\big)+\lambda_6\cdot\big(I(U;Y|W)+I(V;Z|W)-I(U;V|W)+I(W;Z)\big)$. We would like to define random variables $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$, $\widetilde{X}$, $\widetilde{Y}$ and $\widetilde{Z}$ jointly distributed according to $p(\widetilde{u},\widetilde{v},\widetilde{w},\widetilde{x})q(\widetilde{y},\widetilde{z}|\widetilde{x})$, and satisfying the following properties:

- $\lambda_1\cdot I(W;Y)+\lambda_2\cdot I(W;Z)+\lambda_3\cdot I(UW;Y)+\lambda_4\cdot I(VW;Z)+\lambda_5\cdot(I(U;Y|W)+I(V;Z|W)-I(U;V|W)+I(W;Y))+\lambda_6\cdot(I(U;Y|W)+I(V;Z|W)-I(U;V|W)+I(W;Z))$ is less than or equal to $\lambda_1\cdot I(\widetilde{W};\widetilde{Y})+\lambda_2\cdot I(\widetilde{W};\widetilde{Z})+\lambda_3\cdot I(\widetilde{U}\widetilde{W};\widetilde{Y})+\lambda_4\cdot I(\widetilde{V}\widetilde{W};\widetilde{Z})+\lambda_5\cdot(I(\widetilde{U};\widetilde{Y}|\widetilde{W})+I(\widetilde{V};\widetilde{Z}|\widetilde{W})-I(\widetilde{U};\widetilde{V}|\widetilde{W})+I(\widetilde{W};\widetilde{Y}))+\lambda_6\cdot(I(\widetilde{U};\widetilde{Y}|\widetilde{W})+I(\widetilde{V};\widetilde{Z}|\widetilde{W})-I(\widetilde{U};\widetilde{V}|\widetilde{W})+I(\widetilde{W};\widetilde{Z}))$.
- $|\widetilde{\mathcal{U}}|=|\mathcal{X}|$.
- $|\widetilde{\mathcal{V}}|=|\mathcal{V}|$.
- $|\widetilde{\mathcal{W}}|=|\mathcal{W}|$.

Instead of finding $\widetilde{U}$ that takes values in a set of size at most $|\mathcal{X}|$, it however suffices to find an appropriate $\widetilde{U}$ such that for any $\widetilde{w}$, the conditional distribution $p(\widetilde{u}|\widetilde{w})\neq 0$ for at most $|\mathcal{X}|$ values of $\widetilde{u}$. [12]

We assume that random variables $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$, $\widetilde{X}$, $\widetilde{Y}$ and $\widetilde{Z}$ are respectively defined on the alphabet sets of U, V, W, X, Y and Z. Without loss of generality assume $p(W=w)>0$ for all $w\in\mathcal{W}$. We assume that the joint distribution of $\widetilde{W},\widetilde{X},\widetilde{Y},\widetilde{Z}$ is the same as that of W,X,Y,Z. Therefore $I(W;Y)=I(\widetilde{W};\widetilde{Y})$ and $I(W;Z)=I(\widetilde{W};\widetilde{Z})$. We therefore need to define $p(\widetilde{u},\widetilde{v}|\widetilde{w},\widetilde{x})$ such that

- For any $w\in\mathcal{W}$, $\lambda_3\cdot I(U;Y|W=w)+\lambda_4\cdot I(V;Z|W=w)+\lambda_5\cdot(I(U;Y|W=w)+I(V;Z|W=w)-I(U;V|W=w))+\lambda_6\cdot(I(U;Y|W=w)+I(V;Z|W=w)-I(U;V|W=w))$ is less than or equal to $\lambda_3\cdot I(\widetilde{U};\widetilde{Y}|\widetilde{W}=w)+\lambda_4\cdot I(\widetilde{V};\widetilde{Z}|\widetilde{W}=w)+\lambda_5\cdot(I(\widetilde{U};\widetilde{Y}|\widetilde{W}=w)+I(\widetilde{V};\widetilde{Z}|\widetilde{W}=w)-I(\widetilde{U};\widetilde{V}|\widetilde{W}=w))+\lambda_6\cdot(I(\widetilde{U};\widetilde{Y}|\widetilde{W}=w)+I(\widetilde{V};\widetilde{Z}|\widetilde{W}=w)-I(\widetilde{U};\widetilde{V}|\widetilde{W}=w))$.
- $|\widetilde{\mathcal{V}}|=|\mathcal{V}|$.
- For any w, $p(\widetilde{U}=u|\widetilde{W}=w)\neq 0$ for at most $|\mathcal{X}|$ values of u.

The above statement holds since Lemma 1 of Section III holds.

[12] This is true because Marton's inner bound depends only on the conditional distribution of $\widetilde{U}$ given $\widetilde{W}$, rather than the distribution of $\widetilde{U}$ itself. More specifically, assume that we are given a random variable $\widetilde{U}$ such that for every $\widetilde{w}\in\widetilde{\mathcal{W}}$, there is a subset $\mathcal{A}_{\widetilde{w}}$ of the alphabet set of $\widetilde{U}$ satisfying $|\mathcal{A}_{\widetilde{w}}|=|\mathcal{X}|$, and $p(\widetilde{U}=\widetilde{u}|\widetilde{W}=\widetilde{w})=0$ if $\widetilde{u}\notin\mathcal{A}_{\widetilde{w}}$. Assume that $\mathcal{A}_{\widetilde{w}}=\{a_{\widetilde{w},1},a_{\widetilde{w},2},a_{\widetilde{w},3},...,a_{\widetilde{w},|\mathcal{X}|}\}$. Define $\widetilde{U}'$, a random variable taking values from the set $\{1,2,3,...,|\mathcal{X}|\}$, as follows: $p(\widetilde{U}'=i|\widetilde{W}=\widetilde{w},\widetilde{V}=\widetilde{v},\widetilde{X}=\widetilde{x})=p(\widetilde{U}=a_{\widetilde{w},i}|\widetilde{W}=\widetilde{w},\widetilde{V}=\widetilde{v},\widetilde{X}=\widetilde{x})$. The alphabet set of $\widetilde{U}'$ is of size $|\mathcal{X}|$ and furthermore $I(\widetilde{U}';\widetilde{V}|\widetilde{W})=I(\widetilde{U};\widetilde{V}|\widetilde{W})$ and $I(\widetilde{U}';\widetilde{Y}|\widetilde{W})=I(\widetilde{U};\widetilde{Y}|\widetilde{W})$.

APPENDIX B

In this Appendix, we prove that the closure of $\mathcal{C}_M(q(y,z|x))$ is equal to the closure of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$. In order to show this it suffices to show that any triple (R_0,R_1,R_2) in $\mathcal{C}_M(q(y,z|x))$ is a limit point of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$. Since (R_0,R_1,R_2) is in $\mathcal{C}_M(q(y,z|x))$, random variables U,V,W,X,Y and Z for which equations 1, 2, 3 and 4 are satisfied, exist. First assume U,V,W are discrete random variables taking values in $\{1,2,3,...\}$. For any integer m, let U_m,V_m and W_m be truncated versions of U,V and W defined on $\{1,2,3,...,m\}$ as follows: U_m,V_m and W_m are jointly distributed according to $p(U_m=u,V_m=v,W_m=w)=\frac{p(U=u,V=v,W=w)}{p(U\leq m,V\leq m,W\leq m)}$ for every u, v and w less than or equal to m. Further assume that X_m, Y_m and Z_m are random variables defined on $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ where $p(Y_m=y,Z_m=z,X_m=x|U_m=u,V_m=v,W_m=w)=p(Y=y,Z=z,X=x|U=u,V=v,W=w)$ for every u, v and w less than or equal to m, and for every x, y and z. Note that the joint distribution of U_m,V_m,W_m,X_m,Y_m and Z_m converges to that of U,V,W,X,Y and Z as $m\to\infty$. Therefore the mutual information terms $I(W_m;Y_m)$, $I(W_m;Z_m)$, $I(W_mU_m;Y_m)$, ... (that define a region in $\mathcal{C}_M^{m,m,m}(q(y,z|x))$) converge to the corresponding terms $I(W;Y)$, $I(W;Z)$, $I(WU;Y)$, ... Therefore (R_0,R_1,R_2) is a limit point of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$.

Next assume that some of the random variables U, V and W are continuous. Given any positive q, one can quantize the continuous random variables to a precision q, and get discrete random variables U_q, V_q and W_q. We have already established that any point in the Marton's inner bound region corresponding to U_q,V_q,W_q,X,Y,Z is a limit point of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$. The joint distribution of U_q,V_q,W_q,X,Y,Z converges to that of U,V,W,X,Y,Z as q converges to zero. Therefore the corresponding mutual information terms $I(W_q;Y_q)$, $I(W_q;Z_q)$, $I(W_qU_q;Y_q)$, ... (that define a region in $\mathcal{C}_M(q(y,z|x))$) converge to the corresponding terms $I(W;Y)$, $I(W;Z)$, $I(WU;Y)$,.... Therefore (R_0,R_1,R_2) is a limit point of $\bigcup_{S_u,S_v,S_w\geq 0}\mathcal{C}_M^{S_u,S_v,S_w}(q(y,z|x))$.

APPENDIX C

In this Appendix, we prove that $\mathscr{C}(q(y,z|x))$ is equal to $\mathscr{L}(q(y,z|x))$. Clearly $\mathscr{C}(q(y,z|x))\subset\mathscr{L}(q(y,z|x))$. Therefore we need to show that $\mathscr{L}(q(y,z|x))\subset\mathscr{C}(q(y,z|x))$. Instead we show that $\mathscr{L}_I(q(y,z|x))\subset\mathscr{C}_I(q(y,z|x))$.[13] It suffices to prove that $\mathscr{C}_I(q(y,z|x))$ is convex, and that for any λ_1,

[13]This is true because (R_0,R_1,R_2) being in $\mathscr{L}(q(y,z|x))$ implies that $(R_0,R_0,R_0+R_1,R_0+R_2,R_0+R_1+R_2,R_0+R_1+R_2)$ is in $\mathscr{L}_I(q(y,z|x))$. If $\mathscr{L}_I(q(y,z|x))(q(y,z|x))$ is a subset of $\mathscr{C}_I(q(y,z|x))$, the latter point would belong to $\mathscr{C}_I(q(y,z|x))$. Therefore (R_0,R_1,R_2) belongs to $\mathscr{C}(q(y,z|x))$.

λ_2, ..., λ_6, the maximum of $\sum_{i=1}^{6}\lambda_i R_i$ over triples $(R_1, R_2, ..., R_6)$ in $\mathscr{L}_I(q(y,z|x))$, is less than or equal to the maximum of $\sum_{i=1}^{6}\lambda_i R_i$ over triples $(R_1, R_2, ..., R_6)$ in $\mathscr{C}_I(q(y,z|x))$.

In order to show that $\mathscr{C}_I(q(y,z|x))$ is convex, we take two arbitrary points in $\mathscr{C}_I(q(y,z|x))$. Corresponding to them are joint distributions $p(u_1, v_1, w_1, x_1, y_1, z_1)$ and $p(u_2, v_2, w_2, x_2, y_2, z_2)$. Let Q be a uniform binary random variable independent of all previously defined random variables, and let $U = U_Q$, $V = V_Q$, $W = (W_Q, Q)$, $X = X_Q$, $Y = Y_Q$ and $Z = Z_Q$. Clearly $H(X|UVW) = 0$, and furthermore $I(W;Y) \geq \frac{1}{2}\big(I(W_1;Y_1) + I(W_2;Y_2)\big)$, $I(W;Z) \geq \frac{1}{2}\big(I(W_1;Z_1) + I(W_2;Z_2)\big)$, ... Random variable W is not however defined on an alphabet set of size $|\mathcal{X}| + 4$. However, one can reduce the cardinality of W using the Carathéodory theorem (as in the proof of part two of Lemma 2) by fixing $p(u,v,x,y,z|w)$ and changing the marginal distribution of W in a way that at most $|\mathcal{X}| + 4$ elements get non-zero probability assigned to them. Since we have preserved $p(u,v,x,y,z|w)$ throughout the process, $p(x|u,v,w)$ will remain to belong to the set $\{0,1\}$ after reducing the cardinality of W.

Next, we need to show that for any λ_1, λ_2, ..., λ_6, the maximum of $\sum_{i=1}^{6}\lambda_i R_i$ over triples $(R_1, R_2, ..., R_6)$ in $\mathscr{L}_I(q(y,z|x))$, is less than or equal to the maximum of $\sum_{i=1}^{6}\lambda_i R_i$ over triples $(R_1, R_2, ..., R_6)$ in $\mathscr{C}_I(q(y,z|x))$. As discussed in the proof of theorem 1, without loss of generality we can assume λ_i is non-negative for $i = 1, 2, ..., 6$.

Take an arbitrary point $(R_1, R_2, ..., R_6)$ in $\mathscr{L}_I(q(y,z|x))$. By definition there exists random variables U, V, W, X, Y and Z for which

$$\begin{aligned}\sum_{i=1}^{6}\lambda_i R_i \leq \lambda_1\cdot I(W;Y) + \lambda_2\cdot I(W;Z) + \lambda_3\cdot I(UW;Y) + \lambda_4\cdot I(VW;Z) +&\\ \lambda_5\cdot\big(I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Y)\big) +&\\ \lambda_6\cdot\big(I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Z)\big).&\end{aligned} \tag{27}$$

Fix $p(u,v,w)$. The right hand side of equation (27) would then be a convex function of $p(x|u,v,w)$.[14] Therefore its maximum occurs at the extreme points when $p(x|u,v,w) \in \{0,1\}$ whenever $p(u,v,w) \neq 0$. Therefore random variables $\widehat{U}, \widehat{V}, \widehat{W}, \widehat{X}, \widehat{Y}$ and $\widehat{Z}$ exists for which

$$\begin{aligned}\lambda_1\cdot I(W;Y) + \lambda_2\cdot I(W;Z) + ... + \lambda_6\cdot\big(I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Z)\big) \leq&\\ \lambda_1\cdot I(\widehat{W};\widehat{Y}) + \lambda_2\cdot I(\widehat{W};\widehat{Z}) + ... + \lambda_6\cdot\big(I(\widehat{U};\widehat{Y}|\widehat{W}) + I(\widehat{V};\widehat{Z}|\widehat{W}) - I(\widehat{U};\widehat{V}|\widehat{W}) + I(\widehat{W};\widehat{Z})\big)&\end{aligned}$$

and furthermore $p(\widehat{x}|\widehat{u},\widehat{v},\widehat{w}) \in \{0,1\}$ for all $\widehat{x}$, $\widehat{u}$, $\widehat{v}$ and $\widehat{w}$ where $p(\widehat{u},\widehat{v},\widehat{w}) > 0$.

[14]This is true because $I(W;Y)$ is convex in the conditional distribution $p(y|w)$; similarly $I(U;Y|W=w)$ is convex for any fixed value of w. The term $I(U;V|W)$ that appears with a negative sign is constant since the joint distribution of $p(u,v,w)$ is fixed.

APPENDIX D

In this Appendix, we complete the proof of theorem 2 by showing that given any random variables U, V, W, X, Y and Z where $UVW \to X \to YZ$ holds, U and V are binary, $H(X|UVW)$ is zero, the transition matrices $P_{Y|X}$ and $P_{Z|X}$ have positive elements, and for any value of w where $p(w) > 0$, either $I(U;V|W = w, Y) = 0$ or $I(U;V|W = w, Z) = 0$ holds, the following inequality is true:

$$I(U;Y|W = w) + I(V;Z|W = w) - I(U;V|W = w) \leq T(p(X = 1|W = w)).$$

We assume $I(U;V|W = w, Y) = 0$ (the proof for the case $I(U;V|W = w, Z) = 0$ is similar). First consider the case in which the individual capacity $C_{P_{Y|X}}$ is zero. We will then have $I(U;Y|W = w) = 0$ and $T(p(X = 1|W = w)) = I(X;Z|W = w) \geq I(V;Z|W = w) - I(U;V|W = w)$. Therefore the inequality holds in this case. Assume therefore that $C_{P_{Y|X}}$ is non-zero.

It suffices to prove the following proposition:

Proposition: For any random variables U, V, X, Y and Z satisfying

- $UV \to X \to YZ$,
- $H(X|UV) = 0$,
- $|\mathcal{U}| = |\mathcal{V}| = |\mathcal{X}| = 2$,
- for all $y \in \mathcal{Y}$, $p(Y = y|X = 0)$ and $p(Y = y|X = 1)$ are non-zero,
- $C_{P_{Y|X}} \neq 0$,
- $I(U;V|Y) = 0$,

one of the following two cases must be true: (1) at least one of the random variables X, U or V is constant, (2) Either $U = X$ or $U = 1 - X$ or $V = X$ or $V = 1 - X$.

Proof: Assume that neither (1) nor (2) holds. Since $H(X|UV) = 0$, there are 2^4 possible descriptions for $p(x|uv)$, some of which are ruled out because neither (1) nor (2) holds. In the following we prove that $X = U \oplus V$ and $X = U \wedge V$ can not hold. The proof for other cases is essentially the same.

Since $C_{P_{Y|X}} \neq 0$ implies that the transition matrix $P_{Y|X}$ has linearly independent rows. This implies the existence of $y_1, y_2 \in \mathcal{Y}$ for which $p(X = 1|Y = y_1) \neq p(X = 1|Y = y_2)$.[15] Furthermore since X is not constant, and $p(Y = y_1|X = 0), p(Y = y_1|X = 1), p(Y = y_2|X = 0)$ and $p(Y = y_2|X = 1)$ are

[15] If this is not the case we have $p(X = 1|Y = y_1) = p(X = 1|Y = y_2)$ for all $y_1, y_2 \in \mathcal{Y}$. This would imply that X and Y are independent. Since X is not constant, independence of X and Y implies that $P(Y = y|X = 1) = p(Y = y|X = 0)$ for all $y \in \mathcal{Y}$. Therefore the transition matrix $P_{Y|X}$ has linearly dependent rows. Hence $I(X;Y) = 0$ for all $p(x)$. Therefore $C_{P_{Y|X}} = 0$ which is a contradiction.

all non-zero, both $p(X=1|Y=y_1)$ and $p(X=1|Y=y_2)$ are in the open interval $(0,1)$. Note that $I(U;V|Y)=0$ implies that $I(U;V|Y=y_1)=0$ and $I(U;V|Y=y_2)=0$.

Let $a_{i,j}=p(U=i,V=j)$ for $i,j\in\{0,1\}$. First assume that $X=U\oplus V$. We have

- $p(u=0,v=0|y=y_i)=\frac{a_{0,0}}{a_{0,0}+a_{1,1}}p(X=0|Y=y_i)$,
- $p(u=0,v=1|y=y_i)=\frac{a_{0,1}}{a_{0,1}+a_{1,0}}p(X=1|Y=y_i)$,
- $p(u=1,v=0|y=y_i)=\frac{a_{1,0}}{a_{0,1}+a_{1,0}}p(X=1|Y=y_i)$,
- $p(u=1,v=1|y=y_i)=\frac{a_{1,1}}{a_{0,0}+a_{1,1}}p(X=0|Y=y_i)$.

Therefore $I(U;V|Y=y_i)=0$ for $i=1,2$ implies that

$$p(u=1,v=1|y=y_i)\times p(u=0,v=0|y=y_i)=p(u=0,v=1|y=y_i)\times p(u=1,v=0|y=y_i).$$

Therefore

$$\frac{a_{0,0}a_{1,1}}{(a_{0,0}+a_{1,1})^2}p(X=0|Y=y_i)^2=\frac{a_{0,1}a_{1,0}}{(a_{0,1}+a_{1,0})^2}p(X=1|Y=y_i)^2,$$

or alternatively

$$\frac{\sqrt{a_{0,0}a_{1,1}}}{a_{0,0}+a_{1,1}}p(X=0|Y=y_i)=\frac{\sqrt{a_{1,0}a_{0,1}}}{a_{1,0}+a_{0,1}}p(X=1|Y=y_i). \tag{28}$$

Since X is not deterministic, $P(X=0)=a_{0,0}+a_{1,1}$ and $P(X=1)=a_{1,0}+a_{0,1}$ are non-zero. Next, if either of $a_{0,0}$ or $a_{1,1}$ are zero, it implies that $a_{1,0}$ or $a_{0,1}$ is zero. But this implies that either U or V are constant random variables which is a contradiction. Hence $\frac{\sqrt{a_{0,0}a_{1,1}}}{a_{0,0}+a_{1,1}}$ and $\frac{\sqrt{a_{1,0}a_{0,1}}}{a_{1,0}+a_{0,1}}$ are non-zero. But then equation 28 uniquely specifies $p(X=1|Y=y_i)$, implying that $p(X=1|Y=y_1)=p(X=1|Y=y_2)$ which is again a contradiction.

Next assume that $X=U\wedge V$. We have:

- $p(u=0,v=0|y=y_i)=\frac{a_{0,0}}{a_{0,0}+a_{0,1}+a_{1,0}}p(X=0|Y=y_i)$,
- $p(u=0,v=1|y=y_i)=\frac{a_{0,1}}{a_{0,0}+a_{0,1}+a_{1,0}}p(X=0|Y=y_i)$,
- $p(u=1,v=0|y=y_i)=\frac{a_{1,0}}{a_{0,0}+a_{0,1}+a_{1,0}}p(X=0|Y=y_i)$,
- $p(u=1,v=1|y=y_i)=p(X=1|Y=y_i)$.

Note that $P(X=0)=a_{0,0}+a_{0,1}+a_{1,0}$ is non-zero. Independence of U and V given $Y=y_i$ implies that

$$p(u=1,v=1|y=y_i)\times p(u=0,v=0|y=y_i)=p(u=0,v=1|y=y_i)\times p(u=1,v=0|y=y_i).$$

Therefore

$$\frac{a_{0,0}}{a_{0,0}+a_{0,1}+a_{1,0}}p(X=0|Y=y_i)p(X=1|Y=y_i)=\frac{a_{1,0}a_{0,1}}{(a_{0,0}+a_{0,1}+a_{1,0})^2}p(X=0|Y=y_i)^2,$$

or alternatively

$$a_{0,0} \cdot p(X = 1|Y = y_i) = \frac{a_{1,0}a_{0,1}}{a_{0,0} + a_{0,1} + a_{1,0}} p(X = 0|Y = y_i), \tag{29}$$

If $a_{0,0}$ is zero, either $a_{1,0}$ or $a_{0,1}$ must also be zero, but this implies that either U or V are constant random variables which is a contradiction. Therefore $a_{0,0}$ is non-zero. But then equation 29 uniquely specifies $p(X = 1|Y = y_i)$, implying that $p(X = 1|Y = y_1) = p(X = 1|Y = y_2)$ which is again a contradiction.

ACKNOWLEDGEMENT

The authors would like to thank Chandra Nair for suggesting a shortcut to simplify the original proof, and Young Han Kim for valuable comments that improved the presentation of the article. 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 grant numbers CCF-0500234, CCF-0635372, CNS-0627161 and ARO MURI grant W911NF-08-1-0233 "Tools for the Analysis and Design of Complex Multi-Scale Networks."

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: Akadmiai 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] Yingbin Liang, Venugopal V. Veeravalli, H. Vincent Poor, "Resource Allocation for Wireless Fading Relay Channels: Max-Min Solution", IEEE Trans. IT, 53 (10): 3432-3453 (2007).