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

Amin Aminzadeh Gohari and Venkat Anantharam<br>Department of Electrical Engineering and Computer Science University of California, Berkeley<br>\{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 traditional use of the Carathéodory theorem, the main known tool for proving cardinality bounds, does not yield a finite cardinality result. One of the main contributions of this paper is the introduction of a new tool 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 need to 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.

Lastly, we establish a conjecture of [12] that Marton's inner bound and the recent outer bound of Nair and El Gamal do not match in general.


## I. Introduction

In this paper, we consider two-receiver general broadcast channels. A two-receiver broadcast channel is characterized by the conditional distribution $q(y, z \mid x)$ 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 $M_{0}, M_{1}$ and $M_{2}$ 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 $\zeta: \mathcal{M}_{0} \times \mathcal{M}_{1} \times \mathcal{M}_{2} \rightarrow \mathcal{X}^{n}$, and sends it over the broadcast channel $q(y, z \mid x)$ 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 $\left(\widehat{M}_{0}{ }^{(2)}, \widehat{M}_{2}\right)$ respectively. The average probability of error is then taken to be the probability that $\left(\widehat{M}_{0}^{(1)}, \widehat{M}_{1}, \widehat{M}_{0}^{(2)}, \widehat{M}_{2}\right)$ is not equal to $\left(M_{0}, M_{1}, M_{0}, M_{2}\right)$.

The capacity region of the broadcast channel is defined as the set of all triples $\left(R_{0}, R_{1}, R_{2}\right)$ such that for any $\epsilon>0$, there is some integer $n$, uniform random variables $M_{0}, M_{1}, M_{2}$ with alphabet sets $\left|\mathcal{M}_{i}\right| \geq 2^{n\left(R_{i}-\epsilon\right)}$ (for $i=0,1,2$ ), encoding function $\zeta$, and decoding functions $\vartheta_{y}$ and $\vartheta_{z}$ such that the average probability of error is less than or equal to $\epsilon$.

The capacity region of the broadcast channel is not known except in certain special cases. The best achievable region of triples $\left(0, R_{1}, R_{2}\right)$ 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 $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$, of

$$
\begin{align*}
& R_{0}, R_{1}, R_{2} \geq \\
& R_{0} \leq \min (I(W ; Y), I(W ; Z)) ;  \tag{1}\\
& R_{0}+R_{1} \leq I(U W ; Y) ;  \tag{2}\\
& R_{0}+R_{2} \leq I(V W ; Z) ;  \tag{3}\\
& R_{0}+R_{1}+R_{2} \leq I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W) \\
&+\min (I(W ; Y), I(W ; Z)) . \tag{4}
\end{align*}
$$

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 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 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 $H(X \mid U V W)=0$ is identical to Marton's inner bound.

One of the main contributions of this paper is the perturbation technique. At the heart of this technique lies the following observation: consider an arbitrary set of finite random variables $X_{1}, X_{2}, \ldots, X_{n}$ jointly distributed according to $p_{0}\left(x_{1}, x_{2}, \ldots, x_{n}\right)$. One can represent a perturbation of this joint distribution by a vector consisting of the first derivative of the individual probabilities $p_{0}\left(x_{1}, x_{2}, \ldots, x_{n}\right)$ for all values of $x_{1}, x_{2}, \ldots, x_{n}$. We however suggest the following perturbation that can be represented by a real valued random variable, $L$, jointly distributed by $X_{1}, X_{2}, \ldots, X_{n}$ and satisfying $\mathbb{E}[L]=0, \mid \mathbb{E}\left[L \mid X_{1}=x_{1}, X_{2}=\right.$ $\left.x_{2}, \ldots, X_{n}=x_{n}\right] \mid<\infty$ for all values of $x_{1}, x_{2}, \ldots, x_{n}$ :

$$
p_{\epsilon}\left(\widehat{X}_{1}=x_{1}, \ldots, \widehat{X}_{n}=x_{n}\right)=p_{0}\left(X_{1}=x_{1}, \ldots, X_{n}=x_{n}\right) \cdot\left(1+\epsilon \cdot \mathbb{E}\left[L \mid X_{1}=x_{1}, \ldots, X_{n}=x_{n}\right]\right),
$$

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

$$
p_{\epsilon}\left(\widehat{X}_{i \in I}=x_{i \in I}\right)=p_{0}\left(X_{i \in I}=x_{i \in I}\right) \cdot\left(1+\epsilon \cdot \mathbb{E}\left[L \mid X_{i \in I}=x_{i \in I}\right]\right) .
$$

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

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

Lemma 2 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 outer bound of Nair and El Gamal 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. Since the original submission of this paper, Nair, Wang and Geng [15] showed that the inequality $I(U ; Y)+I(V ; Z)-I(U ; V) \leq \max (I(X ; Y), I(X ; Z))$ holds for all binary input broadcast channels. The authors employ a generalized version of the perturbation method introduced in this paper that also allows for additive perturbations. The authors of [13] prove various results that help to restrict the search space for computing the sum-rate for Marton's inner bound.

The outline of this paper is as follows. In section II, we introduce the basic notation and definitions we use. Section III] contains the main results of the paper followed by section $\nabla$ which gives formal proofs for the results. Section IV describes the new ideas, and appendices complete the proof of theorems from section V

## II. Definitions and Notation

Let $\mathbb{R}$ denote the set of real numbers. All the logarithms throughout this paper are in base two, unless stated otherwise. Let $\mathcal{C}(q(y, z \mid x))$ denote the capacity region of the broadcast channel $q(y, z \mid x)$. We use $X_{1: k}$ to denote $\left(X_{1}, X_{2}, \ldots, X_{k}\right)$; similarly we use $Y_{1: k}$ and $Z_{1: k}$ to denote $\left(Y_{1}, Y_{2}, \ldots, Y_{k}\right)$ and $\left(Z_{1}, Z_{2}, \ldots, Z_{k}\right)$ 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: $\Delta(A)=\left\{\vec{v} \in \mathbb{R}^{d}: \vec{v} \leq \vec{w}\right.$ for some $\left.\vec{w} \in A\right\}$.

Definition 2: Let $\mathcal{C}_{M}(q(y, z \mid x))$ denote Marton's inner bound on the channel $q(y, z \mid x) . \mathcal{C}_{M}(q(y, z \mid x))$ is defined as the union over non-negative triples $\left(R_{0}, R_{1}, R_{2}\right)$ satisfying equations 1, 2, 3, and 4 over random

[^0]variables $U, V, W, X, Y, Z$, having the joint distribution $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$. Please note that the auxiliary random variables $U, V$ and $W$ may be discrete or continuous random variables.

Definition 3: The region $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$ is defined as the union of non-negative triples $\left(R_{0}, R_{1}, R_{2}\right)$ satisfying equations 1, 2, 3and 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 $p(u, v, w, x, y, z)=$ $p(u, v, w, x) q(y, z \mid x)$. Note that $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x)) \subset \mathcal{C}_{M}^{S_{u}^{\prime}, S_{v}^{\prime}, S_{w}^{\prime}}(q(y, z \mid x))$ whenever $S_{u} \leq S_{u}^{\prime}, S_{v} \leq S_{v}^{\prime}$ and $S_{w} \leq S_{w}^{\prime}$.

Definition 4: Let $\mathscr{L}(q(y, z \mid x))$ be equal to $\mathcal{C}_{M}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y, z \mid x))$.
Definition 5: The region $\mathscr{C}(q(y, z \mid x))$ 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 $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$ for which $H(X \mid U V W)=0$, of non-negative triples $\left(R_{0}, R_{1}, R_{2}\right)$ satisfying equations [1, 2, 3, and 4, Please note that the definition of $\mathscr{C}(q(y, z \mid x))$ differs from that of $\mathscr{L}(q(y, z \mid x))$ since we have imposed the extra constraint $H(X \mid U V W)=0$ on the auxiliaries. $\mathscr{C}(q(y, z \mid x))$ is a computable subset of the region $\mathcal{C}_{M}(q(y, z \mid x))$.

Definition 6: Given broadcast channel $q(y, z \mid x)$, let $\mathcal{C}_{N E}(q(y, z \mid x))$ denote the union over random variables $U, V, W, X, Y, Z$, having the joint distribution $p(u, v, w, x, y, z)=p(u) p(v) p(w \mid u, v) p(x \mid u, v, w) q(y, z \mid x)$, of

$$
\begin{aligned}
R_{0}, R_{1}, R_{2} & \geq 0 ; \\
R_{0} & \leq \min (I(W ; Y), I(W ; Z)) ; \\
R_{0}+R_{1} & \leq I(U W ; Y) ; \\
R_{0}+R_{2} & \leq I(V W ; Z) ; \\
R_{0}+R_{1}+R_{2} & \leq I(U W ; Y)+I(V ; Z \mid U W) ; \\
R_{0}+R_{1}+R_{2} & \leq I(V W ; Z)+I(U ; Y \mid V W) .
\end{aligned}
$$

$\mathcal{C}_{N E}(q(y, z \mid x))$ is shown in [11] to be an outer bound to the capacity region of the broadcast channel. This outer bound matches the best known outer bound discussed in [14] when $R_{0}=0$. An alternative characterization of the set of triples $\left(0, R_{1}, R_{2}\right)$ in $\mathcal{C}_{N E}(q(y, z \mid x))$ is as follows [12]: the union over
random variables $U, V, X, Y, Z$ having the joint distribution $p(u, v, x, y, z)=p(u, v, x) q(y, z \mid x)$, of

$$
\begin{aligned}
R_{1}, R_{2} & \geq 0 \\
R_{1} & \leq I(U ; Y) \\
R_{2} & \leq I(V ; Z) ; \\
R_{1}+R_{2} & \leq I(U ; Y)+I(V ; Z \mid U) ; \\
R_{1}+R_{2} & \leq I(V ; Z)+I(U ; Y \mid V) .
\end{aligned}
$$

## III. Statement of results

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

Corollary 1: $\mathcal{C}_{M}(q(y, z \mid x))$ is closed since $\mathscr{C}(q(y, z \mid x))$ is also a subset of $\mathcal{C}_{M}(q(y, z \mid x))$.
Theorem 2: There are broadcast channels for which Marton's inner bound and the recent outer bound of Nair and El Gamal do not match.

## IV. 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.

Given a broadcast channel $q(y, z \mid x)$ 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 $p(u v \mid x) p(x) q(y, z \mid x)$ where $\lambda$ and $\gamma$ 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 $\min \left(|\mathcal{X}|, S_{u}\right)$ and $\min \left(|\mathcal{X}|, S_{v}\right)$. It suffices to prove the following lemma:

Lemma 1: Given an arbitrary broadcast channel $q(y, z \mid x)$, an arbitrary input distribution $p(x)$, nonnegative reals $\lambda$ and $\gamma$, and natural numbers $S_{u}$ and $S_{v}$ where $S_{u}>|\mathcal{X}|$ the following holds:

$$
\begin{gathered}
\sup _{U V \rightarrow X \rightarrow Y Z ;|\mathcal{U}| \leq S_{u} ;|\mathcal{V}| \leq S_{v}} I(U ; Y)+I(V ; Z)-I(U ; V)+\lambda I(U ; Y)+\gamma I(V ; Z)= \\
I(\widehat{U} ; \widehat{Y})+I(\widehat{V} ; \widehat{Z})-I(\widehat{U} ; \widehat{V})+\lambda I(\widehat{U} ; \widehat{Y})+\gamma I(\widehat{V} ; \widehat{Z}),
\end{gathered}
$$

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 $|\widehat{\mathcal{U}}|<S_{u},|\widehat{\mathcal{V}}| \leq S_{v}$.

## A. Proof based on the perturbation method

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 $p_{0}(u, v, x, y, z)=p_{0}(u, v, x) q(y, z \mid x)$. 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 $\mathbb{E}[L(U, V, X) \mid X]=0$. 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

$$
\begin{gathered}
p_{\epsilon}(\widehat{U}=u, \widehat{V}=v, \widehat{X}=x, \widehat{Y}=y, \widehat{Z}=z)= \\
p_{0}(U=u, V=v, X=x, Y=y, Z=z) \cdot(1+\epsilon \cdot \mathbb{E}[L(U, V, X) \mid U=u, V=v, X=x, Y=y, Z=z]),
\end{gathered}
$$

or equivalently according to

$$
\begin{gathered}
p_{\epsilon}(\widehat{U}=u, \widehat{V}=v, \widehat{X}=x, \widehat{Y}=y, \widehat{Z}=z)= \\
p_{0}(U=u, V=v, X=x, Y=y, Z=z)(1+\epsilon \cdot L(u, v, x))= \\
p_{0}(U=u, V=v, X=x) q(Y=y, Z=z \mid X=x)(1+\epsilon \cdot L(u, v, x)) .
\end{gathered}
$$

The parameter $\epsilon$ is a real number that can take values in $\left[-\bar{\epsilon}_{1}, \bar{\epsilon}_{2}\right]$ where $\bar{\epsilon}_{1}$ and $\bar{\epsilon}_{2}$ are some positive reals representing the maximum and minimum values of $\epsilon$, i.e. $\min _{u, v, x} 1-\bar{\epsilon}_{1} \cdot L(u, v, x)=\min _{u, v, x} 1+$ $\bar{\epsilon}_{2} \cdot L(u, v, x)=0$. Since $L$ is a function of $U, V$ and $X$ only, for any value of $\epsilon$, the Markov chain $\widehat{U} \widehat{V} \rightarrow \widehat{X} \rightarrow \widehat{Y} \widehat{Z}$ holds, and $p(\widehat{Y}=y, \widehat{Z}=z \mid \widehat{X}=x)$ is equal to $q(Y=y, Z=z \mid X=x)$ for all $x, y, z$ where $p(X=x)>0$. Furthermore $\mathbb{E}[L(U, V, X) \mid X]=0$ implies that the marginal distribution of $X$ is preserved by this perturbation. This is because

$$
p_{\epsilon}(\widehat{X}=x)=p_{0}(X=x) \cdot(1+\epsilon \cdot \mathbb{E}[L(U, V, X) \mid X=x]) .
$$

[^1]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 $\epsilon$ achieves its maximum at $\epsilon=0$ (by our assumption). Therefore its first derivative at $\epsilon=0$ should be zero, and its second derivative should be less than or equal to zero. We use the following lemma to compute the first derivative and the second derivative of the above expression.

Lemma 2: Given any finite random variable $X$, and real valued random variable $L$ where $\mid \mathbb{E}[L \mid X=$ $x] \mid<\infty$ 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 $p_{\epsilon}(\widehat{X}=x)=p_{0}(X=x) \cdot(1+\epsilon \cdot \mathbb{E}[L \mid X=x])$, where $\epsilon$ is a real number in the interval $\left[-\bar{\epsilon}_{1}, \bar{\epsilon}_{2}\right]$. $\bar{\epsilon}_{1}$ and $\bar{\epsilon}_{2}$ are positive reals for which $\min _{x} 1-\bar{\epsilon}_{1} \cdot \mathbb{E}[L \mid X=x] \geq 0$ and $\min _{x} 1+\bar{\epsilon}_{2} \cdot \mathbb{E}[L \mid X=x] \geq 0$ hold. Then

1) $\left.H(\widehat{X})\right|_{\epsilon=0}=H(X)$, and $\left.\frac{\partial}{\partial \epsilon} H(\widehat{X})\right|_{\epsilon=0}=H_{L}(X)$ where $H_{L}(X)$ is defined as $H_{L}(X)=\sum_{x \in \mathcal{X}} p(X=$ $x) \mathbb{E}[L \mid X=x] \log \frac{1}{p(X=x)}$ for any finite random variable $X$ and real valued random variable $L$ where $|\mathbb{E}[L \mid X=x]|<\infty$ for all $x \in \mathcal{X}$.
2) $\forall \epsilon \in\left(-\bar{\epsilon}_{1}, \bar{\epsilon}_{2}\right), \frac{\partial^{2}}{\partial \epsilon^{2}} H(\widehat{X})=-\log e \cdot \mathbb{E}\left[\frac{\mathbb{E}[L \mid X]^{2}}{1+\epsilon \in \mathbb{E}[L \mid X]}\right]=-\log (e) \cdot I(\epsilon)$ where the Fisher Information $I(\epsilon)$ is defined as $I(\epsilon)=\sum_{x}\left(\frac{\partial}{\partial \epsilon} \log _{e}\left(p_{\epsilon}(\widehat{X}=x)\right)\right)^{2} p_{\epsilon}(\widehat{X}=x)$. In particular $\left.\frac{\partial^{2}}{\partial \epsilon^{2}} H(\widehat{X})\right|_{\epsilon=0}=$ $-\log e \cdot \mathbb{E}\left[\mathbb{E}[L \mid X]^{2}\right]$.
3) $H(\widehat{X})=H(X)+\epsilon H_{L}(X)-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid X])]$ where $r(x)=(1+x) \log (1+x)$.

Using the above lemma, one can compute the first derivative and set it to zero, and thereby get the following equation:

$$
\begin{equation*}
I_{L}(U ; Y)+I_{L}(V ; Z)-I_{L}(U ; V)+\lambda I_{L}(U ; Y)+\gamma I_{L}(V ; Z)=0, \tag{5}
\end{equation*}
$$

where $I_{L}(X ; Y)=H_{L}(X)-H_{L}(X \mid Y)=H_{L}(Y)-H_{L}(Y \mid X), H_{L}(X \mid Y)=\sum_{y \in \mathcal{Y}} p(Y=y) H_{L}(X \mid Y=$ $y)$, and $H_{L}(X \mid Y=y)=\sum_{x \in \mathcal{X}} p(X=x \mid Y=y) \mathbb{E}[L \mid X=x, Y=y] \log \frac{1}{p(X=x \mid Y=y)}$ for any finite random variables $X$ and $Y$ and real valued random variable $L$ where $|\mathbb{E}[L \mid X=x, Y=y]|<\infty$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.

In order to compute the second derivative, one can expand the expression through entropy terms and use Lemma 2 to compute the second derivative for each term. We can use the assumption that $\mathbb{E}[L(U, V, X) \mid X]=0$ (which implies $\mathbb{E}[L(U, V, X) \mid Y]=0$ and $\mathbb{E}[L(U, V, X) \mid Z]=0$ ) 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

[^2]of $I(\widehat{U} ; \widehat{Y})$ at $\epsilon=0$ will be equal to $-\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U]^{2}\right]+\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U Y]^{2}\right]$, the second derivative of $I(\widehat{V} ; \widehat{Z})$ at $\epsilon=0$ will be equal to $-\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid V]^{2}\right]+\log e$. $\mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid V Z]^{2}\right]$, and the second derivative of $-I(\widehat{U} ; \widehat{V})$ at $\epsilon=0$ will be equal to $+\log e$. $\mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U]^{2}\right]+\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid V]^{2}\right]-\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U V]^{2}\right]$. 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 $+\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U Y]^{2}\right]+\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid V Z]^{2}\right]-\log e \cdot \mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U V]^{2}\right]$. Hence we conclude that for any non-zero function $L: \mathcal{U} \times \mathcal{V} \times \mathcal{X} \rightarrow \mathbb{R}$ where $\mathbb{E}[L(U, V, X) \mid X]=0$ we must have:
\[

$$
\begin{equation*}
\mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U Y]^{2}\right]+\mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid V Z]^{2}\right]-\mathbb{E}\left[\mathbb{E}[L(U, V, X) \mid U V]^{2}\right] \leq 0 . \tag{6}
\end{equation*}
$$

\]

Next, take an arbitrary non-zero function $L^{\prime}: \mathcal{U} \rightarrow \mathbb{R}$ where $\mathbb{E}\left[L^{\prime}(U) \mid X\right]=0$. Since $|\mathcal{U}|=S_{u}>|\mathcal{X}|$, such a non-zero function $L^{\prime}$ exists. Note that the direction of perturbation $L^{\prime}$ being only a function of $U$ implies that

$$
\begin{gathered}
p_{\epsilon}(\widehat{U}=u, \widehat{V}=v, \widehat{X}=x, \widehat{Y}=y, \widehat{Z}=z)= \\
p_{\epsilon}(\widehat{U}=u) p_{0}(V=v, X=x, Y=y, Z=z \mid U=u)
\end{gathered}
$$

In other words, the perturbation only changes the marginal distribution of $U$, but preserves the conditional distribution of $p_{0}(V=v, X=x, Y=y, Z=z \mid U=u)$.

Note that

$$
\mathbb{E}\left[\mathbb{E}\left[L^{\prime}(U) \mid U V\right]^{2}\right]=\mathbb{E}\left[\mathbb{E}\left[L^{\prime}(U) \mid U Y\right]^{2}\right]=\mathbb{E}\left[L^{\prime}(U)^{2}\right] .
$$

This implies that $\mathbb{E}\left[\mathbb{E}\left[L^{\prime}(U) \mid V Z\right]^{2}\right]$ should be non-positive. But this can happen only when $\mathbb{E}\left[L^{\prime}(U) \mid V Z\right]=$ 0 . Therefore any arbitrary function $L^{\prime}: \mathcal{U} \rightarrow \mathbb{R}$ where $\mathbb{E}\left[L^{\prime}(U) \mid X\right]=0$ must also satisfy $\mathbb{E}\left[L^{\prime}(U) \mid V Z\right]=$ 0 . In other words, any arbitrary direction of perturbation $L^{\prime}$ that is a function of $U$ and preserves the marginal distribution of $X$, must also preserve the marginal distribution of $V Z, 4$

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

$$
{ }^{4} \text { Note that } p_{\epsilon}(\widehat{V}=v, \widehat{Z}=z)=p_{0}(V=v, Z=z) \cdot(1+\epsilon \cdot \mathbb{E}[L(U, V, X) \mid V=v, Z=z])=p_{0}(V=v, Z=z) .
$$

of $\epsilon$ is constant $5^{5}$ Using the last part of Lemma 2 one can write:

$$
\begin{gather*}
I(\widehat{U} ; \widehat{Y})=I(U ; Y)+\epsilon \cdot I_{L}(\widehat{U} ; \widehat{Y})-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid U])]-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid Y])]+\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid U Y])]= \\
 \tag{7}\\
I(U ; Y)+\epsilon \cdot I_{L}(\widehat{U} ; \widehat{Y})
\end{gather*}
$$

where $r(x)=(1+x) \log (1+x)$. Equation (7) holds because $\mathbb{E}[L \mid Y]=0$ and $\mathbb{E}[L \mid U]=\mathbb{E}[L \mid U Y]$. Similarly using the last part of Lemma 2, one can write:

$$
\begin{gather*}
I(\widehat{U} ; \widehat{V})=I(U ; V)+\epsilon \cdot I_{L}(\widehat{U} ; \widehat{V})-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid U])]-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid V])]+\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid U V])]= \\
 \tag{8}\\
I(U ; V)+\epsilon \cdot I_{L}(\widehat{U} ; \widehat{V})
\end{gather*}
$$

where $r(x)=(1+x) \log (1+x)$. Equation (8) holds because $\mathbb{E}[L \mid V]=0$ and $\mathbb{E}[L \mid U]=\mathbb{E}[L \mid U V]$. 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 $\epsilon$ is equal to

$$
\begin{gather*}
I(U ; Y)+I(V ; Z)-I(U ; V)+\lambda I(U ; Y)+\gamma I(V ; Z)+ \\
\epsilon \cdot\left(I_{L}(U ; Y)+I_{L}(V ; Z)-I_{L}(U ; V)+\lambda I_{L}(U ; Y)+\gamma I_{L}(V ; Z)\right) \tag{9}
\end{gather*}
$$

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 $\epsilon$ is constant. Since the function $L^{\prime}$ is non-zero, setting $\epsilon=-\bar{\epsilon}_{1}$ or $\epsilon=\bar{\epsilon}_{2}$ 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:

$$
p_{\epsilon}(\widehat{U}=u)=p_{0}(U=u) \cdot\left(1+\epsilon L^{\prime}(u)\right) .
$$

This perturbation does not increase the support and would decrease it by at least one when $\epsilon$ is at its maximum or minimum, i.e. when $\epsilon=-\bar{\epsilon}_{1}$ or $\epsilon=\bar{\epsilon}_{2}$. 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.

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 $p_{0}(u, v, x, y, z)=p_{0}(u, v, x) q(y, z \mid x)$, equations 5 and 6 must hold for any non-zero function $L: \mathcal{U} \times \mathcal{V} \times \mathcal{X} \rightarrow \mathbb{R}$ where $\mathbb{E}[L(U, V, X) \mid X]=0$. The proof used these properties to a limited extent.

[^3]
## B. Alternative proof

In this subsection we provide an alternative proof for Lemma Assume that 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 $p_{0}(u, v, x, y, z)=$ $p_{0}(u, v, x) q(y, z \mid x)$. Without loss of generality we can assume that $p(u)>0$ for all $u \in \mathcal{U}$. Let us fix $p_{0}(v, x \mid u) q(y, z \mid x)$ and vary the marginal distribution of $U$ in such a way that the marginal distribution of $X$ is preserved. In other words, we consider the set of p.m.f's $q(u)$ satisfying $\sum_{u, v} q(u) p_{0}(v, x \mid u)=p_{0}(x)$ for all $x \in \mathcal{X}$. We can then view the expression $I(U ; Y)+I(V ; Z)-I(U ; V)+\lambda I(U ; Y)+\gamma I(V ; Z)$ as a function of a p.m.f $q(u)$ defined on $\mathcal{U}$. Here $U, V, X, Y, Z$ are jointly distributed as $q(u) p_{0}(v, x \mid u) q(y, z \mid x)$. We claim that $I(U ; Y)+I(V ; Z)-I(U ; V)+\lambda I(U ; Y)+\gamma I(V ; Z)$ is convex function over $q(u)$. To see this note that $I(U ; Y)+I(V ; Z)-I(U ; V)=H(Y)-H(Y \mid U)-H(V \mid Z)+H(V \mid U)$. Since the marginal distribution of $X$ is preserved, $H(Y)$ is fixed. The term $-H(Y \mid U)+H(V \mid U)$ is linear in $q(u)$, and $-H(V \mid Z)$ is convex in $q(u)$. Therefore $I(U ; Y)+I(V ; Z)-I(U ; V)$ is a convex function over $q(u)$. Next, note that $\lambda I(U ; Y)=\lambda H(Y)-\lambda H(Y \mid U)$ is linear in $q(u)$, and $\gamma I(V ; Z)=\gamma H(Z)-\gamma H(Z \mid V)$ is convex in $q(u)$. The latter is because the marginal distribution of $X$ is preserved and hence $H(Z)$ is fixed. All in all, we can conclude that $I(U ; Y)+I(V ; Z)-I(U ; V)+\lambda I(U ; Y)+\gamma I(V ; Z)$ is convex in $q(u)$. This implies that it will have a maximum at the extreme points of the domain. We claim that any extreme point of the domain corresponds to a p.m.f $q(u)$ with support at most $|\mathcal{X}|$. This completes the proof. The domain of the function is the polytope formed by the set of vectors $(q(u): u \in \mathcal{U})$ satisfying the following constraints

$$
\begin{aligned}
& q(u) \geq 0, \quad \forall u \in \mathcal{U} \\
& \sum_{u \in \mathcal{U}} q(u)=1 \\
& \sum_{u, v} q(u) p_{0}(v, x \mid u)=p_{0}(x), \quad \forall x \in \mathcal{X}
\end{aligned}
$$

Note that the equation $\sum_{u \in \mathcal{U}} q(u)=1$ is redundant and implied by the others because $1=\sum_{x} p_{0}(x)=$ $\sum_{x} \sum_{u, v} q(u) p_{0}(v, x \mid u)=\sum_{u} \sum_{v, x} q(u) p_{0}(v, x \mid u)=\sum_{u} q(u)$. Thus, we can describe the domain of the function by

$$
\begin{aligned}
& q(u) \geq 0, \quad \forall u \in \mathcal{U} \\
& \sum_{u, v} q(u) p_{0}(v, x \mid u)=p_{0}(x), \quad \forall x \in \mathcal{X}
\end{aligned}
$$

Any extreme point of this polytope must lie on at least $|\mathcal{U}|$ hyperplanes because the polytope lies in $\mathbb{R}^{|\mathcal{U}|}$. Because there are $|\mathcal{X}|$ equations of the type $\sum_{u, v} q(u) p_{0}(v, x \mid u)=p_{0}(x)$, any extreme point has to pick
up at least $|\mathcal{U}|-|\mathcal{X}|$ equation of the type $q(u) \geq 0$. This implies that $q(u)=0$ for at least $|\mathcal{U}|-|\mathcal{X}|$ different values of $u \in \mathcal{U}$. Therefore the support of any extreme point must be less than or equal to $|\mathcal{U}|-(|\mathcal{U}|-|\mathcal{X}|)=|\mathcal{X}|$.

## V. Proofs

Proof of Theorem [7. We begin by showing that for any natural numbers $S_{u}, S_{v}, S_{w}$, one has $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x)) \subset \mathcal{C}_{M}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y, z \mid x))=\mathscr{L}(q(y, z \mid x))$. This is proved in two steps:

1) $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x)) \subset \mathcal{C}_{M}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x))$.
2) $\mathcal{C}_{M}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x)) \subset \mathcal{C}_{M}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y, z \mid x))$.

The first step that imposes a cardinality bound on the alphabet set of $W$ follows just from a standard application of the strengthened Carathéodory theorem of Fenchel and is left to the reader. The difficult part is the second step. To show this it suffices to prove more generally that

$$
\begin{equation*}
\mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x)) \subset \mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y, z \mid x)) \tag{10}
\end{equation*}
$$

where $\mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}$ is defined as the union of real four tuples ( $R_{1}^{\prime}, R_{2}^{\prime}, R_{3}^{\prime}, R_{4}^{\prime}$ ) satisfying

$$
\begin{align*}
& R_{1}^{\prime} \leq \min (I(W ; Y), I(W ; Z)) ;  \tag{11}\\
& R_{2}^{\prime} \leq I(U W ; Y) ;  \tag{12}\\
& R_{3}^{\prime} \leq I(V W ; Z) ;  \tag{13}\\
& R_{4}^{\prime} \leq I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W) \\
&+\min (I(W ; Y), I(W ; Z)) . \tag{14}
\end{align*}
$$

over auxiliary random variables satisfying the cardinality bounds $|\mathcal{U}| \leq S_{u},|\mathcal{V}| \leq S_{v}$ and $|\mathcal{W}| \leq S_{w}$. Note that the region $\mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}$ specifies $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}$, since given any $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$ the corresponding vector in $\mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}$ is providing the values for the right hand side of the 4 inequalities that define the region $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}$. Also note that $\mathcal{C}_{M-I}(q(y, z \mid x))$ is defined as a subset of $\mathbb{R}^{4}$, and not $\mathbb{R}_{+}^{4}$.

It is proved in Appendix A that $\mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x))$ is convex and closed for any $S_{u}$ and $S_{v}$. Thus, to prove equation (10) it suffices to show that for any real $\lambda_{1}, \lambda_{2}, \lambda_{3}, \lambda_{4}$,

$$
\max _{\left(R_{1}^{\prime}, R_{2}^{\prime}, R_{3}^{\prime}, R_{4}^{\prime}\right) \in \mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}} \sum_{i=1: 4} \lambda_{i} R_{i}^{\prime} \leq \max _{\left(R_{1}^{\prime}, R_{2}^{\prime}, R_{3}^{\prime}, R_{4}^{\prime}\right) \in \mathcal{C}_{M-I}^{|x|,|x|,|\mathcal{X}|+4}} \sum_{i=1: 4} \lambda_{i} R_{i}^{\prime} .
$$

It suffices to prove this for the case of $\lambda_{i} \geq 0$ for $i=1: 4$, since if $\lambda_{i}$ is negative for some $i, R_{i}^{\prime}$ can be made to converge to $-\infty$ causing $\sum_{i=1}^{4} \lambda_{i} R_{i}^{\prime}$ to converge to $\infty$ on both sides.

Take a point $\left(R_{1}^{\prime}, R_{2}^{\prime}, R_{3}^{\prime}, R_{4}^{\prime}\right) \in \mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}$ that maximizes $\sum_{i=1: 4} \lambda_{i} R_{i}^{\prime}$. Corresponding to the point is a joint distribution $p(u, v, w, x)$ where $|U| \leq S_{u},|V| \leq S_{v}$ and $|W| \leq|\mathcal{X}|+4$ and

$$
\begin{aligned}
\sum_{i=1: 4} \lambda_{i} R_{i}^{\prime}= & \lambda_{1} \min (I(W ; Y), I(W ; Z))+\lambda_{2} I(U W ; Y)+\lambda_{3} I(V W ; Z) \\
& +\lambda_{4}(\min (I(W ; Y), I(W ; Z))+I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)) .
\end{aligned}
$$

Let us fix $p(w, x)$. We would like to define $p(\widehat{u}, \widehat{v} \mid w, x)$ such that $|\widehat{U}| \leq|X|,|\widehat{V}| \leq|X|$ achieving the same or larger weighted sum. Because we have fixed $p(w, x)$, the terms $I(W ; Y)$ and $I(W ; Z)$ are fixed. Since $I(U W ; Y)=I(W ; Y)+\sum_{w} p(w) I(U ; Y \mid W=w), I(V W ; Z)=I(W ; Z)+\sum_{w} p(w) I(V ; Z \mid W=$ $w)$ and $I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)=\sum_{w} p(w)[I(U ; Y \mid W=w)+I(V ; Z \mid W=w)-$ $I(U ; V \mid W=w)]$, we can construct $p(\widehat{u}, \widehat{v}, x \mid w)$ for each $w$ individually. In other words, given the marginal distribution $p(x \mid w)$, we would like to construct $p(\widehat{u}, \widehat{v}, x \mid w)$ such that
$\lambda_{2} I(U ; Y \mid W=w)+\lambda_{3} I(V ; Z \mid W=w)+\lambda_{4}(I(U ; Y \mid W=w)+I(V ; Z \mid W=w)-I(U ; V \mid W=w)) \leq$ $\lambda_{2} I(\widehat{U} ; Y \mid W=w)+\lambda_{3} I(\widehat{V} ; Z \mid W=w)+\lambda_{4}(I(\widehat{U} ; Y \mid W=w)+I(\widehat{V} ; Z \mid W=w)-I(\widehat{U} ; \widehat{V} \mid W=w))$.

When $\lambda_{4}>0$, after a normalization we get the problem studied in section IV When $\lambda_{4}=0$, clearly $\widehat{U}=\widehat{V}=X$ works. This completes the proof. Thus, we have proved that for any arbitrary natural numbers $S_{u}, S_{v}, S_{w}$, one has $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x)) \subset \mathcal{C}_{M}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y, z \mid x))=\mathscr{L}(q(y, z \mid x))$.

We now complete the proof of the theorem. In Appendices B and C we prove that the closure of $\mathcal{C}_{M}(q(y, z \mid x))$ is equal to the closure of $\bigcup_{S_{u}, S_{v}, S_{w} \geq 0} \mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$, and that $\mathscr{C}(q(y, z \mid x))$ is equal to $\mathscr{L}(q(y, z \mid x))$. Using the result that $\mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x)) \subset \mathcal{C}_{M}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y, z \mid x))=\mathscr{L}(q(y, z \mid x))$, we get that the closure of $\mathcal{C}_{M}(q(y, z \mid x))$ is equal to the closure of $\mathscr{L}(q(y, z \mid x))$. Lastly note that $\mathscr{L}(q(y, z \mid x))$ is closed because of the cardinality constraints on its auxiliary random variables ${ }_{6}^{6}$

Proof of Theorem 2: We construct a broadcast channel with binary input alphabet for which Marton's inner bound and the recent outer bound of Nair and El Gamal do not match.

We begin by proving that for any arbitrary binary input broadcast channel $q(y, z \mid x)$ such that for all $y \in \mathcal{Y}$ and $z \in \mathcal{Z}, q(Y=y \mid X=0), q(Y=y \mid X=1), q(Z=z \mid X=0)$ and $q(Z=z \mid X=1)$ are non-zero, the following holds:

[^4]Lemma: If $\mathcal{C}_{M}(q(y, z \mid x))=\mathcal{C}_{N E}(q(y, z \mid x))$, the maximum sum rate $R_{1}+R_{2}$ over triples $\left(R_{0}, R_{1}, R_{2}\right)$ in Marton's inner bound is equal to

$$
\begin{gather*}
\max \left(\min _{\gamma \in[0,1]}\left(\max _{\substack{p(w x) q(y, z \mid x) \\
|\mathcal{W}|=2}} \gamma I(W ; Y)+(1-\gamma) I(W ; Z)+\sum_{w} p(w) T(p(X=1 \mid W=w))\right),\right. \\
\max \begin{array}{l}
p(u, v) p(x \mid u v) q(y, z \mid x) \\
|\mathcal{U}|=|\mathcal{V}|=2, I(U ; V)=0, H(X \mid U V)=0
\end{array}  \tag{15}\\
I(U ; Y)+I(V ; Z))
\end{gather*}
$$

where $T(p)=\max \{I(X ; Y), I(X ; Z) \mid P(X=1)=p\}$.
Before proceeding to prove the above lemma, note that if the expression of equation 15 turns out to be strictly less than the maximum of the sum rate $R_{1}+R_{2}$ over triples $\left(R_{0}, R_{1}, R_{2}\right)$ in $\mathcal{C}_{N E}(q(y, z \mid x))$ (which is given in [12]), it will serve as an evidence for $\mathcal{C}_{M}(q(y, z \mid x)) \neq \mathcal{C}_{N E}(q(y, z \mid x))$. The maximum of the sum rate $R_{1}+R_{2}$ over triples $\left(R_{0}, R_{1}, R_{2}\right)$ in $\mathcal{C}_{N E}(q(y, z \mid x))$ is known to be [12]

$$
\max _{p(u, v, x) q(y, z \mid x)} \min (I(U ; Y)+I(V ; Z), I(U ; Y)+I(V ; Z \mid U), I(V ; Z)+I(U ; Y \mid V)),
$$

which can be written as (see Bound 4 in [12])

$$
\begin{aligned}
& \max _{p(u, v, x) q(y, z \mid x)} \min (I(U ; Y)+I(V ; Z), I(U ; Y)+I(X ; Z \mid U), I(V ; Z)+I(X ; Y \mid V)) . \\
& |\mathcal{U}|=|\mathcal{V}|=3, I(U ; V \mid X)=0
\end{aligned}
$$

The constraint $I(U ; V \mid X)=0$ is imposed because the outer bound depends only on the marginals $p(u, x)$ and $p(v, x)$. There are examples for which the expression of equation 15 turns out to be strictly less than the maximum of the sum rate $R_{1}+R_{2}$ over triples $\left(R_{0}, R_{1}, R_{2}\right)$ in $\mathcal{C}_{N E}(q(y, z \mid x))$. For instance given any two positive reals $\alpha$ and $\beta$ in the interval $(0,1)$, consider the broadcast channel for which $|\mathcal{X}|=|\mathcal{Y}|=|\mathcal{Z}|=2, p(Y=0 \mid X=0)=\alpha, p(Y=0 \mid X=1)=\beta, p(Z=0 \mid X=0)=1-\beta, p(Z=$ $0 \mid X=1)=1-\alpha$. Assuming $\alpha=0.01$, Figure 1 plots maximum of the sum rate for $C_{N E}(q(y, z \mid x))$, and maximum of the sum rate for $C_{M}(q(y, z \mid x))$ (assuming that $C_{N E}(q(y, z \mid x))=C_{M}(q(y, z \mid x))$ ) as a function of $\beta$. 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.

Proof of the lemma: The maximum of the sum rate $R_{1}+R_{2}$ over triples $\left(R_{0}, R_{1}, R_{2}\right)$ in $\mathcal{C}_{M}(q(y, z \mid x))$ is equal to

$$
\begin{align*}
& \max _{p(u, v, w, x) q(y, z \mid x)} I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+\min (I(W ; Y), I(W ; Z)) .  \tag{16}\\
& |\mathcal{U}|=2,|\mathcal{V}|=2 \\
& H(X \mid U V W)=0
\end{align*}
$$



Fig. 1. Red curve (top curve): sum rate for $C_{N E}(q(y, z \mid x))$; Blue curve (bottom curve): sum rate for $C_{M}(q(y, z \mid x))$ assuming that $C_{N E}(q(y, z \mid x))=C_{M}(q(y, z \mid x))$.

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

$$
\begin{gather*}
\max \left(\max _{p(w x) q(y, z \mid x)} \min (I(W ; Y), I(W ; Z))+\sum_{w} p(w) T(p(X=1 \mid W=w)),\right.  \tag{17}\\
\left.\max _{\substack{ \\
p(u, v) p(x \mid u v) q(y, z \mid x) \\
|\mathcal{U}|=|\mathcal{V}|=2, I(U ; V)=0, H(X \mid U V)=0}} I(U ; Y)+I(V ; Z)\right) .
\end{gather*}
$$

Next, we show that the expression of equation 17 is equal to the the expression given in the lemma.
The expression of equation 16 is greater than or equal to the expression of equation 177 For the first part of the proof we thus need to prove that the expression of equation 16 is less than or equal to the expression of equation 17 Take the joint distribution $p(u, v, w, x)$ that maximizes the expression of equation 16, Let $\widetilde{U}=(U, W)$ and $\widetilde{V}=(V, W)$. The maximum of the sum rate $R_{1}+R_{2}$ over
${ }^{7}$ Consider the following special cases: 1) given $W=w$, let $(U, V)=(X$, constant $)$ if $I(X ; Y \mid W=w) \geq I(X ; Z \mid W=w)$, and $(U, V)=($ constant,$X)$ otherwise. This would produce the first part of the expression given in the lemma. 2) Assume that $W$ is constant, and $U$ is independent of $V$. This would produce the second part of the expression given in the lemma.
triples $\left(R_{0}, R_{1}, R_{2}\right)$ in $\mathcal{C}_{N E}(q(y, z \mid x))$ is greater than or equal to $\min (I(\widetilde{U} ; Y)+I(\widetilde{V} ; Z), I(\widetilde{U} ; Y)+$ $I(\widetilde{V} ; Z \mid \widetilde{U}), I(\widetilde{V} ; Z)+I(\widetilde{U} ; Y \mid \widetilde{V}))$ (see Bound 3 in [12|]). Since $\mathcal{C}_{N E}(q(y, z \mid x))=\mathcal{C}_{M}(q(y, z \mid x))$, we must have:

$$
\begin{gathered}
\min (I(U W ; Y)+I(V W ; Z), I(U W ; Y)+I(V W ; Z \mid U W), I(U W ; Z)+I(U W ; Y \mid V W)) \leq \\
I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+\min (I(W ; Y), I(W ; Z))
\end{gathered}
$$

Or alternatively

$$
\begin{gathered}
\min (\max (I(W ; Y), I(W ; Z))+I(U ; V \mid W), \\
I(W ; Y)-\min (I(W ; Y), I(W ; Z))+I(U ; V \mid W Z), \\
I(W ; Z)-\min (I(W ; Y), I(W ; Z))+I(U ; V \mid W Y)) \leq 0 .
\end{gathered}
$$

Since each expression is also greater than or equal to zero, 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 $I(U ; V \mid W)=0$,
2) $I(U ; V \mid W Y)=0$,
3) $I(U ; V \mid W Z)=0$.

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

$$
\begin{array}{ll}
\max & I(U ; Y)+I(V ; Z) \\
p(u, v) p(x \mid u v) q(y, z \mid x) & \\
|\mathcal{U}|=|\mathcal{V}|=2, I(U ; V)=0, H(X \mid U V)=0 &
\end{array}
$$

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

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

DRAFT

This completes the first part of the proof.
Next, we would like to show that the expression of equation 17 is equal to the the expression given in the lemma. In order to show this, note that (see Observation 1 of [13])

$$
\begin{equation*}
\max _{p(w, x) q(y, z \mid x)} \min (I(W ; Y), I(W ; Z))+\sum_{w} p(w) T(p(X=1 \mid W=w)) \tag{18}
\end{equation*}
$$

is equal to

$$
\begin{equation*}
\min _{\gamma \in[0,1]}\left(\max _{\substack{p(w x) q(y, z \mid x) \\|\mathcal{W}|=2}} \gamma I(W ; Y)+(1-\gamma) I(W ; Z)+\sum_{w} p(w) T(p(X=1 \mid W=w))\right) \tag{19}
\end{equation*}
$$

The expression given in equation 18 can be written as

$$
\max _{p(w, x) q(y, z \mid x)} \min \left(I(W ; Y)+\sum_{w} p(w) T(p(X=1 \mid W=w)), I(W ; Z)+\sum_{w} p(w) T(p(X=1 \mid W=w))\right) .
$$

This expression can be rewritten as

$$
\min _{\gamma \in[0,1]}\left(\max _{p(w x) q(y, z \mid x)} \gamma I(W ; Y)+(1-\gamma) I(W ; Z)+\sum_{w} p(w) T(p(X=1 \mid W=w))\right) .
$$

It remains to prove the cardinality bound of two on $W$. This is done using the strengthened Carathéodory theorem of Fenchel. Take an arbitrary $p(w, x) q(y, z \mid x)$. The vector $w \rightarrow p(W=w)$ belongs to the set of vectors $w \rightarrow p(\widetilde{W}=w)$ satisfying the constraints $\sum_{w} p(\widetilde{W}=w)=1, p(\widetilde{W}=w) \geq 0$ and $p(X=1)=\sum_{w} p(X=1 \mid W=w) p(\widetilde{W}=w)$. The first two constraints ensure that $w \rightarrow p(\widetilde{W}=w)$ corresponds to a probability distribution, and the third constraint ensures that one can define a random variable $\widetilde{W}$, jointly distributed with $X, Y$ and $Z$ according to $p(\widetilde{w}, x) q(y, z \mid x)$ and further satisfying $p(X=x \mid \widetilde{W}=w)=p(X=x \mid W=w)$. Since $w \rightarrow p(W=w)$ belongs to the above set, it can be written as the convex combination of some of the extreme points of this set. The expression $\sum_{w}[-(1-\gamma) H(Z \mid W=w)-\gamma H(Y \mid W=w)+T(p(X=1 \mid W=w))] p(\widetilde{W}=w)$ is linear in $p(\widetilde{W}=w)$, therefore this expression for $w \rightarrow p(W=w)$ 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 $w \rightarrow p(\widetilde{W}=w)$ satisfying the constraints $\sum_{w} p(\widetilde{W}=w)=1, p(\widetilde{W}=w) \geq 0$ and $p(X=1)=\sum_{w} p(X=1 \mid W=w) p(\widetilde{W}=w)$ 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. The equation $H(\widehat{X})=H(X)+\epsilon H_{L}(X)-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid X])]$ where $r(x)=$


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 $\frac{\partial^{2}}{\partial x^{2}} r(x)=\frac{\log (e)}{1+x}>0$.
$(1+x) \log (1+x)$ is true because:

$$
\begin{gathered}
H(\widehat{X})=-\sum_{\widehat{x}} p_{\epsilon}(\widehat{x}) \log p_{\epsilon}(\widehat{x}) \\
=-\sum_{\widehat{x}} p_{0}(\widehat{x})(1+\epsilon \cdot \mathbb{E}[L \mid X=\widehat{x}]) \cdot \log \left(p_{0}(\widehat{x}) \cdot(1+\epsilon \cdot \mathbb{E}[L \mid X=\widehat{x}])\right) \\
=-\sum_{\widehat{x}} p_{0}(\widehat{x})(1+\epsilon \cdot \mathbb{E}[L \mid X=\widehat{x}]) \cdot\left[\log \left(p_{0}(\widehat{x})\right)+\log (1+\epsilon \cdot \mathbb{E}[L \mid X=\widehat{x}])\right] \\
=H(X)-\epsilon \sum_{\widehat{x}} p_{0}(\widehat{x}) \mathbb{E}[L \mid X=\widehat{x}] \log \left(p_{0}(\widehat{x})\right)- \\
\sum_{\widehat{x}} p_{0}(\widehat{x})(1+\epsilon \cdot \mathbb{E}[L \mid X=\widehat{x}]) \cdot \log (1+\epsilon \cdot \mathbb{E}[L \mid X=\widehat{x}]) \\
=H(X)+\epsilon H_{L}(X)-\mathbb{E}[r(\epsilon \cdot \mathbb{E}[L \mid X])]
\end{gathered}
$$

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:
$\frac{\partial}{\partial \epsilon} H(\widehat{X})=H_{L}(X)-\mathbb{E}[\mathbb{E}[L \mid X]\{\log (1+\epsilon \cdot \mathbb{E}[L \mid X])+\log e\}]=H_{L}(X)-\mathbb{E}[\mathbb{E}[L \mid X] \log (1+\epsilon \cdot \mathbb{E}[L \mid X])]$,
where at $\epsilon=0$ is equal to $H_{L}(X)$.
Next, we have:

$$
\begin{gathered}
\frac{\partial^{2}}{\partial \epsilon^{2}} H(\widehat{X})=-\frac{\partial}{\partial \epsilon} \mathbb{E}[\mathbb{E}[L \mid X] \log (1+\epsilon \cdot \mathbb{E}[L \mid X])] \\
-\mathbb{E}\left[\mathbb{E}[L \mid X] \frac{\mathbb{E}[L \mid X]}{1+\epsilon \cdot \mathbb{E}[L \mid X]} \log e\right]=-\log e \cdot \mathbb{E}\left[\frac{\mathbb{E}[L \mid X]^{2}}{1+\epsilon \cdot \mathbb{E}[L \mid X]}\right]
\end{gathered}
$$

DRAFT

On the other hand,

$$
\begin{gathered}
I(\epsilon)=\sum_{x}\left(\frac{\partial}{\partial \epsilon} \log _{e}\left(p_{\epsilon}(\widehat{X}=x)\right)\right)^{2} p_{\epsilon}(\widehat{X}=x)= \\
\sum_{x}\left(\frac{\partial}{\partial \epsilon} \log _{e}\left(p_{0}(X=x) \cdot(1+\epsilon \cdot \mathbb{E}[L \mid X=x])\right)\right)^{2} p_{0}(X=x) \cdot(1+\epsilon \cdot \mathbb{E}[L \mid X=x])= \\
\sum_{x}\left(\frac{\partial}{\partial \epsilon} \log _{e}(1+\epsilon \cdot \mathbb{E}[L \mid X=x])\right)^{2} p_{0}(X=x) \cdot(1+\epsilon \cdot \mathbb{E}[L \mid X=x])= \\
\sum_{x}\left(\frac{\mathbb{E}[L \mid X=x]}{1+\epsilon \cdot \mathbb{E}[L \mid X=x]}\right)^{2} p_{0}(X=x) \cdot(1+\epsilon \cdot \mathbb{E}[L \mid X=x])= \\
\sum_{x} \frac{\mathbb{E}[L \mid X=x]^{2}}{1+\epsilon \cdot \mathbb{E}[L \mid X=x]} p_{0}(X=x)=\mathbb{E}\left[\frac{\mathbb{E}[L \mid X]^{2}}{1+\epsilon \cdot \mathbb{E}[L \mid X]}\right]
\end{gathered}
$$

## Appendix A

In this appendix we show that $\mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x))$ is convex and closed for any $S_{u}$ and $S_{v}$. We begin by proving that the region $\mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}$ is closed. Since the ranges of all the involved 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 $I(U V W ; Y Z \mid X)=0$ and $p(y, z \mid x)=q(y, z \mid x)$ will be a compact set (when viewed as a subset of the ambient 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 $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$, of the region defined by equations 11,14 is compact, and thus closed.

Next we prove that $\mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x))$ is convex. Since $\mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$ is a subset of $\mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x))$ as mentioned in step 1 in the proof of Theorem 11 it suffices to show that $\bigcup_{S_{w} \geq 0} \mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$ is convex. Take two arbitrary points $\left(R_{1}, R_{2}, \ldots, R_{4}\right)$ and $\left(\widetilde{R_{1}}, \widetilde{R_{2}}, \ldots, \widetilde{R_{4}}\right)$ in $\bigcup_{S_{w} \geq 0} \mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$. Corresponding to $\left(R_{1}, \ldots, R_{4}\right)$ and $\left(\widetilde{R_{1}}, \ldots, \widetilde{R_{4}}\right)$ are joint distributions $p_{0}(u, v, w, x, y, z)=p_{0}(u, v, w, x) q(y, z \mid x)$ on $U, V, W, X, Y, Z$, and $p_{0}(\widetilde{u}, \widetilde{v}, \widetilde{w}, \widetilde{x}, \widetilde{y}, \widetilde{z})=p_{0}(\widetilde{u}, \widetilde{v}, \widetilde{w}, \widetilde{x}) q(\widetilde{y}, \widetilde{z} \mid \widetilde{x})$ 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: $R_{1} \leq \min (I(W ; Y), I(W ; Z))$, $R_{2} \leq I(U W ; Y), \ldots, \widetilde{R_{1}} \leq \min (I(\widetilde{W} ; \widetilde{Y}), I(\widetilde{W} ; \widetilde{Z})), \widetilde{R_{2}} \leq I(\widetilde{U} \widetilde{W} ; \widetilde{Y}), \ldots$ etc.

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 $(U, V, W Q, X, Y, Z)$ 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 $p(\widehat{Y}=y, \widehat{Z}=z \mid \widehat{X}=x)=q(\widehat{Y}=y, \widehat{Z}=$
$z \mid \widehat{X}=x), I(\widehat{U} \widehat{V} \widehat{W} ; \widehat{Y} \widehat{Z} \mid \widehat{X})=0$, and furthermore

$$
\begin{gathered}
I(\widehat{W} ; \widehat{Y}) \geq \frac{1}{2} I(W ; Y)+\frac{1}{2} I(\widetilde{W} ; \widetilde{Y}) \\
I(\widehat{W} ; \widehat{Z}) \geq \frac{1}{2} I(W ; Z)+\frac{1}{2} I(\widetilde{W} ; \widetilde{Z}) \\
I(\widehat{U} \widehat{W} ; \widehat{Y}) \geq \frac{1}{2} I(U W ; Y)+\frac{1}{2} I(\widetilde{U} \widetilde{W} ; \widetilde{Y})
\end{gathered}
$$

Hence $\left(\frac{1}{2} R_{1}+\frac{1}{2} \widetilde{R_{1}}, \frac{1}{2} R_{2}+\frac{1}{2} \widetilde{R_{2}}, \ldots, \frac{1}{2} R_{4}+\frac{1}{2} \widetilde{R_{4}}\right)$ belongs to $\bigcup_{S_{w} \geq 0} \mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$. Thus $\bigcup_{S_{w} \geq 0} \mathcal{C}_{M-I}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))=\mathcal{C}_{M-I}^{S_{u}, S_{v},|\mathcal{X}|+4}(q(y, z \mid x))$ is convex.

## Appendix B

In this appendix, we prove that the closure of $\mathcal{C}_{M}(q(y, z \mid x))$ is equal to the closure of $\bigcup_{S_{u}, S_{v}, S_{w} \geq 0} \mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$. In order to show this it suffices to show that any triple $\left(R_{0}, R_{1}, R_{2}\right)$ in $\mathcal{C}_{M}(q(y, z \mid x))$ is a limit point of $\bigcup_{S_{u}, S_{v}, S_{w} \geq 0} \mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$. Since $\left(R_{0}, R_{1}, R_{2}\right)$ is in $\mathcal{C}_{M}(q(y, z \mid x))$, 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 $\{1,2,3, \ldots\}$. For any integer $m$, let $U_{m}, V_{m}$ and $W_{m}$ be truncated versions of $U, V$ and $W$ defined on $\{1,2,3, \ldots, m\}$ as follows: $U_{m}, V_{m}$ and $W_{m}$ are jointly distributed according to $p\left(U_{m}=u, V_{m}=v, W_{m}=w\right)=\frac{p(U=u, V=v, W=w)}{p(U \leq m, V \leq m, W \leq m)}$ 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 $p\left(Y_{m}=y, Z_{m}=z, X_{m}=x \mid U_{m}=u, V_{m}=v, W_{m}=w\right)=p(Y=y, Z=z, X=x \mid U=$ $u, V=v, W=w)$ 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 $m \rightarrow \infty$. Therefore the mutual information terms $I\left(W_{m} ; Y_{m}\right), I\left(W_{m} ; Z_{m}\right), I\left(W_{m} U_{m} ; Y_{m}\right), \ldots$ (that define a region in $\left.\mathcal{C}_{M}^{m, m, m}(q(y, z \mid x))\right)$ converge to the corresponding terms $I(W ; Y), I(W ; Z), I(W U ; Y), \ldots$ Therefore $\left(R_{0}, R_{1}, R_{2}\right)$ is a limit point of $\bigcup_{S_{u}, S_{v}, S_{w} \geq 0} \mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$.

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 $\bigcup_{S_{u}, S_{v}, S_{w} \geq 0} \mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$. 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 $I\left(W_{q} ; Y_{q}\right), I\left(W_{q} ; Z_{q}\right), I\left(W_{q} U_{q} ; Y_{q}\right)$, ... (that define a region in $\mathcal{C}_{M}(q(y, z \mid x))$ ) converge to the corresponding terms $I(W ; Y), I(W ; Z), I(W U ; Y), \ldots$. Therefore $\left(R_{0}, R_{1}, R_{2}\right)$ is a limit point of $\bigcup_{S_{u}, S_{v}, S_{w} \geq 0} \mathcal{C}_{M}^{S_{u}, S_{v}, S_{w}}(q(y, z \mid x))$.

## Appendix C

In this appendix, we prove that $\mathscr{C}(q(y, z \mid x))$ is equal to $\mathscr{L}(q(y, z \mid x))$. Clearly $\mathscr{C}(q(y, z \mid x)) \subset \mathscr{L}(q(y, z \mid x))$. Therefore we need to show that $\mathscr{L}(q(y, z \mid x)) \subset \mathscr{C}(q(y, z \mid x))$.

We need two definitions before proceeding. Let $\mathscr{L}^{\prime}(q(y, z \mid x))$ be a subset of $\mathbb{R}^{6}$ defined as the union of

$$
\begin{gathered}
\Delta(\{(I(W ; Y), I(W ; Z), I(U W ; Y), I(V W ; Z), \\
I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+I(W ; Y), \\
I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+I(W ; Z))\}),
\end{gathered}
$$

over random variables $U, V, W, X, Y, Z$, having the joint distribution $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$ and satisfying the cardinality constraints $|\mathcal{U}| \leq|\mathcal{X}|,|\mathcal{V}| \leq|\mathcal{X}|$ and $|\mathcal{W}| \leq|\mathcal{X}|+4 . \mathscr{C}^{\prime}(q(y, z \mid x))$ is defined similarly, except that the additional constraint $H(X \mid U V W)=0$ is imposed on the auxiliary random variables. Note that the region $\mathscr{L}^{\prime}(q(y, z \mid x))$ specifies $\mathscr{L}(q(y, z \mid x))$, since given any $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$ the corresponding vector in $\mathscr{L}^{\prime}(q(y, z \mid x))$ is providing the values for the right hand side of the 6 inequalities that define the region $\mathscr{L}(q(y, z \mid x))$. Similarly $\mathscr{C}^{\prime}(q(y, z \mid x))$ specifies $\mathscr{C}(q(y, z \mid x))$.

Instead of showing that $\mathscr{L}(q(y, z \mid x)) \subset \mathscr{C}(q(y, z \mid x))$, it suffices to show that $\mathscr{L}^{\prime}(q(y, z \mid x)) \subset$ $\mathscr{C}^{\prime}(q(y, z \mid x)) \cdot 8$ It suffices to prove that $\mathscr{C}^{\prime}(q(y, z \mid x))$ is convex, and that for any $\lambda_{1}, \lambda_{2}, \ldots, \lambda_{6}$, the maximum of $\sum_{i=1}^{6} \lambda_{i} R_{i}$ over triples $\left(R_{1}, R_{2}, \ldots, R_{6}\right)$ in $\mathscr{L}^{\prime}(q(y, z \mid x))$, is less than or equal to the maximum of $\sum_{i=1}^{6} \lambda_{i} R_{i}$ over triples $\left(R_{1}, R_{2}, \ldots, R_{6}\right)$ in $\mathscr{C}^{\prime}(q(y, z \mid x))$.

In order to show that $\mathscr{C}^{\prime}(q(y, z \mid x))$ is convex, we take two arbitrary points in $\mathscr{C}^{\prime}(q(y, z \mid x))$. Corresponding to them are joint distributions $p\left(u_{1}, v_{1}, w_{1}, x_{1}, y_{1}, z_{1}\right)$ and $p\left(u_{2}, v_{2}, w_{2}, x_{2}, y_{2}, z_{2}\right)$. Let $Q$ be a uniform binary random variable independent of all previously defined random variables, and let $U=U_{Q}$, $V=V_{Q}, W=\left(W_{Q}, Q\right), X=X_{Q}, Y=Y_{Q}$ and $Z=Z_{Q}$. Clearly $H(X \mid U V W)=0$, and furthermore $I(W ; Y) \geq \frac{1}{2}\left(I\left(W_{1} ; Y_{1}\right)+I\left(W_{2} ; Y_{2}\right)\right), I(W ; Z) \geq \frac{1}{2}\left(I\left(W_{1} ; Z_{1}\right)+I\left(W_{2} ; Z_{2}\right)\right), \ldots$ etc. Random variable $W$ is not defined on an alphabet set of size $|\mathcal{X}|+4$. However, one can reduce the cardinality of $W$ using the Carathéodory theorem by fixing $p(u, v, x, y, z \mid w)$ 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
${ }^{8}$ This is true because $\left(R_{0}, R_{1}, R_{2}\right)$ being in $\mathscr{L}(q(y, z \mid x))$ implies that $\left(R_{0}, R_{0}, R_{0}+R_{1}, R_{0}+R_{2}, R_{0}+R_{1}+R_{2}, R_{0}+R_{1}+R_{2}\right)$ is in $\mathscr{L}^{\prime}(q(y, z \mid x))$. If $\mathscr{L}^{\prime}(q(y, z \mid x))(q(y, z \mid x))$ is a subset of $\mathscr{C}^{\prime}(q(y, z \mid x))$, the latter point would belong to $\mathscr{C}^{\prime}(q(y, z \mid x))$. Therefore $\left(R_{0}, R_{1}, R_{2}\right)$ belongs to $\mathscr{C}(q(y, z \mid x))$.
preserved $p(u, v, x, y, z \mid w)$ throughout the process, $p(x \mid u, v, w)$ will continue to belong to the set $\{0,1\}$ after reducing the cardinality of $W$.

Next, we need to show that for any $\lambda_{1}, \lambda_{2}, \ldots, \lambda_{6}$, the maximum of $\sum_{i=1}^{6} \lambda_{i} R_{i}$ over triples $\left(R_{1}, R_{2}, \ldots, R_{6}\right)$ in $\mathscr{L}^{\prime}(q(y, z \mid x))$, is less than or equal to the maximum of $\sum_{i=1}^{6} \lambda_{i} R_{i}$ over triples $\left(R_{1}, R_{2}, \ldots, R_{6}\right)$ in $\mathscr{C}^{\prime}(q(y, z \mid x))$. As discussed in the proof of theorem without loss of generality we can assume $\lambda_{i}$ is non-negative for $i=1,2, \ldots, 6$.

Take an arbitrary point $\left(R_{1}, R_{2}, \ldots, R_{6}\right)$ in $\mathscr{L}^{\prime}(q(y, z \mid x))$. By definition there exist random variables $U, V, W, X, Y$ and $Z$ for which

$$
\begin{gather*}
\sum_{i=1}^{6} \lambda_{i} R_{i} \leq \lambda_{1} \cdot I(W ; Y)+\lambda_{2} \cdot I(W ; Z)+\lambda_{3} \cdot I(U W ; Y)+\lambda_{4} \cdot I(V W ; Z)+  \tag{20}\\
\lambda_{5} \cdot(I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+I(W ; Y))+ \\
\lambda_{6} \cdot(I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+I(W ; Z))
\end{gather*}
$$

Fix $p(u, v, w)$. The right hand side of equation (20) would then be a convex function of $p(x \mid u, v, w)$. ${ }^{9}$ Therefore its maximum occurs at the extreme points when $p(x \mid u, v, w) \in\{0,1\}$ whenever $p(u, v, w) \neq 0$. Therefore random variables $\widehat{U}, \widehat{V}, \widehat{W}, \widehat{X}, \widehat{Y}$, and $\widehat{Z}$ exist for which

$$
\begin{aligned}
& \lambda_{1} \cdot I(W ; Y)+\lambda_{2} \cdot I(W ; Z)+\ldots+\lambda_{6} \cdot(I(U ; Y \mid W)+I(V ; Z \mid W)-I(U ; V \mid W)+I(W ; Z)) \leq \\
& \quad \lambda_{1} \cdot I(\widehat{W} ; \widehat{Y})+\lambda_{2} \cdot I(\widehat{W} ; \widehat{Z})+\ldots+\lambda_{6} \cdot(I(\widehat{U} ; \widehat{Y} \mid \widehat{W})+I(\widehat{V} ; \widehat{Z} \mid \widehat{W})-I(\widehat{U} ; \widehat{V} \mid \widehat{W})+I(\widehat{W} ; \widehat{Z}))
\end{aligned}
$$

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

## 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 $p(u, v, w, x, y, z)=p(u, v, w, x) q(y, z \mid x)$ holds, $U$ and $V$ are binary, $H(X \mid U V W)$ is zero, the transition matrices $P_{Y \mid X}$ and $P_{Z \mid X}$ have positive elements, and for any value of $w$ where $p(w)>0$, either $I(U ; V \mid W=w, Y)=0$ or $I(U ; V \mid W=w, Z)=0$ holds, the following inequality is true:

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

[^5]We assume $I(U ; V \mid W=w, Y)=0$ (the proof for the case $I(U ; V \mid W=w, Z)=0$ is similar). First consider the case in which the individual capacity $C_{P_{Y \mid X}}$ is zero. We will then have $I(U ; Y \mid W=w)=0$ and $T(p(X=1 \mid W=w))=I(X ; Z \mid W=w) \geq I(V ; Z \mid W=w)-I(U ; V \mid W=w)$. Therefore the inequality holds in this case. Assume therefore that $C_{P_{Y \mid X}}$ is non-zero.

It suffices to prove the following proposition:
Proposition: For any random variables $U, V, X, Y$ and $Z$ satisfying

- $U V \rightarrow X \rightarrow Y Z$,
- $H(X \mid U V)=0$,
- $|\mathcal{U}|=|\mathcal{V}|=|\mathcal{X}|=2$,
- for all $y \in \mathcal{Y}, p(Y=y \mid X=0)$ and $p(Y=y \mid X=1)$ are non-zero,
- $C_{P_{Y \mid X}} \neq 0$,
- $I(U ; V \mid Y)=0$,
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 $H(X \mid U V)=0$, there are $2^{4}$ possible descriptions for $p(x \mid u v)$, 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 $C_{P_{Y \mid X}} \neq 0$, we conclude that the transition matrix $P_{Y \mid X}$ has linearly independent rows. This implies the existence of $y_{1}, y_{2} \in \mathcal{Y}$ for which $p\left(X=1 \mid Y=y_{1}\right) \neq p\left(X=1 \mid Y=y_{2}\right) .10$ Furthermore since $X$ is not constant, and $p\left(Y=y_{1} \mid X=0\right), p\left(Y=y_{1} \mid X=1\right), p\left(Y=y_{2} \mid X=0\right)$, and $p\left(Y=y_{2} \mid X=1\right)$ are all non-zero, both $p\left(X=1 \mid Y=y_{1}\right)$ and $p\left(X=1 \mid Y=y_{2}\right)$ are in the open interval $(0,1)$. Note that $I(U ; V \mid Y)=0$ implies that $I\left(U ; V \mid Y=y_{1}\right)=0$ and $I\left(U ; V \mid Y=y_{2}\right)=0$.

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

- $p\left(u=0, v=0 \mid y=y_{i}\right)=\frac{a_{0,0}}{a_{0,0}+a_{1,1}} p\left(X=0 \mid Y=y_{i}\right)$,
- $p\left(u=0, v=1 \mid y=y_{i}\right)=\frac{a_{0,1}}{a_{0,1}+a_{1,0}} p\left(X=1 \mid Y=y_{i}\right)$,
- $p\left(u=1, v=0 \mid y=y_{i}\right)=\frac{a_{1,0}}{a_{0,1}+a_{1,0}} p\left(X=1 \mid Y=y_{i}\right)$,
- $p\left(u=1, v=1 \mid y=y_{i}\right)=\frac{a_{1,1}}{a_{0,0}+a_{1,1}} p\left(X=0 \mid Y=y_{i}\right)$.

[^6]Therefore $I\left(U ; V \mid Y=y_{i}\right)=0$ for $i=1,2$ implies that

$$
p\left(u=1, v=1 \mid y=y_{i}\right) \times p\left(u=0, v=0 \mid y=y_{i}\right)=p\left(u=0, v=1 \mid y=y_{i}\right) \times p\left(u=1, v=0 \mid y=y_{i}\right) .
$$

Therefore

$$
\frac{a_{0,0} a_{1,1}}{\left(a_{0,0}+a_{1,1}\right)^{2}} p\left(X=0 \mid Y=y_{i}\right)^{2}=\frac{a_{0,1} a_{1,0}}{\left(a_{0,1}+a_{1,0}\right)^{2}} p\left(X=1 \mid Y=y_{i}\right)^{2},
$$

or alternatively

$$
\begin{equation*}
\frac{\sqrt{a_{0,0} a_{1,1}}}{a_{0,0}+a_{1,1}} p\left(X=0 \mid Y=y_{i}\right)=\frac{\sqrt{a_{1,0} a_{0,1}}}{a_{1,0}+a_{0,1}} p\left(X=1 \mid Y=y_{i}\right) . \tag{21}
\end{equation*}
$$

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 $V$ is a constant random variable 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 21 uniquely specifies $p\left(X=1 \mid Y=y_{i}\right)$, implying that $p\left(X=1 \mid Y=y_{1}\right)=p\left(X=1 \mid Y=y_{2}\right)$ which is again a contradiction.

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

- $p\left(u=0, v=0 \mid y=y_{i}\right)=\frac{a_{0,0}}{a_{0,0}+a_{0,1}+a_{1,0}} p\left(X=0 \mid Y=y_{i}\right)$,
- $p\left(u=0, v=1 \mid y=y_{i}\right)=\frac{a_{0,1}}{a_{0,0}+a_{0,1}+a_{1,0}} p\left(X=0 \mid Y=y_{i}\right)$,
- $p\left(u=1, v=0 \mid y=y_{i}\right)=\frac{a_{1,0}}{a_{0,0}+a_{0,1}+a_{1,0}} p\left(X=0 \mid Y=y_{i}\right)$,
- $p\left(u=1, v=1 \mid y=y_{i}\right)=p\left(X=1 \mid Y=y_{i}\right)$.

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

$$
p\left(u=1, v=1 \mid y=y_{i}\right) \times p\left(u=0, v=0 \mid y=y_{i}\right)=p\left(u=0, v=1 \mid y=y_{i}\right) \times p\left(u=1, v=0 \mid y=y_{i}\right) .
$$

Therefore

$$
\frac{a_{0,0}}{a_{0,0}+a_{0,1}+a_{1,0}} p\left(X=0 \mid Y=y_{i}\right) p\left(X=1 \mid Y=y_{i}\right)=\frac{a_{1,0} a_{0,1}}{\left(a_{0,0}+a_{0,1}+a_{1,0}\right)^{2}} p\left(X=0 \mid Y=y_{i}\right)^{2},
$$

or alternatively

$$
\begin{equation*}
a_{0,0} \cdot p\left(X=1 \mid Y=y_{i}\right)=\frac{a_{1,0} a_{0,1}}{a_{0,0}+a_{0,1}+a_{1,0}} p\left(X=0 \mid Y=y_{i}\right) \tag{22}
\end{equation*}
$$

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 $V$ is a constant random variable which is a contradiction. Therefore $a_{0,0}$ is non-zero. But then equation 22 uniquely specifies $p\left(X=1 \mid Y=y_{i}\right)$, implying that $p\left(X=1 \mid Y=y_{1}\right)=p\left(X=1 \mid Y=y_{2}\right)$ which is again a contradiction.

## ACKNOWLEDGEMENT

The authors would like to thank Chandra Nair for suggesting a short cut 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] 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.
[13] A. A. Gohari, A. El Gamal and V. Anantharam, On an Outer bound and an Inner Bound for the General Broadcast Channel, "Proceedings of the 2010 IEEE International Symposium on Information Theory", Austin, Texas, Jun. 13-18, pp. 540-544, 2010
[14] C. Nair, "A note on outer bounds for broadcast channel," Presented at International Zurich Seminar (2010), available at http://arxiv.org/abs/1101.0640
[15] C. Nair, Z. V. Wang, and Y. Geng, An information inequality and evaluation of Marton's inner bound for binary input broadcast channels, "Proceedings of the 2010 IEEE International Symposium on Information Theory", Austin, Texas, Jun. 13-18, pp.550-554, 2010


[^0]:    ${ }^{1}$ The conjecture is as follows: [Conjecture 1 12]: Given any five random variables $U, V, X, Y, Z$ satisfying $I(U V ; Y Z \mid X)=0$, 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 $p(y, z \mid x)$ is BSSC with parameter $\frac{1}{2}$.

[^1]:    ${ }^{2}$ Since the ranges of all the random variables are finite and the conditional mutual information function is continuous, the set of admissible joint probability distributions $p(u, v, x, y, z)$ where $I(U V ; Y Z \mid X)=0$ and $p(y, z, x)=q(y, z \mid x) p(x)$ 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 $p(u, v, x, y, z)=$ $p(u, v \mid x) p(x) q(y, z \mid x)$, 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.

[^2]:    ${ }^{3}$ The terms $\mathbb{E}[L(U, V, X) \mid Y]=0$ and $\mathbb{E}[L(U, V, X) \mid Z]=0$ must be zero if $\mathbb{E}[L(U, V, X) \mid X]=0$

[^3]:    ${ }^{5}$ The authors would like to thank Chandra Nair for suggesting this shortcut to simplify the original proof.

[^4]:    ${ }^{6}$ Since the ranges of all the involved 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 $I(U V W ; Y Z \mid X)=0$ and $p(y, z \mid x)=q(y, z \mid x)$ will be a compact set (when viewed as a subset of the ambient Euclidean space). The fact that mutual information function is continuous implies that the Marton region defined by taking the union over random variables $U, V, W, X, Y, Z$ satisfying the cardinality bounds is a compact set, and thus closed.

[^5]:    ${ }^{9}$ This is true because $I(W ; Y)$ is convex in the conditional distribution $p(y \mid w)$; similarly $I(U ; Y \mid W=w)$ is convex for any fixed value of $w$. The term $I(U ; V \mid W)$ that appears with a negative sign is constant since the joint distribution of $p(u, v, w)$ is fixed.

[^6]:    ${ }^{10}$ If this were not the case we would have we have $p\left(X=1 \mid Y=y_{1}\right)=p\left(X=1 \mid Y=y_{2}\right)$ 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 $P(Y=y \mid X=1)=$ $p(Y=y \mid X=0)$ for all $y \in \mathcal{Y}$. Therefore the transition matrix $P_{Y \mid X}$ has linearly dependent rows. Hence $I(X ; Y)=0$ for all $p(x)$. Therefore $C_{P_{Y \mid X}}=0$ which is a contradiction.

