Results and Techniques in Multiuser Information Theory

Amin Aminzadeh Gohari

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2010-115
http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-115.html

August 16, 2010

Results and Techniques in Multiuser Information Theory

by

Amin Aminzadeh Gohari

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Engineering-Electrical Engineering and Computer Sciences

in the

GRADUATE DIVISION
of the
UNIVERSITY OF CALIFORNIA, BERKELEY

Committee in charge:
Professor Venkatachalam Anantharam, Chair
Professor Martin J. Wainwright
Professor Donald E. Sarason

Fall 2010

Results and Techniques in Multiuser Information Theory

by

Amin Aminzadeh Gohari

Abstract

Results and Techniques in Multiuser Information Theory

by

Amin Aminzadeh Gohari
Doctor of Philosophy in Engineering-Electrical Engineering and Computer Sciences

University of California, Berkeley

Professor Venkatachalam Anantharam, Chair

In this dissertation we develop new techniques and apply them to prove new results in multiuser information theory. In the first part of the dissertation, we introduce the "potential function method," and apply it to prove converses for a series of multiterminal network capacity problems. In the second part of the dissertation, we introduce the "perturbation method," and apply it to the general broadcast channel problem, a fundamental open problem in information theory. Furthermore, we address a number of computational issues associated with the general broadcast channel.

The first part of the dissertation is devoted to the "potential function method" and its application to multiterminal networks. This method works by finding certain properties of expressions which will imply that they dominate the capacity region, and then proving a given bound by a verification argument. We show that this method can provide a unified framework for proving converses. We begin by considering the category of rate region problems without output feedback. The "dynamic programming flavor" of the technique and its use of one-step equations are brought up here. To demonstrate the use of technique in problems with feedback, we consider the problem of information-theoretically secure secret key agreement under the well-known *source model* and *channel model*. The concept of "state" and its evolution during the interactive communication by the parties are brought up here. The upper bounds we prove in this section are new and are strictly better than their corresponding previously best known upper bounds (our new lower bounds are relegated to an appendix in the end of the dissertation as they were not derived using the potential function method). Finally, we demonstrate the use of technique in a problem that involves transmission of dependent sources over strong interference channels. The new feature is that the notion of achievable rate regions is replaced by that of admissible sources. The result proved in this section is also new.

The second part of the dissertation begins by discussing the "perturbation method," and its application to the general broadcast channel problem. The perturbation method 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 corre-

sponding Fisher information. We apply this tool to make Marton's inner bound for the general broadcast channel computable. Before this, the latter region was not computable (except in certain special cases) as no bounds on the cardinality of its auxiliary random variables existed. 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. 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. We continue the second part of the dissertation with several results on computing a number of regions associated with the general broadcast channels. For instance, we prove various results that help to restrict the search space for computing the sum-rate for Marton's inner bound.

Professor Venkatachalam Anantharam
Dissertation Committee Chair

To mom and dad

Contents

List of Figures

List of Tables

Acknowledgments

I have benefited from the support and help of a number of people during my graduate studies. First and foremost, I owe my deepest gratitude to my esteemed research advisor, Prof. Venkat Anantharam for his continued support. The impact of his helps, patience and advices on the growth of my research skills could hardly be overestimated. I have immensely benefited from his broad knowledge of various disciplines of mathematics, sharp insights and systematic thinking. I had the opportunity to learn from him the importance of rigor and preciseness.

I appreciate Prof. Martin Wainwright for his support, kindness, friendliness and sympathy. I will keep the nice memories of my interaction with Martin. Martin helped me in getting used to the research environment in Berkeley. I regret missing out the opportunity to collaborate with him as intensely as I used to do in the beginning of my graduate studies.

I am highly honored, also, for having Professor Donald Sarason in my dissertation and qualifying exam committees. I would like to express my sincere gratitude to him for patiently reviewing the contents of this thesis. I would like to also thank Prof. David Tse for chairing my qualifying exam committee, and for all I have learnt from him; David is a great teacher. I would also like to convey thanks to Prof. Abbas El Gamal, Prof. Young-Han Kim and Prof. Chandra Nair for their help and support.

My sincere words of appreciation go to Prof. Anant Sahai. I was very lucky for having the opportunity to take information theory with him, only to intensify my interest to do research in information theory. I have benefited from his insightful, clear and attractive teaching style.

I want to also deeply thank Ruth Gjerde, Patrick Hernan, Mary Byrnes and everyone else at the Graduate Office for making everything so simple and convenient for graduate students. In particular, I am very grateful to Ruth for her many helps when I was outside the US.

Throughout the past several years, I have enjoyed the support and friendship of Ali Ghazizadeh, Pulkit Grover, Omid Etesami, Arash Ali Amini, Mohammad Ali Maddah-Ali, Ali Afshar, Artin Der Minassian, Massieh Najafi, Salman Avestimehr, Bobak Nazer, Anand Sarwate, Shufei Lei, Chul Kim, Sharon Moon and many others. I have been tremendously lucky to have the opportunity to interact with them. I cherish these friendships and never take them for granted. I miss my colleagues in the Wireless Foundations, especially my dear friend Pulkit Grover.

Last but not least, I want to express my gratitude to my dear mother and father. I am where I am because of their love and support. No words can do justice to describe what I owe to my family. I also want to sincerely thank my brother Amir for his continued support since he came to the US. Last but not least, I would like to thank all my teachers in Iran.

Chapter 1

Dissertation Overview

Information theory was developed by Claude Shannon in 1948 to find the fundamental limits of storage and communications systems. Information theory proofs consist of direct proofs or achievability proofs (establishing the inclusion of a given region in the capacity region) and converse proofs (establishing the inclusion of the capacity region in a given region). Many techniques have been introduced to address the direct and the converse parts of various problems. Historically, these techniques date back to Shannon himself. He introduced significant techniques such as random coding, and important concepts such as typicality of sequences. Later researchers came up with other techniques such as superposition coding, time sharing random variable, the use of Carathéodory theorem to prove cardinality bounds and deterministic models. The techniques used in the achievability proofs are generally more intuitive and structured; for instance, see the recent textbook on network information theory by El Gamal and Kim [15] for a systematic presentation of these proofs using the so-called "Packing Lemma" and "Covering Lemma". On the other hand, the converse proofs generally lack such transparency and meaningfulness. The main issue is moving from an $n-$letter expression to a single-letter expression which is usually done on a case by case basis. There is no systematic and unified algorithm that would result in the appropriate choice of auxiliary random variables. The converse proofs sometimes depend on the Csiszár sum lemma, or other identities that hold for a collection of n-random variables. Therefore, it is desirable to find a unified framework for proving converses. We discuss such framework in the first part of this dissertation. We introduce the "potential function method" and apply it to prove converses for a series of problems in multiterminal networks.

In the second part of the dissertation, we introduce the "perturbation method" and apply it to the general broadcast channel with two outputs. This is a fundamental open problem in information theory whose theoretical and practical importance is widely acknowledged. There has been some progress in cracking special cases of this old but open problem – notably Gaussian MIMO Broadcast Channels without a common message– yet, after decades of research we still cannot compute the capacity

region of this simple-looking multiterminal network. The presented results contribute to our understanding of this classical problem.

This dissertation is divided into two parts. An overview of the structure of each part is in order.

The first part of this dissertation is devoted to the "potential function method". This method works by finding certain properties of expressions which will imply that they dominate the capacity region, and then proving a given bound by a verification argument. We show that this method provides a unified framework for proving converses. We begin by considering the category of rate region problems without output feedback. The following sample problems are selected from this category: point-to-point communication, degraded broadcast channel, the Gelfand & Pinsker problem, a classical source coding problem, and the rate distortion problem with side information. We recover the known converses for these problems. Furthermore, the attention of the reader is drawn to the fact that the main portion of these converse proofs remains invariant. The derivation of the auxiliary random variables is done in a systematic and recursive manner, rather than in one shot as is commonly done. Each step of the recursion is systematic and algorithmic so that a computer program could be written to generate the auxiliaries. The "dynamic programming flavor" of the technique and its use of one-step equations are emphasized here. Extending these proofs to the cases with output feedback makes the terminology and the discussion heavier. To demonstrate the applicability of this technique to the problems with feedback, we consider the problem of information-theoretically secure secret key agreement under the well-known *source model* and *channel model*. In both of these models multiple terminals wish to create a shared secret key that is secure from a passive eavesdropper. The terminals have access to a noiseless public communication channel and an additional resource that depends on the model. In the source model, the resource is an external source that repeatedly beams correlated randomness to the terminals; whereas in the channel model, the resource is a secure but noisy discrete memoryless broadcast channel. Applying the potential function method, we prove new outer bounds under both the source model and the channel model. The concept of "state" and its evolution during the interactive communication by the parties is emphasized here. It is worth mentioning that we have also derived new lower bounds, but those are relegated to an appendix in the end of the dissertation as they were not derived using the potential function method.

Finally, we demonstrate the use of the potential function method in the problem of transmission of dependent sources over strong interference channels. The new feature is that the notion of achievable rate regions is replaced by that of admissible sources. Among other things, we emphasize that the new method differs from the traditional ones in that for a given network structure, we *simultaneously* consider all possible networks compatible with that structure and think of the rate region as a function from such networks to subsets of the positive orthant. We then identify properties of such a function which need to be satisfied for it to give rise to an outer bound.

The desired outer bound is then proved by a verification argument. To elaborate on this, we apply the technique to recover and further generalize the outer bound part of the recent result of Maric, Yates and Kramer on strong interference channels with a common message to include dependent sources. In the papers [21, 22], we have applied the same technique to 1) generalize the well known cut-set bound to the problem of lossy transmission of functions of dependent sources over a discrete memoryless multiterminal network, and to 2) simplify the recent outer bound of Liang, Kramer and Shamai on the capacity region of a general broadcast channel, and to generalize it to include dependent sources.

The second part of the dissertation begins by introducing the "perturbation method," and its application to the general broadcast channel problem. The perturbation method 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. We apply this tool to make Marton's inner bound for the general broadcast channel computable. Before this work, Marton's inner bound was not computable (except in certain special cases) as no bounds on the cardinality of its auxiliary random variables existed. It was not even known whether this inner bound was 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. 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.

In the rest of the second part of this dissertation, we report the subsequent research that was done along the direction of computing Marton's inner bound. Although existence of cardinality bounds renders Marton's inner bound computable, it is still hard to evaluate the region. We prove various results which help to restrict the search space for computing the sum-rate for Marton's inner bound. For binary input broadcast channels, we show that the computation can be further simplified if we assume that Marton's inner bound and the recent outer bound of Nair and El Gamal match at the given channel. These results are used to show that the inner and the outer bounds do not match for some broadcast channels, thus establishing a conjecture of Nair and Zizhou [45]. Furthermore, we show that unlike in the Gaussian case, for a degraded broadcast channel even without a common message, Marton's coding scheme without a superposition variable is in general insufficient for obtaining the capacity region.

We end the second part of the dissertation by mentioning a few other results that were left off since they did not concern the computation of Marton's inner bound. We establish the capacity region along certain directions and show that it coincides with Marton's inner bound. We show that the Nair-El Gamal outer bound can be made fully computable. Lastly, we discuss an idea that may lead to a larger inner bound.

Part I

On the converse proofs in multiuser Information Theory

Chapter 2

Rate region problems without output feedback

Converse proofs generally lack the transparency, meaningfulness and structure of the achievability proofs in information theory. This is partly due to the fact that the auxiliary random variables showing up in the converse proof can involve the past and/or the future of auxiliary random variables, and it is not always easy to assign meanings to these expressions in an operational sense.

In this chapter we introduce the technique by reproving converses for several well-known problems in which the transmitter(s) do not receive feedback from receivers or other transmitters. Nor are the transmitters concerned with communication of dependent messages. The problems we consider are Point-to-point communication, Degraded broadcast channel, the Gelfand & Pinsker problem, a classical source coding problem, and the rate distortion problem with side information. We show the technique in action in these examples without providing a general formulation of the technique in this chapter. Extending these proofs to cases with output feedback makes the terminology and the discussion heavier. The general formulation will be discussed in later chapters.

The main portion of the following converse proofs is fixed and invariant. The derivation of the auxiliary random variables is done in a systematic and recursive manner, rather than in one shot as is commonly done. Each step of the recursion is systematic and algorithmic so that a computer program could be written to generate the auxiliary random variables.

2.1 Point-to-point communication

We begin with the point-to-point communication problem. Let X and Y respectively represent the input and the output of the channel. We use the conditional probability distribution function of Y given X, $q(y|x)$, to describe the statistical

behavior of the channel.

The following proof for the point-to-point communication problem may seem to have the same complexity as the traditional proof, but it allows for a systematic generalization to other problems.

Proposition: Given a channel $q(y|x)$, we would like to show that any achievable communication rate belongs to the set $\mathcal{R}\big(q(y|x)\big) = \{R : 0 \leq R \leq \sup_{p(x)} I(X;Y)\}$.

Proof: 1) The first step is to note that the closure of the union over the n-letter regions

$$\bigcup_{n\geq 0} \frac{1}{n}\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n)\big)$$

is an outer bound to the capacity region, where

$$q(y_1y_2...y_n|x_1x_2...x_n) = \prod_{i=1}^{n} q(y_i|x_i).$$

Proving that the closure of this n-letter expression is an outer bound to the capacity region is straightforward by the Fano inequality.

2) The second (and the main) step is to show that $\bigcup_{n\geq 0} \frac{1}{n}\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n)\big)$ is equal to $\mathcal{R}\big(q(y|x)\big)$. This step is the single-letterising step. This is usually done in one shot, but here we do it iteratively and stage by stage. In order to accomplish this, it is enough to prove the following statement:

1. For every n,

$$\begin{aligned}&\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n)\big) \subset \\ &\mathcal{R}\big(q(y_1y_2...y_{n-1}|x_1x_2...x_{n-1})\big) \oplus \mathcal{R}\big(q(y_n|x_n)\big).\end{aligned} \tag{2.1}$$

   where $\oplus$ stands for the point by point sum (Minkowski sum) of the intervals (see Definition 10 of section 5.2 for the definition of Minkowski sum).

This is because the statement implies that

$$\begin{aligned}&\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n)\big) \subset \\ &\mathcal{R}\big(q(y_1|x_1)\big) \oplus \cdots \oplus \mathcal{R}\big(q(y_{n-1}|x_{n-1})\big) \oplus \mathcal{R}\big(q(y_n, z_n|x_n)\big) \\ &= n \times \mathcal{R}\big(q(y,z|x)\big).\end{aligned}$$

In order to prove the equation (2.1), it is sufficient to show that for any arbitrary channel $q(y\widetilde{y}|x\widetilde{x})$ that factorizes as $q(\widetilde{y}|\widetilde{x}) \cdot q(y|x)$, we have (note that here $\widetilde{x}, \widetilde{y}$ are playing the role of $x_1x_2...x_{n-1}$, $y_1y_2...y_{n-1}$)

$$\mathcal{R}\big(q(y\widetilde{y}|x\widetilde{x})\big) \subset \mathcal{R}\big(q(\widetilde{y}|\widetilde{x})\big) \oplus \mathcal{R}\big(q(y|x)\big).$$

Take an arbitrary point R belonging to $\mathcal{R}\big(q(y\widetilde{y}|x\widetilde{x})\big)$. Corresponding to this point is a joint distribution $p(x\widetilde{x})$ where $R \leq I(X\widetilde{X};Y\widetilde{Y})$. We would like to prove that there are two points in $\mathcal{R}\big(q(\widetilde{y}|\widetilde{x})\big)$ and $\mathcal{R}\big(q(y|x)\big)$ that add up to a number greater than or equal to $I(X\widetilde{X};Y\widetilde{Y})$. Since $I(X\widetilde{X};Y\widetilde{Y}) = H(Y\widetilde{Y}) - H(Y\widetilde{Y}|X\widetilde{X}) = H(Y\widetilde{Y}) - H(Y|X) - H(\widetilde{Y}|\widetilde{X}) \leq I(X;Y) + I(\widetilde{X};\widetilde{Y})$ we get the desired result since $I(X;Y)$ belongs to $\mathcal{R}\big(q(y|x)\big)$, and $I(\widetilde{X};\widetilde{Y})$ belongs to $\mathcal{R}\big(q(\widetilde{y}|\widetilde{x})\big)$.

3) The third (and the last) step is to show that $\mathcal{R}\big(q(y|x)\big)$ is a closed set. Since the ranges of all the involving random variables are limited and the mutual information function is continuous, the set of joint probability distributions $p(x,y)$ where $p(x,y) = q(y|x)p(x)$ 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 $p(x)$ of $I(X;Y)$ is a compact set, and thus closed.

2.2 The Gelfand and Pinsker problem

Proposition: We are given a channel $q(y|x,s)$ where x is the input and s is the state of the channel. The state of the channel is i.i.d. according to $q(s)$ and is known at the encoder. The achievable rate depends on the channel $q(y|x,s)$, and the marginal $q(s)$. Here we would like to prove the converse result of the Gelfand and Pinsker problem, i.e. to show that any communication rate belongs to the set $\mathcal{R}\big(q(y|x,s),q(s)\big) = \{R : 0 \leq R \leq \sup_{p(u,x|s)} I(U;Y) - I(U;S)\}$.

Proof: 1) The first step is to note that the closure of the union over the n-letter regions

$$\bigcup_{n\geq 0} \frac{1}{n}\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n,s_1s_2...s_n),q(s_1s_2...s_n)\big)$$

is an outer bound to the capacity region, where

$$q(y_1y_2...y_n|x_1x_2...x_n,s_1s_2...s_n) = \prod_{i=1}^{n} q(y_i|x_i,s_i),$$

$$q(s_1s_2...s_n) = \prod_{i=1}^{n} q(s_i).$$

Proving that the closure of this n-letter expression is an outer bound to the capacity region is straightforward by the Fano inequality.

2) The second (and the main) step is to show that

$$\bigcup_{n\geq 0} \frac{1}{n}\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n,s_1s_2...s_n),q(s_1s_2...s_n)\big)$$

is equal to $\mathcal{R}\big(q(y|x,s),q(s)\big)$. This step is the single-letterising step. This is usually done in one shot, but here we do it iteratively and stage by stage. This would make it possible to find the auxiliary random variable in a systematic manner. In order to accomplish this, it is enough to prove the following statement:

1. For every n,

$$\begin{aligned}&\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n,s_1s_2...s_n),q(s_1s_2...s_n)\big)\subset\\&\mathcal{R}\big(q(y_1...y_{n-1}|x_1...x_{n-1},s_1...s_{n-1}),q(s_1s_2...s_{n-1})\big)\oplus\\&\mathcal{R}\big(q(y_n|x_n,s_n),q(s_n)\big)\end{aligned}$$

where $\oplus$ stands for the point by point sum (Minkowski sum) of the intervals.

This is because the statement implies that

$$\begin{aligned}&\mathcal{R}\big(q(y_1y_2...y_n|x_1x_2...x_n,s_1s_2...s_n),q(s_1s_2...s_n)\big)\subset\\&\mathcal{R}\big(q(y_1|x_1,s_1),q(s_1)\big)\oplus\cdots\oplus\\&\mathcal{R}\big(q(y_{n-1}|x_{n-1},s_{n-1}),q(s_{n-1})\big)\oplus\mathcal{R}\big(q(y_n|x_n,s_n),q(s_n)\big)\\&=n\times\mathcal{R}\big(q(y|x,s),q(s)\big).\end{aligned}$$

In order to prove the first statement, it is sufficient to show that for any arbitrary channel $q(y\widetilde{y}|x\widetilde{x},s\widetilde{s})$ that factorizes as $q(\widetilde{y}|\widetilde{x},\widetilde{s})\cdot q(y|x,s)$, and $q(s\widetilde{s})$ that factorizes as $q(s)q(\widetilde{s})$, we have

$$\mathcal{R}\big(q(y\widetilde{y}|x\widetilde{x},s\widetilde{s}),q(s\widetilde{s})\big)\subset\mathcal{R}\big(q(\widetilde{y}|\widetilde{x},\widetilde{s}),q(\widetilde{s})\big)\oplus\mathcal{R}\big(q(y|x,s),q(s)\big).$$

Take an arbitrary point R belonging to $\mathcal{R}\big(q(y\widetilde{y}|x\widetilde{x},s\widetilde{s}),q(s\widetilde{s})\big)$. Corresponding to this point is a joint distribution $p(u,x\widetilde{x}|s\widetilde{s})$ where $R\leq I(U;Y\widetilde{Y})-I(U;S\widetilde{S})$. We would like to prove that there are two points in $\mathcal{R}\big(q(\widetilde{y}|\widetilde{x},\widetilde{s}),q(\widetilde{s})\big)$ and $\mathcal{R}\big(q(y|x,s),q(s)\big)$ that add up to a number greater than or equal to $I(U;Y\widetilde{Y})-I(U;S\widetilde{S})$. Please note that the following Markov chains hold: $UYXS-\widetilde{S}\widetilde{X}-\widetilde{Y}$, and $U\widetilde{Y}\widetilde{X}\widetilde{S}-SX-Y$. Thus for taking a point from the set $\mathcal{R}\big(q(\widetilde{y}|\widetilde{x},\widetilde{s}),q(\widetilde{s})\big)$, we can search for a random variable $\widetilde{U}$ by taking some combination of the four random variables U, Y, X, S. There are $2^4=16$ possibilities in total. Similarly for taking a point from the set $\mathcal{R}\big(q(y|x,s),q(s)\big)$, we can search for a random variable U' by taking some combination of the four random variables U, $\widetilde{Y}$, $\widetilde{X}$, $\widetilde{S}$. There are $2^4=16$ possibilities in total. The easiest approach is to write a computer program that tries all 16*16 cases using the information theoretic inequality verifier program that is available (see [58] or [50]). It is however not hard to guess the following choice of auxiliaries $\widetilde{U}=UY$ and $U'=U\widetilde{S}$. We need to verify that $I(U;Y\widetilde{Y})-I(U;S\widetilde{S})\leq I(U';Y)-I(U';S)+I(\widetilde{U};\widetilde{Y})-I(\widetilde{U};\widetilde{S})$, or equivalently $I(U;Y\widetilde{Y})-I(U;S\widetilde{S})\leq I(U\widetilde{S};Y)-I(U\widetilde{S};S)+I(UY;\widetilde{Y})-I(UY;\widetilde{S})$, which can be easily verified using the fact that $I(S;\widetilde{S})=0$.

3) The third (and the last) step is to show that $\mathcal{R}\big(q(y|x,s),q(s)\big)$ is a closed set. Note that in computing $\mathcal{R}\big(q(y|x,s),q(s)\big)$ one can use the strengthened Carathéodory theorem of Fenchel to bound the cardinality of U from above by $|\mathcal{X}||\mathcal{S}|$. Since the ranges of all the involved random variables are limited and the mutual information function is continuous, one can use arguments similar to the one mentioned in the proof of point-to-point converse to show that $\mathcal{R}\big(q(y|x,s),q(s)\big)$ is closed.

2.3 Degraded Broadcast Channel

Proposition: Consider a degraded broadcast channel $q(y,z|x) = q(y|x)q(z|y)$. It is known that the following region is the capacity region for this channel: let $\mathcal{R}\big(q(y,z|x)\big)$ be the set of all non-negative (R_1,R_2) such that there exists a joint distribution $p(u,x)$ for which $R_1 \leq I(X;Y|U)$ and $R_2 \leq I(U;Z)$ where X,Y,Z and U are jointly distributed according to $p(u,x)\cdot q(y,z|x)$. Here we would like to prove that $\mathcal{R}\big(q(y,z|x)\big)$ is an outer bound to the capacity region.

Proof: 1) The first step is to note that the closure of the union over the n-letter regions

$$\bigcup_{n\geq 0}\frac{1}{n}\mathcal{R}\big(q(y_1y_2...y_n,z_1z_2...z_n|x_1x_2...x_n)\big)$$

is an outer bound to the capacity region, where

$$q(y_1y_2...y_n,z_1z_2...z_n|x_1x_2...x_n)=\prod_{i=1}^{n}q(y_i,z_i|x_i).$$

Proving that the closure of this n-letter expression is an outer bound to the capacity region is straightforward by the Fano inequality.

2) The second (and the main) step is to show that

$$\bigcup_{n\geq 0}\frac{1}{n}\mathcal{R}\big(q(y_1y_2...y_n,z_1z_2...z_n|x_1x_2...x_n)\big)$$

is equal to $\mathcal{R}\big(q(y,z|x)\big)$. This step is the single-letterising step. This is usually done in one shot, but here we do it iteratively and stage by stage. This would make it possible to find the auxiliary random variable in a systematic manner. In order to accomplish this, it is enough to prove the following two statements:

1. For every n,

$$\begin{aligned}&\mathcal{R}\big(q(y_1y_2...y_n,z_1z_2...z_n|x_1x_2...x_n)\big)\subset\\&\mathcal{R}\big(q(y_1...y_{n-1},z_1...z_{n-1}|x_1...x_{n-1})\big)\oplus\mathcal{R}\big(q(y_n,z_n|x_n)\big),\end{aligned}$$

where $\oplus$ stands for the vector by vector sum (Minkowski sum) of the regions.

2. $\mathcal{R}\big(q(y,z|x)\big)$ is convex.

This is because the two statements together imply that

$$\begin{aligned}&\mathcal{R}\big(q(y_1y_2...y_n,z_1z_2...z_n|x_1x_2...x_n)\big)\subset\\&\mathcal{R}\big(q(y_1,z_1|x_1)\big)\oplus\mathcal{R}\big(q(y_2,z_2|x_2)\big)\cdots\oplus\mathcal{R}\big(q(y_n,z_n|x_n)\big)\\&\subset n\times\text{Convex Hull of }\mathcal{R}\big(q(y,z|x)\big)=n\times\mathcal{R}\big(q(y,z|x)\big).\end{aligned}$$

Proving the convexity is straightforward. In order to prove the first statement, it is sufficient to show that for any arbitrary channel $q(y\widetilde{y},z\widetilde{z}|x\widetilde{x})$ that factorizes as $q(\widetilde{y},\widetilde{z}|\widetilde{x})\cdot q(y,z|x)$, we have

$$\mathcal{R}\big(q(y\widetilde{y},z\widetilde{z}|x\widetilde{x})\big)\subset\mathcal{R}\big(q(\widetilde{y},\widetilde{z}|\widetilde{x})\big)\oplus\mathcal{R}\big(q(y,z|x)\big).$$

Take an arbitrary point (R_1,R_2) belonging to $\mathcal{R}\big(q(y\widetilde{y},z\widetilde{z}|x\widetilde{x})\big)$. Corresponding to this point is a joint distribution $p(u,x\widetilde{x})$ where $R_1\leq I(X\widetilde{X};Y\widetilde{Y}|U)$ and $R_2\leq I(U;Z\widetilde{Z})$. We would like to prove that there are two points in $\mathcal{R}\big(q(\widetilde{y},\widetilde{z}|\widetilde{x})\big)$ and $\mathcal{R}\big(q(y,z|x)\big)$ whose first coordinate adds up to a number greater than or equal to $I(X\widetilde{X};Y\widetilde{Y}|U)$, and whose second coordinate adds up to a number greater than or equal to $I(U;Z\widetilde{Z})$.

Since $p(u,x\widetilde{x},y\widetilde{y},z\widetilde{z})=p(u,x\widetilde{x})\cdot q(y,z|x)\cdot q(\widetilde{y},\widetilde{z}|\widetilde{x})$, we have the following Markov chains: $U\widetilde{X}\widetilde{Y}\widetilde{Z}-X-YZ$ and $UXYZ-\widetilde{X}-\widetilde{Y}\widetilde{Z}$. One can therefore write a computer program that searches for the random variable U' from the sixteen subsets of $\{U,\widetilde{X},\widetilde{Y},\widetilde{Z}\}$, and searches for $\widetilde{U}$ from the sixteen subsets of $\{U,X,Y,Z\}$. For each choice of U' and $\widetilde{U}$, the program can use an information-theoretic-inequality-verifier (see [58] or [50]) to check whether equations

$$I(U;Z\widetilde{Z})\leq I(U';Z)+I(\widetilde{U};\widetilde{Z}),\tag{2.2}$$

and

$$I(X\widetilde{X};Y\widetilde{Y}|U)\leq I(X;Y|U')+I(\widetilde{X};\widetilde{Y}|\widetilde{U}).\tag{2.3}$$

are satisfied under the given constraints.

In the above problem, there is however a natural choice for U' and $\widetilde{U}$: the expansion $I(U;Z\widetilde{Z})=I(U;Z)+I(U;\widetilde{Z}|Z)\leq I(U;Z)+I(UZ;\widetilde{Z})$ suggests setting $U'=U$ and $\widetilde{U}=UZ$. But we need to verify that equation (2.3) is also satisfied for this choice of random variables. Note that $I(X\widetilde{X};Y\widetilde{Y}|U)=H(Y\widetilde{Y}|U)-H(Y\widetilde{Y}|UX\widetilde{X})=H(Y\widetilde{Y}|U)-H(Y|X)-H(\widetilde{Y}|\widetilde{X})$ since $p(u,x\widetilde{x},y\widetilde{y},z\widetilde{z})=p(u,x\widetilde{x})\cdot q(y,z|x)\cdot q(\widetilde{y},\widetilde{z}|\widetilde{x})$. The right hand side of the equation (2.3) is equal to $I(X;Y|U')+I(\widetilde{X};\widetilde{Y}|\widetilde{U})=I(X;Y|U)+I(\widetilde{X};\widetilde{Y}|UZ)=H(Y|U)-H(Y|X)+H(\widetilde{Y}|UZ)-H(\widetilde{Y}|\widetilde{X})$. Hence the right hand side is greater than or equal to the left hand side if and only if $H(\widetilde{Y}|UZ)\geq H(\widetilde{Y}|UY)$. The latter is true because of the degradedness of the channel which implies that $H(\widetilde{Y}|UY)=H(\widetilde{Y}|UYZ)$. The proof is complete now.

3) The third (and the last) step is to show that $\mathcal{R}\big(q(y,z|x)\big)$ is a closed set. Note that in computing $\mathcal{R}\big(q(y,z|x)\big)$ one can use the strengthened Carathéodory theorem of Fenchel to bound the cardinality of U from above by $|\mathcal{X}|+1$. Since the ranges of all the involved random variables are limited and the mutual information function is continuous, one can use arguments similar to the one mentioned in the proof of point-to-point converse to show that $\mathcal{R}\big(q(y,z|x)\big)$ is closed.

2.4 A classical source coding problem

Proposition: Three parties are observing i.i.d. copies of X, Y and Z. There is a communication link of rate R_1 from X to Z, and a communication link of rate R_2 from Y to Z. The Z party wants to reconstruct the i.i.d. copies of X. The achievable rates (R_1, R_2) depend on the joint distributions $q(x, y, z)$. The answer to this problem is known. Here we would like to prove the converse to it, i.e. to show that any achievable rate pair (R_1, R_2) belongs to $\mathcal{R}\big(q(x, y, z)\big)$ defined as

$$\bigcup_{U-Y-XZ} \left\{ \begin{array}{l} R_1 \geq H(X|ZU) \\ R_2 \geq I(U;Y|Z). \end{array} \right.$$

Proof: 1) The first step is to note that the closure of the union over the n-letter regions

$$\bigcup_{n\geq 0} \frac{1}{n}\mathcal{R}\big(q(x_1x_2...x_n, y_1y_2...y_n, z_1z_2...z_n)\big)$$

is an outer bound to the capacity rate region, where

$$q(x_1x_2...x_n, y_1y_2...y_n, z_1z_2...z_n) = \prod_{i=1}^{n} q(x_i, y_i, z_i).$$

Proving that the closure of this n-letter expression is an outer bound to the capacity region is straightforward.

2) The second (and the main) step is to show that $\bigcup_{n\geq 0} \frac{1}{n}\mathcal{R}\big(q(x_1x_2...x_n, y_1y_2...y_n, z_1z_2...z_n)\big)$ is equal to $\mathcal{R}\big(q(y, z|x)\big)$. This step is the single-letterizing step. This is usually done in one shot, but here we do it iteratively and stage by stage. This would make it possible to find the auxiliary random variable in a systematic manner. In order to accomplish this, it is enough to prove the following two statements:

1. For every n,

$$\begin{array}{l} \mathcal{R}\big(q(x_1x_2...x_n, y_1y_2...y_n, z_1z_2...z_n)\big) \subset \\ \mathcal{R}\big(q(x_1...x_{n-1}, y_1...y_{n-1}, z_1...z_{n-1})\big) \oplus \mathcal{R}\big(q(x_n, y_n, z_n)\big), \end{array}$$

   where $\oplus$ stands for the vector by vector sum (Minkowski sum) of the regions.

2. $\mathcal{R}\big(q(x, y, z)\big)$ is convex.

This is because the two statements together imply that

$$\begin{array}{l} \mathcal{R}\big(q(x_1x_2...x_n, y_1y_2...y_n, z_1z_2...z_n)\big) \subset \\ \mathcal{R}\big(q(x_1, y_1, z_1)\big) \oplus \mathcal{R}\big(q(x_2, y_2, z_2)\big) \oplus \cdots \oplus \mathcal{R}\big(q(x_n, y_n, z_n)\big) \\ \subset n \times \text{Convex Hull of } \mathcal{R}\big(q(x, y, z)\big) = n \times \mathcal{R}\big(q(x, y, z)\big). \end{array}$$

Proving the convexity is straightforward. In order to prove the first statement, it is sufficient to show that for any arbitrary channel $q(x\widetilde{x}, y\widetilde{y}, z\widetilde{z})$ that factorizes as $q(\widetilde{x}, \widetilde{y}, \widetilde{z}) \cdot q(x, y, z)$, we have

$$\mathcal{R}\big(q(x\widetilde{x}, y\widetilde{y}, z\widetilde{z})\big) \subset \mathcal{R}\big(q(\widetilde{x}, \widetilde{y}, \widetilde{z})\big) \oplus \mathcal{R}\big(q(x, y, z)\big).$$

Take an arbitrary point (R_1, R_2) belonging to $\mathcal{R}\big(q(x\widetilde{x}, y\widetilde{y}, z\widetilde{z})\big)$. Corresponding to this point is a random variable $U - Y\widetilde{Y} - X\widetilde{X}Z\widetilde{Z}$ where $R_1 \geq H(X\widetilde{X}|Z\widetilde{Z}U)$ and $R_2 \geq I(U; Y\widetilde{Y}|Z\widetilde{Z})$. We would like to prove that there are two points in $\mathcal{R}\big(q(\widetilde{x}, \widetilde{y}, \widetilde{z})\big)$ and $\mathcal{R}\big(q(x, y, z)\big)$ whose first coordinate adds up to a number less than or equal to $H(X\widetilde{X}|Z\widetilde{Z}U)$, and whose second coordinate adds up to a number less than or equal to $I(U; Y\widetilde{Y}|Z)$.

Since $p(u, x\widetilde{x}, y\widetilde{y}, z\widetilde{z}) = q(x, y, z) \cdot q(\widetilde{x}, \widetilde{y}, \widetilde{z}) \cdot p(u|y\widetilde{y})$, we have the following Markov chains: $U\widetilde{X}\widetilde{Y}\widetilde{Z} - Y - XZ$ and $UXYZ - \widetilde{Y} - \widetilde{X}\widetilde{Z}$. One can therefore write a computer program that searches for the random variable U' from the sixteen subsets of $\{U, \widetilde{X}, \widetilde{Y}, \widetilde{Z}\}$, and searches for $\widetilde{U}$ from the sixteen subsets of $\{U, X, Y, Z\}$. For each choice of U' and $\widetilde{U}$, the program can use an information-theoretic-inequality-verifier to check whether equations

$$H(X\widetilde{X}|Z\widetilde{Z}U) \geq H(X|ZU') + H(\widetilde{X}|\widetilde{Z}\widetilde{U}), \tag{2.4}$$

and

$$I(U; Y\widetilde{Y}|Z\widetilde{Z}) \geq I(U'; Y|Z) + I(\widetilde{U}; \widetilde{Y}|\widetilde{Z}) \tag{2.5}$$

are satisfied under the given constraints.

In the above problem, there is however a natural choice for U' and $\widetilde{U}$: the expansion $H(X\widetilde{X}|Z\widetilde{Z}U) = H(X|Z\widetilde{Z}U) + H(\widetilde{X}|XZ\widetilde{Z}U)$ suggests setting $U' = U\widetilde{Z}$ and $\widetilde{U} = UZX$. But we need to verify that equation (2.5) is also satisfied for this choice of random variables. In other words:

$$I(U; Y\widetilde{Y}|Z\widetilde{Z}) \stackrel{?}{\geq} I(U\widetilde{Z}; Y|Z) + I(UZX; \widetilde{Y}|\widetilde{Z}).$$

Since the triples (X, Y, Z) and $(\widetilde{X}, \widetilde{Y}, \widetilde{Z})$ are independent, we have:

$$I(U\widetilde{Z}; Y|Z) + I(UZX; \widetilde{Y}|\widetilde{Z}) = I(U; Y|Z\widetilde{Z}) + I(U; \widetilde{Y}|\widetilde{Z}ZX).$$

Therefore we need to verify $I(U; \widetilde{Y}|\widetilde{Z}ZY) \stackrel{?}{\geq} I(U; \widetilde{Y}|\widetilde{Z}ZX)$. Noting the Markov chain $U - Y\widetilde{Y} - X\widetilde{X}Z\widetilde{Z}$, and independence of the triples (X, Y, Z) and $(\widetilde{X}, \widetilde{Y}, \widetilde{Z})$, we can write:

$$\begin{aligned}
&I(U; \widetilde{Y}|\widetilde{Z}ZX) \leq I(UY; \widetilde{Y}|\widetilde{Z}ZX) = \\
&I(Y; \widetilde{Y}|\widetilde{Z}ZX) + I(U; \widetilde{Y}|\widetilde{Z}ZXY) \leq \\
&I(U; \widetilde{Y}|\widetilde{Z}ZXY) = H(U|\widetilde{Z}ZXY) - H(U|\widetilde{Z}ZXY\widetilde{Y}) \\
&= H(U|\widetilde{Z}ZXY) - H(U|\widetilde{Z}ZY\widetilde{Y}) \leq \\
&H(U|\widetilde{Z}ZY) - H(U|\widetilde{Z}ZY\widetilde{Y}) = I(U; \widetilde{Y}|\widetilde{Z}ZY).
\end{aligned}$$

This completes the proof.

3) The third (and the last) step is to show that $\mathcal{R}\big(q(x,y,z)\big)$ is a closed set. Note that in computing $\mathcal{R}\big(q(x,y,z)\big)$ one can use the strengthened Carathéodory theorem of Fenchel to bound the cardinality of U from above by $|\mathcal{Y}|+1$. Since the ranges of all the involving random variables are limited and the mutual information function is continuous, one can use arguments similar to the one mentioned in the proof of point-to-point converse to show that $\mathcal{R}\big(q(x,y,z)\big)$ is closed.

2.5 Rate distortion with side information

Proposition: Two parties are observing i.i.d. copies of X and Y. There is a communication link of rate R from X to Y. The Y party wants to reconstruct the i.i.d. copies of X within some average distortion D for some given distortion function $d(x,\hat{x})$. The achievable rate R depends on the joint distribution $q(x,y)$ and D. The answer to this problem is known. Here we would like to prove the converse to it, i.e. to show that any achievable rate R belongs to $\mathcal{R}\big(q(x,y),D\big)$ defined as $\mathcal{R}\big(q(x,y),D\big)=\{R: R\geq \inf_{p(w|x),f} I(W;X|Y)\}$, where the minimization is over all $p(w|x)$ and functions $f:\mathcal{Y}\times\mathcal{W}\mapsto\mathcal{X}$ such that $\mathbb{E}[d(X,f(Y,W)]\leq D$.

Proof: 1) The first step is to note that for any $D'>D$, the closure of the union over the n-letter regions

$$\bigcup_{n\geq 0}\frac{1}{n}\mathcal{R}\big(q(x_1x_2...x_n,y_1y_2...y_n),nD'\big)$$

is an outer bound to the capacity region, where

$$q(x_1x_2...x_n,y_1y_2...y_n)=\prod_{i=1}^{n}q(x_i,y_i).$$

Proving that the closure of this n-letter expression is an outer bound is straightforward.

2) The second (and the main) step is to show that $\bigcup_{n\geq 0}\frac{1}{n}\mathcal{R}\big(q(x_1x_2...x_n,y_1y_2...y_n),nD'\big)$ is equal to $\mathcal{R}\big(q(x,y),D'\big)$, and further $\lim_{D'\to D}\mathcal{R}\big(q(x,y),D'\big)=\mathcal{R}\big(q(x,y),D\big)$.

In this document, we only focus on the first part of the claim; the limit can be proven using compactness arguments and noting that a cardinality bound on W can be established. It suffices to prove that

1. For every n and D_1,

$$\begin{aligned}&\mathcal{R}\big(q(x_1x_2...x_n,y_1y_2...y_n),D_1\big)\subset\\&\mathcal{R}\big(q(x_1x_2...x_{n-1},y_1y_2...y_{n-1}),D_2\big)\oplus\mathcal{R}\big(q(x,y),D_3\big)\end{aligned}$$

   for some D_2 and D_3 satisfying $D_2+D_3\leq D_1$.

2. $\mathcal{R}\big(q(x,y),D\big)$ is convex in D in the following sense: given any D_1 and D_2,

$$\frac{1}{2}\mathcal{R}\big(q(x,y),D_1\big)\oplus\frac{1}{2}\mathcal{R}\big(q(x,y),D_2\big)\subset\mathcal{R}\big(q(x,y),\frac{1}{2}D_1+\frac{1}{2}D_2\big).$$

Here, we omit the proof for the convexity statement. In order to show the first statement, it is sufficient to show that for any arbitrary $q(x\widetilde{x}, y\widetilde{y})$ that factorizes as $q(\widetilde{x}, \widetilde{y})q(x, y)$, we have

$$\mathcal{R}\big(q(x\widetilde{x}, y\widetilde{y}), D_1\big) \subset \mathcal{R}\big(q(x, y), D_3\big) \oplus \mathcal{R}\big(q(\widetilde{x}, \widetilde{y}), D_2\big)$$

for some D_2 and D_3 satisfying $D_2 + D_3 \leq D_1$. On the right hand side, we use distortion function d on $\mathcal{X}$ and $\widetilde{d}$ on $\widetilde{\mathcal{X}}$. The distortion function on the left hand side on $\mathcal{X} \times \widetilde{\mathcal{X}}$ is assumed to be the sum of d and $\widetilde{d}$.

Take an arbitrary point R belonging to $\mathcal{R}\big(q(x\widetilde{x}, y\widetilde{y}), D_1\big)$. Corresponding to this point is $p(w|x\widetilde{x})$ and function $f : \mathcal{Y} \times \widetilde{\mathcal{Y}} \times \mathcal{W} \mapsto \mathcal{X} \times \widetilde{\mathcal{X}}$. We can represent f as $f = (f_1, f_2)$ where $f_1 : \mathcal{Y} \times \widetilde{\mathcal{Y}} \times \mathcal{W} \mapsto \mathcal{X}$ and $f_2 : \mathcal{Y} \times \widetilde{\mathcal{Y}} \times \mathcal{W} \mapsto \widetilde{\mathcal{X}}$ such that $\mathbb{E}[d(X, f_1(Y, \widetilde{Y}, W)] + \mathbb{E}[\widetilde{d}(\widetilde{X}, f_2(Y, \widetilde{Y}, W)] \leq D_1$. We have $R \geq I(W; X\widetilde{X}|Y\widetilde{Y})$. We would like to prove that there are D_2 and D_3 satisfying $D_2 + D_3 \leq D_1$, and two points in $\mathcal{R}\big(q(x, y), D_3\big)$ and $\mathcal{R}\big(q(\widetilde{x}, \widetilde{y}), D_2\big)$ that add up to a number less than or equal to $I(W; X\widetilde{X}|Y\widetilde{Y})$.

Please note that the following condition holds here:

$$p(w, x, \widetilde{x}, y, \widetilde{y}) = q(x, y)q(\widetilde{x}, \widetilde{y})p(w|x, \widetilde{x}).$$

Thus for taking a point from the set $\mathcal{R}\big(q(\widetilde{x}, \widetilde{y}), D_2\big)$, we can search for a random variable $\widetilde{W}$ by taking some combination of the four random variables W, Y, X and $\widetilde{X}$. There are $2^4 = 16$ possibilities in total. Similarly for taking a point from the set $\mathcal{R}\big(q(x, y), D_3\big)$, we can search for a random variable W' by taking some combination of the four random variables W, $\widetilde{Y}$, $\widetilde{X}$ and X. There are $2^4 = 16$ possibilities in total.

It is natural to take $D_2 = \mathbb{E}[d(X, f_1(Y, \widetilde{Y}, W)]$ and $D_3 = \mathbb{E}[\widetilde{d}(\widetilde{X}, f_2(Y, \widetilde{Y}, W)]$. This also suggests taking $\widetilde{W} = WY$ and $W' = W\widetilde{Y}$. We need to verify

$$I(W; X\widetilde{X}|Y\widetilde{Y}) \stackrel{?}{\geq} I(W\widetilde{Y}; X|Y) + I(WY; \widetilde{X}|\widetilde{Y}).$$

Using the fact that $q(x, \widetilde{x}, y, \widetilde{y}) = q(x, y)q(\widetilde{x}, \widetilde{y})$, we can write

$$\begin{aligned}
&I(W; X\widetilde{X}|Y\widetilde{Y}) = H(X\widetilde{X}|Y\widetilde{Y}) - H(X\widetilde{X}|WY\widetilde{Y}) = \\
&H(X|Y) + H(\widetilde{X}|\widetilde{Y}) - H(X|WY\widetilde{Y}) - H(\widetilde{X}|WXY\widetilde{Y}) = \\
&I(W\widetilde{Y}; X|Y) + I(WXY; \widetilde{X}|\widetilde{Y}) \geq \\
&I(W\widetilde{Y}; X|Y) + I(WY; \widetilde{X}|\widetilde{Y}).
\end{aligned}$$

3) The third (and the last) step is to show that $\mathcal{R}\big(q(x, y), D\big)$ is a closed set. Note that in computing $\mathcal{R}\big(q(x, y), D\big)$ one can use the strengthened Carathéodory theorem of Fenchel to bound the cardinality of W from above by $|\mathcal{X}| + 1$. Since the ranges of all the involved random variables are limited and the mutual information function is continuous, one can use arguments similar to the one mentioned in the proof of point-to-point converse to show that $\mathcal{R}\big(q(x, y), D\big)$ is closed.

Table 2.1: The main part of the proof structure for the multiple access channel

Conditions that one needs to verify in the second step of the proof	Choice of auxiliaries
For $Q, X, \widetilde{X}, Y, \widetilde{Y}, Z\widetilde{Z} \sim p(q)p(x,\widetilde{x}\|q)p(y,\widetilde{y}\|q)q(z\|x,y)q(\widetilde{z}\|\widetilde{x},\widetilde{y})$ have	$Q' = Q$
$I(X\widetilde{X}; Z\widetilde{Z}\|Y\widetilde{Y}Q) \le I(X; Z\|YQ') + I(\widetilde{X}; \widetilde{Z}\|\widetilde{Y}\widetilde{Q})$,	
$I(Y\widetilde{Y}; Z\widetilde{Z}\|X\widetilde{X}Q) \le I(Y; Z\|XQ') + I(\widetilde{Y}; \widetilde{Z}\|\widetilde{X}\widetilde{Q})$,	$\widetilde{Q} = Q$
$I(X\widetilde{X}Y\widetilde{Y}; Z\widetilde{Z}\|Q) \le I(XY; Z\|Q') + I(\widetilde{X}\widetilde{Y}; \widetilde{Z}\|\widetilde{Q})$.	

Table 2.2: The main part of the proof structure for a converse to the general broadcast channel

Conditions that one needs to verify in the second step of the proof			Choice of auxiliaries
For $U, V, X, \widetilde{X}, Y, \widetilde{Y}, Z\widetilde{Z} \sim p(u,v,x,\widetilde{x})q(y,z\|x)q(\widetilde{y},\widetilde{z}\|\widetilde{x})$ have			
$I(U; Y\widetilde{Y})$	$\le$	$I(U'; Y) + I(\widetilde{U}; \widetilde{Y})$,	
$I(V; Z\widetilde{Z})$	$\le$	$I(V'; Z) + I(\widetilde{V}; \widetilde{Z})$,	$U' = U\widetilde{Z}$
$I(U; Y\widetilde{Y}) + I(V; Z\widetilde{Z}\|U)$	$\le$	$I(U'; Y) + I(V'; Z\|U')$	$V' = V\widetilde{Z}$
		$+I(\widetilde{U}; \widetilde{Y}) + I(\widetilde{V}; \widetilde{Z}\|\widetilde{U})$,	$\widetilde{U} = UY$
$I(V; Z\widetilde{Z}) + I(U; Y\widetilde{Y}\|V)$	$\le$	$I(V'; Z) + I(U'; Y\|V')$	$\widetilde{V} = VY$
		$+I(\widetilde{V}; \widetilde{Z}) + I(\widetilde{U}; \widetilde{Y}\|\widetilde{V})$.	

2.6 Multiple Access Channel

Given a MAC channel $q(z|x,y)$, let

$$\mathcal{R}\big(q(z|x,y)\big) = \bigcup_{p(q)p(x|q)p(y|q)q(z|x,y)} \begin{cases} R_1, R_2 \ge 0 \\ R_1 \le I(X; Z|YQ), \\ R_2 \le I(Y; Z|XQ), \\ R_1 + R_2 \le I(XY; Z|Q). \end{cases}$$

We would like to show that $\mathcal{R}$ is an outer bound to the capacity region of a MAC. The structure of the proof is similar to the ones given above. Therefore we have omitted the details. However, the structure of the second (and the main) step of the proof is provided in Table 2.1.

2.7 General Broadcast Channel

Given a broadcast channel $q(y, z|x)$, let (see [46])

$$\mathcal{R}\big(q(y,z|x)\big) = \bigcup_{p(u,v,x)q(y,z|x)} \begin{cases} R_1, R_2 \geq 0 \\ R_1 \leq I(U;Y), \\ R_2 \leq I(V;Z), \\ R_1 + R_2 \leq I(U;Y) + I(V;Z|U), \\ R_1 + R_2 \leq I(V;Z) + I(U;Y|V). \end{cases}$$

We would like to show that $\mathcal{R}$ is an outer bound to the capacity region of a BC. The structure of the proof is similar to the ones given above. Therefore we have omitted the details. However, the structure for the second (and the main) step of the proof is provided in Table 2.2.

Chapter 3

Problems with feedback

In this chapter we discuss the extension of the approach discussed in chapter 2 to problems in multiterminal networks with feedback.

For simplicity let us begin with the point-to-point communication problem with feedback. We would like to prove the following:

Proposition: Given a channel $q(y|x)$ assisted with full feedback, we would like to show that any achievable communication rate belongs to the set

$$\mathcal{R}\big(q(y|x)\big) = \{R : 0 \leq R \leq \sup_{p(x)} I(X;Y)\}.$$

A naive extension of the approach described in the previous chapter would not work since the n-letter $q(y_1y_2...y_n|x_1x_2...x_n)$ would not factorize as $\prod_{i=1}^{n} q(y_i|x_i)$. This is because Y_i can depend on X_i, X_{i+1}, X_{i+2}, ..., X_n. Furthermore, the single-letter definition of $\mathcal{R}$ does involve any term reflecting the feedback information. Another difference is the fact that feedback is imposing a particular *time order* on indices $1, 2, 3, ..., n$; there is a non-symmetric time flow that needs to be captured.

In the next chapters we will use the concept of "information state" and its evolution during the interactive communication by the parties to resolve this issue. Assume that the transmitter has message W and creates X_i from $WY_{1:i-1}$, the message W and the past output feedbacks. At the beginning, the transmitter and the receiver have W and a constant random variable respectively. At the j^{th} stage, the transmitter and the receiver have $WY_{1:j}$ and $Y_{1:j}$ respectively. Roughly speaking, we will represent the *information state* of the whole system at the j^{th} stage by the pair (conditional distribution of what the parties know at the j^{th} stage given what they know at the beginning, the joint distribution of what the parties know at the beginning). The "information state" has a simpler representation when there is no feedback. In such cases, X_i will be a deterministic function of W. Therefore the conditional distribution of $Y_{1:j}$ given W, that is $p(y_{1:j}|w)$, factorizes as $\prod_{i=1}^{j} p(y_i|x_i)$. For this reason, lack of output feedback makes the terminology and the discussion lighter.

The remaining chapters of the first part of the thesis adopt the idea of "information state". But before getting there, it is worthwhile to briefly mention another approach that could have been adopted to deal with the point-to-point communication problem with feedback.

Given a channel $q(y|x)$, we say that $\mathbf{X} = (X_1, X_2, ..., X_n)$, $\mathbf{Y} = (Y_1, Y_2, ..., Y_n)$ and W obey the feedback rule under $q(y|x)$ if $WY_{1:i-1} \to X_i \to Y_i$ and $p(y_i|x_i) = q(y_i|x_i)$ hold for $i = 1, 2, 3, ..., n$. We show this by the notation $W \to \mathbf{X} \overset{q}{\rightleftharpoons} \mathbf{Y}$. The two-sided arrow $\overset{q}{\rightleftharpoons}$ means that there is a two-way interaction, and that the forward channel is q. Unfortunately, we can define $W \to \mathbf{X} \rightleftharpoons \mathbf{Y}$ only when random variables $\mathbf{X}$ and $\mathbf{Y}$ are ordered vectors defined on $\mathcal{X}^n \times \mathcal{Y}^n$ for some n.

Note that when $n = 1$, the relation $W \to \mathbf{X} \overset{q}{\rightleftharpoons} \mathbf{Y}$ simply reduces to $W \to X \to Y$ together with $p(y|x) = q(y|x)$. We can thus re-express $\mathcal{R}$ as

$$\mathcal{R}\big(q(y|x)\big) = \{R : 0 \le R \le \sup_{p(x,y,w): W \to X \overset{q}{\rightleftharpoons} Y} I(W;Y)\}.$$

Using this expression, define the n-letter $\mathcal{R}_n\big(q(y|x)\big)$ as

$$\{R : 0 \le R \le \sup_{p(\mathbf{x},\mathbf{y},w): W \to \mathbf{X} \overset{q}{\rightleftharpoons} \mathbf{Y}} I(W;\mathbf{Y})\}$$

for n-tuples $\mathbf{X}$ and $\mathbf{Y}$.

We can now continue with the proof:

Proof: 1) The first step is to note that the closure of the union over the n-letter regions $\bigcup_{n\ge 0} \frac{1}{n}\mathcal{R}_n\big(q(y|x)\big)$ is an outer bound to the capacity region. Proving that this n-letter expression is an outer bound to the capacity region is straightforward.

2) The second (and the main) step is to show that $\bigcup_{n\ge 0} \frac{1}{n}\mathcal{R}_n\big(q(y|x)\big)$ is equal to $\mathcal{R}\big(q(y|x)\big)$. This step is the single-letterizing step. In order to do this iteratively, it is enough to prove the following statement:

1. For every n,

$$\mathcal{R}_n\big(q(y|x)\big) \subset \mathcal{R}_{n-1}\big(q(y|x)\big) \oplus \mathcal{R}\big(q(y|x)\big).$$

where $\oplus$ stands for the point by point sum (Minkowski sum) of the intervals.

In order to prove this, it is sufficient to show that for any arbitrary channel $p(w, (\widetilde{\mathbf{x}}, x), (\widetilde{\mathbf{y}}, y))$ satisfying $W \to (\widetilde{\mathbf{X}}, X) \overset{q}{\rightleftharpoons} (\widetilde{\mathbf{Y}}, Y)$, one can find $p(w', x, y)$ satisfying $W' \to X \overset{q}{\rightleftharpoons} Y$ and $p(\widetilde{w}, \widetilde{\mathbf{x}}, \widetilde{\mathbf{y}})$ satisfying $\widetilde{W} \to \widetilde{\mathbf{X}} \overset{q}{\rightleftharpoons} \widetilde{\mathbf{Y}}$ such that

$$I(W; Y\widetilde{\mathbf{Y}}) \le I(W'; Y) + I(\widetilde{W}; \widetilde{\mathbf{Y}}). \tag{3.1}$$

The condition $W \to (\widetilde{\mathbf{X}}, X) \overset{q}{\rightleftharpoons} (\widetilde{\mathbf{Y}}, Y)$ implies that $W \to \widetilde{\mathbf{X}} \overset{q}{\rightleftharpoons} \widetilde{\mathbf{Y}}$. Thus, it is natural to take $\widetilde{W} = W$. Equation 3.1 then suggests setting $W' = W\widetilde{\mathbf{Y}}$. It remains to verify $W\widetilde{\mathbf{Y}} \to X \overset{q}{\rightleftharpoons} Y$. Or, in other words $W\widetilde{\mathbf{Y}} \to X \to Y$. But this is immediate from $W \to (\widetilde{\mathbf{X}}, X) \overset{q}{\rightleftharpoons} (\widetilde{\mathbf{Y}}, Y)$ as the last of the "obeying the feedback rule" condition.

3) The third (and the last) step is to show that $\mathcal{R}\big(q(y|x)\big)$ is a closed set. This was argued in the proof of point-to-point converse in the previous section.

Chapter 4

Interactive communication for secret key generation

In this chapter we introduce the potential function method and apply it to two important problems in Information-theoretic security as well as a problem of communication for omniscience. It is worthwhile to briefly motivate Information-theoretic security as a subfield, before getting into the specifics of our problems.

The rapidly flourishing wireless networks have created challenging demands on reliable and secure communication in the past decade. Unlike wireline links, wireless links are inherently open, and thus very susceptible to eavesdropping and jamming. In order to preserve privacy, it is desirable to embed security mechanisms in various layers of the system. Whereas complexity based encryption schemes can be used at higher network levels, channel coding ideas based on *information-theoretic notion of security* can be used at the physical layer.

Information-theoretic security demands that the evesdropper(s) learn a negligible amount about the secret message regardless of the computational power of the adversary. Therefore it is the most stringent form of security. It was once commonly considered infeasible in view of Shannon's one time pad result. The following recognitions have however led to a rethinking of this pessimistic viewpoint: first, Information-theoretic security can utilize the physical properties of wireless channels (e.g. the broadcasting properties) to provide security at the physical layer. Second, in many environments requiring secret key generation, it is possible to provide external randomness to the agents. For instance, sensor networks are often deployed in places where it is possible to beam randomness, e.g. from a satellite. These observations have led to significant work over the last decade to develop protocols to extract high rate secret keys. Nonetheless, Information-theoretic security still remains to be less practical compared to the computational security.

In this chapter we study a fundamental problem in information-theoretic security in which a group of agents together with an eavesdropper have access to possibly correlated random sources of information. These agents want to use public discussion to generate a common key that is secret from the eavesdropper. As discussed above, this problem is of practical importance because it exploits the physical characteristics of wireless networks such as the broadcasting property to provide security at the *physical layer*, whereas com-

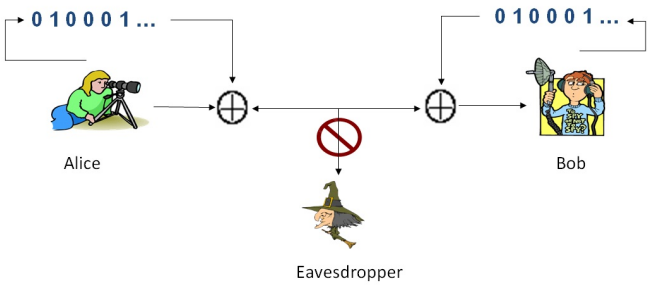

Figure 4.1: Shannon's one time pad

plexity based encryption schemes are traditionally used at the higher network levels, and furthermore, because sensor networks are often deployed in places where it is possible to beam randomness, e.g. from a satellite. The source-model and channel-model are of theoretical interest since they quantify the fundamental limits of extracting a secret key from given resource. Outside the context of security, one can motivate the source-model capacity $S(X_1; X_2 \| Z)$ as representing the "*private common information*" of random variables X_1 and X_2 against a third random variable Z, in some operational sense. The natural conjecture $I(X_1; X_2|Z)$, for instance, would not satisfy the expected property that the "private common information" should be less than the common information, since $I(X_1; X_2|Z) \leq I(X_1; X_2)$ does not always hold.

4.1 Introduction

The problem of secret key generation by multiple terminals, information-theoretically secure from an eavesdropper was originally formulated by Shannon [52]. Shannon considered the scenario in which Alice wants to transmit a message securely to Bob in the presence of an eavesdropper. As shown in Figure 4.1, Alice and Bob have access to a public communication link. Secure communication is possible if Alice and Bob share a secret key to encrypt and decrypt the message respectively. For example, Alice can take the binary addition of her message with the secret key, thereby keeping the eavesdropper absolutely ignorant about the message. However, Bob can decode the intended message. Shannon proved that this strategy is indeed optimal in the sense of using up the minimum number of secret bits per message bit. This is a pessimistic result since it is saying that the shared key must be at least as long as the message. Generation and distribution of such a long key is not practical in many applications. Shannon's work has been much developed and modified to address this issue; see for example [1], [11] and [39]. In an early work, Wyner [56] studied what may be called a "degraded broadcast scenario". In this setting Alice is connected to Bob by a discrete memoryless channel. The eavesdropper, Eve, receives a noisy version of the output at Bob's end. In a subsequent work, Csiszár and Körner [11] generalized Wyner's model by assuming that Alice is connected to Bob and Eve through a broadcast channel. The channel from Alice to Eve in this model is not necessarily a degraded version of the

channel between Alice and Bob. In this scenario, the secret key capacity, as one might expect, would be zero if the channel from Alice to Eve is stronger than the channel from Alice to Bob. The scenario considered by Csiszár and Körner was further generalized by Maurer [39]. Maurer made the interesting observation that even if the channel from Alice to Eve is stronger than the channel from Alice to Bob, Alice and Bob may still be able to generate a common secret key that is information-theoretically secure from Eve, in an asymptotic sense, if we allow Bob to send authenticated but public messages to Alice. In some sense in this result the communication between Alice and Bob is being used to agree about features of the noise realization in the broadcast channel that are independent of Eve's knowledge: this is the secret key. This observation led to the formulation of the two main models in this area, introduced by the works of Ahlswede and Csiszár [1], Csiszár and Narayan [13] and Maurer [39], called the *source model* and *channel model*. In both models there are m terminals interested in secret key generation against an adversary Eve. In the source model, the m terminals and Eve have access to n independently and identically distributed (i.i.d.) repetitions of jointly distributed random variables X_i $(i = 1, 2, ..., m)$ and Z respectively. Following the reception of the n i.i.d. repetitions of $(X_1, X_2, ..., X_m, Z)$, in the traditional source model the m terminals are allowed to have interactive authenticated public communication. The public channel is assumed to be noiseless. In the channel model, a secure discrete memoryless broadcast channel (DMBC) $\mathrm{q}(x_2, x_3, ...x_m, z|x_1)$ exists from the first terminal to all other terminals (including Eve). The input of the DMBC is governed by the first terminal while the other terminals (including Eve) observe the outputs of the broadcast channel at their end. In the traditional channel model, after each use of the channel by the first terminal, all the m terminals are allowed to engage in arbitrarily many rounds of interactive authenticated communication over a public channel. Again, the public channel is assumed to be noiseless. We generalize both models somewhat by allowing the public communication only among the first u $(1 \leq u \leq m)$ of the terminals; terminals $u + 1, ..., m$ can listen and have to participate in secret key generation, but do not talk. This generalization has the technical advantage of putting one-way secret key generation and interactive secret key generation on the same footing and includes the standard model as a special one. Further, and more importantly, it provides an approach to study the secret key capacity by splitting it into parts in a sense that will become clear after understanding the main results of section 4.4.2. Following the communication, each terminal generates a random variable S_i as its secret key, $i = 1, 2, 3, ..., m$. All S_i's should with probability close to 1 be equal to each other and they should be approximately independent of Eve's whole information after the communication. In the source model, Eve's whole information after the communication consists of the n i.i.d repetitions of Z and the public discussion, whereas in the channel model Eve's whole information after the communication is the n outputs of the DMBC at Eve's terminal and the public discussion. The achieved secret key rate would then be roughly $\frac{1}{n}H(S_1)$. The highest achievable secret key rate, asymptotic in n, is called the secret key capacity. For a precise formulation see section 4.2.

Another problem discussed in this chapter is the problem of *communication for omniscience*. This problem is a generalization of a similar one considered by Csiszár and Narayan [12]. In some special cases, Csiszár and Narayan [12] derived a single-letter characterization of the source model secret key capacity, notably when all the legitimate terminals know Z,

that is $H(Z|X_i) = 0$ for $i = 1, 2, 3, ..., m$. This was done by bringing out a connection between a problem of communication for omniscience (CFO) by the terminals and the secret key generation problem. In the CFO problem, as defined in [12], the requirement at the end of the communication is not a secret key, but that all the terminals become approximately omniscient about each other's random variables. The goal is to minimize the communication rate required to achieve this. In this thesis we relax the requirement that all the legitimate terminals know Z and define a broader notion of communication for omniscience, called the problem of *communication for omniscience by a neutral observer* (still abbreviated as CFO). In the CFO problem, as defined in this thesis, the m terminals at the end of the communication wish to create a shared random variable which when provided to a neutral observer who has access to the i.i.d. copies of Z seen by Eve, allows the observer to reconstruct the i.i.d. copies of the variables $(X_1, X_2, ..., X_u)$ (where $1 \leq u \leq m$ is as before). The CFO rate is the minimum conditional entropy of the communication, conditioned on the information available to Eve, measured on a per observation basis. We use our technique for proving converses to show that our CFO problem is equivalent to the problem of secret key generation (see section 4.2 for the precise formulation of the definitions and section 4.4.2 for a precise formulation of the results). This result generalizes the one of [12] but does not appear to lead to a single letter characterization of the secret key capacity.

4.2 Definitions and Notation

Throughout this chapter we assume that there are m legitimate terminals and one eavesdropper; random variables X_1, X_2, ..., X_m and Z will be $m + 1$ possibly dependent random variables taking values from finite sets $\mathcal{X}_1$, $\mathcal{X}_2$, ..., $\mathcal{X}_m$ and $\mathcal{Z}$. In the source model, we begin with a given joint distribution on X_1, X_2, ..., X_m and Z; we assume that the i-th legitimate terminal observes i.i.d. copies of X_i whereas the eavesdropper observes i.i.d. copies of Z. In the channel model however, X_1 represents the input to a discrete memoryless broadcast channel (DMBC), $q(x_2, x_3, ..., x_m, z|x_1)$, and X_2, ..., X_m and Z represent the outputs at the legitimate terminals 2, 3, ..., m and at the eavesdropper. In both models, the eavesdropper is passive.

Every random variable in this chapter takes values in a finite set. Given random variables $X(1), X(2), ..., X(n)$, we write $X^{1:i}$ for $(X(1), X(2), ..., X(i))$. For $X^{1:n}$ we will often instead write X^n.

Some previous works consider secret key generation in the case where only one terminal is allowed to participate in public discussion, called the *one-way secret key capacity*. Our models more generally include the case in which only a subset of terminals is allowed to participate in the public discussion. Without loss of generality, we assume that terminals $1, 2, ..., u$ $(1 \leq u \leq m)$ are allowed to talk while terminals $u + 1, u + 2, ..., m$ are silent.

The definitions for the source model and channel model are provided in the following two subsections:

Source Model

Definition 1. Given n i.i.d repetitions of the jointly distributed random variables $(X_1, X_2, ..., X_m, Z)$, the pair $(n, \mathbf{C})$, where $\mathbf{C} = (C_1, C_2, ..., C_r)$ is a finite set of finite random variables, is considered a *valid communication* if the following two properties hold:

- $H(C_k|C_1, C_2, ..., C_{k-1}, X_{j_k}^n) = 0$ where $1 \leq j_k \leq m$ is such that $j_k = k$ modulo m. This means that the indexing of the communications is done in round-robin order and each communication is adapted to the available information of the communicator;
- $C_k = 0$ whenever $u + 1 \leq j_k \leq m$ where j_k is defined as above. This means that the terminals $u + 1, u + 2, ..., m$ are not allowed to participate in the communication.[1]

Please note that if $(n, \mathbf{C})$ is valid, then one has $H(\mathbf{C}|X_1^n, X_2^n, ..., X_m^n) = 0$.

The communication is conducted by the m terminals in an interactive way, over an authenticated but insecure channel (called the public channel); the eavesdropper is assumed to remain passive throughout, but hears the messages sent over the public channel.

Definition 2. Let ϵ be a positive real number. Take some valid communication $(n, \mathbf{C})$ and assume that, following the communication, the m terminals create finite random variables S_1, S_2, ..., S_m satisfying the following conditions:

1. $H(S_j|\mathbf{C}, X_j^n) = 0$ for all $1 \leq j \leq m$. This condition is saying that S_j is created by the j-th terminal using the information available to the terminal following the communication $\mathbf{C}$ on the public channel;
2. $P(S_1 = S_2 = S_3 = ... = S_m) > 1 - \epsilon$. This condition ensures that the legitimate terminals are, with probability close to 1, generating a shared key;
3. $\frac{1}{n} I(S_1; Z^n, \mathbf{C}) < \epsilon$. This ensures that the generated key is almost hidden from the eavesdropper.

We call such a strategy a *secret key (SK) generation* strategy, and denote it by SK(n, ϵ, S_1, S_2, S_3, ..., S_m, $\mathbf{C}$). The corresponding *secret key rate* is defined as $\frac{1}{n} H(S_1)$. The intuitive reason for this terminology is that we are measuring the amount of secret bits generated per i.i.d. observation of X_1, X_2, ..., X_m and Z.

Discussion: We basically use the same multi-terminal model as in [12] when all the m terminals are interested in secret key generation. We have however relaxed the uniformity condition on the generated secret key i.e. equation (2) in [12]. Maurer in [39] argued that the assumption of uniformity could always be added without loss of generality. A rigorous treatment of this point can be found in Lemma 5 of [42]. The idea is as follows: roughly speaking, a protocol that achieves a non-uniformly distributed key can be converted into one that does so at the cost of a negligible reduction in the key rate. The idea is to repeat the protocol several times and take the new key to be the concatenation of the keys generated

[1] By $C_k = 0$, we mean $P(C_k = 0) = 1$. In effect this means the alphabet for random variables representing the public communication by terminals $u + 1, u + 2, ..., m$ is of size one.

by one of the terminals in each execution of the protocol, when the sequence of individual secret keys is *typical*. If the sequence is not typical, the key is set as an error symbol. This results in an almost uniformly distributed key. In order to enable the other legitimate terminals to reconstruct the key with probability close to 1 an error correction message is created by the distinguished terminal and revealed on the public channel.

Furthermore, in this chapter we have adopted the notion of *weak secrecy* (where the equivocation *rate* of the key is made arbitrarily small), rather than the notion of *strong secrecy* (where the *total* equivocation of the key is made arbitrarily small). Maurer and Wolf showed that the weak and strong secret key rates are equal for the case of two legitimate terminals [42]. The idea is similar to the one mentioned above, i.e. to carry out the protocol several times, and send the error correction message on the public channel. Lastly, the leftover hash lemma is used to create a key about which the eavesdropper has almost no knowledge (according to the strong notion of secrecy). The strong notion of secrecy, and its equivalence with the weak notion of secrecy for certain models, was also studied in an earlier work by Csiszár in [14] using a different technique.

Definition 3. Let ϵ be a positive real number. Take some valid communication $(n, \mathbf{C})$ and assume that following the communication, the m terminals create finite random variables T_1, T_2, ..., T_m satisfying the following conditions:

1. $H(T_j|\mathbf{C}, X_j^n) = 0$ for all $1 \leq j \leq m$. This condition is saying that T_j is created by the j-th terminal using the information available to the terminal following the communication $\mathbf{C}$ on the public channel;

2. $P(T_1 = T_2 = T_3 = ... = T_m) > 1-\epsilon$. This condition ensures that the random variables generated at the legitimate terminals form common randomness with probability close to 1;

3. $\frac{1}{n}H(X_1^n, X_2^n, ..., X_u^n|Z^n, T_1) < \epsilon$. This condition ensures that the generated common randomness together with Z^n covers almost all of the information content of $X_1^n, X_2^n, ..., X_u^n$.

We call such a strategy a *communication for omniscience by a neutral observer* (CFO) strategy, and denote it by CFO (n, ϵ, T_1, T_2, T_3, ..., T_m, $\mathbf{C}$). The corresponding *conditional CFO rate* is defined as $\frac{1}{n}H(\mathbf{C}|Z^n)$.

Discussion: Intuitively speaking, a communication for omniscience (CFO) protocol works as follows: The terminals will conduct a public discussion in order to agree, with probability close to 1, on a common randomness, but there is no secrecy constraint. We can assume that there is a neutral terminal, say Charles, who receives Z^n from Eve and the common randomness obtained by the terminals. Charles is required to become omniscient about $X_1^n, X_2^n, ..., X_u^n$. The cost of the communication, called the conditional CFO rate, would be the entropy rate of the overall communication conditioned on Z^n.

Consider the special case in which $u = m$, and all the legitimate terminals know Z, that is $H(Z|X_i) = 0$ for $i = 1, 2, 3, ..., m$. Charles has access to Z^nT_1. Suppose that he has learnt $X_1^n, X_2^n, ..., X_m^n$, meaning that $\frac{1}{n}H(X_1^n, X_2^n, ..., X_m^n|Z^nT_1)$ is small. Since $H(Z^n|X_1^n) = 0$, $\frac{1}{n}H(X_1^n, X_2^n, ..., X_m^n|X_1^nT_1)$ will be small too, meaning that the first terminal should have

learned the random variables of all terminals. Furthermore since $T_1 = T_2 = ... = T_m$ with high probability, the other terminals should have also learned the random variables of all the terminals. Therefore, the communication for omniscience by a neutral observer would be transformed to a simple communication for omniscience, as studied by Csiszár and Narayan [12]. The communication cost, i.e. the conditional CFO rate of communication, in this case is equal to the total entropy rate of the communication conditioned on Z^n. Since Z^n is known to all terminals at the beginning of the communication and, without loss of generality, the successive communications can be made independent of each other and of Z^n, one could have chosen them so that the communication cost as we measure it is identical to the cost as measured by Csiszár and Narayan. Therefore the communication for omniscience by a neutral observer is a generalization of the communication for omniscience of [12].

Definition 4. Given positive ϵ, the ϵ-secret capacity when the terminals cannot randomize,

$$S^{\epsilon}_{no-r}(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z),$$

is defined as the limsup of the maximal SK rate as n converges infinity.[2] Please note that the superscript "(s)" is used to denote the silent terminals. Similarly, the ϵ-CFO capacity,

$$T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z),$$

is defined as the liminf of the minimal conditional CFO rate as n converges infinity.

The SK capacity when the terminals cannot randomize,

$$S_{no-r}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z),$$

and the CFO capacity,

$$T(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z),$$

are defined as:

$$\begin{aligned}
&S_{no-r}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z) = \\
&\lim_{\epsilon \to 0} S^{\epsilon}_{no-r}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z), \\
&T(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z) = \\
&\lim_{\epsilon \to 0} T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z).
\end{aligned}$$

The SK capacity when the terminals can randomize, $S(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$, is defined as the supremum of $S_{no-r}(X_1M_1; X_2M_2; X_3M_3; X_uM_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ over all $(M_1, M_2, ..., M_u)$ satisfying:

$$p(M_1, ..., M_u, X_1, ..., X_m, Z) = p(M_1)p(M_2)...p(M_u)p(X_1, ..., X_m, Z).$$

[2] It is easy to see that the limsup (resp liminf) is actually a limit, but the definitions made this way are technically convenient.

Channel Model

In the channel model, the m legitimate terminals have access to two resources: an authenticated but public communication channel, and a discrete memoryless broadcast channel (DMBC), described by the conditional law $\mathrm{q}(x_2, x_3, ..., x_m, z|x_1)$. Any message sent on the public channel will be heard by all terminals including the eavesdropper. The eavesdropper is assumed to be passive and cannot tamper with the messages sent on the public channel. The input of the broadcast channel X_1 is controlled by the first legitimate terminal. The DMBC has outputs X_2, X_3, ..., X_m at the remaining $m-1$ legitimate terminals, and output Z at the eavesdropper.

Before providing a formal definition, we begin with an intuitive description of a secret key generation scheme in the channel model.

The secret key generation scheme begins by the first terminal inserting random variable $X_1(1)$ at the input of $\mathrm{q}(x_2, x_3, ..., x_m, z|x_1)$. The other legitimate terminals and the eavesdropper receive $X_2(1)$, ..., $X_m(1)$ and $Z(1)$, respectively. The first terminal is assumed to have access to private randomness, implying that the random variable $X_1(1)$ need not be a constant. We then assume that the legitimate terminals engage in $r(1)$ rounds of interactive public discussion over the authenticated public channel; the number of communication rounds, $r(1)$, can be arbitrarily large. In order to enable the possibility of private randomization during the public discussion we assume that the first u terminals are provided with random variables M_1, M_2, ..., M_u that are mutually independent of each other and of $(X_1(1), X_2(1), ..., X_m(1), Z)$.[3] We use $\mathbf{C}_1 = (C_{1,1}, C_{1,2}, ..., C_{1,r(1)})$ to represent this interactive public discussion. More specifically, $C_{1,1}$ is a message created by the first terminal as a function of $X_1(1)M_1$, and revealed to all the other terminals (including the eavesdropper). Then the second terminal creates $C_{1,2}$ as a function of the information available to the second terminal at this stage, i.e. $C_{1,1}X_2(1)M_2$, and reveals it to all other terminals. The messages $C_{1,3}$, $C_{1,4}$, ... are created and revealed in a similar manner. Note that if $r(1) > m$, $C_{1,m+1}$ will be created by the first terminal. This means that the indexing of the communications is done in round robin order. Furthermore, since we insist that only the first u terminals can engage in public discussion, the messages created by terminals $u+1$, $u+2$, ..., m must be vacuous (for instance $C_{1,u+1} = C_{1,u+2} = 0$; see footnote 1). The eavesdropper remains passive throughout, and only hears the public discussions and its observations from the DMBC. Following the interactive public discussion of the first stage, the first terminal inserts $X_1(2)$ at the input of the DMBC. This input is adapted to the information available to the first terminal at that stage, i.e. $\mathbf{C}_1X_1(1)M_1$. The other legitimate terminals and the eavesdropper receive $X_2(2)$, ..., $X_m(2)$ and $Z(2)$, respectively. Then the terminals engage in $r(2)$ rounds of interactive communication over the public channel, where $r(2)$ is an arbitrary natural number. We use $\mathbf{C}_2 = (C_{2,1}, C_{2,2}, ..., C_{2,r(2)})$ to represent this interactive public discussion. For instance, $C_{2,1}$ is created as a function of the information available to the first terminal, i.e. $\mathbf{C}_1X_1(1)X_1(2)M_1$. The message $C_{2,2}$ is created by the second terminal as a function of the information available to the terminal, i.e. $\mathbf{C}_1C_{2,1}X_2(1)X_2(2)M_2$; the message $C_{2,3}$ is created by the third terminal as a function

[3]Therefore the total source of private randomness available to the first u terminals are $M_1X_1(1)$, M_2, M_3, ... and M_u.

of $\mathbf{C}_1 C_{2,1} C_{2,2} X_3(1) X_3(2) M_3$, etc. This process is repeated for n stages. At the end, the m terminals create the secret keys S_1, ..., S_m. These keys should be equal to each other with probability close to 1 and almost independent of the total information available to the eavesdropper, i.e. the n observations from the DMBC, Z^n, and the messages $\mathbf{C}_1$, $\mathbf{C}_2$, ..., $\mathbf{C}_n$ sent over the public channel.

For the special case of $u = m = 2$, the secret key generation scheme can be described as follows:

$$\begin{gathered}
\to (X_1(1), X_2(1), Z(1)) \\
\to (X_1(1)M_1, X_2(1)M_2, Z(1)) \\
\to (X_1(1)M_1C_{1,1}, X_2(1)M_2C_{1,1}, Z(1)C_{1,1}) \\
\\
\to (X_1(1)M_1C_{1,1}C_{1,2}, X_2(1)M_2C_{1,1}C_{1,2}, Z(1)C_{1,1}C_{1,2}) \\
\to \cdots \to (X_1(1)M_1\mathbf{C}_1, X_2(1)M_2\mathbf{C}_1, Z(1)\mathbf{C}_1) \\
\to (X_1(1)X_1(2)M_1\mathbf{C}_1, X_2(1)X_2(2)M_2\mathbf{C}_1, Z(1)Z(2)\mathbf{C}_1) \\
\\
\to (X_1(1)X_1(2)M_1\mathbf{C}_1C_{2,1}, X_2(1)X_2(2)M_2\mathbf{C}_1C_{2,1}, Z(1)Z(2)\mathbf{C}_1C_{2,1}) \\
\to (X_1(1)X_1(2)M_1\mathbf{C}_1C_{2,1}C_{2,2}, X_2(1)X_2(2)M_2\mathbf{C}_1C_{2,1}C_{2,2}, Z(1)Z(2)\mathbf{C}_1C_{2,1}C_{2,2}) \\
\\
\to \cdots \\
\to (X_1(1)X_1(2)M_1\mathbf{C}_1\mathbf{C}_2, X_2(1)X_2(2)M_2\mathbf{C}_1\mathbf{C}_2, Z(1)Z(2)\mathbf{C}_1\mathbf{C}_2) \\
\to (X_1(1)X_1(2)X_1(3)M_1\mathbf{C}_1\mathbf{C}_2, X_2(1)X_2(2)X_2(3)M_2\mathbf{C}_1\mathbf{C}_2, Z(1)Z(2)Z(3)\mathbf{C}_1\mathbf{C}_2) \\
\\
\to (X_1(1)X_1(2)X_1(3)M_1\mathbf{C}_1\mathbf{C}_2C_{3,1}, X_2(1)X_2(2)X_2(3)M_2\mathbf{C}_1\mathbf{C}_2C_{3,1}, Z(1)Z(2)Z(3)\mathbf{C}_1\mathbf{C}_2C_{3,1}) \\
\to \cdots \\
\to (X_1^n M_1\mathbf{C}, X_2^n M_2\mathbf{C}, Z^n\mathbf{C}) \\
\to (S_1, S_2, Z^n\mathbf{C})
\end{gathered}$$

A formal definition of a secret key generation scheme is as follows:

Definition 5. Let ϵ be a positive real number, M_1, M_2, ..., M_u, X_1^n, X_2^n, ..., X_m^n, Z^n and S_1, S_2, ..., S_m be finite random variables, and $\mathbf{C} = (\mathbf{C}_1, \mathbf{C}_2, ..., \mathbf{C}_n)$ be a collection of n finite sets of finite random variables $\mathbf{C}_i : i = 1, 2, ..., n$, where $\mathbf{C}_i = (C_{i,1}, C_{i,2}, ..., C_{i,r(i)})$ for some natural number $r(i)$ $(i = 1, 2, 3..., n)$. Consider the following conditions:

1. $p(M_1, M_2, ..., M_u, X_1(1), X_2(1), ..., X_m(1), Z) =$
   $p(M_1)...p(M_u)p(X_1(1), X_2(1), ..., X_m(1), Z)$.
   This condition is saying that external random variables provided to the u terminals, i.e. $M_1, M_2, ..., M_u$, before the first round of communication are mutually independent of each other and of the random variables corresponding to the first use of the DMBC.

2. For $i = 1, 2, ..., n$:

$$p\Big(X_2(i) = x_2(i), ..., X_m(i) = x_m(i), Z(i) = z(i) \Big| \\ X_1^{1:i} = x_1^{1:i}, X_2^{1:i-1} = x_2^{1:i-1}, ..., X_m^{1:i-1} = x_m^{1:i-1}, \\ Z^{1:i-1} = z^{1:i-1}, M_1 = m_1, ..., M_u = m_u \Big) = \\ \mathrm{q}(x_2(i), ..., x_m(i), z(i)|x_1(i)).$$

   This condition is essentially saying that the outputs received by the terminals 2, 3, ..., m at the i-th stage, i.e. $X_2(i), ..., X_m(i), Z(i)$ depend only on $X_1(i)$, and the DMBC $\mathrm{q}(x_2(i), ..., x_m(i), z(i)|x_1(i))$;

3. For $i = 2, ..., n$,

$$H(X_1(i)|\mathbf{C}_1, \mathbf{C}_2, ..., \mathbf{C}_{i-1}, X_1^{1:i-1}, M_1) = 0.$$

   This condition is saying that $X_1(i)$ is created by the first terminal at the i-th stage using the information available to the terminal at that stage;

4. $H(C_{i,k}|\mathbf{C}_1, \mathbf{C}_2, ..., \mathbf{C}_{i-1}, C_{i,1}, C_{i,2}, ..., C_{i,k-1}, X_{j_k}^{1:i} M_{j_k})$ is zero whenever $1 \leq j_k \leq u$, where $1 \leq j_k \leq m$ is such that $j_k = k$ modulo m. This means that the indexing of the communications in each stage is done in round robin order and each communication is adapted to the available information of the communicator. Furthermore for $1 \leq i \leq n$, $C_{i,k} = 0$ whenever $u + 1 \leq j_k \leq m$ where j_k is defined as above. This means that the terminals $u+1, u+2, ..., m$ are not allowed to participate in the communication;

5. $H(S_j|\mathbf{C}, X_j^n M_j) = 0$ for $1 \leq j \leq u$, and $H(S_j|\mathbf{C}, X_j^n) = 0$ for $u + 1 \leq j \leq m$. This means that the secret key S_j is created by j-th terminal at the end of the entire process. For instance, the information available to the j-th terminal $1 \leq j \leq u$ is the whole public communications, i.e. $\mathbf{C}$, the observations made from the DMBC, i.e. X_j^n, and the private source of randomness M_j;

6. $P(S_1 = S_2 = S_3 = ... = S_m) > 1-\epsilon$. This ensures that the secret keys generated at the legitimate terminals are equal to each other high probability close to 1;

7. $\frac{1}{n} I(S_1; Z^n, \mathbf{C}) < \epsilon$. This ensures that the generated key is almost hidden from the eavesdropper.

We represent such a secret key generation scheme by $\mathrm{SK}_C(n, \epsilon, S_1, S_2, S_3, ..., S_m, \mathbf{C}, M_1, M_2, ..., M_u, X_1^n, X_2^n, ..., X_m^n, Z^n)$. The secret key rate of the scheme is defined as $\frac{1}{n} H(S_1)$. In other words, we are measuring the amount of secret bits generated *per use* of the DMBC.

Definition 6. Given $\epsilon > 0$, $C^{\epsilon}_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$, the ϵ-secret key capacity, is defined as the limsup of the maximal SK_C rate as n converges infinity.
$C^{\epsilon}_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$ represents the maximal secret key rate when the probability of mismatch among the secret keys S_1, S_2, ..., S_m, and the leakage rate $\frac{1}{n}I(S_1; Z^n, \mathbf{C})$ are bounded from above by ϵ.

Definition 7. $C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$, the channel model secret key capacity, is defined as:

$$\lim_{\epsilon \to 0} C^{\epsilon}_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1)).$$

Discussion: Note that we have allowed the first user to participate in the public discussion and to randomize (by randomize we mean the messages put on the public channel are not necessarily *deterministic* functions of the random variables received). Further, all the terminals who participate in the public discussion, i.e. terminals $1 \leq i \leq u$, are allowed to randomize. The assumption on the participation of the first terminal in the public discussion can be removed but this terminal must be allowed to randomize. Otherwise, the inputs to the broadcast channel will be always a deterministic function of the public communication and thus known to the eavesdropper, resulting in zero secret key rate. It is legitimate to differentiate between the ability to randomize and the ability to participate in the public discussion as long as the first user is concerned. For the sake of notational simplicity, however, we allow the first user to participate in the public discussion.

4.3 Review of the known results

Calculation of the exact secret key capacity remains an unsolved problem, although some lower and upper bounds on this quantity are known. In the source model, for the case of $m = 2$, the best known upper bound is that of Renner and Wolf [51]. This bound, known as the *double intrinsic information bound*, is equal to $\inf_U[H(U) + I(X_1; X_2 \downarrow ZU)]$, where $I(X_1; X_2 \downarrow Z)$ is defined as $\inf_{X_1X_2 \to Z \to \overline{Z}} I(X_1; X_2|\overline{Z})$ and is called the *intrinsic information* [41]. The essentially best known lower bound, proved using random binning arguments, is due to Ahlswede and Csiszár [1]: the maximum of $\sup_{V \to U \to X_1 \to X_2 Z} \big(I(U; X_2|V) - I(U; Z|V)\big)$ and $\sup_{V \to U \to X_2 \to X_1 Z} \big(I(U; X_1|V) - I(U; Z|V)\big)$. [4] In the channel model, for the case of $m = 2$, the best known upper bound explicitly mentioned in the literature, as far as we are aware, is

$$\min[\sup_{p(x_1)} I(X_1; X_2), \sup_{p(x_1)} I(X_1; X_2|Z))],$$

[4] Maurer provided a different technique for deriving lower bounds on the secret key capacity in [39]. He proved, for instance, that even when the maximum of the two one-way secret key capacities vanishes, the secret key capacity may still be positive. This technique however seems to give us a rather low secret key rate in this case. A generally applicable single letter form of a lower bound based on the ideas in [39] is not known.

which was proposed by Maurer [39]. This can however be easily generalized to $\inf_{\overline{Z}\to Z\to X_1X_2}[\sup_{p(x_1)} I(X_1;X_2|\overline{Z})]$. The essentially best know lower bound, as far as we are aware, is

$$\sup_{p(x_1)} \max\Big\{ \sup_{V\to U\to X_1\to X_2Z} [I(U;X_2|V) - I(U;Z|V)], \\ \sup_{V\to U\to X_2\to X_1Z} [I(U;X_1|V) - I(U;Z|V)]\Big\},$$

which one can find in [12], [39]. Recently, Csiszár and Narayan have derived new sufficient conditions for tight upper bounds [13].

4.4 The source model and the CFO problem

4.4.1 The proof technique at an intuitive level

In this section, we illustrate the main proof technique at an intuitive level. Roughly speaking, the technique used for deriving the upper bounds is to consider functions of joint distributions which satisfy specific properties that eventually lead to their dominating the secret key capacity. More specifically, in the source model, we consider a specific class of functions of joint distributions, called potential functions, and show that they satisfy the following property: for any secret key generating protocol, the potential function starts from the upper bound and decreases as we move along the protocol, and eventually becomes equal to the secret key rate of the protocol. It was pointed to us by one of the reviewers for a journal paper published on this, that our technique is similar to that of "secret key monotones" of Lemma 2.10 of [38]. We now provide the details:

Consider the special case of $u = m = 2$. One can view $S_{no-r}(X_1;X_2\|Z)$ as a function from the set of all joint distributions $p(x_1,x_2,z)$ defined on arbitrary finite sets $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{Z}$ to non-negative real numbers. Our technique for proving upper bounds on the secret key capacity is to identify certain properties of $S_{no-r}(X_1;X_2\|Z)$ as a function, and then consider the class of all functions that have those properties and show that each of them is an upper bound on $S_{no-r}(X_1;X_2\|Z)$. The function $S_{no-r}(X_1;X_2\|Z)$ has the following properties:

1. For any natural number n, we have $n\cdot S_{no-r}(X_1;X_2\|Z) \geq S_{no-r}(X_1^n;X_2^n\|Z^n)$;
2. For any random variable F such that $H(F|X_1)=0$ or $H(F|X_2)=0$, we have: $S_{no-r}(X_1;X_2\|Z) \geq S_{no-r}(X_1F;X_2F\|ZF)$;
3. For any random variables X_1', X_2' such that $H(X_1'|X_1) = H(X_2'|X_2) = 0$, we have: $S_{no-r}(X_1;X_2\|Z) \geq S_{no-r}(X_1';X_2'\|Z)$;
4. $S_{no-r}(X_1;X_2\|Z) \geq H(X_1|Z) - H(X_1|X_2) = I(X_1;X_2) - I(X_1;Z)$.

In order to show that the first property holds, take a particular secret key generation scheme for the triple (X_1^n, X_2^n, Z^n). This scheme consists of taking say n' i.i.d. copies of (X_1^n, X_2^n, Z^n), conducting a public discussion and then generating a secret key. One can however simulate the same scheme on the left hand side by taking nn' i.i.d copies of (X_1, X_2, Z), conducting the same public discussion, and then generating the same secret key. The difference in the number of i.i.d. copies observed is compensated for by the factor n on the left hand side. Using the same simulation idea, one can show that properties 2 and 3 also hold. Property 4 holds since $H(X_1|Z) - H(X_1|X_2) = I(X_1; X_2) - I(X_1; Z)$ is known to be a lower bound on $S_{no-r}(X_1; X_2\|Z)$ (see for example [1]).

Next, take an arbitrary function $\varphi(X_1; X_2\|Z)$, from the set of all joint distributions $p(x_1, x_2, z)$ defined on arbitrary finite sets $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{Z}$ to non-negative real numbers. Assume that $\varphi(X_1; X_2\|Z)$ satisfies the above three properties:

1. For any natural number n, we have $n \cdot \varphi(X_1; X_2\|Z) \geq \varphi(X_1^n; X_2^n\|Z^n)$;
2. For any random variable F such that $H(F|X_1) = 0$ or $H(F|X_2) = 0$, we have: $\varphi(X_1; X_2\|Z) \geq \varphi(X_1F; X_2F\|ZF)$;
3. For any random variables X_1', X_2' such that $H(X_1'|X_1) = H(X_2'|X_2) = 0$, we have: $\varphi(X_1; X_2\|Z) \geq \varphi(X_1'; X_2'\|Z)$;
4. $\varphi(X_1; X_2\|Z) \geq H(X_1|Z) - H(X_1|X_2) = I(X_1; X_2) - I(X_1; Z)$.

We claim that any such function $\varphi(X_1; X_2\|Z)$ dominates $S_{no-r}(X_1; X_2\|Z)$, i.e. $\varphi(X_1; X_2\|Z) \geq S_{no-r}(X_1; X_2\|Z)$. The rough sketch of the proof is as follows. Take a secret key generation scheme that generates a secret key rate close to $S_{no-r}(X_1; X_2\|Z)$. The terminals observe n i.i.d. copies of (X_1, X_2, Z), conduct the communication $\mathbf{C} = (C_1, C_2, ..., C_r)$, and generate the secret keys S_1 and S_2 where $S_1 \cong S_2$, and $\frac{1}{n}H(S_1) \cong S_{no-r}(X_1; X_2\|Z)$. We then have:

$$
\begin{aligned}
& n \cdot \varphi(X_1; X_2\|Z) \geq \varphi(X_1^n; X_2^n\|Z^n) \geq && (4.1)\\
& \varphi(X_1^n C_1; X_2^n C_1\|Z^n C_1) \geq && (4.2)\\
& \varphi(X_1^n C_1 C_2; X_2^n C_1 C_2\|Z^n C_1 C_2) \geq && (4.3)\\
& ... \geq
\end{aligned}
$$

$$
\begin{aligned}
& \varphi(X_1^n \mathbf{C}; X_2^n \mathbf{C}\|Z^n \mathbf{C}) \geq \\
& \varphi(S_1; S_2\|Z^n \mathbf{C}) \geq && (4.4)\\
& H(S_1|Z^n \mathbf{C}) - H(S_1|S_2) && (4.5)\\
& \cong n \cdot S_{no-r}(X_1; X_2\|Z),
\end{aligned}
$$

where equation (4.1) holds because of property 1; equation (4.2) holds because of property 2 and the fact that $H(C_1|X_1^n) = 0$; equation (4.3) holds because of property

2 and the fact that $H(C_2|C_1X_1^n) = 0$; equation (4.4) holds because of property 3 and the fact that $H(S_1|X_1^n\mathbf{C}) = H(S_2|X_2^n\mathbf{C}) = 0$; equation (4.5) holds because of property 4. The above chain of inequalities imply that $\varphi(X_1; X_2\|Z) \geq S_{no-r}(X_1; X_2\|Z)$.

Note that the triples

$$(X_1^n, X_2^n, Z^n), (X_1^nC_1, X_2^nC_1, Z^nC_1),$$
$$(X_1^nC_1C_2, X_2^nC_1C_2, Z^nC_1C_2), ...,$$
$$(X_1^n\mathbf{C}, X_2^n\mathbf{C}, Z^n\mathbf{C}), (S_1, S_2, Z^n\mathbf{C}),$$

can be thought of as representing the sequence of the information states of the system during the simulation of the secret key generation scheme. The function $\varphi(.)$ associates a value to the information state of the system in such a way that, as the scheme is conducted, the value associated to the information state decreases (as shown in equations (4.2), (4.3)). Thus, it is justified to view $\varphi(.)$ as a *potential function*.

The above result could make the converse proofs systematic. Suppose we would like to prove that $I(X_1; X_2|Z)$ constitutes an upper bound on $S_{no-r}(X_1; X_2\|Z)$. It suffices to verify that $\varphi(X_1; X_2\|Z) = I(X_1; X_2|Z)$ satisfies the above four properties: the first property holds since $I(X_1^n; X_2^n|Z^n) = nI(X_1; X_2|Z)$; the second property holds since if we for instance assume that $H(F|X_1) = 0$, we will have $I(X_1; X_2|Z) = I(X_1F; X_2|Z) = I(F; X_2|Z) + I(X_1; X_2|ZF) \geq I(X_1F; X_2F|ZF)$; the third property holds since $I(X_1; X_2|Z) \geq I(X_1'; X_2'|Z)$ whenever $H(X_1'|X_1) = H(X_2'|X_2) = 0$; the fourth property holds since $I(X_1; X_2|Z) - \big(H(X_1|Z) - H(X_1|X_2)\big) = I(X_1; Z|X_2) \geq 0$.

In order to find a new upper bound, therefore, one might seek a function that satisfies the above conditions. Given any such function, the proof would consist of verification of these properties. In order to find a new upper bound, one can think of a given function $\varphi(X_1; X_2\|Z)$ as a point in the set of all functions that satisfy the four properties, and try to slightly perturb the expression so that all the four properties remain satisfied. Theorems 4 and 5 that will be discussed later were derived using such a trial and error process.

4.4.2 Statement of the new converses

In this section we state the main results. We use the potential function method to prove them in section 4.4.3 and the appendices. Following the formal statement of each result, a brief informal discussion is provided to clarify the statement.

Sufficient conditions for being an upper bound on the SK capacity

Theorem 1. Let $\varphi(X_1; X_2; X_3; ...; X_m\|Z)$ be a real-valued function from the set of all probability distributions defined on $(X_1, X_2, X_3, ..., X_m, Z)$, where $X_1, X_2, ..., X_m$ and Z take values from arbitrary finite sets. $\varphi(X_1; X_2; X_3; ...; X_m\|Z)$ is an upper bound on $S(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}\|Z)$ if it satisfies all of the following properties

(1-5). $\varphi(X_1; X_2; X_3; ...; X_m \| Z)$ is an upper bound on

$$S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$$

if it satisfies properties (1-4).

1. For any natural number n:

$$n\varphi(X_1; X_2; ...; X_m \| Z) \geq \varphi(X_1^n; X_2^n; ...; X_m^n \| Z^n) \ ;$$

2. For any random variable F such that for some $1 \leq i \leq u$ we have $H(F|X_i) = 0$, it holds that:

$$\varphi(X_1; X_2; ...; X_m \| Z) \geq \varphi(X_1 F; X_2 F; ...; X_m F \| Z F) \ ;$$

3. For any random variables $X_1', X_2', ..., X_m'$ such that $H(X_i'|X_i) = 0$ for all $1 \leq i \leq m$, we have:

$$\varphi(X_1; X_2; ...; X_m \| Z) \geq \varphi(X_1'; X_2'; ...; X_m' \| Z) \ ;$$

4. $\varphi(X_1; X_2; ...; X_m \| Z) \geq H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i)$;

5. For any set of random variables $(M_1, M_2, ..., M_u)$ satisfying

$$\begin{aligned} &p(M_1, M_2, ..., M_u, X_1, X_2, ..., X_m, Z) = \\ &p(M_1)p(M_2)...p(M_u)p(X_1, X_2, ..., X_m, Z), \end{aligned} \tag{4.6}$$

we have:

$$\begin{aligned} &\varphi(X_1; X_2; ...; X_m \| Z) \geq \\ &\varphi(X_1 M_1; X_2 M_2; ...; X_u M_u; X_{u+1}; ...; X_m \| Z). \end{aligned}$$

Further, $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ itself satisfies all of these properties and
$S_{no-r}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ satisfies properties (1-4).

Discussion: The domain of φ in Theorem 1 is the set of *all* probability distributions on *all* products of $m+1$ finite sets. Condition 1 corresponds to the notion of taking blocks of observations. Condition 2 corresponds to the notion of terminal i communicating over the authenticated public channel. Condition 3 corresponds to the notion of each terminal choosing to ignore part of its available information. The right hand side of condition 4 is a choice of an easily proved and technically convenient lower bound on the secret key capacity; other such expressions could also have been used instead. Condition 5 is relevant to the case where the speaking terminals are allowed to independently randomize. ■

Sufficient conditions for being a lower bound on the CFO capacity

Theorem 2. Let $\psi(X_1; X_2; X_3; ...; X_m \| Z)$ be a real-valued function from the set of all probability distributions defined on $(X_1, X_2, X_3, ..., X_m, Z)$, where $X_1, X_2, ..., X_m$ and Z take values from arbitrary finite sets. $\psi(X_1; X_2; X_3; ...; X_m \| Z)$ is a lower bound on
$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ if it satisfies the following properties:

1. For any natural number n:

$$n\psi(X_1; X_2; ...; X_m \| Z) \leq \psi(X_1^n; X_2^n; ...; X_m^n \| Z^n);$$

2. For any random variable F such that for some $1 \leq i \leq u$ we have $H(F|X_i) = 0$, it holds that:

$$\psi(X_1; X_2; ...; X_m \| Z) \leq \psi(X_1 F; X_2 F; ...; X_m F \| Z F) + H(F|Z) \ ;$$

3. For any random variables $X_1', X_2', ..., X_m'$ such that $H(X_i'|X_i) = 0$ for all $1 \leq i \leq m$, we have:

$$\psi(X_1; X_2; ...; X_m \| Z) \leq \psi(X_1'; X_2'; ...; X_m' \| Z) + H(X_1 ... X_u | X_1' ... X_u' Z);$$

4. $\psi(X_1; X_2; ...; X_m \| Z)$ is bounded from above by

$$H(X_2 ... X_u | X_1 Z) + \sum_{i=2}^{m} H(X_1 | X_i).$$

Further, $T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ satisfies these properties.

Discussion: As in the case of φ of Theorem 1, here ψ should be thought of as defined on the set of *all* probability distributions on *all* products of $m+1$ finite sets. Condition 1 corresponds to the notion of forming blocks. Condition 2 corresponds to the notion of terminal i communicating over the authenticated public channel and paying the cost $H(F|Z)$ for this. Condition 3 corresponds to each terminal choosing to work with only part of its observation; intuitively the missing part can later be shared by incurring a conditional CFO rate of at most $H(X_1 X_2 ... X_u | X_1' X_2' ... X_u' Z)$. The right hand side of condition 4 is a convenient choice of an easily proved upper bound on the CFO rate; other such choices could also have been used instead. It should however be noted that the choice in condition 4 is concave over probability distributions and this was important in the proof of some additional properties of the CFO rate given in [21]. ■

Connection between the SK and the CFO capacities

Theorem 3. For any joint distribution $p(x_1, x_2, ..., x_m, z)$, we have:

$$S_{no-r}(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) + T(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) = H(X_1 X_2 ... X_u | Z).$$

Discussion: This establishes the equivalence between the problem of secret key generation and the problem of communication for omniscience by a neutral observer, generalizing the result of [12]. ■

New upper bound on the SK capacity

Theorem 4. For an arbitrary natural number t and finite random variables $J_1, J_2, ..., J_t$, arbitrarily jointly distributed with $X_1, X_2, ..., X_m$ and Z, $S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is bounded above by

$$\max_i (S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i)) +$$
$$S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ... J_t^{(s)} \| Z).$$

Discussion: To understand this claim, start with the case $t = 1$. One can think of J_1 as trying to define a "split" in the secret key capacity: one looks for a secret key among the m terminals that is secret from an entity that gets i.i.d. copies of J_1 (the first term on the right hand side of the upper bound) and then for a secret key that is shared by a terminal getting i.i.d. repetitions of J_1 (who is not allowed to talk) but is secret from the original eavesdropper (the second term on the right hand side of the upper bound). The claim is that the true secret key cannot exceed the sum of the two rates got in this "split" way.

The case of general t can be intuitively understood as follows: suppose there are t fictitious terminals, with the i-th terminal receiving i.i.d. copies of J_i. The secret key generated by the m original terminals is split into two components: one that is shared with *each* of the fictitious terminals $J_1, J_2, ..., J_t$, and one that is independent of *some* fictitious terminal J_i, $1 \leq i \leq t$. Assuming that S_1 is the secret key, we can write:

$$\frac{1}{n} H(S_1) = \frac{1}{n} \min_{1 \leq i \leq t} I(S_1; J_i^n) + \frac{1}{n} \max_{1 \leq i \leq t} H(S_1 | J_i^n). \tag{4.7}$$

One can argue that the term $\frac{1}{n} \min_{1 \leq i \leq t} I(S_1; J_i^n)$ represents a secret key rate that could be created in a way that is shared with *each* of the silent fictitious terminals $J_1, J_2, ..., J_t$; and the term $\frac{1}{n} \max_{1 \leq i \leq t} H(S_1 | J_i^n)$ represents a part S_1 that is independent of some J_i^n, $1 \leq i \leq t$.

Although the upper bound can be interpreted in the above way, we originally derived it following the trial and error process discussed in section 4.4.1. ■

Theorem 4 leads to some corollaries that appear to deserve separate statements.

Corollary 1. $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is bounded above by

$$\inf_J \big(S(X_1 J; X_2 J; ...; X_u J; (X_{u+1} J)^{(s)}; ...; (X_m J)^{(s)} \| J) + S(X_1 X_2 ... X_m; J^{(s)} \| Z) \big),$$

where the infimum is taken over finite random variables J arbitrarily jointly distributed with $X_1, X_2, ..., X_m$ and Z.

A single letter characterization of $S(X_1 J; X_2 J; ...; X_u J; (X_{u+1} J)^{(s)}; ...; (X_m J)^{(s)} \| J)$ is given in Theorem 6 of [23]. A single letter characterization for the second term $S(X_1 X_2 ... X_m; J^{(s)} \| Z)$, the one-way secret key capacity from $X_1 X_2 ... X_m$ to J in the presence of the eavesdropper Z, is also known (see [1, Theorem 1]). ■

Corollary 2. For $u = m = 2$, we have

$$\begin{aligned} S(X_1; X_2 \| Z) &\leq \inf_J \big(S(X_1; X_2 \| J) + S(X_1 X_2; J^{(s)} \| Z) \big) \\ &\leq \inf_J \big(I(X_1; X_2 | J) + S(X_1 X_2; J^{(s)} \| Z) \big). \end{aligned}$$

A single letter characterization for the second term $S(X_1 X_2; J^{(s)} \| Z)$ is known (see [1, Theorem 1]). This bound is no worse than the Renner-Wolf double intrinsic information upper bound, and furthermore there exists a joint distribution on X_1, X_2 and Z for which the new bound is strictly tighter than the Renner-Wolf upper bound. ■

A variant of Corollary 1 can be proved by the verification technique that was used to prove Theorem 1. This is stated as the next result.

Theorem 5. Let $\mathbb{R}_{\geq 0}$ denote the set of non-negative real numbers. Given any function $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}_{\geq 0}$, define the *$f$-one-way secret key capacity* as

$$S_{f-one-way}(X; Y^{(s)} \| Z) = \sup_{V \to U \to X \to Y Z} [f(H(U|ZV)) - f(H(U|YV))].$$

Then for any arbitrary strictly increasing convex function $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}_{\geq 0}$, and for any finite random variables J arbitrarily jointly distributed with $X_1, X_2, ..., X_m$ and Z, the secret key capacity $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is bounded above by

$$f^{-1}\{ f(S(X_1; X_2; ...; X_u; (X_{u+1})^{(s)}; ...; (X_m)^{(s)} \| J)) + S_{f-one-way}(X_1 X_2 ... X_m; J^{(s)} \| Z) \}.$$

This upper bound is in turn bounded above by

$$f^{-1}\big(f(S(X_1 J; ...; X_u J; (X_{u+1} J)^{(s)}; ...; (X_m J)^{(s)} \| J)) + S_{f-one-way}(X_1 ... X_m; J^{(s)} \| Z) \big).$$

Discussion: The f-one-way secret key capacity can be viewed as a generalization of the one-way key capacity (also known as the forward key capacity) (see [1, Theorem 1,]) since the former reduces to the latter in the special case of $f(x) = x$. The upper bound given in Theorem 5 reduces to that of Corollary 1 in the special case of $f(x) = x$. We don't know if this bound strictly improves that of Corollary 1. The weaker form of the bound given in the statement of the theorem is useful because there is a single letter characterization for $S(X_1J; X_2J; ...; X_uJ; (X_{u+1}J)^{(s)}; ...; (X_mJ)^{(s)} \| J)$, given in Theorem 6.

The two upper bounds given in this theorem can be understood as perturbations of those given in Theorem 4 and its corollaries. This upper bound was obtained by the trial and error process described at the end of section 4.4.1. ■

4.4.3 Proofs

Proof of Theorem 1: Fix a probability distribution $p(x_1, x_2, ..., x_m, z)$ on $\mathcal{X}_1 \times \mathcal{X}_2 \times ... \times \mathcal{X}_m \times \mathcal{Z}$ where $\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_m, \mathcal{Z}$ are finite sets. We begin by proving that $\varphi(X_1; X_2; X_3; ...; X_m \| Z)$ is an upper bound on $S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ if it satisfies properties (1-4).

For every positive δ and ϵ, one can find some secret key generation scheme SK(n, ϵ, S_1, S_2, S_3,..., S_m, $\mathbf{C}$) whose key rate is within δ of
$S_{no-r}^{\epsilon}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$. We have:

$$
\begin{aligned}
& n\varphi(X_1; X_2; X_3; ...; X_m \| Z) \geq \\
& \varphi(X_1^n; X_2^n; X_3^n; ...; X_m^n \| Z^n) && (4.8)\\
& \geq \varphi(X_1^n C_1; X_2^n C_1; ...; X_m^n C_1 \| Z^n C_1) && (4.9)\\
& \geq \varphi(X_1^n C_1 C_2; X_2^n C_1 C_2; ...; X_m^n C_1 C_2 \| Z^n C_1 C_2) && (4.10)\\
& ... \geq \varphi(X_1^n \mathbf{C}; X_2^n \mathbf{C}; .....; X_m^n \mathbf{C} \| Z^n \mathbf{C}) && (4.11)\\
& \geq \varphi(S_1; S_2; ...; S_m \| Z^n \mathbf{C}) && (4.12)\\
& \geq H(S_1 | Z^n \mathbf{C}) - \sum_{j=2}^{m} H(S_1 | S_j) && (4.13)\\
& \geq n S_{no-r}^{\epsilon}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)\} \\
& - n\delta - (m-1)[h(\epsilon) + \epsilon n \log \prod_{i=1}^{m} |\mathcal{X}_i|]. && (4.14)
\end{aligned}
$$

Inequalities (4.8), (4.9), (4.10), (4.11), (4.12), (4.13) are true respectively because of the properties 1, 2, 2, 2, 3, 4. Inequality (4.14) holds because of the Fano inequality and the fact that the secret key rate of SK(n, ϵ, S_1, S_2, S_3,..., S_m, $\mathbf{C}$) is within δ of

$$S_{no-r}^{\epsilon}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z).$$

Therefore we get

$$\varphi(X_1; X_2; X_3; ...; X_m \| Z) \geq$$
$$S^{\epsilon}_{no-r}(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)\} - \delta - (m-1)[\frac{h(\epsilon)}{n} + \epsilon \log \prod_{i=1}^{m} |\mathcal{X}_i|].$$

We get the desired result by letting ϵ and δ converge to zero.

Next, in order to show that $\varphi(X_1; X_2; X_3; ...; X_m \| Z)$ would be an upper bound on

$$S(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$$

if it satisfies all the five properties, we note that for any M_1, M_2, ..., M_u (satisfying equation (4.6)),

$$\varphi(X_1; X_2; X_3; ...; X_m \| Z) \geq$$
$$\varphi(X_1 M_1; X_2 M_2; ...; X_u M_u; X_{u+1}; ...; X_m \| Z) \geq \tag{4.15}$$
$$S_{no-r}(X_1 M_1; ...; X_u M_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z). \tag{4.16}$$

Inequality (4.15) is true because of the property 5, and inequality (4.16) holds because φ satisfies the first four properties. Therefore for any M_1, M_2, ..., M_u satisfying equation (4.6), we have

$$\varphi(X_1; X_2; X_3; ...; X_m \| Z) \geq$$
$$S_{no-r}(X_1 M_1; X_2 M_2; ...; X_u M_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z),$$

implying that φ is an upper bound on $S(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$.

Lastly, we need to show that

$$S(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$$

and

$$S_{no-r}(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$$

themselves satisfy the five (respectively the first four) properties.

$S(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ satisfies properties 1, 2, 3 and 5 and $S_{no-r}(X_1; X_2; X_3; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ satisfies properties 1, 2 and 3 because every valid SK generation scheme for the right hand side of the inequalities can be converted to one for the left hand side. In 1, the terminals observing $(X_1, X_2, ..., X_m)$ can first observe n i.i.d. copies of their random variables and then simulate the SK generation scheme for the right hand side. In 2, they can take i.i.d repetitions of F by the i-th terminal as the first non-trivial communication and then simulate the SK generation scheme for the right hand side. In 3, they can create X_i''s first and then simulate

the SK generation scheme for the right hand side. In 5, the terminals $1 \leq i \leq u$ can respectively create $M_1, M_2, \ldots, M_u$ first and then simulate the SK generation scheme for the right hand side.

For property 4, note that both the terms $S(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ and $S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ are greater than or equal to the one-way secret key capacity from X_1 to $X_2, X_3, ..., X_m$ in the presence of Z, which in turn is greater than or equal to $\min_{2 \leq i \leq m}(I(X_1; X_i) - I(X_1; Z))$. This expression is greater than or equal to the right hand side of 4. ■

Proof of Theorem 2: Fix a probability distribution $p(x_1, x_2, ..., x_m, z)$ on $\mathcal{X}_1 \times \mathcal{X}_2 \times ... \times \mathcal{X}_m \times \mathcal{Z}$ where $\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_m, \mathcal{Z}$ are finite sets. For every $\delta > 0$ and $\epsilon > 0$, one can find a CFO strategy (n, ϵ, T_1, T_2, T_3, ..., T_m, $\mathbf{C}$), whose conditional CFO rate is within δ of $T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$. We have:

$$
\begin{aligned}
& n\psi(X_1; X_2; X_3; ...; X_m \| Z) \leq \\
& \psi(X_1^n; X_2^n; X_3^n; ...; X_m^n \| Z^n) && (4.17)\\
& \leq \psi(X_1^n C_1; X_2^n C_1; ...; X_m^n C_1 \| Z^n C_1) + H(C_1 | Z^n) && (4.18)\\
& \leq \psi(X_1^n C_1 C_2; X_2^n C_1 C_2; ...; X_m^n C_1 C_2 \| Z^n C_1 C_2) + \\
& H(C_1 C_2 | Z^n) && (4.19)\\
& ... \leq \psi(X_1^n \mathbf{C}; X_2^n \mathbf{C}; ...; X_m^n \mathbf{C} \| Z^n \mathbf{C}) + H(\mathbf{C} | Z^n) && (4.20)\\
& \leq \psi(T_1; T_2; ...; T_m \| Z^n \mathbf{C}) + \\
& H(X_1^n X_2^n ... X_u^n | T_1 T_2 ... T_u Z^n) + H(\mathbf{C} | Z^n) && (4.21)\\
& \leq H(T_2 ... T_u | T_1 Z^n \mathbf{C}) + \\
& \sum_{j=2}^{m} H(T_1 | T_j) + \\
& H(X_1^n X_2^n ... X_u^n | T_1 T_2 ... T_u Z^n) + H(\mathbf{C} | Z^n) && (4.22)\\
& \leq h(\epsilon) + \epsilon \cdot n \log \prod_{i=1}^{u} |\mathcal{X}_i| + \\
& (m-1)[h(\epsilon) + \epsilon \cdot n \log \prod_{i=1}^{m} |\mathcal{X}_i|] + n\epsilon \\
& + nT^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) + n\delta. && (4.23)
\end{aligned}
$$

Inequalities (4.17), (4.18), (4.19), (4.20), (4.21), (4.22) are true respectively because of the properties 1, 2, 2, 2, 3, 4. Inequality (4.23) is true due to the Fano inequality, and the fact that the conditional CFO rate of (n, ϵ, T_1, T_2, T_3, ..., T_m, $\mathbf{C}$) is within δ of $T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$.

Therefore we get

$$\psi(X_1; X_2; X_3; ...; X_m \| Z) \leq$$
$$T^{\epsilon}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) + \delta + \frac{m}{n}[h(\epsilon) + \epsilon \cdot n \log \prod_{i=1}^{m} |\mathcal{X}_i|] + \epsilon.$$

The theorem is proved by taking the limit as ϵ and δ go to zero.
$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ itself satisfies the four properties.

For property 1, note that the terminals observing $(X_1, X_2, ..., X_m)$ can first observe n i.i.d. copies of their random variables and then pretend that they are in the situation on the right hand side of 1. For property 2, they can take i.i.d repetitions of F by the i-th terminal as the first non-trivial communication, and then pretend that they are in the situation corresponding to the first term on the right hand side of 2. The total cost would be the sum of $H(F|Z)$ and the remaining conditional CFO rate of the left hand side.

Regarding property 3, we first intuitively sketch the proof: one possible communication for omniscience for $(X_1, X_2, ..., X_m, Z)$ is to first conduct a communication for omniscience for $(X_1', X_2', ..., X_m', Z)$. The terminal who wants to become omniscient, Charles, would be able to approximately learn $(X_1', X_2', ..., X_u', Z)$ with the conditional CFO rate of $T(X_1'; X_2'; X_3'; ...; X_u'; X_{u+1}^{'(s)}; ...; X_m^{'(s)} \| Z)$. If Charles exactly knew $(X_1', X_2', ..., X_u', Z)$, the u terminals could use a Slepian-Wolf type communication scheme to reveal
$H(X_1X_2...X_u|X_1'X_2'...X_u'Z)$ bits on the public channel, thereby enabling Charles to receive these bits as a common randomness and become omniscient. The total conditional CFO rate is no more than

$$T(X_1'; X_2'; X_3'; ...; X_u'; X_{u+1}^{'(s)}; ...; X_m^{'(s)} \| Z) + H(X_1X_2...X_u|X_1'X_2'...X_u'Z).$$

Even though Charles does not exactly know $(X_1', X_2', ..., X_u'; Z)$, this Slepian-Wolf algorithm still works.

We now prove the property more precisely. Fix $\epsilon > 0$ and $\delta > 0$.
$T^{\epsilon}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ is defined as the liminf of the minimal conditional CFO rate as n converges infinity. Therefore we can find a large enough n such that the following requirements are satisfied:

- There is a CFO strategy (n, ϵ, T_1, T_2, T_3, ..., T_m, $\mathbf{C}$) whose conditional CFO rate is within δ of $T^{\epsilon}(X_1'; X_2'; X_3'; ...; X_u'; X_{u+1}^{'(s)}; ...; X_m^{'(s)} \| Z)$;
- There is a communication with the total entropy of at most

  $$n(H(X_1....X_u|X_1'X_2'...X_u'Z) + \delta)$$

  for the following Slepian-Wolf type problem: u terminals having i.i.d. repetitions of X_1, X_2, ..., X_u want to transmit their information to a receiver who has

i.i.d. repetitions of $X_1'X_2'...X_u'Z$ as side information. In this Slepian-Wolf type problem, it is desired to have $\frac{1}{n}H(X_1^n....X_u^n|X_1'^nX_2'^n...X_u'^nZ^n$, Communication$) \leq \delta$.

The terminals first follow CFO(n, ϵ, T_1, T_2, T_3, ..., T_m, $\mathbf{C}$) and then the u terminals X_1, X_2, ..., X_u insert the corresponding communications for the Slepian-Wolf problem on the public channel. Let $\mathbf{C}'$ denote the *whole* communication ($\mathbf{C}'$ includes $\mathbf{C}$).

We prove that the CFO(n, $\epsilon+\delta$, $T_1\mathbf{C}'$, $T_2\mathbf{C}'$, ..., $T_m\mathbf{C}'$, $\mathbf{C}'$) is valid and further the conditional CFO rate is less than or equal to

$$\begin{aligned}&T^{\epsilon}(X_1';X_2';X_3';...;X_u';X_{u+1}^{'(s)};...;X_m^{'(s)}\|Z)\\&+H(X_1....X_u|X_1'X_2'...X_u'Z)+2\delta.\end{aligned}$$

Using the inequality

$$H(X|YW)\leq H(X|ZW)+H(Z|YW)$$

for any four random variables X, Y, Z, W, we have

$$\begin{aligned}&\frac{1}{n}H(X_1^n....X_u^n|T_1\mathbf{C}'Z^n)\leq\\&\frac{1}{n}H(X_1^n....X_u^n|X_1'^nX_2'^n...X_u'^n\mathbf{C}'Z^n)+\\&\frac{1}{n}H(X_1'^nX_2'^n...X_u'^n|T_1\mathbf{C}'Z^n)\leq\delta+\epsilon.\end{aligned}$$

The other requirements for the CFO to be valid can be easily checked.

The conditional CFO rate, i.e. $\frac{1}{n}H(\mathbf{C}'|Z^n)$ is bounded above by

$$\begin{aligned}&\frac{1}{n}H(\mathbf{C}|Z^n)+\frac{1}{n}H(\mathbf{C}'|\mathbf{C})\leq\\&T^{\epsilon}(X_1';X_2';...;X_u';X_{u+1}^{'(s)};...;X_m^{'(s)}\|Z)\\&+\delta+H(X_1X_2...X_u|X_1'X_2'...X_u'Z)+\delta.\end{aligned}$$

For property 4, the idea is that, in the first phase, the first terminal transmits messages to the other terminals enabling them to find X_1 with probability close to 1. The entropy of the communication from the first terminal to the i-th terminal would be roughly $n\cdot H(X_1|X_i)$, and this is an upper bound for the conditional entropy of the communication given Z^n. Now, since all the terminals can include X_1 as a common randomness, Charles would be able to calculate X_1Z. In the second stage, the first u terminals reveal roughly $n\cdot H(X_1X_2...X_u|X_1Z)$ bits on the public channel. Since this now becomes a common randomness, it can be passed to Charles, enabling him to learn $X_1X_2...X_u$. The total conditional CFO rate of this communication scheme

would be bounded above by $\sum H(X_i|X_1) + H(X_1X_2...X_u|X_1Z)$ on a per observation basis, asymptotically as $n \to \infty$. ■

Proof of Theorem 3: It can be easily shown that $\psi(X_1; X_2; X_3; ...; X_m \| Z)$ satisfies the four properties of Theorem 2 if and only if $H(X_1X_2...X_u|Z) - \psi(X_1; X_2; X_3; ...; X_m \| Z)$ satisfies the four properties of Theorem 1.

$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ itself satisfies the four properties of Theorem 2. Hence

$$H(X_1X_2...X_u|Z) - T(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) \geq$$
$$S_{no-r}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z).$$

Further since $S_{no-r}(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ itself satisfies the four properties of Theorem 1, we get

$$H(X_1X_2...X_u|Z) -$$
$$S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) \leq$$
$$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z).$$

Therefore

$$H(X_1X_2...X_u|Z) =$$
$$S_{no-r}(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z) +$$
$$T(X_1; X_2; X_3; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z).$$

■

Proof of Theorem 4: Theorem 1 allows one to systematically prove the correctness of the upper bound by treating it as an algebraic expression satisfying certain properties. More specifically, we simply need to prove that

$$\varphi(X_1; X_2; X_3; ...; X_m \| Z) =$$
$$\inf_{J_1, J_2, ..., J_t} [\max_i (S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i)) +$$
$$S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z)]$$

satisfies the five properties of Theorem 1, where the infimum is taken over finite random variables $J_1, J_2, ..., J_t$ arbitrarily jointly distributed with $X_1, X_2, ..., X_m$ and Z.

Property *1*: It is enough to prove that for any $J_1, J_2, ..., J_t$, there exist $J_1', J_2', ..., J_t'$

such that:

$$
\begin{aligned}
& n \left\{ \max_i (S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i)) + \right. \\
& \left. S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z) \right\} \\
& \geq \max_i (S(X_1^n; X_2^n; ...; X_u^n; (X_{u+1}^n)^{(s)}; ...; (X_m^n)^{(s)} \| J_i')) + \\
& S(X_1^n; ...; X_u^n; (X_{u+1}^n)^{(s)}; ...; (X_m^n)^{(s)}; J_1^{'(s)}; ...; J_t^{'(s)} \| Z^n).
\end{aligned}
$$

We take J_i' to be J_i^n for $1 \leq i \leq t$. The inequality holds since the secret key function itself satisfies the first property of Theorem 1.

Property *2*: Let $H(F \mid X_i) = 0$, where $1 \leq i \leq u$. It is enough to prove that for any $J_1, J_2, ..., J_t$, there exist $J_1', J_2', ..., J_t'$ such that:

$$
\begin{aligned}
& \max_i (S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i)) + \\
& S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z) \\
& \geq \max_i (S(X_1F; X_2F; ...; X_uF; X_{u+1}^{(s)}F; ...; X_m^{(s)}F \| J_i')) + \\
& S(X_1F; ...; X_uF; (X_{u+1}F)^{(s)}; ...; (X_mF)^{(s)}; J_1^{'(s)}; ...; J_t^{'(s)} \| ZF).
\end{aligned}
$$

We take J_i' to be J_iF for $1 \leq i \leq t$. The inequality holds since the secret key function itself satisfies the second property of Theorem 1.

The proof for property *3* is similar to that for the two preceding properties.

Property *4*: It is enough to prove that for any $J_1, J_2, ..., J_t$,

$$
\begin{aligned}
& \max_i (S(X_1; X_2; ...; X_u; X_{u+1}^{(s)} ...; X_m^{(s)} \| J_i)) + \\
& S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z)
\end{aligned}
$$

is greater than or equal to $H(X_1|Z) - \sum_{k=2}^{m} H(X_1|X_k)$.

We have:

$$
\begin{aligned}
& S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z) \geq \\
& S(X_1; X_2^{(s)}; X_3^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z) \geq \\
& \min(\min_{1 \leq i \leq t} I(X_1; J_i), \min_{2 \leq k \leq m} I(X_1; X_k)) \\
& - I(X_1; Z).
\end{aligned}
$$

Since the secret key function itself satisfies the fourth property of Theorem 1, we have:

$$
\begin{aligned}
& S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i) \geq \\
& H(X_1) - I(X_1; J_i) - \sum_k H(X_1|X_k).
\end{aligned}
$$

This implies that

$$\max_i S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i) \geq$$
$$H(X_1) - \min_i I(X_1; J_i) - \sum_{k=2}^{m} H(X_1|X_k).$$

There are two cases:

- If $\min_i I(X_1; J_i) \leq \min_k I(X_1; X_k)$:
  We have:

$$S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z) \geq$$
$$\min_i I(X_1; J_i) - I(X_1; Z) =$$
$$H(X_1) - \max_i H(X_1|J_i) - I(X_1; Z).$$

  Therefore

$$\max_i S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J_i) +$$
$$S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; ...J_t^{(s)} \| Z) \geq$$
$$H(X_1) - I(X_1; Z) - \sum_{k=2}^{m} H(X_1|X_k) =$$
$$H(X_1|Z) - \sum_{k=2}^{m} H(X_1|X_k).$$

- If $\min_i I(X_1; J_i) > \min_{2 \leq k \leq m} I(X_1; X_k)$:
  We have:

$$S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}; J_1^{(s)}; J_2^{(s)}; ...J_t^{(s)} \| Z) \geq$$
$$\min_{2 \leq k \leq m} I(X_1; X_k) - I(X_1; Z) \geq$$
$$H(X_1) - \sum_{k=2}^{m} H(X_1|X_k) - I(X_1; Z) =$$
$$H(X_1|Z) - \sum_{k=2}^{m} H(X_1|X_k).$$

Property *5*: It is enough to prove that for any $J_1, J_2, ..., J_t$, there exists $J_1', J_2', ..., J_t'$

such that:

$$\max_i(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i))+$$
$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{(s)};J_2^{(s)};...J_t^{(s)}\|Z)\geq$$
$$\max_i(S(X_1M_1;X_2M_2;...;X_uM_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J_i'))+$$
$$S(X_1M_1;...;X_uM_u;X_{u+1}^{(s)};...;X_m^{(s)};J_1^{'(s)};...J_t^{'(s)}\|Z).$$

We define $J_1', J_2', ..., J_t'$ such that for every $x_1, ..., x_m, z, j_1, ..., j_t$,

$$p(J_1'=j_1,...,J_t'=j_t|X_1=x_1,...,X_m=x_m,Z=z)=$$
$$p(J_1=j_1,...,J_t=j_t|X_1=x_1,...,X_m=x_m,Z=z),$$

and

$$p(M_1,...,M_u,X_1,...,X_m,Z,J_1'...,J_t')=$$
$$p(M_1)p(M_2)...p(M_u)p(X_1,...,X_m,Z,J_1'...,J_t').$$

The proof is finished by noting that the secret key function itself satisfies the fifth property of Theorem 1. ■

Proof of Corollary 1. We get the desired result by applying Theorem 4 for the case of $t=1$ and noting that

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J)\leq$$
$$S(X_1J;X_2J;...;X_uJ;(X_{u+1}J)^{(s)};...;(X_mJ)^{(s)}\|J)$$

and

$$S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)};J^{(s)}\|Z)\leq$$
$$S(X_1X_2...X_m;J^{(s)}\|Z).$$

■

Proof of Corollary 2. This is a straightforward special case of Corollary 1. In the case of two terminals we have:

$$S(X_1;X_2\|Z)\leq$$
$$\inf_J\left(S(X_1;X_2\|J)+S(X_1X_2;J^{(s)}\|Z)\right)\leq$$
$$\inf_J\left(S(X_1J;X_2J\|J)+S(X_1X_2;J^{(s)}\|Z)\right).$$

The infimum is taken over all finite random variables J arbitrarily jointly distributed with (X_1, X_2, Z).

We get the desired upper bound by noting that $S(X_1J;X_2J\|J)=I(X_1;X_2|J)$.

$\inf_J I(X_1;X_2|J)+S(X_1X_2;J^{(s)}\|Z)$ could be further bounded above by

$$\inf_J \big(I(X_1;X_2|J)+I(X_1X_2;J|Z)\big).$$

One can use the strengthened Carathéodory theorem of Fenchel to get the cardinality bound of $|\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}|$ on the size of the alphabet of J. Therefore the infimum over finite random variables J is a minimum. It is enough to prove that $\min_J \big(I(X_1;X_2|J)+I(X_1X_2;J|Z)\big)$ strictly improves the Renner-Wolf double intrinsic information upper bound. In order to prove that the new bound is not worse than the double intrinsic information bound, it is sufficient to prove that for any random variable U there is a random variable J such that $I(X_1;X_2|J)+I(X_1X_2;J|Z)\leq H(U)+\min_{\overline{Z}:X_1X_2\rightarrow ZU\rightarrow\overline{Z}} I(X_1;X_2|\overline{Z})$. Choosing $J=\overline{Z}$, we will have $I(X_1;X_2|J)=I(X_1;X_2|\overline{Z})$ and also

$$I(X_1X_2;J|Z)=I(X_1X_2;U|Z)-I(X_1X_2;U|ZJ)\leq I(X_1X_2;U|Z)\leq H(U).$$

Therefore $\min_J \big(I(X_1;X_2|J)+I(X_1X_2;J|Z)\big)$ is no worse than the double intrinsic information bound. Appendix I of section 4.4.4 contains an example for which $\min_J \big(I(X_1;X_2|J)+I(X_1X_2;J|Z)\big)$ is strictly better than the double intrinsic information bound. ■

Proof of Theorem 5: Take an arbitrary strictly increasing convex function $f:\mathbb{R}_{\geq 0}\mapsto\mathbb{R}_{\geq 0}$. Without loss of generality we can assume $f(0)=0$, because for any positive constant c, $g(x)=f(x)+c$ satisfies the following equations:

- $S_{g-one-way}(X;Y^{(s)}\|Z)=S_{f-one-way}(X;Y^{(s)}\|Z)$;
- $g^{-1}\big(g(a)+b\big)=f^{-1}\big(f(a)+b\big)$ for any non-negative a and b.

Since

$$S(X_1J;X_2J;...;X_uJ;(X_{u+1}J)^{(s)};...;(X_mJ)^{(s)}\|J)\geq$$
$$S(X_1;X_2;...;X_u;(X_{u+1})^{(s)};...;(X_m)^{(s)}\|J),$$

and f is increasing, it suffices to prove the first bound in the statement of the theorem. In order to show this, it suffices to verify the five conditions of Theorem 1 for

$$\inf_J f^{-1}\{f(S(X_1;...;X_u;(X_{u+1})^{(s)};...;(X_m)^{(s)}\|J)) \tag{4.24}$$
$$+S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)\}. \tag{4.25}$$

This is done in Appendix II of section 4.4.4. The proof uses the standard fact that the convexity of f implies that it is continuous, and that $f(x+a)-f(x)$ is an increasing function in x for any fixed a. ■

Table 4.1: Joint probability distribution of X and Y

	X			
Y	0	1	2	3
0	$\frac{1}{8}$	$\frac{1}{8}$	0	0
1	$\frac{1}{8}$	$\frac{1}{8}$	0	0
2	0	0	$\frac{1}{4}$	0
3	0	0	0	$\frac{1}{4}$

4.4.4 Appendices

Appendix I

In this appendix we prove the existence of a joint probability distribution on X, Y, Z for which the new bound is strictly better than the double intrinsic information bound. In this appendix, we use the notation $\mathcal{L}(X)$ to refer to the law of the random variable X.

We need the following Lemmas which we will prove at the end of this appendix.

Lemma A1.1 Assume that $\inf_U[H(U) + I(X;Y \downarrow ZU)] = \min_J[I(X;Y|J) + I(XY;J|Z)]$, then there is a sequence of random variables U_i, $i = 1, 2, ...$ taking values in finite sets $\mathcal{U}_i$, and a sequence of positive real numbers δ_i converging to zero, such that:

1. $H(U_i) + I(X;Y \downarrow ZU_i) \to \inf_U[H(U) + I(X;Y \downarrow ZU)]$ as $i \to \infty$;
2. $H(U_i|XYZ) \to 0$ as $i \to \infty$;
3. $I(U_i;Z) \to 0$ as $i \to \infty$;
4. $|p(U_i = u_i|X = x, Y = y, Z = z) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i \ \forall u_i \in \mathcal{U}_i, \ (x,y,z) : \ p(x,y,z) > 0$;
5. The total variation distance $d(\mathcal{L}(U_i|Z = z_1), \mathcal{L}(U_i|Z = z_2)) \to 0$ as $i \to \infty \ \ \forall z_1, z_2 : \ p(Z = z_1) > 0, p(Z = z_2) > 0$.

■

Lemma A1.2 Continuity of the intrinsic information $I(X;Y \downarrow Z)$: $\forall \xi > 0, \exists \delta > 0$ such that for all random variables T having entropy less than δ, we have

$$|I(X;Y \downarrow ZT) - I(X;Y \downarrow Z)| < \xi.$$

■

We will perturb the example provided by Renner and Wolf in order to prove that their bound is better than the intrinsic information bound. Table (4.1) shows the joint probability distribution between X and Y in that example. Z is defined as:

$$Z = \begin{cases} (X + Y) \mod 2 & \text{if } X \in \{0,1\}, \\ X \mod 2 & \text{if } X \in \{2,3\}. \end{cases}$$

Renner and Wolf proved that for the choice of $U = \lfloor \frac{X}{2} \rfloor$, one has:

$$I(X;Y \downarrow Z) = \frac{3}{2}, \qquad I(X;Y \downarrow ZU) = 0.$$

And therefore their bound would be less than or equal to $H(U) + I(X;Y \downarrow ZU) = 1$, while $I(X;Y \downarrow Z) = \frac{3}{2} > 1$.

Let V be a binary random variable, satisfying the $V \to U \to XYZ$ Markov property and defined as follows:

$$\begin{aligned} p(U=0|V=0) &= \alpha_1, & p(U=1|V=0) &= 1-\alpha_1, \\ p(U=0|V=1) &= \alpha_2, & p(U=1|V=1) &= 1-\alpha_2. \end{aligned}$$

Clearly, there exist α_1 and α_2 such that the intersection of

$$\Big\{0, \alpha_1, 1-\alpha_1, \frac{1}{2}\alpha_1, 1-\frac{1}{2}\alpha_1, 1\Big\}$$

and

$$\Big\{0, \alpha_2, 1-\alpha_2, \frac{1}{2}\alpha_2, 1-\frac{1}{2}\alpha_2, 1\Big\}$$

is the set $\big\{0,1\big\}$. If the constraint is not satisfied for some α_1 and α_2, then it would be enough to perturb α_1 or α_2 by a tiny amount.

Let $\widetilde{X} = X, \widetilde{Y} = Y, \widetilde{Z} = (Z,V)$. We would like to prove that the new bound is strictly better than the double intrinsic information bound for the triple $(\widetilde{X},\ \widetilde{Y}, \widetilde{Z})$.

We have:

$$\begin{aligned} &p(X=x, Y=y|\widetilde{Z}=(0,0)) = \\ &\frac{1}{2}\alpha_1 \mathbf{1}[(x,y)=(0,0)] + \frac{1}{2}\alpha_1 \mathbf{1}[(x,y)=(1,1)] + \\ &(1-\alpha_1)\mathbf{1}[(x,y)=(2,2)], \end{aligned}$$

and

$$\begin{aligned} &p(X=x, Y=y|\widetilde{Z}=(0,1)) = \\ &\frac{1}{2}\alpha_2 \mathbf{1}[(x,y)=(0,0)] + \frac{1}{2}\alpha_2 \mathbf{1}[(x,y)=(1,1)] + \\ &(1-\alpha_2)\mathbf{1}[(x,y)=(2,2)]. \end{aligned}$$

Assuming that the new bound is not better than the double intrinsic information bound, we can apply Lemma A1.1 to get a sequence U_i having the five properties given in Lemma A1.1. Using the property 4, we have:

$$|p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0)) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i;$$
$$|p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0)) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i;$$
$$|p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0)) - \frac{1}{2}| \geq \frac{1}{2} - \delta_i.$$

Therefore $p(U_i = u|\widetilde{Z} = (0,0))$ is within the $3\delta_i$ distance of a point in the set $\{0, \alpha_1, 1-\alpha_1, \frac{1}{2}\alpha_1, 1-\frac{1}{2}\alpha_1, 1\}$.

Similarly, $p(U_i = u|\widetilde{Z} = (0,1))$ is within the $3\delta_i$ distance of a point in the set $\{0, \alpha_2, 1-\alpha_2, \frac{1}{2}\alpha_2, 1-\frac{1}{2}\alpha_2, 1\}$.

Since the total variation distance between the distribution of $\mathcal{L}(U_i|\widetilde{Z} = (0,0))$ and $\mathcal{L}(U_i|\widetilde{Z} = (0,1))$ converges to zero, and the intersection of the sets $\{0, \alpha_2, 1-\alpha_2, \frac{1}{2}\alpha_2, 1-\frac{1}{2}\alpha_2, 1\}$ and $\{0, \alpha_1, 1-\alpha_1, \frac{1}{2}\alpha_1, 1-\frac{1}{2}\alpha_1, 1\}$ is just $\{0,1\}$, one can conclude that there is some natural number i_0 such that for $\forall\ i > i_0,\ \forall u \in \mathcal{U}_i$, the probabilities

$p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0))$,
$p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0))$,
$p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0))$
are either all less than $\frac{1}{2}$ or all greater than $\frac{1}{2}$.

Let $h(x) = x\log(\frac{1}{x})$. We would like to bound from above the entropy of the distribution of $\mathcal{L}(U_i|\widetilde{Z} = (0,0))$ in terms of $h\big(p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0))\big)$, $h\big(p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0))\big)$, $h\big(p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0))\big)$. Since entropy is a concave function, we cannot use Jensen's inequality to bound from above $H\big(\mathcal{L}(U_i|\widetilde{Z} = (0,0))\big)$, which is a convex combination of these probabilities. However, noting that the three mentioned probabilities are all on the same side of $\frac{1}{2}$, and that $h(x)$ is monotonic for all $x < \frac{1}{2}$ and for all $x > \frac{1}{2}$, we can derive the following bound:

$$\begin{aligned}
&H\big(\mathcal{L}(U_i|\widetilde{Z} = (0,0)))\big) < \\
&\max\Big(h\big(p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0))\big), \\
&\qquad h\big(p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0))\big), \\
&\qquad h\big(p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0))\big)\Big) < \\
&\qquad h\big(p(U_i = u|\widetilde{X} = 0, \widetilde{Y} = 0, \widetilde{Z} = (0,0))\big) + \\
&\qquad h\big(p(U_i = u|\widetilde{X} = 1, \widetilde{Y} = 1, \widetilde{Z} = (0,0))\big) + \\
&\qquad h\big(p(U_i = u|\widetilde{X} = 2, \widetilde{Y} = 2, \widetilde{Z} = (0,0))\big)
\end{aligned}$$

Therefore

$$\sum_u h\big(p(U_i|\widetilde{Z}=(0,0))\big) <$$
$$\sum_u h\big(p(U_i=u|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0))\big)+$$
$$\sum_u h\big(p(U_i=u|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0))\big)+$$
$$\sum_u h\big(p(U_i=u|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0))\big) =$$
$$H(U_i|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0))+$$
$$H(U_i|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0))+$$
$$H(U_i|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0)).$$

Since the terms

$$H(U_i|\widetilde{X}=0,\widetilde{Y}=0,\widetilde{Z}=(0,0)),$$
$$H(U_i|\widetilde{X}=1,\widetilde{Y}=1,\widetilde{Z}=(0,0)),$$
$$H(U_i|\widetilde{X}=2,\widetilde{Y}=2,\widetilde{Z}=(0,0))$$

converge to zero as i converges to infinity, we have $H(U_i|\widetilde{Z}=(0,0))\to 0$ as $i\to\infty$. Similarly, $H(U_i|\widetilde{Z}=(0,1))\to 0$, etc. Thus, $H(U_i|\widetilde{Z})\to 0$ as $i\to\infty$.

But property 3 of Lemma A1.1 states that $I(U_i;\widetilde{Z})\to 0$ as $i\to\infty$. Thus, we conclude that $H(U_i)\to 0$ as $i\to\infty$.

Hence, the limit of $H(U_i)+I(X;Y\downarrow ZU_i)$ is the same as that of $I(X;Y\downarrow ZU_i)$. Property 1 of Lemma A1.1 states that the series converges to the double intrinsic information upper bound which is assumed to be equal to $\min_J[I(\widetilde{X};\widetilde{Y}|J)+I(\widetilde{X}\widetilde{Y};J|\widetilde{Z})]$.

Evaluating the expression at $J=\widetilde{Z}U$, gives us

$$0+I(XY;UZV|ZV)=I(XY;U|ZV)\le 1.$$

Therefore we should have: $\lim_{i\to\infty} I(X;Y\downarrow ZU_i)\le 1$. On the other hand, Renner and Wolf have shown that $I(X;Y\downarrow Z)=\frac{3}{2}$. But this is in contradiction with Lemma A1.2 noting that $H(U_i)\to 0$ as $i\to\infty$. ■

Now, we prove the Lemmas mentioned at the beginning of this appendix.

Proof of Lemma A1.1: Take a sequence U_1, U_2, ... such that

$$H(U_i)+I(X;Y\downarrow ZU_i)\to \inf_U[H(U)+I(X;Y\downarrow ZU)].$$

For every U_i, there exists J_i such that $I(X;Y \downarrow ZU_i) = I(X;Y|J_i)$, and also $XY \to ZU_i \to J_i$ forming a Markov chain, since the infimum in the definition of the intrinsic information can be shown to be a minimum (see [5]).

We have:

$$\begin{aligned}
&I(XY;J_i|Z) = \\
&I(XY;U_i|Z) - I(XY;U_i|ZJ_i) \leq \\
&I(XY;U_i|Z) = H(U_i|Z) - H(U_i|XYZ) = \\
&H(U_i) - I(U_i;Z) - H(U_i|XYZ).
\end{aligned}$$

Hence

$$\begin{aligned}
&H(U_i) + I(X;Y \downarrow ZU_i) \geq \\
&[I(U_i;Z) + H(U_i|XYZ)] + \\
&[I(X;Y|J_i) + I(XY;J_i|Z)] \geq \\
&[I(U_i;Z) + H(U_i|XYZ)] + \\
&\min_J [I(X;Y|J) + I(XY;J|Z)] = \\
&[I(U_i;Z) + \\
&H(U_i|XYZ)] + \inf_U [H(U) + I(X;Y \downarrow ZU)].
\end{aligned}$$

Taking the limit as $i \to \infty$, we conclude that $[I(U_i;Z) + H(U_i|XYZ)] \to 0$ as $i \to \infty$. Therefore properties 2 and 3 are proved.

Since $H(U_i|XYZ) \to 0$, so do $H(U_i|X = x, Y = y, Z = z)$ for all (x,y,z) such that $p(x,y,z) > 0$. Therefore for all $u \in \mathcal{U}_i$, $p(U_i = u|X = x, Y = y, Z = z) \log \frac{1}{p(U_i = u|X = x, Y = y, Z = z)}$ should go to zero. Therefore property 4 is proved.

In order to prove property 5, we note that

$I(U_i;Z) = \sum_{z:p(z)>0} p(z).D(\mathcal{L}(U_i|Z = z) \| \mathcal{L}(U_i)) \to 0$.

Therefore if $p(z_1)$ and $p(z_2)$ are positive, both $D(\mathcal{L}(U_i|Z = z_1) \| \mathcal{L}(U_i))$ and $D(\mathcal{L}(U_i|Z = z_2) \| \mathcal{L}(U_i))$ converge to zero. The Pinsker inequality, $D(p\|q) \geq \frac{1}{2\ln(2)} d^2(p,q)$ implies that both $d(\mathcal{L}(U_i|Z = z_1), \mathcal{L}(U_i))$ and $d(\mathcal{L}(U_i|Z = z_2), \mathcal{L}(U_i))$ converge to zero, and therefore the total variation distance $d(\mathcal{L}(U_i|Z = z_1), \mathcal{L}(U_i|Z = z_2))$ should also go to zero. ■

Proof of Lemma A1.2: Assume that $I(X;Y \downarrow ZT) = I(X;Y|J)$ for some $XY \to ZT \to J$ (this is possible because the infimum in the definition of the intrinsic information can be shown to be a minimum [5]).

$H(T) > H(T|Z) > p(Z = z)H(T|Z = z)$. Therefore $H(T|Z = z) < \frac{\delta}{\min(p(z):p(z)>0)} := Q$.

The denominator, $\min(p(z) : p(z) > 0)$, is a fixed constant depending on z. Intuitively, since $H(T|Z = z)$ is small, with probability close to one it will be a constant. More precisely, assume that

$p(T = T_z|Z = z) \geq p(T = t|Z = z)$ for all t.

Since $H(T|Z=z) \geq h(p(T=T_z|Z=z))$, we have $h(p(T=T_z|Z=z)) \leq Q$. Let $c_1 \leq \frac{1}{2}$ and $c_2 = 1 - c_1$ be the two solutions of the equation $h(x) = Q$ in the interval $[0,1]$. c_2 goes to one as δ goes to zero. $h(p(T=T_z|Z=z)) \leq Q$ implies $p(T=T_z|Z=z) \leq c_1$ or $p(T=T_z|Z=z) \geq c_2$.

If $p(T=T_z|Z=z) \leq c_1$, we will have $p(T=t|Z=z) \leq c_1$ for all t. Therefore $H(T|Z=z) \geq \log \frac{1}{c_1}$.

We also have $H(T|Z=z) < \frac{\delta}{\min(p(z):p(z)>0)}$. If δ goes to zero, $\frac{1}{c_1}$ goes to infinity, but $\frac{\delta}{\min(p(z):p(z)>0)}$ converges zero. Hence, for small enough δ, we must have $p(T = T_z|Z=z) \geq c_2$.

Define a random variable J' taking values on the same set as J such that

- $XY \to Z \to J'$ forms a Markov chain,
- $p(J'=j|Z=z) = p(J=j|Z=z, T=T_z)$.

We can furthermore couple J and J' so that $P(J \neq J') \leq 1 - c_2$ by first drawing J' and then changing it with probability $1 - c_2$. Let V be the indicator function of the event $J = J'$.

$$
\begin{aligned}
&|I(X;Y|JJ') - I(X;Y|J)| = |I(X;Y|JJ'V) - I(X;Y|J)| \leq \\
&|I(X;Y|JJ'V) - I(X;Y|JV)| + H(V) = \\
&p(V=0)|I(X;Y|JJ'V=0) - I(X;Y|JV=0)| + H(V) \leq \\
&2p(V=0)H(XY) + H(V).
\end{aligned}
$$

Similarly, we can show that

$$|I(X;Y|JJ') - I(X;Y|J')| \leq 2p(V=0)H(XY) + H(V).$$

These two inequalities show that

$$|I(X;Y|J') - I(X;Y|J)| \leq 4p(V=0)H(XY) + 2H(V).$$

Since $p(V=0)$ and $H(V)$ converge to zero as δ goes to zero, we have: $\forall \xi > 0, \exists \delta > 0$ such that for all random variables T having entropy less than δ, we have

$$I(X;Y \downarrow Z) - I(X;Y \downarrow ZT) < \xi.$$

It would be enough to prove that $I(X;Y \downarrow ZT) \leq I(X;Y \downarrow Z)$ to complete the proof. Assume J satisfies the Markov chain property $XY \to Z \to J$. Define a random variable J' taking values on the same set as J such that

$$
\begin{aligned}
&p(J'=j|X=x, Y=y, Z=z, T=t) = \\
&p(J=j|X=x, Y=y, Z=z).
\end{aligned}
$$

We have $I(J';T|XYZ)=0$ and $I(J';XY|Z)=I(J;XY|Z)=0$. Therefore
$I(J';XYT|Z)=I(J';XY|Z)+I(J';T|XYZ)=0$.

Since $I(J';XYT|Z)=I(J';T|Z)+I(J';XY|ZT)$, we have $I(J';XY|ZT)=0$ and therefore the following Markov chain holds:

$XY\rightarrow ZT\rightarrow J'$.

Furthermore, we have $I(X;Y|J')=I(X;Y|Z)$. This proves that

$$I(X;Y\downarrow ZT)\leq I(X;Y\downarrow Z).$$

■

Appendix II

In this appendix, we verify that

$$\inf_J f^{-1}\big(f(S(X_1;X_2;...;X_u;(X_{u+1})^{(s)}...;(X_m)^{(s)}\|J))+ S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)\big)$$

satisfies the five conditions of Theorem 1, where the infimum is taken over finite random variables J arbitrarily jointly distributed with $X_1,X_2,...,X_m$ and Z.

Property 1.

It is enough to show that for any J there exists some J' such that

$$\begin{aligned}&n\cdot f^{-1}\{f(S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J))\\&+S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)\}\geq\\&f^{-1}\{f(S(X_1^n;X_2^n;...;X_u^n;(X_{u+1}^n)^{(s)};...;(X_m^n)^{(s)}\|J'))+\\&S_{f-one-way}(X_1^nX_2^n...X_m^n;J'^{(s)}\|Z^n)\}.\end{aligned}$$

We prove that $J'=J^n$ is an appropriate choice.

We will first prove that we will be done if we can prove that

$$\begin{aligned}&n\cdot S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)\geq\\&S_{f-one-way}(X_1^nX_2^n...X_m^n;(J^n)^{(s)}\|Z^n).\end{aligned}$$

Let

$s=S(X_1;X_2;...;X_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J)$,

$b=S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z)$,

$c=S_{f-one-way}(X_1^nX_2^n...X_m^n;(J^n)^{(s)}\|Z^n)\leq nb$.

We have:

$f^{-1}\{f(ns)+c\}\leq f^{-1}\{f(ns)+nb\}$.

It suffices to prove that:

$nf^{-1}\{f(s)+b\}\geq f^{-1}\{f(ns)+nb\}$

or equivalently

$f(nf^{-1}\{f(s)+b\}) \geq f(ns)+nb$.

Let $t = f^{-1}\{f(s)+b\} - s$. We can then write this inequality as: $f(ns+nt) \geq f(ns)+nb$. According to the definition of t, we have $b = f(s+t)-f(s)$. Thus, we can rewrite the inequality as

$f(ns+nt) - f(ns) \geq n.(f(s+t)-f(s))$.

This inequality holds because f is increasing and convex.

It remains to show that

$$n \cdot S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z) \geq$$
$$S_{f-one-way}(X_1^nX_2^n...X_m^n; (J^n)^{(s)} \| Z^n).$$

Take some arbitrary U and V satisfying $V \to U \to X_1^nX_2^n...X_m^n - J^nZ^n$. We will prove that there exist $\widetilde{U}$ and $\widetilde{V}$ satisfying

$\widetilde{V} \to \widetilde{U} \to \widetilde{X_1}\widetilde{X_2}...\widetilde{X_m} \to \widetilde{J}\widetilde{Z}$

such that $(\widetilde{X_1}, \widetilde{X_2}, ..., \widetilde{X_m}, \widetilde{J}, \widetilde{Z})$ has the same joint distribution as $(X_1, X_2, ..., X_m, J, Z)$ and

$$f(H(U|Z^nV)) - f(H(U|J^nV)) =$$
$$n \cdot \left[f(H(\widetilde{U}|\widetilde{Z}\widetilde{V})) - f(H(\widetilde{U}|\widetilde{J}\widetilde{V})) \right].$$

We start with the left hand side:

$$f(H(U|Z^nV)) - f(H(U|J^nV)) =$$
$$\sum_{i=1}^{n} \Big\{ f(H(U|Z^{i+1:n}J^{1:i-1}VZ(i))) -$$
$$f(H(U|Z^{i+1:n}J^{1:i-1}VJ(i))) \Big\}.$$

By letting $V_i = Z^{i+1:n}J^{1:i-1}V$ and $U_i = (U, V_i)$ for $i = 1...n$, we can write the above equality as:

$$f(H(U|Z^nV)) - f(H(U|J^nV)) =$$
$$\sum_{i=1}^{n} f(H(U_i|V_iZ(i))) - f(H(U_i|V_iJ(i))).$$

For every i, we have $V_i \to U_i \to X_1(i)X_2(i)...X_m(i) \to J(i)Z(i)$. We would like to define an appropriate $(\widetilde{U}, \widetilde{V}, \widetilde{X_1}, \widetilde{X_2}, ..., \widetilde{X_m}, \widetilde{J}, \widetilde{Z})$ whose $f(H(\widetilde{U}|\widetilde{Z}\widetilde{V})) - f(H(\widetilde{U}|\widetilde{J}\widetilde{V}))$ is

$\frac{1}{n}(\sum_{i=1}^{n} f(H(U_i|V_iZ(i)) - f(H(U_i|V_iJ(i))))$.

This would be possible if the following region is convex:

$\{r \in \mathbb{R} | \exists U, V$ satisfying $(V \to U \to X_1X_2...X_m \to JZ)$ such that $r = f(H(U|ZV)) - f(H(U|JV))\}$.

Since we can continuously move from

$$V_1 \to U_1 \to X_1X_2...X_m \to JZ$$

to

$$V_2 \to U_2 \to X_1X_2...X_m \to JZ$$

while having the expressions $H(U|ZV) = H(UVZ) - H(ZV)$ and $H(U|JV) = H(UJV) - H(JV)$ change continuously, the above region has to be convex (the entropy function is continuous in the whole probability simplex). The proof for this part is now completed.

Property 2.

Let $H(F|X_i) = 0$, where $1 \leq i \leq m$. It is enough to show that for any J, the following inequality holds:

$$\begin{aligned}
&f^{-1}\{f(S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J)) + \\
&S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z)\} \geq \\
&f^{-1}\{f(S(X_1F; ...; X_uF; (X_{u+1}F)^{(s)}; ...; (X_mF)^{(s)} \| JF)) + \\
&S_{f-one-way}(X_1X_2...X_mF; (JF)^{(s)} \| ZF)\}.
\end{aligned}$$

It is clear that

$$\begin{aligned}
&S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J) \geq \\
&S(X_1F; ...; X_uF; (X_{u+1}F)^{(s)}; ...; (X_mF)^{(s)} \| JF)
\end{aligned}$$

because the secret key capacity itself satisfies the second property of Theorem 1. It remains to show that

$$\begin{aligned}
&S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z) \geq \\
&S_{f-one-way}(X_1X_2...X_mF; (JF)^{(s)} \| ZF).
\end{aligned}$$

Since $H(F|X_i) = 0$, we can rewrite the last inequality as:

$$\begin{aligned}
&S_{f-one-way}(X_1X_2...X_m; J^{(s)} \| Z) \geq \\
&S_{f-one-way}(X_1X_2...X_m; (JF)^{(s)} \| ZF).
\end{aligned}$$

Take some arbitrary U and V satisfying $V \to U \to X_1X_2...X_m \to JZF$. It can be verified that for $\widetilde{U} = UF$ and $\widetilde{V} = VF$, the Markov property $\widetilde{V} \to \widetilde{U} \to$

$X_1X_2...X_m \to JZ$ holds. For this choice of $\widetilde{V}$ and $\widetilde{U}$:

$$f(H(\widetilde{U}|\widetilde{V}Z)) - f(H(\widetilde{U}|\widetilde{V}J)) =$$
$$f(H((UF)|(VF)Z)) - f(H((UF)|(VF)J)) =$$
$$f(H(U|V(ZF))) - f(H(U|V(JF))).$$

The proof for this part is now complete.

Property 3.

By taking an approach similar to the one we took in the proof of the second condition, it would suffice to show that

$$S_{f-one-way}(X_1X_2...X_m; J\|Z) \geq$$
$$S_{f-one-way}(X_1'X_2'...X_m'; J\|Z).$$

Take U and V satisfying $V \to U \to X_1'X_2'...X_m' \to JZ$. Define U_1 and V_1 in the following way:

$$p(U_1, V_1, X_1, X_2, ..., X_m, Z, J) =$$
$$p(V_1|U_1)p(U_1|X_1', X_2', ..., X_m')p(X_1, X_2, ..., X_mZJ),$$
$$p(V_1|U_1) = p(V|U),$$
$$p(U_1|X_1', X_2', ..., X_m') = p(U|X_1', X_2', ..., X_m').$$

It can be proved that $V_1 \to U_1 \to X_1X_2...X_m \to JZ$ and that (V_1, U_1, J, Z) has the same joint distribution as (V, U, J, Z), implying $f(H(U_1|V_1Z)) - f(H(U_1|V_1J)) = f(H(U|VZ)) - f(H(U|VJ))$. The proof for this part is now complete.

Property 4.

We need to prove that

$$f^{-1}\{f(S(X_1; X_2; ...; X_m\|J))+$$
$$S_{f-one-way}(X_1X_2...X_m; J\|Z)\} \geq$$
$$H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

If $H(X_1|Z) \leq \sum_{i=2}^{m} H(X_1|X_i)$, the inequality clearly holds. So we assume $H(X_1|Z) > \sum_{i=2}^{m} H(X_1|X_i)$.

Using the fact that $S(X_1, X_2, ..., X_m\|J)$ itself satisfies property 4 of Theorem 1 and the definition of $S_{f-one-way}$, one can lower bound

$$f^{-1}\{f(S(X_1; X_2; ...; X_m\|J))+$$
$$S_{f-one-way}(X_1X_2...X_m; J\|Z)\}$$

by

$$f^{-1}\Big\{f(\max[0, H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)])+ \\ \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\Big\}.$$

Having assumed that $H(X_1|Z) > \sum_{i=2}^{m} H(X_1|X_i)$, one of the following three cases must occur. In each case, we will prove that

$$f^{-1}\{f(S(X_1, ..., X_m \| J)) + S_{f-one-way}(X_1 ... X_m; J \| Z)\} \\ \geq H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

1. $H(X_1|Z) \leq H(X_1|J)$: In this case,

$$f(H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)) \geq \\ f(H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i)) > 0.$$

Therefore the lower bound

$$f^{-1}\{f(\max[0, H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)])+ \\ \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$$

equals

$$f^{-1}\{f(H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i))\}$$

and is itself bounded below by

$$f^{-1}\{f(H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i))\} = \\ H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

2. $H(X_1|Z) > \sum_{i=2}^{m} H(X_1|X_i) \geq H(X_1|J)$: In this case, the lower bound

$$f^{-1}\{f(\max[0, H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)]) + \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$$

equals

$$f^{-1}\{f(H(X_1|Z)) - f(H(X_1|J))\}.$$

But since

$$f(H(X_1|Z)) - f(H(X_1|Z) - H(X_1|J)) \geq f(H(X_1|J)) - f(0),$$

the term $f^{-1}\{f(H(X_1|Z)) - f(H(X_1|J))\}$ can be bounded below by $H(X_1|Z) - H(X_1|J)$ which in turn can be bounded below by

$$H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

3. $H(X_1|Z) > H(X_1|J) > \sum_{i=2}^{m} H(X_1|X_i)$: In this case the lower bound

$$f^{-1}\{f(\max[0, H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)]) + \max[0, f(H(X_1|Z)) - f(H(X_1|J))]\}$$

equals

$$f^{-1}\{f(H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)) + f(H(X_1|Z)) - f(H(X_1|J))\}.$$

Since

$$H(X_1|Z) > H(X_1|J),$$
$$f(H(X_1|Z)) - f(H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i)) \geq f(H(X_1|J)) - f(H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i)).$$

Therefore:

$$f(H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i))+$$
$$f(H(X_1|Z)) - f(H(X_1|J)) \geq$$
$$f(H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i)).$$

Therefore:

$$f^{-1}\{f(H(X_1|J) - \sum_{i=2}^{m} H(X_1|X_i))+$$
$$f(H(X_1|Z)) - f(H(X_1|J))\} \geq$$
$$f^{-1}\{f(H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i))\} =$$
$$H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

In all the three cases we have proved that

$$f^{-1}\{f(S(X_1, ..., X_m \| J)) + S_{f-one-way}(X_1 ... X_m; J \| Z)\} \geq$$
$$H(X_1|Z) - \sum_{i=2}^{m} H(X_1|X_i).$$

The proof for this part is now complete.

Property 5.

It is enough to show that for any J, there exists J' such that the following inequality holds:

$$f^{-1}\{f(S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J))+$$
$$S_{f-one-way}(X_1 X_2 ... X_m; J^{(s)} \| Z)\} \geq$$
$$f^{-1}\{f(S(X_1 M_1; ...; X_u M_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| J'))+$$
$$S_{f-one-way}(X_1 M_1 ... X_u M_u X_{u+1} ... X_m; J'^{(s)} \| Z)\}.$$

Take an arbitrary J jointly distributed with $(X_1, X_2, ..., X_m, Z)$, and define J' so that

$$p(J' X_1, X_2, ..., X_m, Z, M_1, ..., M_u) =$$
$$p(J' X_1, X_2, ..., X_m, Z) p(M_1, ..., M_u),$$
$$p(J' | X_1, X_2, ..., X_m, Z) = p(J | X_1, X_2, ..., X_m, Z).$$

It is clear that

$$S(X_1;...;X_u;X_{u+1}^{(s)};...;(X_m)^{(s)}\|J) \geq$$
$$S(X_1M_1;...;X_uM_u;X_{u+1}^{(s)};...;X_m^{(s)}\|J')$$

because

$$p(J'|X_1,X_2,...,X_m,Z) = p(J|X_1,X_2,...,X_m,Z)$$

and the secret key capacity itself satisfies property 5 of Theorem 1. It remains to show that

$$S_{f-one-way}(X_1X_2...X_m;J^{(s)}\|Z) \geq$$
$$S_{f-one-way}(X_1M_1X_2M_2....X_uM_uX_{u+1}...X_m;J'^{(s)}\|Z).$$

Take some U and V satisfying $V \to U \to X_1X_2...X_mM_1...M_u \to J'Z$. Since M_1, M_2, ..., M_u are independent of $(X_1,X_2,...,X_m,Z,J')$, $M_1,M_2,...,M_u$ can be thought of as playing the role of an external randomness employed by $X_1X_2...X_m$ to create U and V. Thus, if we let

$p(\widetilde{V},\widetilde{U}|X_1X_2...X_mJZ) = p(V,U|X_1X_2...X_mJ'Z)$

$\widetilde{V},\widetilde{U}$ will satisfy $\widetilde{V} \to \widetilde{U} \to X_1X_2...X_m \to JZ$. For this choice of $\widetilde{V}$ and $\widetilde{U}$:

$$f(H(\widetilde{U}|\widetilde{V}Z)) - f(H(\widetilde{U}|\widetilde{V}J)) =$$
$$f(H(U|VZ)) - f(H(U|VJ)).$$

The proof for this part is now complete. ■

4.5 The channel model

4.5.1 The proof technique at an intuitive level

In this section, we illustrate the main proof technique we use for proving the upper bounds at an intuitive level. Roughly speaking the technique can be described as follows. Take an arbitrary secret key generation scheme that uses the DMBC for say n times. During the simulation of the protocol, the *"secret key reservoir"* (representing the amount of secret key bits built up so far)[5] of the legitimate terminals gradually increases until it reaches its final state where the legitimate terminals create the common secret key. Each use of the DMBC increases the "secret key reservoir" of the terminals, whereas the public discussion that follows after each use of the DMBC allows for coordination and processing of the "secret key reservoir", but does not increase the amount of secret key bits, since the public discussion is observed by

[5]We do not need to define "secret key reservoir" formally.

the eavesdropper. The idea is to quantify this gradual evolution of the "secret key reservoir", bound the derivative of its growth at each stage from above by showing that one use of the DMBC can buy us at most a certain amount of secret bits, and conclude that the final size of the "secret key reservoir" is not bigger than n times the upper bound on its derivative per use of the DMBC. An implementation of this idea requires quantification of the "secret key reservoir" of the m terminals at a given stage of the process. To that end, we take a real-valued function of joint distributions, and evaluate it at the joint distribution of $m+1$ random variables that represent, roughly speaking, the knowledge of the m legitimate terminals and the eavesdropper at the given stage of the secret key generation protocol. Properties that such a function would need to satisfy are identified. The new upper bound is then proved by a verification argument. We now provide the details.

Consider the special case of $u = m = 2$ and take an arbitrary secret key generation protocol $\mathrm{SK}_C(n,\ \epsilon,\ S_1,\ S_2,\ \mathbf{C},\ M_1, M_2,\ X_1^n, X_2^n, Z^n)$. During the simulation of the protocol, the "secret key reservoir" of the legitimate terminals gradually evolves until it reaches its final state where the terminals know enough to create the common secret key. We can represent the state of the system at a given stage of the process by the joint distribution of three random variables that represent, roughly speaking, the knowledge of the two legitimate terminals and the eavesdropper at that stage. The state of the system therefore evolves as follows:

$$
\begin{aligned}
&\to (X_1(1), X_2(1), Z(1))\\
&\to (X_1(1)M_1, X_2(1)M_2, Z(1))\\
&\to (X_1(1)M_1C_{1,1}, X_2(1)M_2C_{1,1}, Z(1)C_{1,1})\\
&\to (X_1(1)M_1C_{1,1}C_{1,2}, X_2(1)M_2C_{1,1}C_{1,2}, Z(1)C_{1,1}C_{1,2})\\
&\to \cdots \to (X_1(1)M_1\mathbf{C}_1, X_2(1)M_2\mathbf{C}_1, Z(1)\mathbf{C}_1)\\
&\to (X_1(1)X_1(2)M_1\mathbf{C}_1, X_2(1)X_2(2)M_2\mathbf{C}_1, Z(1)Z(2)\mathbf{C}_1)\\
&\to (X_1(1)X_1(2)M_1\mathbf{C}_1C_{2,1}, X_2(1)X_2(2)M_2\mathbf{C}_1C_{2,1}, Z(1)Z(2)\mathbf{C}_1C_{2,1})\\
&\to (X_1(1)X_1(2)M_1\mathbf{C}_1C_{2,1}C_{2,2}, X_2(1)X_2(2)M_2\mathbf{C}_1C_{2,1}C_{2,2}, Z(1)Z(2)\mathbf{C}_1C_{2,1}C_{2,2})\\
&\to \cdots\\
&\to (X_1(1)X_1(2)M_1\mathbf{C}_1\mathbf{C}_2, X_2(1)X_2(2)M_2\mathbf{C}_1\mathbf{C}_2, Z(1)Z(2)\mathbf{C}_1\mathbf{C}_2)\\
&\to (X_1(1)X_1(2)X_1(3)M_1\mathbf{C}_1\mathbf{C}_2, X_2(1)X_2(2)X_2(3)M_2\mathbf{C}_1\mathbf{C}_2, Z(1)Z(2)Z(3)\mathbf{C}_1\mathbf{C}_2)\\
&\to (X_1(1)X_1(2)X_1(3)M_1\mathbf{C}_1\mathbf{C}_2C_{3,1}, X_2(1)X_2(2)X_2(3)M_2\mathbf{C}_1\mathbf{C}_2C_{3,1}, Z(1)Z(2)Z(3)\mathbf{C}_1\mathbf{C}_2C_{3,1})\\
&\to \cdots\\
&\to (X_1^nM_1\mathbf{C}, X_2^nM_2\mathbf{C}, Z^n\mathbf{C})\\
&\to (S_1, S_2, Z^n\mathbf{C})
\end{aligned}
$$

Formally speaking, we can represent the state by three finite sets and a joint distribution on these finite sets, i.e. a four-tuple $(\widehat{\mathcal{X}}_1, \widehat{\mathcal{X}}_2, \widehat{\mathcal{Z}}, p(\widehat{x}_1, \widehat{x}_2, \widehat{z}))$. Please note that here we have used random variables $\widehat{X}_1$, $\widehat{X}_2$ and $\widehat{Z}$ to represent the total information available to the terminals at a given stage of the key generation process

(whereas random variables X_1, and X_2, Z were representing the input and outputs to the broadcast channel).

The functions ϕ and φ, and properties imposed on them

To *quantify* the evolution of the "secret key reservoir" of the legitimate parties, we use a function φ defined from the set of all four tuples $(\widehat{\mathcal{X}}_1, \widehat{\mathcal{X}}_2, \widehat{\mathcal{Z}}, p(\widehat{x}_1, \widehat{x}_2, \widehat{z}))$ to non-negative real numbers. We sometimes use the notation $\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z})$ to refer to $\varphi(p(\widehat{x_1}, \widehat{x}_2, \widehat{z}))$ when $(\widehat{X}_1, \widehat{X}_2, \widehat{Z})$ has the law $p(\widehat{x}_1, \widehat{x}_2, \widehat{z})$.[6]

Suppose we would like to prove that some given non-negative function $\phi(\mathrm{q}(x_2, z|x_1))$ is an upper bound on the secret key capacity. It would be enough to prove that each use of the DMBC in each stage, cannot buy us more than $\phi(\mathrm{q}(x_2, z|x_1))$ secret bits. This would imply that n uses of the DMBC does not buy us more than $n \times \phi(\mathrm{q}(x_2, z|x_1))$ secret bits, and therefore the secret key rate achieved will be less than or equal to $\phi(\mathrm{q}(x_2, z|x_1))$ on a per use basis.

Motivated by the above discussion, let us assume that the system is in the state $(\widehat{\mathcal{X}}_1, \widehat{\mathcal{X}}_2, \widehat{\mathcal{Z}}, p(\widehat{x}_1, \widehat{x}_2, \widehat{z}))$, and the terminals decide to use the DMBC. The first terminal would create X_1 as a function of $\widehat{X}_1$, and put it at the input of the DMBC $\mathrm{q}(x_2, z|x_1)$. The second terminal and the eavesdropper will receive X_2 and Z. The state of the system will evolve to $(\widehat{\mathcal{X}}_1 \times \mathcal{X}_1, \widehat{\mathcal{X}}_2 \times \mathcal{X}_2, \widehat{\mathcal{Z}} \times \mathcal{Z}, p(\widehat{x}_1 x_1, \widehat{x}_2 x_2, \widehat{z} z))$. Note that the following statements are true about the joint distribution of $\widehat{X}_1, X_1, \widehat{X}_2, X_2, \widehat{Z}, Z$:

$$H(X_1|\widehat{X}_1) = 0, \tag{4.26}$$

$$\widehat{X}_1 \widehat{X}_2 \widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1 X_2 Z, \tag{4.27}$$

$$p(x_2, z|x_1) = \mathrm{q}(x_2, z|x_1). \tag{4.28}$$

We then expect the quantified state does not increase by more than ϕ. In other words, we would like to have the following property:

1. Whenever equations (4.26), (4.27) and (4.28) hold, we require:

$$\varphi(\widehat{X}_1 X_1; \widehat{X}_2 X_2 \| \widehat{Z} Z) \leq \\ \varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) + \phi(\mathrm{q}(x_2, z|x_1)).$$

Next, we expect the public discussion that follows each use of the DMBC does not increase the "secret key reservoir" (since the public discussion is heard by the eavesdropper). Let us assume that the system is in the state $(\widehat{\mathcal{X}}_1, \widehat{\mathcal{X}}_2, \widehat{\mathcal{Z}}, p(\widehat{x}_1, \widehat{x}_2, \widehat{z}))$, and the i-th legitimate terminal $(1 \leq i \leq 2)$ decides to use the public channel. This terminal creates random variable F, so we must have $H(F|\widehat{X}_i) = 0$. Random

[6] As in the source model notation, we have separated the legitimate parties and the eavesdropper via the symbol $\|$.

variable F is made public and the state of the system evolves to $(\widehat{\mathcal{X}}_1 \times \mathcal{F}, \widehat{\mathcal{X}}_2 \times \mathcal{F}, \widehat{\mathcal{Z}} \times \mathcal{F}, p(\widehat{x}_1 f, \widehat{x}_2 f, \widehat{z} f))$. We then expect the quantified state to stay the same or to decrease. In other words, we would like to have the following property:

2. For any random variable F such that $\exists i : H(F|\widehat{X}_i) = 0$, we require:

$$\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) \geq \varphi(\widehat{X}_1 F; \widehat{X}_2 F \| \widehat{Z} F);$$

Next, since φ is quantifying the "secret key reservoir", and reducing the information available to the legitimate terminals should not increase their "secret key reservoir", we impose the following constraint:

3. For any random variables $\widehat{X}_1', \widehat{X}_2'$ such that $\forall i : H(\widehat{X}_i'|\widehat{X}_i) = 0$, we require:

$$\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) \geq \varphi(\widehat{X}_1'; \widehat{X}_2' \| \widehat{Z}).$$

Next, consider the special case of $\widehat{X}_1 \cong \widehat{X}_2$, and $\widehat{Z}$ being almost independent of $(\widehat{X}_1, \widehat{X}_2)$. In this case, we expect $\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z})$ to be approximately equal to $H(\widehat{X}_1)$. In order to ensure this property, and inspired by the lower bound $I(\widehat{X}_1; \widehat{X}_2) - I(\widehat{X}_1; \widehat{Z})$ on the source model secret key capacity, we impose the following constraint:

4. $\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) \geq H(\widehat{X}_1|\widehat{Z}) - H(\widehat{X}_1|\widehat{X}_2) = I(\widehat{X}_1; \widehat{X}_2) - I(\widehat{X}_1; \widehat{Z})$.

Since φ is quantifying the "secret key reservoir", providing the legitimate terminals with private external randomness should not increase their "secret key reservoir". We therefore impose the following constraint:

5. Whenever random variables M_1, M_2 satisfy

$$p(M_1, M_2, \widehat{X}_1, \widehat{X}_2, \widehat{Z}) = p(M_1) p(M_2) p(\widehat{X}_1, \widehat{X}_2, \widehat{Z}),$$

we require

$$\varphi(\widehat{X}_1; \widehat{X}_2 \| \widehat{Z}) \geq \varphi(\widehat{X}_1 M_1; \widehat{X}_2 M_2 \| \widehat{Z}).$$

Lastly, we assume the following constraint: for any conditional distribution $\mathrm{q}(x_2, z|x_1)$,

$$\sup_{q(x_1)} \varphi(q(x_1)\mathrm{q}(x_2, z|x_1)) < \infty. \tag{4.29}$$

Implication of the properties imposed on ϕ and φ

Claim: Assume that the above conditions 1-5 and equation (4.29) are satisfied for some functions φ and ϕ. Then the channel model secret key capacity, $C_{CH}(2, \mathrm{q}(x_2, z|x_1))$, must be bounded from above by $\phi(\mathrm{q}(x_2, z|x_1))$ for any channel $\mathrm{q}(x_2, z|x_1)$.

Intuitive Proof: Take some DMBC $\mathrm{q}(x_2, z|x_1)$, and a secret key generation protocol $\mathrm{SK}_C(n,\ \epsilon,\ S_1,\ S_2,\ \mathbf{C},\ M_1, M_2,\ X_1^n, X_2^n, Z^n)$ whose secret key rate is approximately equal to $C_{CH}^{\epsilon}(2, \mathrm{q}(x_2, z|x_1)))$. Then we have (here we are using the notation X_1^1 to represent $X_1(1)$, and $X_1^{1:k}$ to represent $X_1(1)...X_1(k)$):

$$
\begin{aligned}
&(n-1)\phi(\mathrm{q}(x_2, z|x_1)) + \sup_{q(x_1)} \varphi(q(x_1)\mathrm{q}(x_2, z|x_1)) \geq \\
&(n-1)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(X_1^1; X_2^1 \| Z^1) \\
&\geq (n-1)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^1; M_2 X_2^1 \| Z^1) && (4.30)\\
&\geq (n-1)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^1 C_{1,1}; M_2 X_2^1 C_{1,1} \| Z^1 C_{1,1}) && (4.31)\\
&\geq (n-1)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^1 C_{1,1} C_{1,2}; M_2 X_2^1 C_{1,1} C_{1,2} \| Z^1 C_{1,1} C_{1,2}) && (4.32)\\
&\geq \cdots \\
&\geq (n-1)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^1 \mathbf{C}_1; M_2 X_2^1 \mathbf{C}_1 \| Z^1 \mathbf{C}_1) \\
&\geq (n-2)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^{1:2} \mathbf{C}_1; M_2 X_2^{1:2} \mathbf{C}_1 \| Z^{1:2} \mathbf{C}_1) && (4.33)\\
&\geq (n-2)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^{1:2} \mathbf{C}_{1:2}; M_2 X_2^{1:2} \mathbf{C}_{1:2} \| Z^{1:2} \mathbf{C}_{1:2}) && (4.34)\\
&\geq (n-3)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(M_1 X_1^{1:3} \mathbf{C}_{1:2}; M_2 X_2^{1:3} \mathbf{C}_{1:2} \| Z^{1:3} \mathbf{C}_{1:2}) && (4.35)\\
&\geq \cdots \\
&\geq \varphi(M_1 X_1^{1:n} \mathbf{C}_{1:n}; M_2 X_2^{1:n} \mathbf{C}_{1:n} \| Z^{1:n} \mathbf{C}_{1:n}) \\
&\geq \varphi(S_1; S_2 \| Z^{1:n} \mathbf{C}_{1:n}) && (4.36)\\
&\geq H(S_1 | Z^{1:n} \mathbf{C}_{1:n}) - H(S_1|S_2) && (4.37)\\
&\cong n C_{CH}^{\epsilon}(2, \mathrm{q}(x_2, z|x_1))) - 0, && (4.38)
\end{aligned}
$$

where equation (4.30) holds because of condition 5; equation (4.31) holds because of condition 2 and the fact that $H(C_{1,1}|M_1 X_1^1) = 0$; equation (4.32) holds because of condition 2 and the fact that $H(C_{1,2}|M_2 X_2^1 C_{1,1}) = 0$; equation (4.33) holds because of condition 1; equation (4.34) is true because we can repeatedly invoke condition 2 for the individual communications within $\mathbf{C}_2$; equation (4.35) holds because of condition 1; equation (4.36) holds because of condition 3 and the fact that $H(S_1|M_1 X_1^{1:n} \mathbf{C}_{1:n}) = H(S_2|M_2 X_2^{1:n} \mathbf{C}_{1:n}) = 0$; equation (4.37) holds because of condition 4; and equation (4.38) holds since the secret key rate of the protocol is approximately equal to $C_{CH}^{\epsilon}(2, \mathrm{q}(x_2, z|x_1)))$, and S_1 is approximately equal to S_2.

Intuitively, the above chain of inequalities imply that

$$\frac{n-1}{n}\phi(\mathrm{q}(x_2, z|x_1)) + \frac{1}{n}\sup_{q(x_1)} \varphi(q(x_1) \cdot \mathrm{q}(x_2, z|x_1))$$

is greater than or equal to $C^{\epsilon}_{CH}(2, \mathrm{q}(x_2, z|x_1)))$. Letting $n \to \infty$ and then $\epsilon \to 0$, we would get that $\phi(\mathrm{q}(x_2, z|x_1))$ is greater than or equal to $C_{CH}(2, \mathrm{q}(x_2, z|x_1))$.

Discussion

As the above proof indicates, as one moves along a given protocol, the expression $\frac{1}{n}\big((n-i)\phi(\mathrm{q}(x_2, z|x_1)) + \varphi(\textit{current state})\big)$ (where i denotes the number of uses of the DMBC so far) is non-increasing. This quantity starts from the upper bound $\phi(\mathrm{q}(x_2, z|x_1))$ and decreases as we move along the protocol, and eventually becomes equal to the secret key rate of the protocol. Thus, it is justified to view the expression as a *potential function*. The reader may compare this with the corresponding discussion in the source model.

In order to show the effectiveness of the technique, and show that it could make the converse proofs systematic, we provide an example:

Example. Prove that $\sup_{p(x_1)} I(X_1; X_2|Z)$ is an upper bound on $C_{CH}(2, \mathrm{q}(x_2, z|x_1))$.

Proof. Let $\varphi(\widehat{X}_1; \widehat{X}_2\|\widehat{Z}) = I(\widehat{X}_1; \widehat{X}_2|\widehat{Z})$ and $\phi(\mathrm{q}(x_2, z|x_1)) = \sup_{p(x_1)} I(X_1; X_2|Z)$. Clearly equation (4.29) is satisfied. We need to verify the five properties. The first property holds since whenever equations (4.26), (4.27) and (4.28) are hold, we have

$$\begin{aligned}
&I(\widehat{X}_1X_1; \widehat{X}_2X_2|\widehat{Z}Z) = \\
&H(\widehat{X}_2X_2|\widehat{Z}Z) - H(\widehat{X}_2X_2|\widehat{Z}Z\widehat{X}_1X_1) = \\
&H(\widehat{X}_2X_2|\widehat{Z}Z) - H(\widehat{X}_2|\widehat{Z}\widehat{X}_1) - H(X_2|ZX_1) \leq \\
&H(\widehat{X}_2|\widehat{Z}) + H(X_2|Z) - H(\widehat{X}_2|\widehat{Z}\widehat{X}_1) - H(X_2|ZX_1) = \\
&I(\widehat{X}_1; \widehat{X}_2|\widehat{Z}) + I(X_1; X_2|Z) = \\
&\varphi(\widehat{X}_1; \widehat{X}_2\|\widehat{Z}) + \varphi(X_1; X_2\|Z) \leq \\
&\varphi(\widehat{X}_1; \widehat{X}_2\|\widehat{Z}) + \phi(\mathrm{q}(x_2, z|x_1)).
\end{aligned} \tag{4.39}$$

Equation (4.39) holds because

$$\begin{aligned}
&H(\widehat{X}_2X_2|\widehat{Z}Z\widehat{X}_1X_1) = \\
&H(\widehat{X}_2|\widehat{Z}Z\widehat{X}_1X_1) + H(X_2|\widehat{Z}Z\widehat{X}_1X_1\widehat{X}_2) = \\
&H(\widehat{X}_2|\widehat{Z}\widehat{X}_1) - I(\widehat{X}_2; ZX_1|\widehat{Z}\widehat{X}_1) + \\
&H(X_2|ZX_1) - I(X_2; \widehat{Z}\widehat{X}_1\widehat{X}_2|ZX_1).
\end{aligned}$$

But equation (4.27) implies that

$$\begin{aligned}
&I(\widehat{X}_2; ZX_1|\widehat{Z}\widehat{X}_1) \leq I(\widehat{Z}\widehat{X}_2; ZX_1|\widehat{X}_1) = 0 \\
&I(X_2; \widehat{Z}\widehat{X}_2\widehat{X}_1|ZX_1) \leq I(X_2Z; \widehat{Z}\widehat{X}_2\widehat{X}_1|X_1) = 0.
\end{aligned}$$

The second property holds because assuming that $H(F|\widehat{X}_1) = 0$, we will have

$$\begin{aligned}
&I(\widehat{X}_1;\widehat{X}_2|\widehat{Z}) = I(\widehat{X}_1F;\widehat{X}_2|\widehat{Z}) = \\
&I(F;\widehat{X}_2|\widehat{Z}) + I(\widehat{X}_1;\widehat{X}_2|\widehat{Z}F) \geq \\
&I(\widehat{X}_1F;\widehat{X}_2F|\widehat{Z}F).
\end{aligned}$$

The other properties can be easily verified. ■

In order to find a new upper bound, one can think of a given functions $\varphi(\widehat{X}_1;\widehat{X}_2\|\widehat{Z})$ and $\phi(\mathrm{q}(x_2,z|x_1))$ as a point in the set of all functions that satisfy the properties, and try to slightly perturb the expression so that all the properties remain satisfied.

4.5.2 Statement of the new converses

In this section we state the main results. We use the potential function method to prove them in section 4.5.3 and the appendices. Following the formal statement of each result, a brief informal discussion is provided to clarify the statement.

Sufficient conditions for being an upper bound on the SK_C capacity

Let $\varphi(p(\widehat{x}_1,\widehat{x}_2,...,\widehat{x}_m,\widehat{z}))$ be a real-valued function from the set of *all* probability distributions defined on a product of *any* $m+1$ finite sets. We sometimes use the notation $\varphi(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m\|\widehat{Z})$ to refer to $\varphi(p(\widehat{x}_1,\widehat{x}_2,...,\widehat{x}_m,z))$ when $(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z})$ has the law $p(\widehat{x}_1,...,\widehat{x}_m,\widehat{z})$. Furthermore, let ϕ be a real-valued function from the set of *all* conditional laws $\mathrm{q}(x_2,x_3,...x_m,z|x_1)$ defined on a product of any $m+1$ finite sets. Further assume that for any channel $\mathrm{q}(x_2,x_3,...x_m,z|x_1)$,

$$\sup_{q(x_1)} \varphi(q(x_1)\cdot \mathrm{q}(x_2,x_3,...x_m,z|x_1)) < \infty. \tag{4.40}$$

The following theorem formalizes the ideas discussed in section 4.5.1.

Theorem 6. Given functions ϕ and φ satisfying equation (4.40) for any channel $\mathrm{q}(x_2,x_3,...x_m,z|x_1)$, the function $\phi(\mathrm{q}(x_2,x_3,...x_m,z|x_1))$ will be an upper bound on $C_{CH}(u,\mathrm{q}(x_2,x_3,...x_m,z|x_1))$ (the channel model secret key capacity assuming that only the first u terminals are permitted to talk) if φ satisfies the following 5 conditions for all $p(\widehat{x}_1,\widehat{x}_2,...,\widehat{x}_m,\widehat{z})$:

1. For any random variables $X_1,X_2,...,X_m,Z$ jointly distributed with $\widehat{X}_1,...,\widehat{X}_m,\widehat{Z}$ such that the equations

$$\begin{aligned}
&H(X_1|\widehat{X}_1) = 0, \\
&\widehat{X}_1\widehat{X}_2...\widehat{X}_m\widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1X_2...X_mZ, \\
&p(x_2,x_3,...,x_m,z|x_1) = \mathrm{q}(x_2,x_3,...x_m,z|x_1)
\end{aligned}$$

hold, we have:

$$\varphi(\widehat{X}_1X_1;\widehat{X}_2X_2;...;\widehat{X}_mX_m\|\widehat{Z}Z) \leq$$
$$\varphi(\widehat{X}_1;\widehat{X}_2;...;\widehat{X}_m\|\widehat{Z}) + \phi(\mathrm{q}(x_2,x_3,...x_m,z|x_1));$$

2. For any random variable F such that $\exists i \leq u : H(F|\widehat{X}_i) = 0$, we have:

$$\varphi(\widehat{X}_1;\widehat{X}_2;...;\widehat{X}_m\|\widehat{Z}) \geq \varphi(\widehat{X}_1F;\widehat{X}_2F;...;\widehat{X}_mF\|\widehat{Z}F);$$

3. For any random variables $\widehat{X}'_1, \widehat{X}'_2, ..., \widehat{X}'_m$ such that $\forall i : H(\widehat{X}'_i|\widehat{X}_i) = 0$, we have:

$$\varphi(\widehat{X}_1;\widehat{X}_2;...;\widehat{X}_m\|\widehat{Z}) \geq \varphi(\widehat{X}'_1;\widehat{X}'_2;...;\widehat{X}'_m\|\widehat{Z});$$

4. $\varphi(\widehat{X}_1;\widehat{X}_2;...;\widehat{X}_m\|\widehat{Z}) \geq H(\widehat{X}_1|\widehat{Z}) - \sum_{i=2}^{m} H(\widehat{X}_1|\widehat{X}_i)$;

5. Whenever random variables M_1, M_2, ..., M_u satisfy

$$p(M_1,M_2,...,M_u,\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z}) =$$
$$p(M_1)p(M_2)...p(M_u)p(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z}),$$

we have:

$$\varphi(\widehat{X}_1;\widehat{X}_2;...;\widehat{X}_m\|\widehat{Z}) \geq$$
$$\varphi(M_1\widehat{X}_1;M_2\widehat{X}_2;...;M_u\widehat{X}_u;\widehat{X}_{u+1};...;\widehat{X}_m\|\widehat{Z}).$$

New upper bound on the $\mathbf{SK}_C$ capacity

Before stating the theorem, we make a few definitions. The intuitive meaning of the definitions and of the new upper bound are provided in the discussion that follows the statement of the theorem.

Definitions. Let $[m]$ and $[u]$ respectively denote the sets $\{1,2,...,m\}$, $\{1,2,...,u\}$. For any subset B of $[m]$, let λ_B be a non-negative real number, and $\Lambda = (\lambda_B, B \subseteq [m])$ denote a vector of dimension 2^m whose elements are the λ_B for the various subsets of $[m]$. Let V denote the set of vectors $\Lambda = (\lambda_B, B \subseteq [m])$ satisfying the following equation for any $(R_1,R_2,...,R_u) \in \mathbb{R}^u_{\geq 0}$:

$$\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]} \lambda_B \sum_{j\in B\cap[u]} R_j = \sum_{j=1}^{u} R_j. \tag{4.41}$$

For any subset B of $[m] = \{1,2,3,...,m\}$, we use the notation $\widehat{X}_B$ when referring to the set of random variables $(\widehat{X}_k, k \in B)$. Note that unlike λ_B, $\widehat{X}_B$ is a set of random variables.

We then have the following theorem:

Theorem 7. For any $\Lambda = (\lambda_B, B \subseteq [m]) \in V$, the secret key capacity

$$C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$$

is bounded from above by

$$\sup_{p(x_1)} \left\{ \inf_J \left([H(X_1...X_u|J) - \tau^{\Lambda}(X_1, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J) + I(X_1X_2...X_m; J|Z)] \right) \right\}.$$

In this expression $(X_1, X_2, ..., X_m, J, Z)$ have the law

$$p(x_1)\mathrm{q}(x_2, x_3, ...x_m, z|x_1)p(j|x_1, ..., x_m, z);$$

the infimum is taken over finite random variables J arbitrarily jointly distributed with $X_1, X_2, ..., X_m, Z$; and

$$\tau^{\Lambda}(X_1, X_2, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J) := \sum_{B: B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]} \lambda_B H(X_{B \cap [u]} | X_{B^c} J).$$

Discussion: This upper bound was derived in an attempt to imitate the source model upper bound. In section 4.4.2 we showed that

$$\begin{aligned} &S(X_1; X_2; ...; X_u; (X_{u+1})^{(s)} ...; (X_m)^{(s)} \| Z) \leq \\ &\inf_J \big[S(X_1 J; X_2 J; ...; X_u J; (X_{u+1} J)^{(s)} ...; (X_m J)^{(s)} \| J) \\ &+ I(X_1 X_2 ... X_m; J|Z) \big], \end{aligned} \tag{4.42}$$

where the infimum is taken over finite random variables J arbitrarily jointly distributed with X_1, X_2, ..., X_m and Z. Theorem 6 of [23] provides a single letter expression for the first term in the right hand side of equation (4.42). This upper bound on the secret key capacity in the source model suggests the following upper bound on $C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$:

$$\begin{aligned} &\sup_{p(x_1)} \{ \inf_J [S(X_1 J; ...; X_u J; (X_{u+1} J)^{(s)} ...; (X_m J)^{(s)} \| J) \\ &+ I(X_1 X_2 ... X_m; J|Z)] \}. \end{aligned} \tag{4.43}$$

In order to prove that this expression is an upper bound on $C_{CH}(u, \mathrm{q}(x_2, ..., x_m, z|x_1))$, one simply needs to define appropriate functions ϕ and φ, and then verify the properties of Theorem 6. We were not however able to complete the proof. So, we modified the expression of equation (4.43) for the proof to go through. We first provide an alternative characterization of the expression of equation (4.43), and then mention our modification.

Note that Theorem 6 of [23] provides the following expression:

$$S(X_1J; X_2J; ...; X_uJ; (X_{u+1}J)^{(s)}; ...; (X_mJ)^{(s)} \| J) =$$
$$H(X_1X_2...X_u|J) - \min_{(R_1,R_2,...,R_u)\in\Re}(\sum_{i=1}^{u} R_i)$$

where

$$\Re = \{(R_1, ..., R_u) : \forall B : B \subset [m], B \cap [u] \neq \emptyset, B \neq [m]$$
$$\text{we have } \sum_{j\in B\cap[u]} R_j \geq H(X_{B\cap[u]}|X_{B^c}Z)\}.$$

The intuitive meaning of the quantity R_i is to be found in the context of the problem of communication for omniscience (CFO) discussed in section 4.2, or in [12]. The above expression can be rewritten using the duality theory as follows:

$$S(X_1J; ...; X_uJ; (X_{u+1}J)^{(s)}; ...; (X_mJ)^{(s)} \| J) =$$
$$H(X_1X_2...X_u|J) - \max_{\Lambda\in V}(\tau^{\Lambda}(X_1, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J)) =$$
$$\min_{\Lambda\in V}\left[H(X_1...X_u|J) - \tau^{\Lambda}(X_1, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J)\right]. \tag{4.44}$$

Therefore we can write the expression in equation (4.43) as follows:

$$\sup_{p(x_1)}\left\{\inf_J \min_{\Lambda\in V}\left(H(X_1...X_u|J) - \tau^{\Lambda}(X_1, X_2, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J) + \right.\right.$$
$$\left.\left. I(X_1X_2...X_m; J|Z)\right)\right\}.$$

We modified this expression by swapping $\min_{\Lambda\in V}$ with $\sup_{p(x_1)}\inf_J$ as follows:

$$\min_{\Lambda\in V}\sup_{p(x_1)}\left\{\inf_J \left(H(X_1...X_u|J)\right.\right. \tag{4.45}$$
$$\left.\left. - \tau^{\Lambda}(X_1, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J) + I(X_1...X_m; J|Z)\right)\right\}.$$

Theorem 7 implies that the above expression is an upper bound on $C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$, since for any arbitrary $\Lambda \in V$,

$$C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1)) \leq$$
$$\sup_{p(x_1)}\left\{\inf_J \left(H(X_1...X_u|J)\right.\right.$$
$$\left.\left. - \tau^{\Lambda}(X_1, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J) + I(X_1...X_m; J|Z)\right)\right\}.$$

■

Corollary. In the case of $m = u = 2$, the only possible value for $\lambda_{\{1\}}$ and $\lambda_{\{2\}}$ is one, and the new upper bound on $C_{CH}(2, \mathrm{q}(x_2, z|x_1))$ will be equal to

$$\sup_{p(x_1)} \inf_J [I(X_1; X_2|J) + I(X_1X_2; J|Z)],$$

where the infimum is taken over all finite random variables J, arbitrarily jointly distributed with (X_1, X_2, Z). This upper bound can be intuitively understood as follows: instead of the broadcast channel $\mathrm{q}(x_2, z|x_1)$, consider an extended broadcast channel $\mathrm{q}(x_2, z, j|x_1)$ with a fictitious terminal receiving J. The total secret key is "split" into two parts: one that is independent of J, and one that is shared with J. These two parts correspond to the terms $I(X_1; X_2|J)$ and $I(X_1X_2; J|Z)$ respectively.

The new upper bound is always less than or equal to

$$\inf_{\overline{Z} \to Z \to X_1X_2} \sup_{p(x_1)} I(X_1; X_2|\overline{Z})$$

which in turn is less than or equal to $\min[\sup_{p(x_1)} I(X_1; X_2), \sup_{p(x_1)} I(X_1; X_2|Z))]$. This is because in the new upper bound, the minimum is over finite random variables J arbitrarily jointly distributed with (X_1, X_2, Z); if one takes $J = \overline{Z}$ for some $\overline{Z} \to Z \to X_1X_2$, the term $I(X_1X_2; J|Z)$ will be zero, and the term $I(X_1; X_2|J)$ will be equal to $I(X_1; X_2|\overline{Z})$. Therefore

$$\sup_{p(x_1)} \inf_J [I(X_1; X_2|J) + I(X_1X_2; J|Z)] \leq$$
$$\sup_{p(x_1)} \inf_{\overline{Z} \to Z \to X_1X_2} I(X_1; X_2|\overline{Z}).$$

Lastly, note that

$$\sup_{p(x_1)} \inf_{\overline{Z} \to Z \to X_1X_2} I(X_1; X_2|\overline{Z}) \leq$$
$$\inf_{\overline{Z} \to Z \to X_1X_2} \sup_{p(x_1)} I(X_1; X_2|\overline{Z}).$$

Remark: One can use the strengthened Carathéodory theorem of Fenchel to get the cardinality bound of $|\mathcal{X}_1||\mathcal{X}_2||\mathcal{Z}|$ on the size of the alphabet of J. One can therefore express the new upper bound as

$$\sup_{p(x_1)} \min_J [I(X_1; X_2|J) + I(X_1X_2; J|Z)],$$

where the infimum is replaced with a minimum.

Theorem 8. The new upper bound represents a strict improvement over the previously best known upper bound for the case of $u = m = 2$: there exists an example for which the new upper bound is strictly smaller than $\sup_{p(x_1)} \inf_{\overline{Z} \to Z \to X_1X_2} I(X_1; X_2|\overline{Z})$ which in turn is always less than or equal to $\inf_{\overline{Z} \to Z \to X_1X_2} \sup_{p(x_1)} I(X_1; X_2|\overline{Z})$.

4.5.3 Proofs

Proof of Theorem 6: Fix a probability distribution $\mathrm{q}(x_2, x_3, ..., x_m, z|x_1)$ and assume that $X_1, X_2, ..., X_m$ and Z take values from finite sets $\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_m, \mathcal{Z}$. For every $\delta > 0$ and $\epsilon > 0$, one can find a valid secret key generation scheme, $\mathrm{SK}_C(n,\ \epsilon,\ S_1,\ S_2,\ S_3,\ ...,\ S_m,\ \mathbf{C},\ M_1, M_2, ..., M_u,\ X_1^n, X_2^n, ..., X_m^n, Z^n)$, whose secret key rate is within δ of $C_{CH}^{\epsilon}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$. Furthermore, without loss of generality, we can add the uniformity condition $\frac{1}{n}\log|\mathcal{S}_1| < \frac{1}{n}H(S_1) + \epsilon$.[7] Following the secret key generation scheme, we write the following inequalities:

$$\begin{gathered}(n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \sup_{q(x_1)} \varphi(q(x_1)\mathrm{q}(x_2, x_3, ...x_m, z|x_1)) \\ \geq (n-1)\phi(\mathrm{q}(x_2, \cdots, x_m, z|x_1)) + \varphi(X_1^1; X_2^1; \cdots; X_m^1 \| Z^1) \\ \geq (n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \\ \varphi(M_1X_1^1; M_2X_2^1; \cdots; M_uX_u^1; X_{u+1}^1 \cdots X_m^1 \| Z^1). \end{gathered} \tag{4.46}$$

Equation (4.46) holds because of condition 5 of Theorem 6. Next we have

$$\begin{gathered}(n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \\ \varphi(M_1X_1^1; M_2X_2^1; \cdots; M_uX_u^1; X_{u+1}^1 \cdots X_m^1 \| Z^1) \\ \geq (n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \end{gathered} \tag{4.47}$$

$$\begin{gathered}\varphi(M_1X_1^1C_{1,1}; \cdots; M_uX_u^1C_{1,1}; X_{u+1}^1C_{1,1} \cdots X_m^1C_{1,1} \| Z^1C_{1,1}) \\ \geq (n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \end{gathered} \tag{4.48}$$

$$\varphi(M_1X_1^1C_{1,1}C_{1,2}; \cdots; M_uX_u^1C_{1,1}C_{1,2}; X_{u+1}^1C_{1,1}C_{1,2} \cdots X_m^1C_{1,1}C_{1,2} \| Z^1C_{1,1}C_{1,2}).$$

Equation (4.47) holds because of condition 2 and the fact that $H(C_{1,1}|M_1X_1^1) = 0$. Equation (4.48) holds because of condition 2 and the fact that $H(C_{1,2}|M_2X_2^1C_{1,1}) = 0$. Next we have

$$\begin{gathered}(n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \\ \varphi(M_1X_1^1C_{1,1}C_{1,2}; \cdots; M_uX_u^1C_{1,1}C_{1,2}; X_{u+1}^1C_{1,1}C_{1,2} \cdots X_m^1C_{1,1}C_{1,2} \| Z^1C_{1,1}C_{1,2}) \\ \geq \cdots \\ \geq (n-1)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \\ \varphi(M_1X_1^1\mathbf{C}_1; M_2X_2^1\mathbf{C}_1; \cdots; M_uX_u^1\mathbf{C}_1; X_{u+1}^1\mathbf{C}_1 \cdots X_m^1\mathbf{C}_1 \| Z^1\mathbf{C}_1) \\ \geq (n-2)\phi(\mathrm{q}(x_2, x_3, ...y, x_m, z|x_1)) + \end{gathered} \tag{4.49}$$

$$\begin{gathered}\varphi(M_1X_1^{1:2}\mathbf{C}_1; \cdots; M_uX_u^{1:2}\mathbf{C}_1; X_{u+1}^{1:2}\mathbf{C}_1 \cdots X_m^{1:2}\mathbf{C}_1 \| Z^{1:2}\mathbf{C}_1) \\ \geq (n-2)\phi(\mathrm{q}(x_2, x_3, \cdots, x_m, z|x_1)) + \end{gathered} \tag{4.50}$$

$$\varphi(M_1X_1^{1:2}\mathbf{C}_{1:2}; \cdots; M_uX_u^{1:2}\mathbf{C}_{1:2}; X_{u+1}^{1:2}\mathbf{C}_{1:2} \cdots X_m^{1:2}\mathbf{C}_{1:2} \| Z^{1:2}\mathbf{C}_{1:2}).$$

[7] This point is argued in [39], or Lemma 5 of [42]. Please see the discussion following definition 2 of 4.2 for details.

Equation (4.49) holds because of condition 1. Equation (4.50) is true because we can repeatedly invoke condition 2 for the individual communications of $\mathbf{C}_2$. Next we have

$$\begin{aligned}
&(n-2)\phi(\mathrm{q}(x_2,x_3,\cdots,x_m,z|x_1))+ && (4.51)\\
&\varphi(M_1X_1^{1:2}\mathbf{C}_{1:2};\cdots;M_uX_u^{1:2}\mathbf{C}_{1:2};X_{u+1}^{1:2}\mathbf{C}_{1:2}\cdots X_m^{1:2}\mathbf{C}_{1:2}\|Z^{1:2}\mathbf{C}_{1:2})\\
&\geq (n-3)\phi(\mathrm{q}(x_2,x_3,\cdots,x_m,z|x_1))+ && (4.52)\\
&\varphi(M_1X_1^{1:3}\mathbf{C}_{1:2};\cdots;M_uX_u^{1:3}\mathbf{C}_{1:2};X_{u+1}^{1:3}\mathbf{C}_{1:2}\cdots X_m^{1:3}\mathbf{C}_{1:2}\|Z^{1:3}\mathbf{C}_{1:2})\\
&\geq\cdots\geq\\
&\varphi(M_1X_1^{1:n}\mathbf{C}_{1:n};\cdots M_uX_u^{1:n}\mathbf{C}_{1:n};X_{u+1}^{1:n}\mathbf{C}_{1:n}\cdots X_m^{1:n}\mathbf{C}_{1:n}\|Z^{1:n}\mathbf{C}_{1:n}) && (4.53)\\
&\geq \varphi(S_1;S_2;\cdots;S_m\|Z^{1:n}\mathbf{C}_{1:n}) && (4.54)\\
&\geq H(S_1|Z^{1:n}\mathbf{C}_{1:n})-\textstyle\sum_{j=2}^m H(S_1|S_j) && (4.55)
\end{aligned}$$

$$\geq nC_{CH}^{\epsilon}(u,\mathrm{q}(x_2,x_3,\cdots x_m,z|x_1)))-n\delta-(m-1)[h(\epsilon)+\epsilon\cdot\log|\mathcal{S}_1|].$$

Equation (4.52) holds because of condition 1. Equation (4.53) holds because of condition 3. Equation (4.54) holds because of condition 4, and equation (4.55) is a consequence of Fano's inequality and the fact that the secret key rate of the protocol is within δ of $C_{CH}^{\epsilon}(u,\mathrm{q}(x_2,x_3,...x_m,z|x_1))$.

The above inequalities show that

$$\begin{aligned}
&\frac{n-1}{n}\phi(\mathrm{q}(x_2,x_3,\cdots,x_m,z|x_1))\geq\\
&C_{CH}^{\epsilon}(u,\mathrm{q}(x_2,x_3,...x_m,z|x_1)))-\delta\\
&-\frac{m-1}{n}h(\epsilon)-(m-1)\epsilon\frac{1}{n}\log|\mathcal{S}_1|\\
&-\frac{1}{n}\sup_{q(x_1)}\varphi(q(x_1)\cdot\mathrm{q}(x_2,x_3,...x_m,z|x_1)).
\end{aligned}$$

Note that

$$\begin{aligned}
&\frac{1}{n}\log|\mathcal{S}_1|<\\
&\frac{1}{n}H(S_1)+\epsilon<C_{CH}^{\epsilon}(u,\mathrm{q}(x_2,x_3,...x_m,z|x_1)))+\delta+\epsilon.
\end{aligned}$$

The theorem is proved by first taking the limit as $n\to\infty$, and then letting ϵ and δ converge zero. ■

Proof of Theorem 7: Fix some $\Lambda=(\lambda_B,B\subseteq[m])$ in the set V. In order to prove

Table 4.2: Joint probability distribution of X and Y

Y \ X	0	1	2	3
0	$\frac{1}{2}p_0$	$\frac{1}{2}p_1$	0	0
1	$\frac{1}{2}p_0$	$\frac{1}{2}p_1$	0	0
2	0	0	p_2	0
3	0	0	0	p_3

this theorem, it suffices to verify the five conditions of Theorem 6 when we set:

$$\begin{aligned}
&\varphi(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m\|\widehat{Z}) = \\
&\inf_J \Bigg(H(\widehat{X}_1...\widehat{X}_u|J) - \tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}_{u+1}^{(s)},...,\widehat{X}_m^{(s)}\|J) \\
&+ I(\widehat{X}_1\widehat{X}_2...\widehat{X}_m;J\|\widehat{Z}) \Bigg) \; ; \qquad (4.56) \\
&\phi(p(x_2,x_3,...x_m,z|x_1)) = \sup_{p(x_1)} \varphi\big(p(x_1)\cdot p(x_2,x_3,...x_m,z|x_1)\big).
\end{aligned}$$

In the above expression the infimum is taken over all finite random variables J arbitrarily jointly distributed with $\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z}$.
$\tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}_{u+1}^{(s)},...,\widehat{X}_m^{(s)}\|J)$ is defined as in the statement of the Theorem. In Appendix I of section 4.5.4, the five conditions of Theorem 6 are verified. This completes the proof. ■

Proof of Theorem 8: Since $m = 2$, for simplicity we use the notation X, Y instead of X_1 and X_2 for the rest of the proof. In order to prove that this bound strictly improves $\sup_{p(x)} \inf_{\overline{Z}\to Z\to XY} I(X;Y|\overline{Z})$ we use the example of Renner and Wolf in [51]. X and Y take values from the set $\{0,1,2,3\}$. Assuming that $P(X=i)=p_i$, Table (4.2) characterizes the conditional probability distribution of Y given X. The conditional distribution of Z given X and Y is specified by the following equation:

$$Z = \begin{cases} (X \;+\; Y) \mod 2 & \text{if } X \in \{0,1\}, \\ X \mod 2 & \text{if } X \in \{2,3\}. \end{cases}$$

Renner and Wolf proved that for the choice of $p_i = \frac{1}{4}$ for $i = 0,1,2,3$ and $U = \lfloor \frac{X}{2} \rfloor$, one has

$$I(X;Y\downarrow Z) = \frac{3}{2}, \qquad I(X;Y\downarrow ZU) = 0,$$

where $I(X;Y\downarrow Z)$, known as "the intrinsic information", is defined as $\inf_{\overline{Z}\to Z\to XY} I(X;Y|\overline{Z})$ [51].

Therefore $\sup_{p(x)}[I(X;Y\downarrow Z)] \geq \frac{3}{2}$.

The proof will be complete if one can show that $\sup_{p(x)} \min_J [I(X;Y|J)+I(XY;J|Z)] < \frac{3}{2}$. We show that $\sup_{p(x)} \min_J [I(X;Y|J) + I(XY;J|Z)]$ is in fact less than or equal to one (thus strictly less than $\frac{3}{2}$).

Let

$$J_0 = \begin{cases} U & \text{if U=0,} \\ UZ & \text{if U=1.} \end{cases}$$

We can bound $\sup_{p(x)} \min_J [I(X;Y|J)+I(XY;J|Z)]$ from above by $\sup_{p(x)} [I(X;Y|J_0)+ I(XY;J_0|Z)]$.

Since $I(X;Y|J_0) = 0$ and $I(XY;J_0|Z) \leq 1$ for all $p(x)$, the supremum

$$\sup_{p(x)} \min_J [I(X;Y|J) + I(XY;J|Z)]$$

must be less than or equal to one. ■

4.5.4 Appendices

Appendix I

In this Appendix, we prove that $\varphi(\cdot)$, proposed in equation (4.56), satisfies the five properties of Theorem 6. Recall that the elements of the vector $\Lambda = (\lambda_B, B \subseteq [m])$ satisfy equation (4.41). Let

$$\theta^{\Lambda}(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m;J\|\widehat{Z}) :=$$
$$H(\widehat{X}_1...\widehat{X}_u|J) - \tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}_{u+1}^{(s)},...,\widehat{X}_m^{(s)}\|J) + I(\widehat{X}_1\widehat{X}_2...\widehat{X}_m;J\|\widehat{Z}),$$

where $\tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}_{u+1}^{(s)},...,\widehat{X}_m^{(s)}\|J)$ is as in the statement of Theorem 7. We can then re-express equation (4.56) as

$$\varphi(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m\|\widehat{Z}) =$$
$$\inf_J \left(\theta^{\Lambda}(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m;J\|\widehat{Z})\right),$$

where the infimum is over all finite random variables J arbitrarily jointly distributed with $\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z}$.

Property 1.

It is required to verify that:

$$\inf_{\widetilde{J}}(\theta^{\Lambda}(\widehat{X}_1X_1;\widehat{X}_2X_2;\widehat{X}_3X_3;...;\widehat{X}_mX_m;\widetilde{J}\|\widehat{Z}Z)) \leq$$
$$\inf_{\widetilde{J}'}(\theta^{\Lambda}(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m;\widetilde{J}'\|\widehat{Z})) + \phi(\mathrm{q}(x_2,x_3,...,x_m,z|x_1)). \qquad (4.57)$$

$\phi(\mathrm{q}(x_2, x_3, ..., x_m, z|x_1))$ is by definition greater than or equal to $\varphi(X_1; X_2; ...; X_m \| Z)$ which is equal to

$$\inf_{\widetilde{J}''}(\theta^{\Lambda}(X_1; X_2; X_3; ...; X_m; \widetilde{J}'' \| Z)).$$

In order to show equation (4.57), it suffices to prove that for any J'', the following inequality holds:

$$\begin{aligned}
&\inf_{\widetilde{J}} \theta^{\Lambda}(\widehat{X}_1 X_1; \widehat{X}_2 X_2; \widehat{X}_3 X_3; ...; \widehat{X}_m X_m; \widetilde{J} \| \widehat{Z} Z) \leq \\
&\inf_{\widetilde{J}'} \theta^{\Lambda}(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m; \widetilde{J}' \| \widehat{Z}) + \theta^{\Lambda}(X_1; X_2; X_3; ...; X_m; J'' \| Z). \qquad (4.58)
\end{aligned}$$

Without loss of generality, we can further assume that

$$\widetilde{J}' \to \widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m \widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1 X_2 ... X_m Z \to J'',$$

because the two terms on the right hand side of equation (4.58) depend only on $p(\widetilde{J}' | \widehat{X}_1 ... \widehat{X}_m \widehat{Z})$ and $p(J'' | X_1 ... X_m Z)$.

In order to prove equation (4.58), it suffices to show that for any arbitrary J' satisfying

$$J' \to \widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m \widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1 X_2 ... X_m Z \to J'',$$

the following inequality holds:

$$\begin{aligned}
&\theta^{\Lambda}(\widehat{X}_1 X_1; \widehat{X}_2 X_2; \widehat{X}_3 X_3; ...; \widehat{X}_m X_m; J' J'' \| \widehat{Z} Z) \leq \\
&\theta^{\Lambda}(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m; J' \| \widehat{Z}) + \\
&\theta^{\Lambda}(X_1; X_2; X_3; ...; X_m; J'' \| Z).
\end{aligned}$$

We claim that the following two inequalities hold:

$$\begin{aligned}
&H(\widehat{X}_1 ... \widehat{X}_u X_1 ... X_u | J', J'') \\
&- \tau^{\Lambda}(\widehat{X}_1 X_1, ..., \widehat{X}_u X_u, (\widehat{X}_{u+1} X_{u+1})^{(s)}, ..., (\widehat{X}_m X_m)^{(s)} \| J' J'') \\
&\leq H(\widehat{X}_1 ... \widehat{X}_u | J') - \tau^{\Lambda}(\widehat{X}_1, ..., \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, ..., \widehat{X}_m^{(s)} \| J') + \\
&H(X_1 ... X_u | J'') - \tau^{\Lambda}(X_1, ..., X_u, X_{u+1}^{(s)}, ..., X_m^{(s)} \| J''), \qquad (4.59)
\end{aligned}$$

and

$$\begin{aligned}
&I(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m X_1 X_2 ... X_m; J' J'' | \widehat{Z} Z) \leq \\
&I(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m; J' | \widehat{Z}) + I(X_1 X_2 ... X_m; J'' | Z).
\end{aligned}$$

Starting from the last inequality:

$$
\begin{aligned}
&I(\widehat{X}_1\widehat{X}_2...\widehat{X}_m X_1X_2...X_m; J'J''|\widehat{Z}Z) = \\
&H(J'J''|\widehat{Z}Z) - H(J'J''|\widehat{Z}Z\widehat{X}_1\widehat{X}_2...\widehat{X}_m X_1X_2...X_m) \leq \\
&H(J'|\widehat{Z}Z) + H(J''|\widehat{Z}Z) \\
&- H(J'|\widehat{Z}Z\widehat{X}_1...\widehat{X}_m X_1...X_m) \\
&- H(J''|J'\widehat{Z}Z\widehat{X}_1...\widehat{X}_m X_1...X_m) \leq \qquad (4.60) \\
&H(J'|\widehat{Z}) + H(J''|Z) - H(J'|\widehat{Z}\widehat{X}_1\widehat{X}_2...\widehat{X}_m) \\
&- H(J''|ZX_1X_2...X_m) = \\
&I(\widehat{X}_1\widehat{X}_2...\widehat{X}_m; J'|\widehat{Z}) + I(X_1X_2...X_m; J''|Z).
\end{aligned}
$$

In equation (4.60) we have used the Markov property

$$J' \to \widehat{X}_1\widehat{X}_2...\widehat{X}_m\widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1X_2...X_mZ \to J''.$$

It remains to prove the inequality (4.59). We first prove that for every set $B \subseteq [m]$:

$$
\begin{aligned}
&H(\widehat{X}_{B\cap[u]}X_{B\cap[u]}|\widehat{X}_{B^c}X_{B^c}J'J'') - H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'') = \\
&\big(H(\widehat{X}_{B\cap[u]}|\widehat{X}_{B^c}J') - H(\widehat{X}_1|\widehat{X}_{B^c}J')\big)+ \\
&\big(H(X_{B\cap[u]}|X_{B^c}J'') - H(X_1|X_{B^c}J'')\big).
\end{aligned}
$$

This equality is true because

$$
\begin{aligned}
&H(\widehat{X}_{B\cap[u]}X_{B\cap[u]}|\widehat{X}_{B^c}X_{B^c}J'J'') = \\
&H(\widehat{X}_{B\cap[u]}X_{B\cap[u]}\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'') = \\
&H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'')+ \\
&H(\widehat{X}_{B\cap[u]}X_{B\cap[u]}|\widehat{X}_1\widehat{X}_{B^c}X_{B^c}J'J'') =^{i} \\
&H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'') + H(\widehat{X}_{B\cap[u]}|\widehat{X}_1\widehat{X}_{B^c}X_{B^c}J'J'')+ \\
&H(X_{B\cap[u]}|\widehat{X}_1X_1\widehat{X}_{B\cap[u]}\widehat{X}_{B^c}X_{B^c}J'J'') =^{ii} \\
&H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'') + H(\widehat{X}_{B\cap[u]}|\widehat{X}_1\widehat{X}_{B^c}J')+ \\
&H(X_{B\cap[u]}|X_1X_{B^c}J'') = \\
&H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'') + H(\widehat{X}_{B\cap[u]}|\widehat{X}_{B^c}J') \\
&- H(\widehat{X}_1|\widehat{X}_{B^c}J') + H(X_{B\cap[u]}|X_{B^c}J'') - H(X_1|X_{B^c}J'').
\end{aligned}
$$

In step i we have used the fact that $H(X_1|\widehat{X}_1) = 0$ and in step ii we have used the Markov property

$$J' \to \widehat{X}_1\widehat{X}_2...\widehat{X}_m\widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1X_2...X_mZ \to J''.$$

This property lets us rewrite the inequality we would like to prove in a new form:

$$H(\widehat{X}_1|J',J'')- \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]} \lambda_B H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J',J'') \leq$$
$$H(\widehat{X}_1|J') - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]} \lambda_B H(\widehat{X}_1|\widehat{X}_{B^c}J')+$$
$$H(X_1|J'') - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]} \lambda_B H(X_1|X_{B^c}J'').$$

Further, we can restrict the summation to those sets B such that $1 \in B$ (otherwise the term in question would be zero).

Using equation (4.41), and by setting $R_1 = 1$ and $R_j = 0$ for $1 < j \leq u$, one can get:

$$\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],1\in B} \lambda_B = 1.$$

Therefore

$$H(\widehat{X}_1|J',J'') - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],1\in B} \lambda_B H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'') =$$
$$\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],1\in B} \lambda_B [H(\widehat{X}_1|J',J'')$$
$$- H(\widehat{X}_1|\widehat{X}_{B^c}X_{B^c}J'J'')] =$$
$$\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],1\in B} \lambda_B I(\widehat{X}_1;\widehat{X}_{B^c}X_{B^c}|J'J'').$$

Similarly we can rewrite the two other expressions. It would then suffice to prove that

$$I(\widehat{X}_1;\widehat{X}_{B^c}X_{B^c}|J'J'') \leq I(\widehat{X}_1;\widehat{X}_{B^c}|J') + I(X_1;X_{B^c}|J'')$$

for all $B \subseteq [m]$ such that $B \neq [m]$ and $1 \in B$.

We have:

$$I(\widehat{X}_1;\widehat{X}_{B^c}X_{B^c}|J'J'') =$$
$$H(\widehat{X}_{B^c}X_{B^c}|J'J'') - H(\widehat{X}_{B^c}X_{B^c}|J'J''\widehat{X}_1) \leq$$
$$H(\widehat{X}_{B^c}|J') + H(X_{B^c}|J'') - H(\widehat{X}_{B^c}X_{B^c}|J'J''\widehat{X}_1) =^i$$
$$H(\widehat{X}_{B^c}|J') + H(X_{B^c}|J'')$$
$$- H(\widehat{X}_{B^c}|J'\widehat{X}_1) - H(X_{B^c}|J''X_1) =$$
$$I(\widehat{X}_1;\widehat{X}_{B^c}|J') + I(X_1;X_{B^c}|J'').$$

In step i, we have used $H(X_1|\widehat{X}_1) = 0$ and the Markov property

$$J' \to \widehat{X}_1\widehat{X}_2...\widehat{X}_m\widehat{Z} \to \widehat{X}_1 \to X_1 \to X_1X_2...X_mZ \to J''.$$

■

Property 2.

Let $1 \leq i \leq u$ and let $H(F|\widehat{X}_i) = 0$. We need to prove that:

$$\inf_{\widetilde{J}}(\theta^{\Lambda}(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m; \widetilde{J}\|\widehat{Z})) \geq$$
$$\inf_{\widetilde{J'}}(\theta^{\Lambda}(\widehat{X}_1F; \widehat{X}_2F; \widehat{X}_3F; ...; \widehat{X}_mF; \widetilde{J'}\|\widehat{Z}F)).$$

It is enough to show that for any J there is a J' such that:

$$\theta^{\Lambda}(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m; J\|\widehat{Z}) \geq$$
$$\theta^{\Lambda}(\widehat{X}_1F; \widehat{X}_2F; \widehat{X}_3F; ...; \widehat{X}_mF; J'\|\widehat{Z}F).$$

Let $J' = JF$. Since $I(F; J \mid \widehat{Z}) \geq 0$, one can show that the above inequality would hold if:

$$H(F|J) - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]} \lambda_B H(F|\widehat{X}_{B^c}J) \geq 0.$$

Since $H(F|\widehat{X}_i) = 0$, we can rewrite the above inequality as follows:

$$H(F|J) - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],i\in B} \lambda_B H(F|\widehat{X}_{B^c}J) \geq 0.$$

The term $H(F|\widehat{X}_{B^c}J)$ is bounded from above by $H(F|J)$, hence:

$$H(F|J) - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],i\in B} \lambda_B H(F|\widehat{X}_{B^c}J) \geq$$
$$H(F|J).(1 - \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],i\in B} \lambda_B).$$

But $1-\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],i\in B} \lambda_B = 0$. This could be proved by setting $R_i = 1$, and $R_j = 0$ for any $1 \leq j \leq u$, $j \neq i$ in equation (4.41). ■

Property 3.

We need to prove that:

$$\inf_{\widetilde{J}}(\theta^{\Lambda}(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m; \widetilde{J}\|\widehat{Z})) \geq$$
$$\inf_{\widetilde{J'}}(\theta^{\Lambda}(\widehat{X}'_1; \widehat{X}'_2; \widehat{X}'_3; ...; \widehat{X}'_m; \widetilde{J'}\|\widehat{Z})).$$

It is enough to prove that for any J:

$$\theta^{\Lambda}(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m;J\|\widehat{Z}) \geq$$
$$\theta^{\Lambda}(\widehat{X}'_1;\widehat{X}'_2;\widehat{X}'_3;...;\widehat{X}'_m;J\|\widehat{Z}).$$

It is clear that $I(\widehat{X}_1\widehat{X}_2...\widehat{X}_m;J|\widehat{Z}) \geq I(\widehat{X}'_1\widehat{X}'_2...\widehat{X}'_m;J|\widehat{Z})$. It remains to show that the sum of the first two terms of the expression, that is

$$H(\widehat{X}_1...\widehat{X}_u|J) - \tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}^{(s)}_{u+1},...,\widehat{X}^{(s)}_m\|J)$$

does not increase when we replace $(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z},J)$ with $(\widehat{X}'_1,\widehat{X}'_2,...,\widehat{X}'_m,\widehat{Z},J)$.

Since we can replace the components of $(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m)$ with $(\widehat{X}'_1,\widehat{X}'_2,...,\widehat{X}'_m)$ one at a time, it is enough to consider the case of changing only one component, that is we replace $(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m)$ with $(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_{j-1},\widehat{X}'_j,\widehat{X}_{j+1},...,\widehat{X}_m)$.

The proof can be completed by considering the two cases of $j > u$ and $j \leq u$ separately. In the case $j > u$, we note that $\tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}^{(s)}_{u+1},...,\widehat{X}^{(s)}_m\|J)$ increases term by term while $H(\widehat{X}_1\widehat{X}_2...\widehat{X}_u|J)$ remains constant. In case $j \leq u$, we note that for every set B that does not contain j, the term $-\lambda_B H(\widehat{X}_{B\cap[u]}|\widehat{X}_{B^c}J)$ decreases as we replace $\widehat{X}_j$ by $\widehat{X}'_j$. If the set B includes j, we have:

$$\begin{aligned}
&H(\widehat{X}_{B\cap[u]}|\widehat{X}_{B^c}J) = \\
&H(\widehat{X}_{B\cap[u])-\{j\}}\widehat{X}_j|\widehat{X}_{B^c}J) = H(\widehat{X}_{B\cap[u])-\{j\}}\widehat{X}_j\widehat{X}'_j|\widehat{X}_{B^c}J) = \\
&H(\widehat{X}_{B\cap[u])-\{j\}}\widehat{X}'_j|\widehat{X}_{B^c}J) + H(\widehat{X}_j|\widehat{X}'_j\widehat{X}_{B^c}\widehat{X}_{B\cap[u])-\{j\}}J) \leq \\
&H(\widehat{X}_{B\cap[u])-\{j\}}\widehat{X}'_j|\widehat{X}_{B^c}J) + H(\widehat{X}_j|\widehat{X}'_j\widehat{X}_{[u]-\{j\}}J).
\end{aligned}$$

So, in order to prove the inequality, it would be enough to prove that

$$\begin{aligned}
&H(\widehat{X}_j|\widehat{X}'_j\widehat{X}_{[u]-\{j\}}J) \\
&- \sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],j\in B} \lambda_B H(\widehat{X}_j|\widehat{X}'_j\widehat{X}_{[u]-\{j\}}J) \geq 0.
\end{aligned}$$

But the left hand side is zero since $\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m],j\in B}\lambda_B = 1$. ■

Property 4.

Equation (4.44) implies that for any random variable J arbitrarily jointly distributed with $\widehat{X}_1$, $\widehat{X}_2$, ..., $\widehat{X}_m$ and $\widehat{Z}$ we have:

$$\begin{aligned}
&S(\widehat{X}_1J;\widehat{X}_2J;...;\widehat{X}_uJ;(\widehat{X}_{u+1}J)^{(s)};...;(\widehat{X}_mJ)^{(s)}\|J) \leq \\
&H(\widehat{X}_1\widehat{X}_2...\widehat{X}_u|J) - \\
&\tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}^{(s)}_{u+1},...,\widehat{X}^{(s)}_m\|J).
\end{aligned} \tag{4.61}$$

Therefore:

$$\inf_J \big(S(\widehat{X}_1 J; \widehat{X}_2 J; ...; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)}; ...; (\widehat{X}_m J)^{(s)} \| J) + I(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m; J \| \widehat{Z})\big) \leq$$
$$\inf_J \big(H(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_u | J) - \tau^{\Lambda}(\widehat{X}_1, \widehat{X}_2, ..., \widehat{X}_u, \widehat{X}_{u+1}^{(s)}, ..., \widehat{X}_m^{(s)} \| J) + I(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m; J \| \widehat{Z})\big)$$
$$= \varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m \| \widehat{Z}).$$

Thus,

$$\varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m \| \widehat{Z}) \geq$$
$$\inf_J \big(S(\widehat{X}_1 J; ...; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)} ...; (\widehat{X}_m J)^{(s)} \| J) + I(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m; J^{(s)} \| \widehat{Z})\big). \tag{4.62}$$

According to Theorem 5 of section 4.4.2,

$$\inf_J \big(S(\widehat{X}_1 J; ...; \widehat{X}_u J; (\widehat{X}_{u+1} J)^{(s)} ...; (\widehat{X}_m J)^{(s)} \| J) + I(\widehat{X}_1 \widehat{X}_2 ... \widehat{X}_m; J^{(s)} \| \widehat{Z})\big)$$
$$\geq S(\widehat{X}_1; \widehat{X}_2; ...; \widehat{X}_u; \widehat{X}_{u+1}^{(s)} ...; \widehat{X}_m^{(s)} \| \widehat{Z}). \tag{4.63}$$

According to Theorem 1 of section 4.4.2, the expression $S(\widehat{X}_1; ...; \widehat{X}_u; \widehat{X}_{u+1}^{(s)} ...; \widehat{X}_m^{(s)} \| \widehat{Z})$ satisfies the condition 4 of the same theorem. Thus,

$$S(\widehat{X}_1; \widehat{X}_2; ...; \widehat{X}_u; \widehat{X}_{u+1}^{(s)} ...; \widehat{X}_m^{(s)} \| \widehat{Z}) \geq$$
$$H(\widehat{X}_1 | \widehat{Z}) - \sum_{i=2}^{m} H(\widehat{X}_1 | \widehat{X}_i). \tag{4.64}$$

Equations (4.62), (4.63) and (4.64) imply that

$$\varphi(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m \| \widehat{Z}) \geq H(\widehat{X}_1 | \widehat{Z}) - \sum_{i=2}^{m} H(\widehat{X}_1 | \widehat{X}_i).$$

■

Property 5.
We need to prove that

$$\inf_{\widetilde{J}} (\theta^{\Lambda}(\widehat{X}_1; \widehat{X}_2; \widehat{X}_3; ...; \widehat{X}_m; \widetilde{J} \| \widehat{Z})) \geq$$
$$\inf_{\widetilde{J}'} (\theta^{\Lambda}(\widehat{X}_1 M_1; \widehat{X}_2 M_2; ...; \widehat{X}_u M_u; \widehat{X}_{u+1} ...; \widehat{X}_m; \widetilde{J}' \| \widehat{Z})),$$

where the first infimum is taken over finite random variables $\widetilde{J}$ arbitrarily jointly distributed with $\widehat{X}_1$, $\widehat{X}_2$, ..., $\widehat{X}_m$ and $\widehat{Z}$, and the second infimum is taken over finite random variables $\widetilde{J'}$ arbitrarily jointly distributed with $\widehat{X}_1$, $\widehat{X}_2$, ..., $\widehat{X}_m$, $\widehat{Z}$, M_1, M_2, ..., M_u.

It is enough to prove that for any J, there is a J' such that:

$$\theta^{\Lambda}(\widehat{X}_1;\widehat{X}_2;\widehat{X}_3;...;\widehat{X}_m;J\|\widehat{Z}) \geq$$
$$\theta^{\Lambda}(\widehat{X}_1M_1;\widehat{X}_2M_2;...;\widehat{X}_uM_u;\widehat{X}_{u+1}...;\widehat{X}_m;J'\|\widehat{Z}).$$

We define J' in such a way that it has the same joint distribution with $(\widehat{X}_1,...,\widehat{X}_m,\widehat{Z})$ as J has, and furthermore $(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_m,\widehat{Z},J')$ is independent of $M_1M_2...M_u$. One can then prove that:

$$\begin{aligned}
&H(\widehat{X}_1M_1...\widehat{X}_uM_u|J') - \tau^{\Lambda}(\widehat{X}_1M_1,\widehat{X}_2M_2,...,\widehat{X}_uM_u,\widehat{X}^{(s)}_{u+1},...,\widehat{X}^{(s)}_m\|J')+\\
&I(\widehat{X}_1\widehat{X}_2...\widehat{X}_mM_1...M_u;J'|\widehat{Z}) =\\
&H(\widehat{X}_1...\widehat{X}_u|J) - \tau^{\Lambda}(\widehat{X}_1,\widehat{X}_2,...,\widehat{X}_u,\widehat{X}^{(s)}_{u+1},...,\widehat{X}^{(s)}_m\|J)+\\
&I(\widehat{X}_1\widehat{X}_2...\widehat{X}_m;J|\widehat{Z})+\\
&H(M_1)+...+H(M_u)-\\
&\qquad\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]}\lambda_B\sum_{i\in B\cap[u]}H(M_i).
\end{aligned}$$

But

$$\begin{aligned}
&H(M_1)+H(M_2)+...+H(M_u)\\
&-\sum_{B:B\subset[m],B\cap[u]\neq\emptyset,B\neq[m]}\lambda_B\sum_{i\in B\cap[u]}H(M_i)
\end{aligned}$$

is zero. This could be proved using equation (4.41) and setting $R_j = H(M_j)$ for $1 \leq j \leq u$. ■

Chapter 5

Transmission of correlated sources over multiterminal networks

A (discrete memoryless) general multiterminal network (GMN) is a model for reliable communication of sets of messages among the nodes of a network, and has been extensively used in modeling of wireless systems. In this chapter, we apply the "potential function method" to study the limitations of joint source-channel coding strategies for lossy transmission across GMNs. In this method, for a given network structure, we *simultaneously* consider all possible networks compatible with that structure and think of the rate region as a function from such networks to subsets of the positive orthant. We then identify properties of such a function which would need to be satisfied for it to give rise to an outer bound. The desired outer bound is then proved by a verification argument. This technique also differs from the traditional ones in the single-letterizing step: instead of reducing the n-letter expression to a single-letter expression in *one shot* using time sharing and other auxiliary random variables, we effectively reduce the n-letter expression *inductively* in n steps. This approach is also useful in extending known results for problems with independent sources to ones with dependent sources. To demonstrate this, we apply the technique to recover and further generalize the outer bound part of the recent result of Maric, Yates and Kramer on strong interference channels with a common message to include dependent sources. In [22] and [21], we have applied the same technique to respectively generalize the well known cut-set bound to the problem of lossy transmission of functions of dependent sources over a GMN, and to simplify the recent outer bound of Liang, Kramer and Shamai on the capacity region of a general broadcast channel, and generalize it to include dependent sources.

5.1 The proof technique

Let m and d be natural numbers and $\mathbb{R}_+^d$ the set of all d-tuples of non-negative reals. Intuitively speaking, for a given network structure, we *simultaneously* consider all possible networks compatible with that structure and think of the rate region as a function from such networks to subsets of $\mathbb{R}_+^d$. We then identify properties of such a function which would need to be satisfied in one step of the communication for it to give rise to an outer bound. The outer bound is then proved by a verification argument. Properties that such a function would need to satisfy are identified, intuitively speaking, as follows: take an arbitrary code of length say n over a GMN. During the simulation of the code, the information of the parties begins from the i^{th} party having the i.i.d. repetitions of the random variable $W^{(i)}$, gradually evolves over time with the usage of the network, and eventually after n stages of communication reaches its final state where the parties know enough to estimate their objectives within the desired average distortion. The idea is to quantify this gradual evolution of information, *bound the derivative of the information growth at each stage* from above by showing that one step of communication can buy us at most a certain amount and conclude that at the final stage, i.e. the n^{th} stage, the system cannot reach an information state better than n times the outer bound on the derivative of information growth. An implementation of this idea requires quantification of the information of the m parties at a given stage of the process. To that end, we evaluate the function we started with at a *virtual channel* whose inputs and outputs represent, roughly speaking, the initial and the gained knowledge of the parties at the given stage of the communication. We also need to make sense of the derivative of a region. This is done using Minkowski sums.

Our technique differs from the traditional ones also in the single-letterizing step: the traditional converses begin with the Fano inequality and continue with the single-letterizing step, that is, reducing the n-letter expression to a single-letter expression in *one shot* using time sharing and other auxiliary random variables. However in our technique we effectively reduce the n-letter expression *inductively* in n steps. The i^{th} step will be equivalent to bounding the derivative of the information growth at the i^{th} use of the multiterminal network (see remark 1 of subsection 5.3 following the proof of the main lemma). The inductive approach to the single-letterizing step is also useful in extending known results for problems with independent sources to ones with dependent sources, as will become clear after understanding the main claims of this paper.

5.2 Formal definitions and Notation

As in the previous chapter, throughout this chapter we assume that each random variable takes values in a finite set. $\mathbb{R}$ denotes the set of real numbers and $\mathbb{R}_+$ denotes

Table 5.1: Notation

Variable	Description
$\mathbb{R}$	Real numbers.
$\mathbb{R}_+$	Non-negative real numbers.
$[k]$	The set $\{1, 2, 3, ..., k\}$.
m	Number of nodes of the network.
$q(y^{(1)}, ..., y^{(m)}\|x^{(1)}, ..., x^{(m)})$	The statistical description of a general multi-terminal network.
$W^{(i)}$	Random variable representing the source observed at the i^{th} node.
$M^{(i)}$	Random variable to be reconstructed, in a possibly lossy way, at the i^{th} node.
$\mathcal{X}^{(i)}, \mathcal{Y}^{(i)}$, $\mathcal{W}^{(i)}$, $\mathcal{M}^{(i)}$	Alphabets of $X^{(i)}$, $Y^{(i)}$, $W^{(i)}$, $M^{(i)}$.
$\Delta^{(i)}(\cdot, \cdot)$	Distortion function used by the i^{th} party.
$\zeta_k^{(i)}(\cdot)$	The encoding function used by the i^{th} party at the k^{th} stage.
$\vartheta^{(i)}(\cdot)$	The decoding function at the i^{th} party.
n	Length of the code used.
$\Pi(\cdot)$	Down-set (Definition 11).
$\oplus$	Minkowski sum of two sets (Definition 10).
$\geq$	A vector or a set being greater than or equal another (Definition 11).
Ψ	A permissible set of input distributions; Given input sources and a GMN, Ψ is a set of joint distributions on $\mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \times \mathcal{X}^{(3)} \times \cdots \times \mathcal{X}^{(m)}$. Inputs to the network are required to have a joint distribution belonging to this set.

the set of non-negative reals. For any natural number k, let $[k] = \{1, 2, 3, ..., k\}$. For a set $S \subset [k]$, let S^c denote its compliment, that is $[k] - S$. The context will make the ambient space of S clear.

Although we are dealing with interference channels in this chapter, we discuss the formulation in full generality. We represent a GMN by the conditional distribution

$$q(y^{(1)}, y^{(2)}, ..., y^{(m)} | x^{(1)}, x^{(2)}, ..., x^{(m)}),$$

meaning that the input by the i^{th} party is $X^{(i)}$ and the output at the i^{th} party is $Y^{(i)}$. We assume that the i^{th} party ($1 \leq i \leq m$) has access to i.i.d. repetitions of $W^{(i)}$ before the beginning of the communication. The message that needs to be delivered (in a possibly lossy manner) to the i^{th} party is taken to be $M^{(i)} = f^{(i)}(W^{(1)}, W^{(2)}, ..., W^{(m)})$ for some function $f^{(i)}$. We assume that for any $i \in [m]$, random variables $X^{(i)}$, $Y^{(i)}$, $W^{(i)}$ and $M^{(i)}$ take values from finite sets $\mathcal{X}^{(i)}$, $\mathcal{Y}^{(i)}$, $\mathcal{W}^{(i)}$ and $\mathcal{M}^{(i)}$ respectively. For any natural number n, let $(\mathcal{X}^{(i)})^n$, $(\mathcal{Y}^{(i)})^n$, $(\mathcal{W}^{(i)})^n$ and $(\mathcal{M}^{(i)})^n$ denote the n-th product sets of $\mathcal{X}^{(i)}$, $\mathcal{Y}^{(i)}$, $\mathcal{W}^{(i)}$ and $\mathcal{M}^{(i)}$ respectively. We use $Y_{1:k}^{(i)}$ to denote $(Y_1^{(i)}, Y_2^{(i)}, ..., Y_k^{(i)})$.

For any $i \in [m]$, let the distortion function $\Delta^{(i)}$ be a function $\Delta^{(i)} : \mathcal{M}^{(i)} \times \mathcal{M}^{(i)} \to [0, \infty)$ satisfying $\Delta^{(i)}(m^{(i)}, m^{(i)}) = 0$ for all $m^{(i)} \in \mathcal{M}^{(i)}$. For any natural number n and vectors $(m_1^{(i)}, m_2^{(i)}, ..., m_n^{(i)})$ and $(m_1^{'(i)}, m_2^{'(i)}, ..., m_n^{'(i)})$ from $(\mathcal{M}^{(i)})^n$, let

$$\Delta_n^{(i)}(m_{1:n}^{(i)}, m_{1:n}^{'(i)}) = \frac{1}{n} \sum_{k=1}^{n} \Delta^{(i)}(m_k^{(i)}, m_k^{'(i)}).$$

Roughly speaking, we require the i.i.d. repetitions of random variable $M^{(i)}$ to be reconstructed, by the i^{th} party, within the average distortion $D^{(i)}$.

Definition 8. Given natural number n, an *n-code* is the following set of mappings:

$$\begin{aligned}
\text{For any } i \in [m] : \zeta_1^{(i)} : & \quad (\mathcal{W}^{(i)})^n \longrightarrow \mathcal{X}^{(i)}; \\
\text{For any } i \in [m], k \in [n] - \{1\} : \zeta_k^{(i)} : & \quad (\mathcal{W}^{(i)})^n \times (\mathcal{Y}^{(i)})^{k-1} \longrightarrow \mathcal{X}^{(i)}; \\
\text{For any } i \in [m] : \vartheta^{(i)} : & \quad (\mathcal{W}^{(i)})^n \times (\mathcal{Y}^{(i)})^n \longrightarrow (\mathcal{M}^{(i)})^n.
\end{aligned}$$

Intuitively speaking $\zeta_k^{(i)}$ is the encoding function of the i^{th} party at the k^{th} time instance, and $\vartheta^{(i)}$ is the decoding function of the i^{th} party.

Given positive reals ϵ and $D^{(i)}$ ($1 \leq i \leq m$), and a source marginal distribution $p(w^{(1)}, w^{(2)}, ..., w^{(m)})$, an n-code is said to achieve the average distortion at most $D^{(i)} + \epsilon$ (for all $i \in [m]$) over the channel $q(y^{(1)}, y^{(2)}, ..., y^{(m)} | x^{(1)}, x^{(2)}, ..., x^{(m)})$ if the following condition is satisfied:

Assume that random variables $(W_{1:n}^{(i)}, i \in [m])$ are n i.i.d. repetitions of random variables $(W^{(1)}, W^{(2)}, ..., W^{(m)})$ with joint distribution $p(w^{(1)}, w^{(2)}, ..., w^{(m)})$. Random

variables $X_k^{(i)}$ and $Y_k^{(i)}$ ($k \in [n]$, $i \in [m]$) are defined according to the following constraints:

$$p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)}, x_{1:n}^{(1)}, x_{1:n}^{(2)}, ..., x_{1:n}^{(m)}, y_{1:n}^{(1)}, y_{1:n}^{(2)}, ..., y_{1:n}^{(m)}) =$$

$$\prod_{k=1}^{n} p(w_k^{(1)}, w_k^{(2)}, ..., w_k^{(m)}) \times \prod_{k=1}^{n} q(y_k^{(1)}, y_k^{(2)}, ..., y_k^{(m)} | x_k^{(1)}, x_k^{(2)}, ..., x_k^{(m)}) \times$$

$$\prod_{k=1}^{n} \prod_{i=1}^{m} p(x_k^{(i)} | w_{1:n}^{(i)}, y_{1:k-1}^{(i)});$$

so we may write $X_1^{(i)} = \zeta_1^{(i)}\big(W_{1:n}^{(i)}\big)$, and for any $2 \leq k \leq n$, $X_k^{(i)} = \zeta_k^{(i)}\big(W_{1:n}^{(i)}, Y_{1:k-1}^{(i)}\big)$. Random variables $X_k^{(i)}$ and $Y_k^{(i)}$ represent the input and output of the i^{th} party at the k^{th} time instance and satisfy the following Markov chains:

$$W_{1:n}^{(1)} ... W_{1:n}^{(m)} Y_{1:k-1}^{(1)} ... Y_{1:k-1}^{(m)} \to W_{1:n}^{(i)} Y_{1:k-1}^{(i)} \to X_k^{(i)},$$

$$W_{1:n}^{(1)} ... W_{1:n}^{(m)} Y_{1:k-1}^{(1)} ... Y_{1:k-1}^{(m)} \to X_k^{(1)} ... X_k^{(m)} \to Y_k^{(1)} ... Y_k^{(m)}.$$

Let $M_k^{(i)} = f^{(i)}(W_k^{(1)}, W_k^{(2)}, ..., W_k^{(m)})$. We should then have the following constraint for every $i \in [m]$:

$$\mathbb{E}\left[\Delta_n^{(i)}\left(\vartheta^{(i)}\big(W_{1:n}^{(i)}, Y_{1:n}^{(i)}\big), M_{1:n}^{(i)}\right)\right] \leq D^{(i)} + \epsilon.$$

Definition 9. Given positive reals $D^{(i)}$, a source marginal distribution $p(w^{(1)}, ..., w^{(m)})$ is called an *admissible source* over the channel $q(y^{(1)}, y^{(2)}, ..., y^{(m)} | x^{(1)}, x^{(2)}, ..., x^{(m)})$ for the target reproduction functions $f^{(i)}$ ($i \in [m]$) at the distortion levels $D^{(i)}$ ($i \in [m]$) if for every positive ϵ and sufficiently large n, an n-code achieving the average distortion at most $D^{(i)} + \epsilon$ exists.

Definition 10. For sets K and L of points in $\mathbb{R}_+^d$, let $K \oplus L$ refer to their Minkowski sum: $K \oplus L = \{v_1 + v_2 : v_1 \in K, v_2 \in L\}$. For any real number r, let $r \times K = \{r \cdot v_1 : v_1 \in K\}$. We also define $\frac{K}{r}$ as the set formed by shrinking K through scaling each point of it by a factor $\frac{1}{r}$. Note that in general $r \times K \neq (r_1 \times K) \oplus (r_2 \times K)$ when $r = r_1 + r_2$ but this is true when K is a convex set.

Definition 11. For $\overrightarrow{v_1}$ 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 sets A and B of points in $\mathbb{R}_+^d$, we say $A \leq B$ if and only if for any point $\overrightarrow{a} \in A$, there exists a point $\overrightarrow{b} \in B$ such that $\overrightarrow{a} \leq \overrightarrow{b}$. For a set $A \in \mathbb{R}_+^d$, the down-set $\Pi(A)$ is defined as: $\Pi(A) = \{\overrightarrow{v} \in \mathbb{R}_+^d : \overrightarrow{v} \leq \overrightarrow{w} \text{ for some } \overrightarrow{w} \in A\}$.

Definition 12. Given a network $q(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$, and the source marginal distribution $p(w^{(1)}, w^{(2)}, ..., w^{(m)})$, there may be properties that the inputs to the GMN have to satisfy throughout the communication. For instance in an interference channel or a multiple access channel with no output feedback, if the transmitters observe independent messages, the random variables representing their information stay independent of each other throughout the communication. This is because the transmitters neither interact nor receive any feedback from the outputs. Also, constraints on the set of input distributions when the transmitters are observing i.i.d. copies of correlated random variables are reported in [29]. Other constraints on the inputs to the network might come from practical requirements such as coupled magnitude constraint across inputs in each stage of the communication. Given a multiterminal network $q(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$ and assuming that $\mathcal{X}^{(i)}$ ($i \in [m]$) is the set $X^{(i)}$ is taking values from, let Ψ be a set of joint distributions on $\mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \times \mathcal{X}^{(3)} \times ... \times \mathcal{X}^{(m)}$ for which the following guarantee exists: for any communication protocol, the inputs to the multiterminal network at each time stage have a joint distribution belonging to the set Ψ. Such a set will be called a *permissible set* of input distributions. Some of the results below will be stated in terms of this nebulously defined region Ψ. To get explicit results, simply replace Ψ by the set of all probability distributions on $\mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \times \mathcal{X}^{(3)} \times ... \times \mathcal{X}^{(m)}$.

Definition 8 can be extended in the obvious way to define the notion of an n-code for a permissible set of input distributions Ψ. Definition 9 can also be extended in the obvious way to define the notion of an admissible source for the target reproduction functions $f^{(i)}$ ($i \in [m]$) at distortion levels $D^{(i)}$ ($i \in [m]$) for a permissible set of input distributions Ψ.

Definition 13. We think of an interference channel as a four-input/four-output multiterminal network whose inputs are $X^{(1)}$, $X^{(2)}$, $X^{(3)}$ and $X^{(4)}$, and whose outputs are $Y^{(1)}$, $Y^{(2)}$, $Y^{(3)}$ and $Y^{(4)}$. The set of alphabets is assumed to belong to

$$\mathcal{A}_{interference} := \big\{\big(\mathcal{X}^{(1)}, \mathcal{X}^{(2)}, \mathcal{X}^{(3)}, \mathcal{X}^{(4)}, \mathcal{Y}^{(1)}, \mathcal{Y}^{(2)}, \mathcal{Y}^{(3)}, \mathcal{Y}^{(4)}\big) : |\mathcal{X}^{(3)}| = |\mathcal{X}^{(4)}| = 1\big\},$$

and the conditional law of the network is assumed to belong to

$$\mathcal{Q}_{interference} :=$$
$$\big\{q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}) : H(Y^{(1)}|X^{(1)}) = H(Y^{(2)}|X^{(2)}) = 0\big\}.$$

Apart from notational changes, this is identical to the traditional interference channel.

5.3 The main lemma for proving the converses

Let m and d be natural numbers. Let $\phi(p(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}), \Psi)$ be a function that takes as input an arbitrary pair of

(m-input/m-output multiterminal network,

a permissible set of input distributions for the network),

consistent with the structure of interest (this will be made precise below) and returns a subset of $\mathbb{R}_+^d$. We will now impose some conditions on ϕ, which we first discuss informally and then formally. Apart from these conditions nothing need be assumed about ϕ; in particular there is no need to impose any regularity conditions.

Intuitive discussion of the properties imposed on ϕ

Intuitively speaking, we want the function ϕ to quantify the information state during the simulation of a code: during the simulation of the code, the information of the parties begins from the i^{th} party having $W_{1:n}^{(i)}$ and gradually evolves over time with the use of the network. At the j^{th} stage, the i^{th} party has $W_{1:n}^{(i)}Y_{1:j}^{(i)}$. We represent the information state of the whole system at the j^{th} stage by the virtual channel $p(w_{1:n}^{(1)}y_{1:j}^{(1)}, ..., w_{1:n}^{(m)}y_{1:j}^{(m)}|w_{1:n}^{(1)}, ..., w_{1:n}^{(m)})$ and the single admissible input distribution $p(w_{1:n}^{(1)}, ..., w_{1:n}^{(m)})$. In order to quantify the information state, we map it to a subset of $\mathbb{R}_+^d$ using the function ϕ. We demand that ϕ satisfies two conditions. The first condition is intuitively saying that an additional use of the channel

$$p(y'^{(1)}, y'^{(2)}, ..., y'^{(m)}|x'^{(1)}, x'^{(2)}, ..., x'^{(m)})$$

restricted to input distributions from Ψ can expand ϕ by at most

$$\phi\big(p(y'^{(1)}, y'^{(2)}, ..., y'^{(m)}|x'^{(1)}, x'^{(2)}, ..., x'^{(m)}), \Psi\big).$$

The second condition is intuitively saying that ϕ vanishes if the parties are unable to communicate, that is, if each party receives exactly what it puts at the input of the channel.

Note that all the channels we encounter in the above process (including the virtual channels and the physical channel) fall into a certain class of m-input/m-output multiterminal networks. We can demand that the function ϕ satisfies certain conditions within this class. For instance, assume that the physical channel is an interference channel.

As discussed in the previous section, we think of an interference channel as a four-input/four-output multiterminal network whose inputs are $X^{(1)}$, $X^{(2)}$, $X^{(3)}$ and $X^{(4)}$, and whose outputs are $Y^{(1)}$, $Y^{(2)}$, $Y^{(3)}$ and $Y^{(4)}$. The set of alphabets is assumed to belong to

$$\mathcal{A}_{interference} := \big\{\big(\mathcal{X}^{(1)}, \mathcal{X}^{(2)}, \mathcal{X}^{(3)}, \mathcal{X}^{(4)}, \mathcal{Y}^{(1)}, \mathcal{Y}^{(2)}, \mathcal{Y}^{(3)}, \mathcal{Y}^{(4)}\big) : |\mathcal{X}^{(3)}| = |\mathcal{X}^{(4)}| = 1\big\},$$

and the conditional law of the network is assumed to belong to

$$\mathcal{Q}_{interference} :=$$
$$\big\{q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}) : H(Y^{(1)}|X^{(1)}) = H(Y^{(2)}|X^{(2)}) = 0\big\}.$$

Note that when $|\mathcal{W}^{(3)}| = |\mathcal{W}^{(4)}| = 1$, the virtual channel

$$p(w_{1:n}^{(1)}y_{1:j}^{(1)}, w_{1:n}^{(2)}y_{1:j}^{(2)}, w_{1:n}^{(3)}y_{1:j}^{(3)}, w_{1:n}^{(4)}y_{1:j}^{(4)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, w_{1:n}^{(3)}, w_{1:n}^{(4)})$$

is also an interference channel. This is because $|\mathcal{W}_{1:n}^{(3)}| = |\mathcal{W}_{1:n}^{(4)}| = 1$, and

$$H(W_{1:n}^{(1)}Y_{1:j}^{(1)}|W_{1:n}^{(1)}) = 0$$

and

$$H(W_{1:n}^{(2)}Y_{1:j}^{(2)}|W_{1:n}^{(2)}) = 0.$$

In general, we consider a class of m-input/m-output multiterminal networks whose set of input alphabets $(\mathcal{X}^{(1)}, ..., \mathcal{X}^{(m)}, \mathcal{Y}^{(1)}, ..., \mathcal{Y}^{(m)})$ is in a given set $\mathcal{A}$ and whose conditional law $p(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)})$ is in a given set $\mathcal{Q}$. Furthermore, the set $\mathcal{Q}$ is assumed to include the channel

$$p(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}) = \prod_{i=1}^{m} \mathbf{1}[y^{(i)} = x^{(i)}].$$

Formal statement of the properties imposed on ϕ

Suppose we are given a class of m-input/m-output multiterminal networks, specified by sets $\mathcal{A}$ and $\mathcal{Q}$, as above. The formal statement of the properties imposed on ϕ is as follows. Please see Definitions 10 and 11 of section 5.2 for the notation used.

1. Assume that the conditional law $p(y^{(1)}y'^{(1)}, y^{(2)}y'^{(2)}, ..., y^{(m)}y'^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$ satisfies the following

   $$p(y^{(1)}y'^{(1)}, y^{(2)}y'^{(2)}, ..., y^{(m)}y'^{(m)}|x^{(1)}, ..., x^{(m)}) =$$
   $$p(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)}) \cdot p(y'^{(1)}, y'^{(2)}, ..., y'^{(m)}|x'^{(1)}, x'^{(2)}, ..., x'^{(m)}),$$

   where $X'^{(i)}$ is a deterministic function of $X^{(i)}Y^{(i)}$ (i.e. $H(X'^{(i)}|X^{(i)}Y^{(i)}) = 0$ $(i \in [m])$). We assume that

   $$(\mathcal{X}^{(1)}, ..., \mathcal{X}^{(m)}, \mathcal{Y}^{(1)} \times \mathcal{Y}'^{(1)}, ..., \mathcal{Y}^{(m)} \times \mathcal{Y}'^{(m)}),$$

   $$(\mathcal{X}^{(1)}, ..., \mathcal{X}^{(m)}, \mathcal{Y}^{(1)}, ..., \mathcal{Y}^{(m)})$$

   and

   $$(\mathcal{X}'^{(1)}, ..., \mathcal{X}'^{(m)}, \mathcal{Y}'^{(1)}, ..., \mathcal{Y}'^{(m)})$$

   are in $\mathcal{A}$, and the conditional laws $p(y^{(1)}y'^{(1)}, y^{(2)}y'^{(2)}, ..., y^{(m)}y'^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$, $p(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$ and $p(y'^{(1)}, y'^{(2)}, ..., y'^{(m)}|x'^{(1)}, x'^{(2)}, ..., x'^{(m)})$ are in $\mathcal{Q}$.
   Take an arbitrary input distribution $q(x^{(1)}, x^{(2)}, ..., x^{(m)})$. This input distribution, together with the conditional distribution $p(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$,

impose a joint distribution
$q(x'^{(1)}, x'^{(2)}, ..., x'^{(m)})$ on $(X'^{(1)}, X'^{(2)}, ..., X'^{(m)})$. Then the following constraint needs to be satisfied for any arbitrary set Ψ of joint distributions on $\mathcal{X}'^{(1)} \times \mathcal{X}'^{(2)} \times \cdots \times \mathcal{X}'^{(m)}$ that contains $q(x'^{(1)}, x'^{(2)}, ..., x'^{(m)})$:

$$\phi\Big(p(y^{(1)}y'^{(1)}, ..., y^{(m)}y'^{(m)}|x^{(1)}, ..., x^{(m)}), \{q(x^{(1)}, x^{(2)}, ..., x^{(m)})\}\Big) \subseteq$$
$$\phi\big(p(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}), \{q(x^{(1)}, x^{(2)}, ..., x^{(m)})\}\big)$$
$$\oplus \ \phi\big(p(y'^{(1)}, y'^{(2)}, ..., y'^{(m)}|x'^{(1)}, ..., x'^{(m)}), \Psi\big).$$

2. Assume that

$$p(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}) = \prod_{i=1}^{m} \mathbf{1}[y^{(i)} = x^{(i)}],$$

and that $(\mathcal{X}^{(1)}, ..., \mathcal{X}^{(m)}, \mathcal{Y}^{(1)}, ..., \mathcal{Y}^{(m)})$ is in $\mathcal{A}$. Then we require that for any input distribution $q(x^{(1)}, x^{(2)}, ..., x^{(m)})$, the set

$$\phi\big(p(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}), \{q(x^{(1)}, x^{(2)}, ..., x^{(m)})\}\big)$$

contains only the origin in $\mathbb{R}^d$.

Statement of the Main Lemma

Lemma 1. Take a physical channel $q(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)})$ whose set of input alphabets is in a given set $\mathcal{A}$, and whose conditional law is in a given set $\mathcal{Q}$. Let Ψ be a permissible set of input distributions for this channel. Then for any function ϕ satisfying the above two properties, target distortion levels $D^{(i)}$, and for arbitrary admissible source $W^{(i)}$ $(i \in [m])$ for these distortion levels for which for any n-code for the permissible set of input distributions Ψ, $p(w^{(1)}_{1:n}y^{(1)}_{1:k}, ..., w^{(m)}_{1:n}y^{(m)}_{1:k}|w^{(1)}_{1:n}, ..., w^{(m)}_{1:n})$ is in $\mathcal{Q}$, and $(\mathcal{W}^{(1)}_{1:n}, ..., \mathcal{W}^{(m)}_{1:n}, \mathcal{W}^{(1)}_{1:n} \times \mathcal{Y}^{(1)}_{1:k}, ..., \mathcal{W}^{(m)}_{1:n} \times \mathcal{Y}^{(m)}_{1:k})$ is in $\mathcal{A}$ for all $0 \leq k \leq n$, the following holds:

$$\phi\big(p(w^{(1)}_{1:n}y^{(1)}_{1:n}, ..., w^{(m)}_{1:n}y^{(m)}_{1:n}|w^{(1)}_{1:n}, ..., w^{(m)}_{1:n}), \{p(w^{(1)}_{1:n}, ..., w^{(m)}_{1:n})\}\big) \subseteq$$
$$n \times Convex\ Hull\big\{\phi\big(q(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}), \Psi\big)\big\}.$$

5.3.1 Proof

Proof of Lemma 1: Let random variables $X^{(i)}_k$ and $Y^{(i)}_k$ $(k \in [n], i \in [m])$ respectively represent the inputs and outputs of the multiterminal network. We have:

$$\phi\big(p(w^{(1)}_{1:n}y^{(1)}_{1:n}, w^{(2)}_{1:n}y^{(2)}_{1:n}, ..., w^{(m)}_{1:n}y^{(m)}_{1:n}|w^{(1)}_{1:n}, w^{(2)}_{1:n}, ..., w^{(m)}_{1:n}), \{p(w^{(1)}_{1:n}, w^{(2)}_{1:n}, ..., w^{(m)}_{1:n})\}\big) \subseteq \tag{5.1}$$

$$\phi\big(p(w_{1:n}^{(1)}y_{1:n-1}^{(1)}, w_{1:n}^{(2)}y_{1:n-1}^{(2)}, ..., w_{1:n}^{(m)}y_{1:n-1}^{(m)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)}), \{p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)})\}\big)\oplus$$
$$\phi(q(y_n^{(1)}, y_n^{(2)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)}), \Psi) \subseteq$$
$$\phi\big(p(w_{1:n}^{(1)}y_{1:n-2}^{(1)}, w_{1:n}^{(2)}y_{1:n-2}^{(2)}, ..., w_{1:n}^{(m)}y_{1:n-2}^{(m)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)}), \{p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)})\}\big)\oplus$$
$$\phi(q(y_{n-1}^{(1)}, y_{n-1}^{(2)}, ..., y_{n-1}^{(m)}|x_{n-1}^{(1)}, x_{n-1}^{(2)}, ..., x_{n-1}^{(m)}), \Psi)\oplus$$
$$\phi(q(y_n^{(1)}, y_n^{(2)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)}), \Psi) \subseteq$$
$$\cdots \subseteq$$
$$\phi\big(p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)}), \{p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)})\}\big)\oplus$$
$$\phi(q(y_1^{(1)}, y_1^{(2)}, ..., y_1^{(m)}|x_1^{(1)}, x_1^{(2)}, ..., x_1^{(m)}), \Psi)\oplus$$
$$\phi(q(y_2^{(1)}, y_2^{(2)}, ..., y_2^{(m)}|x_2^{(1)}, x_2^{(2)}, ..., x_2^{(m)}), \Psi) \oplus \cdots$$
$$\phi(q(y_{n-1}^{(1)}, y_{n-1}^{(2)}, ..., y_{n-1}^{(m)}|x_{n-1}^{(1)}, x_{n-1}^{(2)}, ..., x_{n-1}^{(m)}), \Psi)\oplus$$
$$\phi(q(y_n^{(1)}, y_n^{(2)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)}), \Psi) \subseteq \tag{5.2}$$
$$\phi(q(y_1^{(1)}, y_1^{(2)}, ..., y_1^{(m)}|x_1^{(1)}, x_1^{(2)}, ..., x_1^{(m)}), \Psi)\oplus$$
$$\phi(q(y_2^{(1)}, y_2^{(2)}, ..., y_2^{(m)}|x_2^{(1)}, x_2^{(2)}, ..., x_2^{(m)}), \Psi) \oplus \cdots$$
$$\phi(q(y_{n-1}^{(1)}, y_{n-1}^{(2)}, ..., y_{n-1}^{(m)}|x_{n-1}^{(1)}, x_{n-1}^{(2)}, ..., x_{n-1}^{(m)}), \Psi)\oplus$$
$$\phi(q(y_n^{(1)}, y_n^{(2)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)}), \Psi) \subseteq \tag{5.3}$$
$$n \times Convex\ Hull\big\{\phi(q(y^{(1)}, y^{(2)}, ..., y^{(m)}|x^{(1)}, x^{(2)}, ..., x^{(m)}), \Psi)\big\},$$

where in equation (5.1) we have used property (1) because

$$p(w_{1:n}^{(1)}y_{1:n}^{(1)}, w_{1:n}^{(2)}y_{1:n}^{(2)}, ..., w_{1:n}^{(m)}y_{1:n}^{(m)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)}) =$$
$$p(w_{1:n}^{(1)}y_{1:n-1}^{(1)}, w_{1:n}^{(2)}y_{1:n-1}^{(2)}, ..., w_{1:n}^{(m)}y_{1:n-1}^{(m)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, ..., w_{1:n}^{(m)})\cdot p(y_n^{(1)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)})$$

and furthermore $H(X_n^{(i)}|W_{1:n}^{(i)}Y_{1:n-1}^{(i)}) = 0$ for all $i \in [m]$, and also

$$p(y_n^{(1)}, y_n^{(2)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)}) = q(y_n^{(1)}, y_n^{(2)}, ..., y_n^{(m)}|x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)}).$$

Since the n-code must work with the permissible set of input distributions Ψ, the joint distribution $p(x_n^{(1)}, x_n^{(2)}, ..., x_n^{(m)})$ is in Ψ. In equation (5.2) we have used property (2). In equation (5.3), we first note that the conditional distributions

$$q(y_i^{(1)}, y_i^{(2)}, ..., y_i^{(m)}|x_i^{(1)}, x_i^{(2)}, ..., x_i^{(m)})$$

for $i = 1, 2, ..., n$ are all the same. We then observe that whenever

$$\overrightarrow{v_i} \in \phi(q(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}), \Psi)$$

for $i \in [n]$, their average, $\frac{1}{n}\sum_{i=1}^{n}\overrightarrow{v_i}$, falls in the convex hull of

$$\phi(q(y^{(1)}, ..., y^{(m)}|x^{(1)}, ..., x^{(m)}), \Psi).$$

■

Remark 1. The second property of ϕ is used in the proof to reduce the n-letter expression

$$\phi\big(p(w_{1:n}^{(1)}y_{1:n}^{(1)},...,w_{1:n}^{(m)}y_{1:n}^{(m)}|w_{1:n}^{(1)},...,w_{1:n}^{(m)}),\{p(w_{1:n}^{(1)},...,w_{1:n}^{(m)})\}\big)$$

to n single-letter expressions involving $\phi(q(y^{(1)},...,y^{(m)}|x^{(1)},...,x^{(m)}),\Psi)$ in n stages.

5.4 Correlated sources over strong interference channels

5.4.1 Introduction

We prove a new outer bound to the admissible source region of a strong interference channel with arbitrarily correlated sources. As a special case, we recover the converse part of the capacity region given by Maric, Yates and Kramer [36] for strong interference channels with common information.

An interference channel is said to be *strong* if

$$I(X^{(1)};Y^{(3)}|X^{(2)}) \leq I(X^{(1)};Y^{(4)}|X^{(2)}); \tag{5.4}$$
$$I(X^{(2)};Y^{(4)}|X^{(1)}) \leq I(X^{(2)};Y^{(3)}|X^{(1)}), \tag{5.5}$$

for all product distributions on $\mathcal{X}^{(1)}\times\mathcal{X}^{(2)} := \{(x^{(1)},x^{(2)}) : x^{(1)}\in\mathcal{X}^{(1)}, x^{(2)}\in\mathcal{X}^{(2)}\}$. This condition then automatically extends to all joint distributions on $\mathcal{X}^{(1)}\times\mathcal{X}^{(2)}$.

Costa and El Gamal found the capacity region of a strong interference channel when the transmitters send independent private messages to their intended receivers [6]. Recently, this result was extended by Maric, Yates and Kramer, who assumed that the transmitters additionally have a common message that needs to be sent to both the receivers [36]. In this problem a new feature arises: the inputs $X^{(1)}$ and $X^{(2)}$ are no longer guaranteed to be independent throughout the communication, since the transmitters have correlated information. Maric, Yates and Kramer found the capacity region to be the union over $p(u,x^{(1)},x^{(2)},y^{(3)},y^{(4)}) = p(u)p(x^{(1)}|u)p(x^{(2)}|u)q(y^{(3)},y^{(4)}|x^{(1)},x^{(2)})$, of the set of all non-negative triples (R_0,R_1,R_2) satisfying

$$\begin{aligned}
R_1 &\leq I(X^{(1)};Y^{(3)}|X^{(2)},U);\\
R_2 &\leq I(X^{(2)};Y^{(4)}|X^{(1)},U);\\
R_1+R_2 &\leq \min(I(X^{(1)}X^{(2)};Y^{(3)}|U),I(X^{(1)}X^{(2)};Y^{(4)}|U));\\
R_0+R_1+R_2 &\leq \min(I(X^{(1)}X^{(2)};Y^{(3)}),I(X^{(1)}X^{(2)};Y^{(4)})).
\end{aligned} \tag{5.6}$$

In the above expressions R_0 denotes the common message rate, and R_1 and R_2 are respectively the private message rates of the first and second transmitter.

The communication task is formulated as before. In an interference channel with arbitrarily dependent sources, the transmitters are observing i.i.d. repetitions of two, possibly dependent, random variables $W^{(1)}$ and $W^{(2)}$. The transmitters would like to reliably send the i.i.d. copies of $W^{(1)}$ to the receiver $Y^{(3)}$ and the i.i.d. copies of $W^{(2)}$ to the receiver $Y^{(4)}$. To be notationally consistent, we assume that the third and fourth party are observing i.i.d. copies of $W^{(3)}$ and $W^{(4)}$, but that $|\mathcal{W}^{(3)}| = |\mathcal{W}^{(4)}| = 1$ implying that these random variables are constant. Roughly speaking, the source marginal distribution $p(w^{(1)}, w^{(2)}, w^{(3)}, w^{(4)})$ is called admissible if there exists a strategy for reliable transmission of the i.i.d copies of $W^{(1)}$ and $W^{(2)}$ to the intended receivers. A formal definition can be made by setting $M^{(1)} = f^{(1)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(1)}$, $M^{(2)} = f^{(2)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(2)}$, $M^{(3)} = f^{(3)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(1)}$ and $M^{(4)} = f^{(4)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(2)}$. Note that the definitions of $f^{(1)}$ and $f^{(2)}$ reflect the fact that neither transmitter is expected to recover the message of the other transmitter. We require the i^{th} party to reconstruct the i.i.d repetitions of $f^{(i)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)})$ with a vanishing average distortion. The distortion function used by the i^{th} party, $\Delta^{(i)}(m^{(i)}, m^{'(i)})$ (for $1 \leq i \leq 4$) is taken to be the indicator function $\mathbf{1}[m^{(i)} \neq m^{'(i)}]$. Since we are proving an outer bound, the main result can be carried over to the problem of "lossless transmission" since requiring the i^{th} party to reconstruct the i.i.d. repetitions of $M^{(i)} = f^{(i)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)})$ with arbitrarily small average probability of error is no stronger than requiring the i^{th} party to reconstruct the i.i.d repetitions of $M^{(i)}$ with a vanishing average distortion. Further, our notion of correlated source is strictly more general than that considered in [36]. For example, take three mutually independent binary random variables $L \sim Bern(\frac{1}{2})$, $N_1 \sim Bern(p_1)$ and $N_2 \sim Bern(p_2)$ and let $W^{(1)} = L \oplus N_1$ and $W^{(2)} = L \oplus N_2$ where the addition is modulo two. Since the common part of $W^{(1)}$ and $W^{(2)}$ in the sense of Gács and Körner [16] is a constant random variable, one cannot represent the dependence between the i.i.d. copies of $W^{(1)}$ and $W^{(2)}$ through a random variable that is computable by both the parties, a restriction which is required in [36]. However we only prove an outer bound whereas [36] computes the capacity region. Our outer bound reduces to the region of [36] in the case of correlated sources of the type considered there.

The admissible source region of a strong interference channel with correlated sources is not known except in certain special cases. Inner bounds to the admissible source region are reported in [25] and [49]. We are not aware of any previous work discussing any interesting outer bounds on the admissible source region of an interference channel with dependent sources. It is known that the source−channel separation theorem breaks down for multi-access channels [7] and multi-access channels (MACs) are special cases of strong interference channels. One can therefore not expect that finding outer bounds on an interference channel with correlated sources can be resolved by a source−channel separation approach. Further, since the problem of determining the admissible source region for a MAC with correlated sources is still unsolved, determining the admissible region for a strong interference channel

is a difficult one.

5.4.2 Statement of the new converse

An interference channel is a four-input/four-output multiterminal network whose set of alphabets is assumed to belong to

$$\mathcal{A}_{interference} := \big\{\big(\mathcal{X}^{(1)}, \mathcal{X}^{(2)}, \mathcal{X}^{(3)}, \mathcal{X}^{(4)}, \mathcal{Y}^{(1)}, \mathcal{Y}^{(2)}, \mathcal{Y}^{(3)}, \mathcal{Y}^{(4)}\big) : |\mathcal{X}^{(3)}| = |\mathcal{X}^{(4)}| = 1\big\},$$

and whose conditional law is assumed to belong to

$$\mathcal{Q}_{interference} :=$$
$$\big\{q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}) : H(Y^{(1)}|X^{(1)}) = H(Y^{(2)}|X^{(2)}) = 0\big\}.$$

As discussed in subsection 5.4.1, we consider strong interference channels and assume that the third and fourth party are observing i.i.d. copies of $W^{(3)}$ and $W^{(4)}$, but that $|\mathcal{W}^{(3)}| = |\mathcal{W}^{(4)}| = 1$ implying that these random variables are constant. Furthermore, we consider the special case of

$$\begin{aligned} M^{(1)} &= f^{(1)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(1)}, \\ M^{(2)} &= f^{(2)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(2)} \\ M^{(3)} &= f^{(3)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(1)} \\ M^{(4)} &= f^{(4)}(W^{(1)}, W^{(2)}, W^{(3)}, W^{(4)}) = W^{(2)}, \end{aligned}$$

and $D^{(i)} = 0$ for $i = 1, 2, 3, 4$. The distortion function used by the i^{th} party, $\Delta^{(i)}(m^{(i)}, m'^{(i)})$ (for $1 \leq i \leq 4$) is taken to be the indicator function $\mathbf{1}[m^{(i)} \neq m'^{(i)}]$.

We state our main result in terms of the nebulously defined permissible set of input distributions Ψ. To get explicit results, simply replace Ψ by the set of all probability distributions on $\mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \times \mathcal{X}^{(3)} \times \mathcal{X}^{(4)}$. Our main result is the following:

Theorem 9. Take an arbitrary interference channel $q(y^{(1)}, ..., y^{(4)}|x^{(1)}, ..., x^{(4)})$, a permissible set of input distributions Ψ, and an admissible source marginal distribution $p(w^{(1)}, w^{(2)}, w^{(3)}, w^{(4)})$ at zero distortion levels satisfying $|\mathcal{W}^{(3)}| = |\mathcal{W}^{(4)}| = 1$. Then for any random variable L where $W^{(1)} \to L \to W^{(2)}$ holds, there must exist

$$p(u, x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)})$$

such that

$p(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$ is in the convex hull of Ψ,
$p(u, x^{(1)}, x^{(2)}, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}) = p(u)p(x^{(1)}|u)p(x^{(2)}|u)q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)})$,

(note that

$$q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)})$$

can be used for

$$q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$$

because of the standing assumption that $|\mathcal{X}^{(3)}| = |\mathcal{X}^{(4)}| = 1\big)$ such the following inequalities hold:

$$\begin{aligned}
H(W^{(1)}|L) &\leq I(X^{(1)}; Y^{(3)}|X^{(2)}, U); \\
H(W^{(2)}|L) &\leq I(X^{(2)}; Y^{(4)}|X^{(1)}, U); \\
H(W^{(1)}|L) + H(W^{(2)}|L) &\leq \min(I(X^{(1)}X^{(2)}; Y^{(3)}|U), I(X^{(1)}X^{(2)}; Y^{(4)}|U)); \\
H(W^{(1)}W^{(2)}) &\leq \min(I(X^{(1)}X^{(2)}; Y^{(3)}), I(X^{(1)}X^{(2)}; Y^{(4)})); \\
H(W^{(1)}|W^{(2)}) &\leq I(X^{(1)}; Y^{(3)}|X^{(2)}); \\
H(W^{(2)}|W^{(1)}) &\leq I(X^{(2)}; Y^{(4)}|X^{(1)}).
\end{aligned} \tag{5.7}$$

Remark 2. One can use the strengthened Carathéodory theorem of Fenchel to bound the cardinality of U from above by $|\mathcal{X}^{(1)}||\mathcal{X}^{(2)}| + 3$.

5.4.3 Proof

Proof of Theorem 9: In order to apply Lemma 1, we will define $\phi(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \Psi)$, a function that takes as input an arbitrary 4-input/4-output multiterminal network from $\mathcal{Q}_{interference}$, where the alphabets are from $\mathcal{A}_{interference}$ and a subset of probability distributions on $\mathcal{X}^{(1)} \times \mathcal{X}^{(2)} \times \mathcal{X}^{(3)} \times \mathcal{X}^{(4)}$ and returns a subset of $\mathbb{R}_+^8$. We let:

$$\phi(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \Psi) =$$

$$\bigcup_{p(x^{(1)},x^{(2)},x^{(3)},x^{(4)}) \in \Psi} \quad \bigcup_{\substack{U \text{ such that} \\ X^{(1)} \to U \to X^{(2)}, \\ U \to X^{(1)}X^{(2)} \to Y^{(3)}Y^{(4)}}}$$

$$\Pi\Big(\big\{ \big(I(X^{(1)}; Y^{(3)}|X^{(2)}, U),\ I(X^{(2)}; Y^{(4)}|X^{(1)}, U),\ I(X^{(1)}X^{(2)}; Y^{(3)}|U),$$

$$I(X^{(1)}X^{(2)}; Y^{(4)}|U),\ I(X^{(1)}X^{(2)}; Y^{(3)}),\ I(X^{(1)}X^{(2)}; Y^{(4)}),$$

$$I(X^{(1)}; Y^{(3)}|X^{(2)}),\ I(X^{(2)}; Y^{(4)}|X^{(1)}) \big) \big\} \Big).$$

In Appendix I of section 5.4.4, we show that the above choice of ϕ verifies the properties of Lemma 1 for $\mathcal{A}_{interference}$ and $\mathcal{Q}_{interference}$. Take an arbitrary interference channel

$$q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}),$$

an arbitrary admissible source marginal distribution

$$p(w^{(1)}, w^{(2)}, w^{(3)}, w^{(4)})$$

satisfying $|\mathcal{W}^{(3)}| = |\mathcal{W}^{(4)}| = 1$, and a permissible set of input distributions, Ψ. Let $\overline{\Psi}$ denote the convex hull of Ψ; $\overline{\Psi}$ itself is a permissible set of input distributions. The conditions of Lemma 1 are satisfied for $\mathcal{A}_{interference}$ and $\mathcal{Q}_{interference}$ since $|\mathcal{W}^{(3)}_{1:n}| = |\mathcal{W}^{(4)}_{1:n}| = 1$ and $H(W^{(1)}_{1:n}Y^{(1)}_{1:k}|W^{(1)}_{1:n}) = H(W^{(2)}_{1:n}Y^{(2)}_{1:k}|W^{(2)}_{1:n}) = 0$ for any $1 \leq k \leq n$. For any arbitrary positive ϵ and n-code for which at each stage the inputs belong to the permissible set of input distributions Ψ, the lemma implies

$$\phi\big(p(w^{(1)}_{1:n}y^{(1)}_{1:n}, w^{(2)}_{1:n}y^{(2)}_{1:n}, w^{(3)}_{1:n}y^{(3)}_{1:n}, w^{(4)}_{1:n}y^{(4)}_{1:n}|w^{(1)}_{1:n}, w^{(2)}_{1:n}, w^{(3)}_{1:n}, w^{(4)}_{1:n}), \{p(w^{(1)}_{1:n}, w^{(2)}_{1:n}, w^{(3)}_{1:n}, w^{(4)}_{1:n})\}\big) \subseteq$$
$$n \times Convex\ Hull\big\{\phi\big(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \overline{\Psi}\big)\big\}. \tag{5.8}$$

In Appendix II of section 5.4.4 we show that

$$n \times \Big(H(W^{(1)}|L) - O(h(\epsilon)), H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)),$$
$$H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}W^{(2)}) - O(h(\epsilon)),$$
$$H(W^{(1)}W^{(2)}) - O(h(\epsilon)), H(W^{(1)}|W^{(2)}) - O(h(\epsilon)), H(W^{(2)}|W^{(1)}) - O(h(\epsilon))\Big) \in$$
$$\phi\big(p(w^{(1)}_{1:n}y^{(1)}_{1:n}, w^{(2)}_{1:n}y^{(2)}_{1:n}, w^{(3)}_{1:n}y^{(3)}_{1:n}, w^{(4)}_{1:n}y^{(4)}_{1:n}|w^{(1)}_{1:n}, w^{(2)}_{1:n}, w^{(3)}_{1:n}, w^{(4)}_{1:n}), \{p(w^{(1)}_{1:n}, w^{(2)}_{1:n}, w^{(3)}_{1:n}, w^{(4)}_{1:n})\}\big). \tag{5.9}$$

In the above expression $O(h(\epsilon))$ we mean a constant (that depends only on the network $q(y^{(1)}, ..., y^{(4)}|x^{(1)}, ..., x^{(4)})$) times $h(\epsilon)$. Here $h(\cdot)$ is the binary entropy function. Equations (5.8) and (5.9) imply that

$$\Big(H(W^{(1)}|L) - O(h(\epsilon)), H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)),$$
$$H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}W^{(2)}) - O(h(\epsilon)),$$
$$H(W^{(1)}W^{(2)}) - O(h(\epsilon)), H(W^{(1)}|W^{(2)}) - O(h(\epsilon)), H(W^{(2)}|W^{(1)}) - O(h(\epsilon))\Big) \in$$
$$Convex\ Hull\big\{\phi\big(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \overline{\Psi}\big)\big\}.$$

In Appendix III of section 5.4.4 we show that for any interference channel $q(y^{(1)}, ..., y^{(4)}|x^{(1)}, ..., x^{(4)})$, $\phi\big(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \Psi\big)$ is convex when the set Ψ is convex. Hence

$$\Big(H(W^{(1)}|L) - O(h(\epsilon)), H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)),$$

$$H(W^{(1)}|L)+H(W^{(2)}|L)-O(h(\epsilon)), H(W^{(1)}W^{(2)})-O(h(\epsilon)),$$
$$H(W^{(1)}W^{(2)})-O(h(\epsilon)), H(W^{(1)}|W^{(2)})-O(h(\epsilon)), H(W^{(2)}|W^{(1)})-O(h(\epsilon))\Big) \in$$
$$\phi\big(q(y^{(1)},y^{(2)},y^{(3)},y^{(4)}|x^{(1)},x^{(2)},x^{(3)},x^{(4)}),\overline{\Psi}\big).$$

Since $\phi\big(q(y^{(1)},y^{(2)},y^{(3)},y^{(4)}|x^{(1)},x^{(2)},x^{(3)},x^{(4)}),\overline{\Psi}\big)$ is closed (since the cardinality of U can be bounded, as mentioned in remark 2), letting ϵ converge to zero, we get

$$\Big(H(W^{(1)}|L), H(W^{(2)}|L), H(W^{(1)}|L)+H(W^{(2)}|L), H(W^{(1)}|L)+H(W^{(2)}|L),$$
$$H(W^{(1)}W^{(2)}), H(W^{(1)}W^{(2)}), H(W^{(1)}|W^{(2)}), H(W^{(2)}|W^{(1)})\Big) \in$$
$$\phi\big(q(y^{(1)},y^{(2)},y^{(3)},y^{(4)}|x^{(1)},x^{(2)},x^{(3)},x^{(4)}),\overline{\Psi}\big).$$

The above equation completes the proof of Theorem 9. ■

5.4.4 Appendices

Appendix I: Verifying the properties of Lemma 1

In this appendix we show that our choice of ϕ verifies the two properties of the main lemma for $m=4$ when restricted to the class of interference channels. For the first property of the lemma, take a channel

$$p(y^{(1)}y'^{(1)},...,y^{(4)}y'^{(4)}|x^{(1)},...,x^{(4)}) =$$
$$p(y^{(1)},...,y^{(4)}|x^{(1)},...,x^{(4)})\cdot p(y'^{(1)},...,y'^{(4)}|x'^{(1)},...,x'^{(4)})$$

where $H(X'^{(i)}|X^{(i)}Y^{(i)})=0$ for $1\le i\le 4$. Take an arbitrary point from

$$\phi\big(p(y^{(1)}y'^{(1)},...,y^{(4)}y'^{(4)}|x^{(1)},...,x^{(4)}),\{q(x^{(1)},...,x^{(4)})\}\big).$$

The set of input distributions contains only one distribution $q(x^{(1)},...,x^{(4)})$. Therefore we define random variables $X^{(1)},X^{(2)},...,X^{(4)},Y^{(1)},Y'^{(1)},...,Y^{(4)},Y'^{(4)}$ jointly distributed according to

$$p(y^{(1)}y'^{(1)},...,y^{(4)}y'^{(4)}|x^{(1)},...,x^{(4)})\cdot q(x^{(1)},...,x^{(4)}) =$$
$$p(y^{(1)},...,y^{(4)}|x^{(1)},...,x^{(4)})\cdot p(y'^{(1)},...,y'^{(4)}|x'^{(1)},...,x'^{(4)})\cdot q(x^{(1)},...,x^{(4)}).$$

Corresponding to the arbitrary point in

$$\phi\big(p(y^{(1)}y'^{(1)},...,y^{(4)}y'^{(4)}|x^{(1)},...,x^{(4)}),\{q(x^{(1)},...,x^{(4)})\}\big)$$

is a random variable U satisfying

$$X^{(1)} \to U \to X^{(2)}$$

and

$$U \to X^{(1)}X^{(2)} \to Y^{(3)}Y^{(4)}Y^{'(3)}Y^{'(4)}$$

such that the point is coordinate by coordinate less than or equal to the point

$$\overrightarrow{v} = \big(I(X^{(1)};Y^{(3)}Y^{'(3)}|X^{(2)},U),\ I(X^{(2)};Y^{(4)}Y^{'(4)}|X^{(1)},U),\ I(X^{(1)}X^{(2)};Y^{(3)}Y^{'(3)}|U),$$
$$I(X^{(1)}X^{(2)};Y^{(4)}Y^{'(4)}|U),\ I(X^{(1)}X^{(2)};Y^{(3)}Y^{'(3)}),\ I(X^{(1)}X^{(2)};Y^{(4)}Y^{'(4)}),$$
$$I(X^{(1)};Y^{(3)}Y^{'(3)}|X^{(2)}),\ I(X^{(2)};Y^{(4)}Y^{'(4)}|X^{(1)})\big)$$

Since $p(y^{(1)},...,y^{(4)}|x^{(1)},...,x^{(4)})$ and $p(y^{'(1)},...,y^{'(4)}|x^{'(1)},...,x^{'(4)})$ belong to the class of interference channels, we have $H(Y^{(1)}|X^{(1)}) = H(Y^{(2)}|X^{(2)}) = 0$. $H(X^{'(1)}|X^{(1)}Y^{(1)}) = H(X^{'(2)}|X^{(2)}Y^{(2)}) = 0$ then implies that $H(X^{'(1)}|X^{(1)}) = 0$ and $H(X^{'(2)}|X^{(2)}) = 0$. Since $|\mathcal{X}^{(3)}| = |\mathcal{X}^{(4)}| = |\mathcal{X}^{'(3)}| = |\mathcal{X}^{'(4)}| = 1$

$$p(y^{(3)}y^{'(3)},y^{(4)}y^{'(4)}|x^{(1)},x^{(2)},x^{(3)},x^{(4)}) =$$
$$p(y^{(3)},y^{(4)}|x^{(1)},x^{(2)}) \cdot p(y^{'(3)},y^{'(4)}|x^{'(1)},x^{'(2)}).$$

Since $X^{(1)} \to U \to X^{(2)}$ and $U \to X^{(1)}X^{(2)} \to Y^{(3)}Y^{(4)}$, the point

$$\overrightarrow{v_1} = \big(I(X^{(1)};Y^{(3)}|X^{(2)},U),\ I(X^{(2)};Y^{(4)}|X^{(1)},U),\ I(X^{(1)}X^{(2)};Y^{(3)}|U),$$
$$I(X^{(1)}X^{(2)};Y^{(4)}|U),\ I(X^{(1)}X^{(2)};Y^{(3)}),\ I(X^{(1)}X^{(2)};Y^{(4)}),$$
$$I(X^{(1)};Y^{(3)}|X^{(2)}),\ I(X^{(2)};Y^{(4)}|X^{(1)})\big)$$

belongs to $\phi\big(p(y^{(1)},...,y^{(4)}|x^{(1)},...,x^{(4)}),\{q(x^{(1)},x^{(2)},...,x^{(4)})\}\big)$. Next, note that $X^{(1)} \to U \to X^{(2)}$ implies $X^{'(1)} \to U \to X^{'(2)}$ since $H(X^{'(1)}|X^{(1)}) = 0$ and $H(X^{'(2)}|X^{(2)}) = 0$. Furthermore $U \to X^{'(1)}X^{'(2)} \to Y^{'(3)}Y^{'(4)}$ since

$$p(u,x^{(1)},x^{(2)},x^{'(1)},x^{'(2)},y^{'(3)},y^{'(4)}) =$$
$$p(x^{(1)},x^{(2)})p(u|x^{(1)},x^{(2)})p(x^{'(1)},x^{'(2)}|x^{(1)},x^{(2)})p(y^{'(3)},y^{'(4)}|x^{'(1)},x^{'(2)}).$$

Thus the point

$$\overrightarrow{v_2} = \big(I(X^{'(1)};Y^{'(3)}|X^{'(2)},U),\ I(X^{'(2)};Y^{'(4)}|X^{'(1)},U),\ I(X^{'(1)}X^{'(2)};Y^{'(3)}|U),$$
$$I(X^{'(1)}X^{'(2)};Y^{'(4)}|U),\ I(X^{'(1)}X^{'(2)};Y^{'(3)}),\ I(X^{'(1)}X^{'(2)};Y^{'(4)}),$$
$$I(X^{'(1)};Y^{'(3)}|X^{'(2)}),\ I(X^{'(2)};Y^{'(4)}|X^{'(1)})\big)$$

belongs to $\phi\big(p(y^{'(1)},y^{'(2)},...,y^{'(4)}|x^{'(1)},...,x^{'(4)}),\Psi\big)$ where Ψ is a given set that contains $q(x^{'(1)},...,x^{'(4)})$.

It suffices to show that $\overrightarrow{v} \leq \overrightarrow{v_1} + \overrightarrow{v_2}$. This is straightforward, once one observes that

$$p(y'^{(3)}, y'^{(4)}|x^{(1)}, x'^{(1)}, x^{(2)}, x'^{(2)}, u) = p(y'^{(3)}, y'^{(4)}|x'^{(1)}, x^{(2)})$$

and

$$p(x^{(2)}, x'^{(2)}, x^{(1)}, x'^{(1)}, y'^{(3)}, y'^{(4)}|u) =$$
$$p(x^{(2)}|u)p(x'^{(2)}|x^{(2)})p(x^{(1)}|u)p(x'^{(1)}|x^{(1)})p(y'^{(3)}, y'^{(4)}|x'^{(1)}, x'^{(2)}).$$

The proof for the second property is straightforward since $Y^{(3)} = X^{(3)} = constant$, and $Y^{(4)} = X^{(4)} = constant$ implying that all the mutual information terms are zero. ■

Appendix II

In the proof of Theorem 9, we claimed that the point

$$n \times \Big(H(W^{(1)}|L) - O(h(\epsilon)), H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)),$$
$$H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}W^{(2)}) - O(h(\epsilon)),$$
$$H(W^{(1)}W^{(2)}) - O(h(\epsilon)), H(W^{(1)}|W^{(2)}) - O(h(\epsilon)), H(W^{(2)}|W^{(1)}) - O(h(\epsilon)) \Big)$$

is in the set

$$\phi\big(p(w_{1:n}^{(1)}y_{1:n}^{(1)}, w_{1:n}^{(2)}y_{1:n}^{(2)}, w_{1:n}^{(3)}y_{1:n}^{(3)}, w_{1:n}^{(4)}y_{1:n}^{(4)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, w_{1:n}^{(3)}, w_{1:n}^{(4)}), \{p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, w_{1:n}^{(3)}, w_{1:n}^{(4)})\}\big). \tag{5.10}$$

Here $O(h(\epsilon))$ is equal to a constant (that depends only on the network architecture) times $h(\epsilon)$. Here $h(\cdot)$ is the binary entropy function. In this appendix we show that this equation holds.

Here, because of the assumptions on the alphabets, we can think of the overall virtual channel as being $p(y_{1:n}^{(3)}, y_{1:n}^{(4)}|w_{1:n}^{(1)}, w_{1:n}^{(2)})$ and the set of admissible distributions as being $p(w_{1:n}^{(1)}, w_{1:n}^{(2)})$ where random variables $W_{1:n}^{(1)}, W_{1:n}^{(2)}, Y_{1:n}^{(3)}, Y_{1:n}^{(4)}$ are distributed according to

$$p(y_{1:n}^{(3)}, y_{1:n}^{(4)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}) \cdot p(w_{1:n}^{(1)}, w_{1:n}^{(2)})$$

and $L_{1:n}$ is jointly distributed with $W_{1:n}^{(1)}, W_{1:n}^{(2)}, Y_{1:n}^{(3)}, Y_{1:n}^{(4)}$ according to

$$p(y_{1:n}^{(3)}, y_{1:n}^{(4)}, w_{1:n}^{(1)}, w_{1:n}^{(2)}) \cdot \prod_{i=1}^{n} p(l_i|w_i^{(1)}, w_i^{(2)}),$$

and such that we have $W_{1:n}^{(1)} \to L_{1:n} \to W_{1:n}^{(2)}$ and $L_{1:n} \to W_{1:n}^{(1)}W_{1:n}^{(2)} \to Y_{1:n}^{(3)}Y_{1:n}^{(4)}$. The set

$$\phi\big(p(w_{1:n}^{(1)}y_{1:n}^{(1)}, w_{1:n}^{(2)}y_{1:n}^{(2)}, w_{1:n}^{(3)}y_{1:n}^{(3)}, w_{1:n}^{(4)}y_{1:n}^{(4)}|w_{1:n}^{(1)}, w_{1:n}^{(2)}, w_{1:n}^{(3)}, w_{1:n}^{(4)}), \{p(w_{1:n}^{(1)}, w_{1:n}^{(2)}, w_{1:n}^{(3)}, w_{1:n}^{(4)})\}\big)$$

by definition contains the following point:

$$\overrightarrow{v} = \big(I(W_{1:n}^{(1)}; Y_{1:n}^{(3)}|W_{1:n}^{(2)}, L_{1:n}),\ I(W_{1:n}^{(2)}; Y_{1:n}^{(4)}|W_{1:n}^{(1)}, L_{1:n}),\ I(W_{1:n}^{(1)}W_{1:n}^{(2)}; Y_{1:n}^{(3)}|L_{1:n}),$$

$$I(W_{1:n}^{(1)}W_{1:n}^{(2)}; Y_{1:n}^{(4)}|L_{1:n}),\ I(W_{1:n}^{(1)}W_{1:n}^{(2)}; Y_{1:n}^{(3)}),\ I(W_{1:n}^{(1)}W_{1:n}^{(2)}; Y_{1:n}^{(4)}),$$

$$I(W_{1:n}^{(1)}; Y_{1:n}^{(3)}|W_{1:n}^{(2)}),\ I(W_{1:n}^{(2)}; Y_{1:n}^{(4)}|W_{1:n}^{(1)})\big).$$

We show that $\overrightarrow{v}$ is pointwise greater than or equal to

$$n \times \Big(H(W^{(1)}|L) - O(h(\epsilon)), H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)),$$

$$H(W^{(1)}|L) + H(W^{(2)}|L) - O(h(\epsilon)), H(W^{(1)}W^{(2)}) - O(h(\epsilon)),$$

$$H(W^{(1)}W^{(2)}) - O(h(\epsilon)), H(W^{(1)}|W^{(2)}) - O(h(\epsilon)), H(W^{(2)}|W^{(1)}) - O(h(\epsilon))\Big).$$

We only give the proof for the first, third, fifth and seventh element of $\overrightarrow{v}$. The proof for the other coordinates is similar.

- The first coordinate:

$$I(W_{1:n}^{(1)}; Y_{1:n}^{(3)}|W_{1:n}^{(2)}L_{1:n}) = H(W_{1:n}^{(1)}|W_{1:n}^{(2)}L_{1:n}) - H(W_{1:n}^{(1)}|W_{1:n}^{(2)}L_{1:n}Y_{1:n}^{(3)}) =$$

$$n \cdot [H(W^{(1)}|W^{(2)}L) - O(h(\epsilon))$$

because of lemma 2 mentioned at the end of this appendix. Here $h(\cdot)$ denotes the binary entropy function. Note that $H(W^{(1)}|W^{(2)}L) = H(W^{(1)}|L)$.

- The third coordinate:

$$I(W_{1:n}^{(1)}W_{1:n}^{(2)}; Y_{1:n}^{(3)}|L_{1:n}) = H(W_{1:n}^{(1)}W_{1:n}^{(2)}|L_{1:n}) - H(W_{1:n}^{(1)}W_{1:n}^{(2)}|L_{1:n}Y_{1:n}^{(3)}) =$$

$$n \cdot [H(W^{(1)}W^{(2)}|L) - O(h(\epsilon))]$$

because of lemma 2 mentioned at the end of this appendix. Here $h(\cdot)$ denotes the binary entropy function. Furthermore, note that $H(W^{(1)}W^{(2)}|L) = H(W^{(1)}|L) + H(W^{(2)}|L)$.

- The fifth coordinate:

$I(W_{1:n}^{(1)}W_{1:n}^{(2)}; Y_{1:n}^{(3)}) = H(W_{1:n}^{(1)}W_{1:n}^{(2)}) - H(W_{1:n}^{(1)}W_{1:n}^{(2)}|Y_{1:n}^{(3)}) = n \cdot [H(W^{(1)}W^{(2)}) - O(h(\epsilon))]$ because of lemma 2 mentioned at the end of this appendix.

- The seventh coordinate:

$I(W_{1:n}^{(1)}; Y_{1:n}^{(3)}|W_{1:n}^{(2)}) = H(W_{1:n}^{(1)}|W_{1:n}^{(2)}) - H(W_{1:n}^{(1)}|W_{1:n}^{(2)}Y_{1:n}^{(3)}) = n \cdot [H(W^{(1)}|W^{(2)}) - O(h(\epsilon))$ because of lemma 2 mentioned at the end of this appendix. Here $h(\cdot)$ denotes the binary entropy function. ■

Lemma 2. Given any admissible source marginal distribution $p(w^{(1)}, w^{(2)}, w^{(3)}, w^{(4)})$ for a strong interference channel $q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$ satisfying $|\mathcal{W}^{(3)}| = |\mathcal{W}^{(4)}| = 1$, and an arbitrary positive ϵ and n-code, we have:

$$\frac{1}{n}H(W_{1:n}^{(1)}W_{1:n}^{(2)}|Y_{1:n}^{(3)}) = O(h(\epsilon)), \tag{5.11}$$

$$\frac{1}{n}H(W_{1:n}^{(1)}W_{1:n}^{(2)}|Y_{1:n}^{(4)}) = O(h(\epsilon)). \tag{5.12}$$

Proof of Lemma 2: We prove the equation (5.11); the proof of equation (5.12) is similar. Since $q(.|.)$ is a strong interference channel, lemma of section III of [6] implies that the n-letter product channel

$$q(y_{1:n}^{(3)}, y_{1:n}^{(4)}|x_{1:n}^{(1)}, x_{1:n}^{(2)}) = \prod_{i=1}^{n} q(y_i^{(3)}, y_i^{(4)}|x_i^{(1)}, x_i^{(2)})$$

is also a strong interference channel. Therefore [1]

$$I(X_{1:n}^{(2)}; Y_{1:n}^{(3)}|X_{1:n}^{(1)}) \geq I(X_{1:n}^{(2)}; Y_{1:n}^{(4)}|X_{1:n}^{(1)}).$$

This implies that $H(X_{1:n}^{(2)}|Y_{1:n}^{(3)}X_{1:n}^{(1)}) \leq H(X_{1:n}^{(2)}|Y_{1:n}^{(4)}X_{1:n}^{(1)})$. We have $H(X_{1:n}^{(2)}|Y_{1:n}^{(4)}X_{1:n}^{(1)}) \leq H(W_{1:n}^{(2)}|Y_{1:n}^{(4)}X_{1:n}^{(1)}) \leq H(W_{1:n}^{(2)}|\widehat{M}_{1:n}^{(4)})$ since $H(X_{1:n}^{(2)}|W_{1:n}^{(2)}) = 0$. Here $\widehat{M}_{1:n}^{(4)}$ is the reconstruction of $W_{1:n}^{(2)}$ by the third party (the average distortion between $\widehat{M}_{1:n}^{(4)}$ and $\widehat{W}_{1:n}^{(2)}$ is less than or equal to ϵ). $H(W_{1:n}^{(2)}|\widehat{M}_{1:n}^{(4)})$ is equal to $n \cdot O(h(\epsilon))$ for $\epsilon < \frac{1}{2}$ since

$$H(W_{1:n}^{(2)}|\widehat{M}_{1:n}^{(4)}) \leq \sum_{i=1}^{n} H(W_i^{(2)}|\widehat{M}_i^{(4)}) \leq \tag{5.13}$$

$$\sum_{i=1}^{n}[h(p(W_i^{(2)} \neq \widehat{M}_i^{(4)})) + p(W_i^{(2)} \neq \widehat{M}_i^{(4)})\log(|\mathcal{W}^{(2)}|)] \leq \tag{5.14}$$

$$n\big[h(\frac{1}{n}\sum_{i=1}^{n} p(W_i^{(2)} \neq \widehat{M}_i^{(4)})) + \frac{1}{n}\sum_{i=1}^{n} p(W_i^{(2)} \neq \widehat{M}_i^{(4)})\log(|\mathcal{W}^{(2)}|)\big] \tag{5.15}$$

$$= n \cdot O(h(\epsilon)),$$

where in equation (5.13) we have used the Fano inequality, in equation (5.14) we have used the concavity of the binary entropy function, and lastly, in equation (5.15), we have used the fact that the average distortion between $\widehat{M}_{1:n}^{(4)}$ and $W_{1:n}^{(2)}$ is less than or equal to ϵ. Thus, $H(W_{1:n}^{(2)}|\widehat{M}_{1:n}^{(4)}) \leq n \cdot O(h(\epsilon))$.

[1] Note that equations (5.4) and (5.5) hold for all arbitrary distributions on the inputs for a strong interference channel.

Therefore $H(X_{1:n}^{(2)}|Y_{1:n}^{(3)}X_{1:n}^{(1)}) \leq n \cdot O(h(\epsilon))$. Since the average distortion between $\widehat{M}_{1:n}^{(3)}$ and $W_{1:n}^{(1)}$ is less than or equal to ϵ, we have: $H(X_{1:n}^{(1)}|Y_{1:n}^{(3)}) \leq H(W_{1:n}^{(1)}|Y_{1:n}^{(3)}) \leq H(W_{1:n}^{(1)}|\widehat{M}_{1:n}^{(3)}) = n \cdot O(h(\epsilon))$. Thus, $H(X_{1:n}^{(1)}X_{1:n}^{(2)}|Y_{1:n}^{(3)}) \leq n \cdot O(h(\epsilon))$. Next, note that

$$H(W_{1:n}^{(1)}W_{1:n}^{(2)}|Y_{1:n}^{(3)}) \leq H(W_{1:n}^{(1)}W_{1:n}^{(2)}|X_{1:n}^{(1)}X_{1:n}^{(2)}) + H(X_{1:n}^{(1)}X_{1:n}^{(2)}|Y_{1:n}^{(3)})$$

since for any three random variables A, B and C we have $H(A|C) \leq H(A|B) + H(B|C)$. It suffices to show that $H(W_{1:n}^{(1)}W_{1:n}^{(2)}|X_{1:n}^{(1)}X_{1:n}^{(2)}) = n \cdot O(h(\epsilon))$. This is true because

$$H(W_{1:n}^{(1)}W_{1:n}^{(2)}|X_{1:n}^{(1)}X_{1:n}^{(2)}) = H(W_{1:n}^{(1)}W_{1:n}^{(2)}|X_{1:n}^{(1)}X_{1:n}^{(2)}Y_{1:n}^{(3)}Y_{1:n}^{(4)}) \leq$$
$$H(W_{1:n}^{(1)}W_{1:n}^{(2)}|Y_{1:n}^{(3)}Y_{1:n}^{(4)}) \leq H(W_{1:n}^{(1)}|Y_{1:n}^{(3)}) + H(W_{1:n}^{(2)}|Y_{1:n}^{(4)})$$

■

Appendix III: Convexity of ϕ

In this appendix, we show that for any interference channel

$$q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}),$$

$\phi\big(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \Psi\big)$ is convex when the set Ψ is convex. Take two arbitrary points $\overrightarrow{v_1}$ and $\overrightarrow{v_2}$ from this set. Corresponding to these two points are random variables $U_1, X_1^{(i)}, Y_1^{(i)}$ for $i = 1, ..., 4$ and $U_2, X_2^{(i)}, Y_2^{(i)}$ for $i = 1, ..., 4$, where $X_i^{(1)} - U_i - X_i^{(2)}$ and $U_i - X_i^{(1)}X_i^{(2)} - Y_i^{(3)}Y_i^{(4)}$ for $i = 1, 2$ and $\overrightarrow{v_i}$ is coordinate by coordinate less than or equal to

$$\big(I(X_i^{(1)}; Y_i^{(3)}|X_i^{(2)}, U_i),\ I(X_i^{(2)}; Y_i^{(4)}|X_i^{(1)}, U_i),\ I(X_i^{(1)}X_i^{(2)}; Y_i^{(3)}|U_i),$$
$$I(X_i^{(1)}X_i^{(2)}; Y_i^{(4)}|U_i),\ I(X_i^{(1)}X_i^{(2)}; Y_i^{(3)}),\ I(X_i^{(1)}X_i^{(2)}; Y_i^{(4)}),$$
$$I(X_i^{(1)}; Y_i^{(3)}|X_i^{(2)}),\ I(X_i^{(2)}; Y_i^{(4)}|X_i^{(1)})\big)$$

for $i = 1, 2$. Take a binary and uniform random variable Q on $\{1, 2\}$ and let $U = (U_Q, Q)$, $X^{(i)} = X_Q^{(i)}$ and $Y^{(i)} = Y_Q^{(i)}$ for $i = 1, ..., 4$. It can be then verified that $p(x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$ is in Ψ, that the conditional law of $Y^{(1)}, Y^{(2)}, Y^{(3)}, Y^{(4)}$ given $X^{(1)}, X^{(2)}, X^{(3)}, X^{(4)}$ is described by $q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)})$, and that the point

$$\overrightarrow{v} = \big(I(X^{(1)}; Y^{(3)}|X^{(2)}, U),\ I(X^{(2)}; Y^{(4)}|X^{(1)}, U),\ I(X^{(1)}X^{(2)}; Y^{(3)}|U),$$
$$I(X^{(1)}X^{(2)}; Y^{(4)}|U),\ I(X^{(1)}X^{(2)}; Y^{(3)}),\ I(X^{(1)}X^{(2)}; Y^{(4)}),$$
$$I(X^{(1)}; Y^{(3)}|X^{(2)}),\ I(X^{(2)}; Y^{(4)}|X^{(1)})\big)$$

is coordinate by coordinate greater than or equal to $\frac{1}{2}(\overrightarrow{v_1} + \overrightarrow{v_2})$. The proof for the first four coordinates is straightforward. For the fifth coordinate, we use the fact

that $I(X^{(1)}X^{(2)};Y^{(3)}) = I(UX^{(1)}X^{(2)};Y^{(3)}) \geq I(X^{(1)}X^{(2)};Y^{(3)}|U)$. The proof for the sixth, seventh and eighth coordinates is the similar. Since $\overrightarrow{v}$ can be seen to belong to

$$\phi\big(q(y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)}|x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}), \Psi\big),$$

this region must be convex. ■

Part II

The general broadcast channel

In this part of the thesis, we consider two-receiver general broadcast channels. Of particular interest will be the computation of the best known inner and outer bounds. Please note that this part can be read independently of the first part of the thesis. We begin by reviewing the definition of the problem of communicating over a broadcast channel. This will be followed by an outline of this part of the thesis.

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 alphabets 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 alphabets $|\mathcal{M}_i| \geq 2^{n(R_i - \epsilon)}$ (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.

We begin the second part of this dissertation by discussing the main obstacle to computing Marton's inner bound. We will then introduce the "perturbation method" and apply this novel tool to make Marton's inner bound computable. Next, we report the subsequent research that was done along the direction of computing Marton's inner bound. We prove various results that help to restrict the search space for computing the sum-rate for Marton's inner bound. For binary input broadcast channels, we show that the computation can be further simplified if we assume that Marton's inner bound and the recent outer bound of Nair and El Gamal match at the given channel. These results are used to show that the inner and the outer bound do not match for some broadcast channels, thus establishing a conjecture of [45]. We also show that unlike in the Gaussian case, for a degraded broadcast channel even without a common message, Marton's coding scheme without a superposition variable is in general insufficient for obtaining the capacity region. We end the second part of the dissertation by mentioning a few other results that were left off because they did not concern the computation of Marton's inner bound. We establish the capacity region along certain directions and show that it coincides with Marton's inner bound. We show that the Nair-El Gamal outer bound can be made fully computable. Lastly, we discuss an idea that may lead to a larger inner bound.

Chapter 6

Introduction

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 [37, Theorem 2]. Marton's work was subsequently generalized in [10, p. 391, Problem 10(c)], and by Gelfand and Pinsker [18] who established the achievability of the region formed by taking the union over random variables U, V, W, X, Y, Z, having the joint distribution $p(u, v, w, x, y, z) = p(u, v, w, x)q(y, z|x)$, of

$$\begin{aligned} R_0, R_1, R_2 &\geq 0; \\ R_0 &\leq \min(I(W;Y), I(W;Z)); \quad (6.1) \\ R_0 + R_1 &\leq I(UW;Y); \quad (6.2) \\ R_0 + R_2 &\leq I(VW;Z); \quad (6.3) \end{aligned}$$

$$\begin{aligned} R_0 + R_1 + R_2 \leq\ & I(U;Y|W) + I(V;Z|W) - I(U;V|W) \\ & + \min(I(W;Y), I(W;Z)). \quad (6.4) \end{aligned}$$

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. A main result of this chapter 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 [33], which however turns out to be equivalent to Marton's inner bound [35]. 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 $I(W;Y) > I(W;Z)\&V = \textit{constant}$, or $I(W;Y) < I(W;Z)\&U = \textit{constant}$ holds [35]. 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 $R_0 = 0$ [26]; 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. A main result of this chapter 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.

Chapter 7

New cardinality bounds

7.1 The proof technique at an intuitive level

In this section, we demonstrate the use of the "perturbation method" at an intuitive level. In the following discussion, we will repeatedly make use of 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 $[-\bar{\epsilon}_1, \bar{\epsilon}_2]$. Random variable L is a canonical way of representing the direction of perturbation since given any subset of indices $I \subset \{1, 2, 3, ..., n\}$, 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 $X_{i\in I}$:

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

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 $q(y,z|x)$ 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 alphabets 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 3. 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:

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

where random variables $\widehat{U},\widehat{V},\widehat{X},\widehat{Y},\widehat{Z}$ satisfy the following properties: the Markov chain $\widehat{U}\widehat{V}\to\widehat{X}\to\widehat{Y}\widehat{Z}$ 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[1], 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 $L:\mathcal{U}\times\mathcal{V}\times\mathcal{X}\to\mathbb{R}$ 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

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

[1]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.

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 its 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 $\widehat{U}\widehat{V}\to\widehat{X}\to\widehat{Y}\widehat{Z}$ 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. [2]

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 its second derivative should be less than or equal to zero. Using Lemma 5, one can compute the first derivative and set it to zero, and thereby get the following equation:

$$I_L(U;Y)+I_L(V;Z)-I_L(U;V)+\lambda I_L(U;Y)+\gamma I_L(V;Z)=0. \tag{7.1}$$

In order to compute the second derivative, one can expand the expression as entropy terms and use Lemma 5 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 $+\log e\cdot\mathbb{E}[\mathbb{E}[L(U,V,X)|UY]^2]+\log e\cdot\mathbb{E}[\mathbb{E}[L(U,V,X)|VZ]^2]-$

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

$\log e \cdot \mathbb{E}[\mathbb{E}[L(U,V,X)|UV]^2]$. 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:

$$\mathbb{E}[\mathbb{E}[L(U,V,X)|UY]^2] + \mathbb{E}[\mathbb{E}[L(U,V,X)|VZ]^2] - \mathbb{E}[\mathbb{E}[L(U,V,X)|UV]^2] \leq 0. \quad (7.2)$$

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.[3]

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.[4] Using the last part of Lemma 5, one can write:

$$I(\widehat{U};\widehat{Y}) =$$
$$I(U;Y) + \epsilon \cdot I_L(\widehat{U};\widehat{Y}) - \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|U]\big)\big] - \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|Y]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|UY]\big)\big] =$$
$$I(U;Y) + \epsilon \cdot I_L(\widehat{U};\widehat{Y}), \quad (7.3)$$

where $r(x) = (1+x)\log(1+x)$. Equation (7.3) holds because $\mathbb{E}[L|Y] = 0$ and $\mathbb{E}[L|U] = \mathbb{E}[L|UY]$. Similarly using the last part of Lemma 5, one can write:

$$I(\widehat{U};\widehat{V}) =$$
$$I(U;V) + \epsilon \cdot I_L(\widehat{U};\widehat{V}) - \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|U]\big)\big] - \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|V]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|UV]\big)\big] =$$
$$I(U;V) + \epsilon \cdot I_L(\widehat{U};\widehat{V}) \quad (7.4)$$

where $r(x) = (1+x)\log(1+x)$. Equation (7.4) 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

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

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

$I(V;Z) + \epsilon \cdot I_L(\widehat{V};\widehat{Z}) = 0$. 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

$$\begin{aligned} &I(U;Y) + I(V;Z) - I(U;V) + \lambda I(U;Y) + \gamma I(V;Z) + \\ &\epsilon \cdot \big(I_L(U;Y) + I_L(V;Z) - I_L(U;V) + \lambda I_L(U;Y) + \gamma I_L(V;Z)\big). \end{aligned} \tag{7.5}$$

Equation (7.1) 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 $\epsilon = -\bar{\epsilon}_1$ 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:

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

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 $\epsilon = -\bar{\epsilon}_1$ 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 $p_0(u,v,x,y,z) = p_0(u,v,x)q(y,z|x)$, equations (7.1) and (7.2) 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.

7.2 Definitions and Notation

Let $\mathbb{R}$ denote the set of real numbers. All the logarithms throughout this chapter 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 14. 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 15. 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 (6.1), (6.2), (6.3) and (6.4) 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.

Definition 16. 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 17. 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 (6.1), (6.2), (6.3) and (6.4), 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 6-tuple mentioned in Definition 16. 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 18. 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 (6.1), (6.2), (6.3) and (6.4). 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 19. 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 $\left|\mathbb{E}[L|X=x,Y=y]\right| < \infty$ 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 $I_L(X;Y) = H_L(X) - H_L(X|Y) = H_L(Y) - H_L(Y|X)$.

7.3 Statement of the result

Theorem 10. 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 4. 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 5. Given any finite random variable X, and real valued random variable L where $\left|\mathbb{E}[L|X=x]\right| < \infty$ for all $x \in \mathcal{X}$, and $\mathbb{E}[L]=0$, let random variable $\widehat{X}$ be defined on the same alphabet 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 $[-\bar{\epsilon}_1,\bar{\epsilon}_2]$. $\bar{\epsilon}_1$ and $\bar{\epsilon}_2$ are positive reals for which $\min_x 1-\bar{\epsilon}_1\cdot\mathbb{E}[L|X=x]\geq 0$ and $\min_x 1+\bar{\epsilon}_2\cdot\mathbb{E}[L|X=x]\geq 0$ hold. Then

1. $H(\widehat{X})\mid_{\epsilon=0} = H(X)$, and $\frac{\partial}{\partial\epsilon}H(\widehat{X})\mid_{\epsilon=0} = H_L(X)$.

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

3. $H(\widehat{X}) = H(X) + \epsilon H_L(X) - \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|X]\big)\big]$ where $r(x) = (1+x)\log(1+x)$.

7.3.1 Proofs

Proof of Theorem 10: In Appendices II and III of section 7.3.2, 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 4 according to which the region $\mathscr{L}_I(q(y,z|x))$ is closed.[5] To show the latter, it suffices to prove that $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x)) \subset \mathscr{L}_I(q(y,z|x))$.[6] Lemma 4 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 4 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 $\mathscr{L}_I(q(y,z|x))$.[7]

---

[5]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 $\mathscr{L}(q(y,z|x))$.

[6]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 $\mathscr{L}(q(y,z|x))$.

[7]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 $\mathscr{L}_I(q(y,z|x))$.

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. The 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 $\sum_{i=1}^{6}\lambda_i R_i'$ 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 4. 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:

$$\max_{(R_1',...,R_6')\in\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R_i' \leq \max_{(R_1',...,R_6')\in\mathcal{C}_{M-I}^{|\mathcal{X}|,S_v,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R_i' \tag{7.6}$$

$$\max_{(R_1',...,R_6')\in\mathcal{C}_{M-I}^{|\mathcal{X}|,S_v,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R_i' \leq \max_{(R_1',...,R_6')\in\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R_i' \tag{7.7}$$

$$\max_{(R_1',...,R_6')\in\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,S_w}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R_i' \leq \max_{(R_1',...,R_6')\in\mathcal{C}_{M-I}^{|\mathcal{X}|,|\mathcal{X}|,|\mathcal{X}|+4}(q(y,z|x))}\sum_{i=1}^{6}\lambda_i R_i' \tag{7.8}$$

The proof for equation (7.6) is provided in Appendix I of section 7.3.2. The proof for equation (7.7) is similar. Equation (7.8) follows from Lemma 4.

■

Proof of Lemma 4: 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[8], 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

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

$$p(\widetilde{U} = u, \widetilde{V} = v, X = x|\widetilde{W} = w) = p(U = u, V = v, X = x|W = w); \tag{7.9}$$
$$I(\widetilde{W};Y) = I(W;Y);$$
$$I(\widetilde{W};Z) = I(W;Z);$$
$$I(\widetilde{U};Y|\widetilde{W}) = I(U;Y|W);$$
$$I(\widetilde{V};Z|\widetilde{W}) = I(V;Z|W);$$
$$I(\widetilde{U};\widetilde{V}|\widetilde{W}) \leq I(U;V|W).$$

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 $p(\widetilde{U} = u, \widetilde{V} = v, \widetilde{W} = w, X = x)$.

[8]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 $\Delta(\mathcal{A})$.

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 $w \mapsto p(\widetilde{W} = w)$ correspond to a probability distribution, we impose the following two constraints:

$$p(\widetilde{W} = w) \geq 0 \quad \forall w; \tag{7.10}$$

$$\sum_w p(\widetilde{W} = w) = 1. \tag{7.11}$$

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

$$\sum_w p(X = x|W = w)p(W = w) = p(X = x) = \tag{7.12}$$

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

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 (7.12) 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 (7.11); thus it is redundant. This is because $\sum_x p(X = x|W = w) = 1$. Therefore the equation (7.12) imposes $|\mathcal{X}| - 1$ constraints on $p(\widetilde{W} = w)$.

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

$$\sum_w p(\widetilde{W} = w)H(Y|\widetilde{W} = w) = \sum_w p(W = w)H(Y|W = w). \tag{7.13}$$

Please note that because of equation (7.9), $H(Y|\widetilde{W} = w) = H(Y|W = w)$. Similarly in order to enforce $I(\widetilde{W}; Z) = I(W; Z)$, we require

$$\sum_w p(\widetilde{W} = w)H(Z|\widetilde{W} = w) = \sum_w p(W = w)H(Z|W = w). \tag{7.14}$$

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

$$\sum_w p(\widetilde{W} = w)I(\widetilde{U}; Y|\widetilde{W} = w) = \sum_w p(W = w)I(U; Y|W = w), \tag{7.15}$$

and

$$\sum_w p(\widetilde{W} = w)I(\widetilde{V}; Z|\widetilde{W} = w) = \sum_w p(W = w)I(V; Z|W = w). \tag{7.16}$$

Please note that because of equation (7.9), $I(\widetilde{U};Y|\widetilde{W}=w) = I(U;Y|W=w)$ 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

$$\sum_w p(\widetilde{W}=w) I(\widetilde{U};\widetilde{V}|\widetilde{W}=w) \leq \sum_w p(W=w) I(U;V|W=w). \tag{7.17}$$

Because of equation (7.9), $I(\widetilde{U};\widetilde{V}|\widetilde{W}=w) = I(U;V|W=w)$.

The rest of the proof is based on the technique of Fenchel to strengthen the Carathéodory theorem. The region formed by equations (7.10), (7.11), (7.12), (7.13), (7.14), (7.15) and (7.16) contains the vector $w \mapsto p(W=w)$. The vector $w \mapsto p(W=w)$ further lies in the half space defined by equation (7.17). We can write the vector $w \mapsto p(W=w)$ as the convex combination of extreme points of the region formed by equations (7.10), (7.11), (7.12), (7.13), (7.14), (7.15) and (7.16). 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 (7.17). 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 (7.10), (7.11), (7.12), (7.13), (7.14), (7.15) and (7.16). 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 4 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

$$\begin{aligned}
&I(\widehat{W};\widehat{Y})\geq\frac{1}{2}I(W;Y)+\frac{1}{2}I(\widetilde{W};\widetilde{Y});\\
&I(\widehat{W};\widehat{Z})\geq\frac{1}{2}I(W;Z)+\frac{1}{2}I(\widetilde{W};\widetilde{Z});\\
&I(\widehat{U}\widehat{W};\widehat{Y})\geq\frac{1}{2}I(UW;Y)+\frac{1}{2}I(\widetilde{U}\widetilde{W};\widetilde{Y});\\
&\cdots.
\end{aligned}$$

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 5: 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:

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

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 $H_L(X)$.

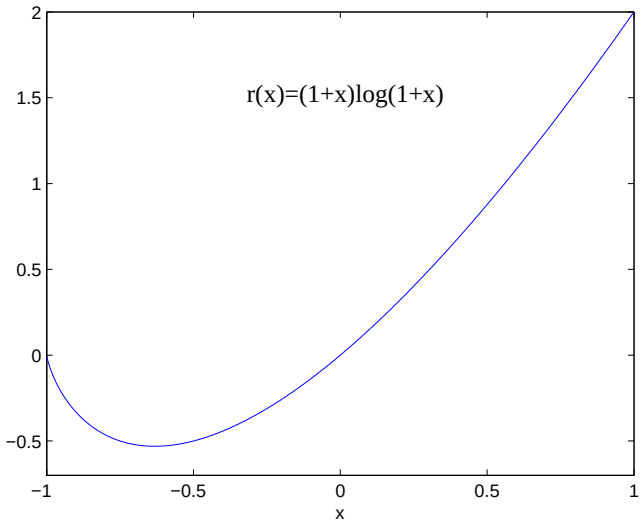

Figure 7.1: Plot of the convex function $r(x) = (1+x)\log(1+x)$ over the interval $[-1,1]$. Note that $r(0) = 0$, $\frac{\partial}{\partial x} r(x) = \log(1+x) + \log(e)$ and $\frac{\partial^2}{\partial x^2} r(x) = \frac{\log(e)}{1+x} > 0$.

Next, we have:

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

On the other hand,

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

■

7.3.2 Appendix

Appendix I

In this appendix we prove equation (7.6) 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.[9] 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 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 $\widetilde{u}$. [10]

We assume that random variables $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$, $\widetilde{X}$, $\widetilde{Y}$ and $\widetilde{Z}$ are respectively defined on the alphabets 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

[9] Note that by Lemma 4, $\mathcal{C}_{M-I}^{S_u,S_v,S_w}(q(y,z|x))$ 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.

[10] 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 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 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 $I(\widetilde{U}';\widetilde{Y}|\widetilde{W}) = I(\widetilde{U};\widetilde{Y}|\widetilde{W})$.

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 3 of Section 7.1 holds.

Appendix II

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 (6.1), (6.2), (6.3) and (6.4) 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 III

In this appendix, we prove that $\mathscr{C}(q(y,z|x))$ is equal to $\mathscr{L}(q(y,z|x))$. Clearly $\mathscr{C}(q(y,z|x))$ is a subset of $\mathscr{L}(q(y,z|x))$. Therefore we need to show that $\mathscr{L}(q(y,z|x)) \subset \mathscr{C}(q(y,z|x))$. Instead we show that $\mathscr{L}_I(q(y,z|x)) \subset \mathscr{C}_I(q(y,z|x))$.[11] It suffices to prove that $\mathscr{C}_I(q(y,z|x))$ is convex, and 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 $\mathscr{C}_I(q(y,z|x))$.

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 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 4) 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 10, 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

$$\sum_{i=1}^{6} \lambda_i R_i \leq \lambda_1 \cdot I(W;Y) + \lambda_2 \cdot I(W;Z) + \lambda_3 \cdot I(UW;Y) + \lambda_4 \cdot I(VW;Z) + \quad (7.18)$$
$$\lambda_5 \cdot \big(I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Y)\big) +$$
$$\lambda_6 \cdot \big(I(U;Y|W) + I(V;Z|W) - I(U;V|W) + I(W;Z)\big).$$

Fix $p(u, v, w)$. The right hand side of equation (7.18) would then be a convex function of $p(x|u, v, w)$.[12] Therefore its maximum occurs at the extreme points

[11] 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 $\mathscr{C}(q(y,z|x))$.

[12] 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.

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 $p(\widehat{u},\widehat{v},\widehat{w}) > 0$.

Chapter 8

Follow up results

In this chapter we report the subsequent research that was done along the direction of computing Marton's inner bound. We prove various results that help to restrict the search space for computing the sum-rate for Marton's inner bound. For binary input broadcast channels, we show that the computation can be further simplified if we assume that Marton's inner bound and the recent outer bound of Nair and El Gamal match at the given channel. These results are used to show that the inner and the outer bound do not match for some broadcast channels, thus establishing a conjecture of [45]. We also show that unlike in the Gaussian case, for a degraded broadcast channel even without a common message, Marton's coding scheme without a superposition variable is in general insufficient for obtaining the capacity region. We end this chapter by mentioning a few other results that were left off because they did not concern the computation of Marton's inner bound. We establish the capacity region along certain directions and show that it coincides with Marton's inner bound. We show that the Nair-El Gamal outer bound can be made fully computable. Lastly, we discuss an idea that may lead to a larger inner bound.

8.1 Definitions and Notation

In this section, we provide other definitions we need for the rest of the dissertation. Given random variables $K_1, K_2 \in \{0, 1, 2, ..., k-1\}$ for a natural number k, $K_1 \oplus K_2$ denotes $(K_1 + K_2) \mod k$.

Definition 20. [46] Let $\mathcal{C}_{NE}(q(y, z|x))$ denote the Nair-El Gamal outer bound on the

channel $q(y,z|x)$, defined as the set of non-negative rate triples (R_0,R_1,R_2) satisfying

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

for some random variables $(U,V,W,X,Y,Z) \sim p(u)p(v)p(w|u,v)p(x|u,v,w)q(y,z|x)$.

Definition 21. [30] Let $\mathcal{C}_{d_1}(q(y,z|x))$ and $\mathcal{C}_{d_2}(q(y,z|x))$ denote the degraded message set capacity regions, i.e. when $R_1=0$ and $R_2=0$, respectively. The capacity region $\mathcal{C}_{d_1}(q(y,z|x))$ is the set of of non-negative rate pairs (R_0,R_2) satisfying

$$\begin{aligned} R_0 &\leq I(W;Y), \\ R_2 &\leq I(X;Z|W), \\ R_0+R_2 &\leq I(X;Z), \end{aligned}$$

for some random variables $(W,X,Y,Z) \sim p(w,x)q(y,z|x)$. The capacity region $\mathcal{C}_{d_2}(q(y,z|x))$ is defined similarly.

Definition 22. The input symbols x_0 and x_1 are said to be indistinguishable by the channel if $q(y|x_0)=q(y|x_1)$ for all y, and $q(z|x_0)=q(z|x_1)$ for all z. A channel $q(y,z|x)$ is said to be irreducible if no two of its inputs symbols are indistinguishable by the channel.

Definition 23. Let $\mathcal{U}=\{u_1,u_2,...,u_{|\mathcal{U}|}\}$, $\mathcal{V}=\{v_1,...,v_{|\mathcal{V}|}\}$ be finite sets, and ξ be a deterministic mapping from $\mathcal{U}\times\mathcal{V}$ to $\mathcal{X}$. One can represent the mapping by a table having $|\mathcal{U}|$ rows and $|\mathcal{V}|$ columns; the rows are indexed by $u_1,u_2,....,u_{|\mathcal{U}|}$ and the columns are indexed by $v_1,v_2,...,v_{|\mathcal{V}|}$. In the cell (i,j), we write $\xi(u_i,v_j)$, for the symbol x that (u_i,v_j) is being mapped to. The profile of the i^{th} row is defined to be a vector of size $|\mathcal{X}|$ counting the number of occurrences of the elements of $\mathcal{X}$ in the i^{th} row. In other words if $\mathcal{X}=\{x_1,x_2,...,x_{|\mathcal{X}|}\}$, the k^{th} element of the profile of the i^{th} row is the number of times that x_k shows up in the i^{th} row of the table. The profile of the j^{th} column is defined similarly. Let the profile of the table to be a vector of size $(|\mathcal{U}|+|\mathcal{V}|)|\mathcal{X}|$ formed by concatenating the profile vectors of the rows and the columns of the table. The profile vector of the mapping ξ is denoted by $\overrightarrow{v_\xi}$.

8.2 On binary input broadcast channels

8.2.1 Statement of the result

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 the 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 11. 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 $\mathcal{C}_M(q(y, z|x)) = \mathcal{C}_{NE}(q(y, z|x))$, the 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

$$\max \Bigg(\min_{\gamma \in [0,1]} \Bigg(\max_{\substack{p(wx)q(y,z|x) \\ |\mathcal{W}| = 2}} \gamma I(W;Y) + (1-\gamma) I(W;Z) + \sum_w p(w) T(p(X = 1|W = w)) \Bigg), \max_{\substack{p(u,v)p(x|uv)q(y,z|x) \\ |\mathcal{U}| = |\mathcal{V}| = 2, I(U;V) = 0, H(X|UV) = 0}} I(U;Y) + I(V;Z) \Bigg), \tag{8.1}$$

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

Remark 3. The expression given in equation (8.1) 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 (8.1) 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 [45]), it will serve as 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 [45]

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

which can be written as (see Bound 4 in [45])

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

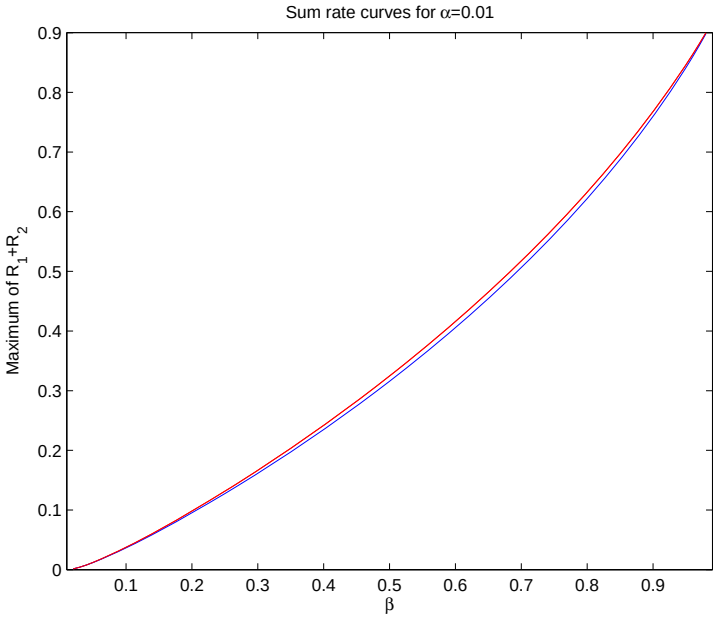

Figure 8.1: Red curve (top curve): sum rate for $C_{NE}(q(y,z|x))$; Blue curve (bottom curve): sum rate for $C_M(q(y,z|x))$ assuming $C_{NE}(q(y,z|x)) = C_M(q(y,z|x))$.

There are examples for which the expression of equation (8.1) 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 $\mathcal{C}_{NE}$. 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 8.1 plots maximum of the sum rate for $C_{NE}(q(y,z|x))$, and the maximum of the 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 cannot be equal for the corresponding broadcast channel.

8.2.2 Proofs

Proof of Theorem 11: The 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

$$\max_{\substack{p(u,v,w,x)q(y,z|x) \\ |\mathcal{U}|=2, |\mathcal{V}|=2 \\ H(X|UVW)=0}} I(U;Y|W) + I(V;Z|W) - I(U;V|W) + \min(I(W;Y), I(W;Z)). \tag{8.2}$$

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

$$\max\Bigg(\max_{p(wx)q(y,z|x)} \min\big(I(W;Y),I(W;Z)\big)+\sum_w p(w)T(p(X=1|W=w)), \quad (8.3)$$

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

Next, we show that the expression of equation 8.3 is equal to the expression given in Theorem 11.

The expression of equation (8.2) is greater than or equal to the expression of equation (8.3).[1] For the first part of the proof we thus need to prove that the expression of equation (8.2) is less than or equal to the expression of equation (8.3). Take the joint distribution $p(u,v,w,x)$ that maximizes the expression of equation (8.2). Let $\widetilde{U}=(U,W)$ and $\widetilde{V}=(V,W)$. 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 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 [45]). 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 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 $I(U;V|W)=0$,
2. $I(U;V|WY)=0$,
3. $I(U;V|WZ)=0$.

[1] 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 11. 2) Assume that W is constant, and U is independent of V. This would produce the second part of the expression given in Theorem 11.

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 of section 8.2.3 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 (8.3) is equal to the the expression given in Theorem 11. In order to show this, we prove that

$$\max_{p(w,x)q(y,z|x)} \min(I(W;Y), I(W;Z)) + \sum_w p(w) T(p(X=1|W=w)) \tag{8.4}$$

is equal to

$$\min_{\gamma\in[0,1]} \Big(\max_{\substack{p(wx)q(y,z|x) \\ |\mathcal{W}|=2}} \gamma I(W;Y) + (1-\gamma) I(W;Z) + \sum_w p(w) T(p(X=1|W=w)) \Big). \tag{8.5}$$

The expression given in equation (8.4) can be written as

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

$$I(W;Z) + \sum_w p(w) T(p(X=1|W=w)) \Bigg).$$

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. 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.

■

8.2.3 Appendix

In this Appendix, we complete the proof of theorem 11 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 $p(X = 1|Y = y_1) \neq p(X = 1|Y = y_2)$.[2] 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 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

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

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

[2] 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.

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

$$\frac{\sqrt{a_{0,0}a_{1,1}}}{a_{0,0}+a_{1,1}}p(X=0|Y=y_i) = \frac{\sqrt{a_{1,0}a_{0,1}}}{a_{1,0}+a_{0,1}}p(X=1|Y=y_i). \tag{8.6}$$

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 (8.6) 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

$$a_{0,0}\cdot p(X=1|Y=y_i) = \frac{a_{1,0}a_{0,1}}{a_{0,0}+a_{0,1}+a_{1,0}}p(X=0|Y=y_i), \tag{8.7}$$

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 (8.7) 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.

8.3 Computing the sum-rate for Marton's Inner Bound

8.3.1 Statement of the result

In this section, we prove a result that helps to restrict the search space for computing the sum-rate for Marton's inner bound.

Computing the sum-rate for Marton's inner bound is closely related to the following maximization problem for $\lambda \in [0,1]$: For any $\lambda \in [0,1]$, let

$$T(\lambda) = \max_{p(u,v,w,x)} \big(\lambda I(W;Y) + (1-\lambda) I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)\big).$$

Observation 1. The maximum of the sum-rate for Marton's inner bound is equal to

$$\min_{\lambda \in [0,1]} T(\lambda).$$

The main theorem of this section restricts the search space for computing $T(\lambda)$. In this section, we only deal with broadcast channels $q(y,z|x)$ with strictly positive transition matrices, i.e. when $q(y|x) > 0, q(z|x) > 0$ for all x, y, z. In order to evaluate $T(\lambda)$ when $q(y|x)$ or $q(z|x)$ become zero for some y or z, one can use the continuity of $T(\lambda)$ in $q(y,z|x)$ and take the limit of $T(\lambda)$ for a sequence of channels with positive entries converging to the desired channel. The reason for dealing with this class of broadcast channels should become clear by the following lemma.

Lemma 6. Take an arbitrary broadcast channel $q(y,z|x)$ with strictly positive transition matrices (i.e. $q(y|x) > 0, q(z|x) > 0$ for all x, y, z). Let $p(u,v,w,x)$ be an arbitrary joint distribution maximizing $T(\lambda)$ for some $\lambda \in [0,1]$. If $p(u,w)$ and $p(v,w)$ are positive for some triple (u,v,w), then it must be the case that $p(u,v,w) > 0$, $p(u,w,y) > 0$ and $p(v,w,z) > 0$ for all y and z.

Theorem 12. Take an arbitrary irreducible broadcast channel $q(y,z|x)$ with strictly positive transition matrices. In computing $T(\lambda)$ for some $\lambda \in [0,1]$, it suffices to take the maximum over auxiliary random variables $p(u,v,w,x)q(y,z|x)$ simultaneously satisfying the following constraints,

- $|\mathcal{U}| \leq \min(|\mathcal{X}|, |\mathcal{Y}|)$, $|\mathcal{V}| \leq \min(|\mathcal{X}|, |\mathcal{Z}|)$, $|\mathcal{W}| \leq |\mathcal{X}|$.
- $H(X|UVW) = 0$. Given w where $p(w) > 0$, we use $x = \xi^{(w)}(u,v)$ to denote the deterministic mapping from $\mathcal{U}_w \times \mathcal{V}_w$ to $\mathcal{X}$. Here $\mathcal{U}_w$ is the set of $u \in \mathcal{U}$ such that $p(u|w) > 0$ and $\mathcal{V}_w$ is the set of $v \in \mathcal{V}$ such that $p(v|w) > 0$.

- For arbitrary w such that $p(w) > 0$, the profile vector of the mapping $\xi^{(w)}$, $\overrightarrow{v_{\xi^{(w)}}}$, cannot be written as

$$\sum_{t=1}^{M} \alpha_t \overrightarrow{v_{\xi_t}},$$

where ξ_t (for $t = 1, 2, 3, ..., M$) are deterministic mappings from $\mathcal{U}_w \times \mathcal{V}_w$ to $\mathcal{X}$ not equal to $\xi^{(w)}$, and α_t are non-negative numbers adding up to one, i.e. $\sum_{t=1}^{M} \alpha_t = 1$.

- For arbitrary w such that $p(w) > 0$, let the functions

$$\begin{aligned} &f_{u,w} : \mathcal{X} \to \mathbb{R} \text{ for every } u \in \mathcal{U}_w, \\ &g_{v,w} : \mathcal{X} \to \mathbb{R} \text{ for every } v \in \mathcal{V}_w, \\ &\text{and } h_w : \mathcal{X} \to \mathbb{R}, \end{aligned}$$

be defined by

$$f_{u,w}(x) = \sum_y q(y|x) \log p(uy|w),$$
$$g_{v,w}(x) = \sum_z q(z|x) \log p(vz|w),$$

$$h_w(x) = \min_{u' \in \mathcal{U}_w, v' \in \mathcal{V}_w} \Big(\log(p(u'v'|w)) - f_{u',w}(x) - g_{v',w}(x) \Big).$$

These definitions make sense because of Lemma 6. Then, for any $u \in \mathcal{U}_w$ and $v \in \mathcal{V}_w$, the following two equations hold:

$$\log(p(uv|w)) = \max_x [f_{u,w}(x) + g_{v,w}(x) + h_w(x)],$$

and

$$\begin{aligned} &p(x_0|u, v, w) = 1 \text{ for some } x_0 \in \mathcal{X} \Rightarrow \\ &x_0 \in argmax_x [f_{u,w}(x) + g_{v,w}(x) + h_w(x)]. \end{aligned}$$

- Given any w, random variables U_w, V_w, X_w, Y_w, Z_w distributed according to $p(u, v, x, y, z|w)$ satisfy the following:

$$\begin{aligned} &I(\overline{U}; Y_w) \geq I(\overline{U}; V_w Z_w) \text{ for any } \overline{U} \to U_w \to V_w X_w Y_w Z_w, \\ &I(\overline{V}; Z_w) \geq I(\overline{V}; U_w Y_w) \text{ for any } \overline{V} \to V_w \to U_w X_w Y_w Z_w. \end{aligned}$$

Discussion 1. The first constraint imposes cardinality bounds on $|\mathcal{U}|$ and $|\mathcal{V}|$ that are better than those reported in section 7.3. *However, we only claim the improved cardinality bounds for $T(\lambda)$ and not the whole capacity region.* The second constraint is not new, and can be found in section 7.3. The other constraints are useful in restricting the search space due to the constraints imposed on $p(u, v, w, x)$. For instance, take arbitrary w where $p(w) > 0$, distinct u_0, u_1 in $\mathcal{U}_w$ and distinct v_0, v_1 in $\mathcal{V}_w$. Assume further that $x_0 = \xi^{(w)}(u_0, v_0) = \xi^{(w)}(u_1, v_1)$ for some x_0. Then the third bullet implies that $x_1 = \xi^{(w)}(u_1, v_0) = \xi^{(w)}(u_0, v_1)$ for some $x_1 \neq x_0$ cannot hold, and the fourth bullet implies that $p(u_0, v_0, w)p(u_1, v_1, w) \leq p(u_1, v_0, w)p(u_0, v_1, w)$. Assume that the first claim is false. Let the mapping ξ_1 to be equal to $\xi^{(w)}$ except that (u_0, v_0) and (u_1, v_1) are mapped to x_1 (instead of x_0), and (u_1, v_0) and (u_0, v_1) are mapped to x_0 (instead of x_1). The mapping ξ_1 has the same profile vector as $\xi^{(w)}$. The condition in the third bullet is violated for the choice of $M = 1$, ξ_1 and $\alpha_1 = 1$. The second claim holds since

$$
\begin{aligned}
&\log p(u_0, v_0|w) + \log p(u_1, v_1|w) = \\
&f_{u_0,w}(x_0) + g_{v_0,w}(x_0) + h_w(x_0) + \\
&f_{u_1,w}(x_0) + g_{v_1,w}(x_0) + h_w(x_0) = \\
&f_{u_0,w}(x_0) + g_{v_1,w}(x_0) + h_w(x_0) + \\
&f_{u_1,w}(x_0) + g_{v_0,w}(x_0) + h_w(x_0) \leq \\
&\max_x f_{u_0,w}(x) + g_{v_1,w}(x) + h_w(x) + \\
&\max_x f_{u_1,w}(x) + g_{v_0,w}(x) + h_w(x) = \\
&\log p(u_0, v_1|w) + \log p(u_1, v_0|w).
\end{aligned}
$$

8.3.2 Proof

Proof of Theorem 12: From the set of pmfs $p(u, v, w, x)$ that maximize the expression $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$, let $p_0(u, v, w, x)$ be the one that achieves the largest value of $I(W;Y) + I(W;Z)$. In Appendix I of section 8.3.3, we prove that one can find $p(\widehat{u}, \widehat{v}, \widehat{w}, \widehat{x})$ such that

- $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$ is equal to $\lambda I(\widehat{W};\widehat{Y}) + (1-\lambda)I(\widehat{W};\widehat{Z}) + I(\widehat{U};\widehat{Y}|\widehat{W}) + I(\widehat{V};\widehat{Z}|\widehat{W}) - I(\widehat{U};\widehat{V}|\widehat{W})$,
- $I(W;Y) + I(W;Z)$ is equal to $I(\widehat{W};\widehat{Y}) + I(\widehat{W};\widehat{Z})$,
- $|\widehat{\mathcal{U}}| \leq \min(|\mathcal{X}|, |\mathcal{Y}|)$,
- $|\widehat{\mathcal{V}}| \leq \min(|\mathcal{X}|, |\mathcal{Z}|)$,
- $|\widehat{\mathcal{W}}| \leq |\mathcal{X}|$,

- $H(\widehat{X}|\widehat{U}\widehat{V}\widehat{W}) = 0$.

Thus the constraints in the first and second bullets are satisfied by $p(\widehat{u}, \widehat{v}, \widehat{w}, \widehat{x})$. In Appendix II of section 8.3.3, we show that $p(\widehat{u}, \widehat{v}, \widehat{w}, \widehat{x})$ will automatically satisfy the third bullet of Theorem 12. In Appendix V of section 8.3.3, we show that the fourth bullet of Theorem 12 holds for any joint distribution that maximizes the expression $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$. In Appendix VI of section 8.3.3, we show that the fifth bullet of Theorem 12 holds for any joint distribution that maximizes the expression $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$, and at the same time has the largest possible value of $I(W;Y) + I(W;Z)$.

■

Proof of Observation 1: This observation was exploited in section 3.1.1 of [28], but no proof for it was given in [28]. In order to prove the observation, one needs to argue that the following exchange of max and min is legitimate:

$$\max_{p(u,v,w,x)} \min_{\lambda \in [0,1]} \lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W) =$$
$$\min_{\lambda \in [0,1]} \max_{p(u,v,w,x)} \lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W).$$

Let $R_{Marton-Sum}$ denote the sum-rate for Martons inner bound. We would like to show that $R_{Marton-Sum}$ is equal to $\min_{0 \leq \lambda \leq 1} T(\lambda)$.

Let $\mathcal{D}$ be the union over all $p(u, v, w, x)$ of real pairs (d_1, d_2) satisfying

$$d_1 \leq I(W;Y) + I(U;Y|W) + I(V;Z|W) - I(U;V|W),$$
$$d_2 \leq I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W).$$

We claim that this region is convex. Take two points (d_1, d_2) and (d_1', d_2') in the region. Corresponding to these are joint distributions $p(u_1, v_1, w_1, x_1)q(y_1, z_1|x_1)$ and $p(u_2, v_2, w_2, x_2)q(y_2, z_2|x_2)$. Take a uniform binary random variable Q independent of all the previously defined random variables. Set $U = U_Q$, $V = V_Q$, $W = (Q, W_Q)$,

$X = X_Q$, $Y = Y_Q$, $Z = Z_Q$. We will then have

$$
\begin{aligned}
&I(W;Y) + I(U;Y|W) + I(V;Z|W) - I(U;V|W) = \\
&I(W_Q, Q; Y_Q) + I(U_Q; Y_Q|W_Q, Q) + \\
&I(V_Q; Z_Q|W_Q, Q) - I(U_Q; V_Q|W_Q, Q) \geq \\
&I(W_Q; Y_Q|Q) + I(U_Q; Y_Q|W_Q, Q) + \\
&I(V_Q; Z_Q|W_Q, Q) - I(U_Q; V_Q|W_Q, Q) = \\
&\frac{1}{2}\big(I(W_1; Y_1) + I(U_1; Y_1|W_1) + \\
&I(V_1; Z_1|W_1) - I(U_1; V_1|W_1)\big) + \\
&\frac{1}{2}\big(I(W_2; Y_2) + I(U_2; Y_2|W_2) + \\
&I(V_2; Z_2|W_2) - I(U_2; V_2|W_2)\big) \geq \\
&\frac{1}{2}(d_1 + d_1').
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
&I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W) \geq \\
&\frac{1}{2}(d_2 + d_2').
\end{aligned}
$$

Thus, the point $(\frac{1}{2}(d_1 + d_1'), \frac{1}{2}(d_2 + d_2'))$ is in the region. Thus, $\mathcal{D}$ is convex.

Next, note that the point $(R_{Marton-Sum}, R_{Marton-Sum})$ is in $\mathcal{D}$. We claim that it is a boundary point of $\mathcal{D}$. If it is an interior point, there must exist $\epsilon > 0$ such that $(R_{Marton-Sum} + \epsilon, R_{Marton-Sum} + \epsilon)$ is in $\mathcal{D}$. This implies the existence of some $p(u, v, w, x)$ where

$$
\begin{aligned}
&R_{Marton-Sum} + \epsilon \leq \\
&I(W;Y) + I(U;Y|W) + I(V;Z|W) - I(U;V|W), \\
&R_{Marton-Sum} + \epsilon \leq \\
&I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W).
\end{aligned}
$$

This implies that

$$
\begin{aligned}
&R_{Marton-Sum} + \epsilon \leq \\
&\min(I(W;Y), I(W;Z)) + I(U;Y|W) + \\
&I(V;Z|W) - I(U;V|W)
\end{aligned}
$$

for some $p(u, v, w, x)$, which is a contradiction.

Using the supporting hyperplane theorem and the fact that $\mathcal{D}$ is convex and closed, one can conclude that there exists a supporting hyperplane to $\mathcal{D}$ at the boundary

point $(R_{Marton-Sum}, R_{Marton-Sum})$. We claim that this supporting hyperplane must have the equation $\lambda^* d_1 + (1-\lambda^*)d_2 = T(\lambda^*)$ for some $\lambda^* \in [0,1]$. The proof is as follows: any supporting hyperplane has the formula $\lambda^* d_1 + (1-\lambda^*)d_2 = k$ for some real λ^* and real k. We claim that λ^* must be in $[0,1]$ and $k = T(\lambda^*)$. Assume that for instance $\lambda^* < 0$. We know that $\mathcal{D}$ must be entirely contained in one of the two closed half-spaces determined by the hyperplane. Note that the points $(0,0)$, $(-\infty, 0)$ and $(0, -\infty)$ are in $\mathcal{D}$ (take $p(u,v,w,x)$ satisfying $I(U;V|W) = 0$ in the definition of $\mathcal{D}$). The value of $\lambda^* d_1 + (1-\lambda^*)d_2$ at these points is equal to 0, $+\infty$ and $-\infty$ respectively. Thus, $\mathcal{D}$ cannot possibly be entirely contained in one of the two closed half-spaces determined by the hyperplane. Similarly the case $1-\lambda^* < 0$ can be refuted. Therefore λ^* must be in $[0,1]$. Since the points $(-\infty, 0)$ and $(0, -\infty)$ are in $\mathcal{D}$, the half-space determined by the hyperplane that contains $\mathcal{D}$ is the one determined by the equation $\lambda^* d_1 + (1-\lambda^*)d_2 \leq k$ for some k. Since the half-space has at least one point of $\mathcal{D}$, the value of k must be equal to $\max_{(d_1,d_2)\in\mathcal{R}} \lambda^* d_1 + (1-\lambda^*)d_2$. The latter is equal to $T(\lambda^*)$. Thus, the supporting hyperplane at the boundary point $(R_{Marton-Sum}, R_{Marton-Sum})$ has the equation $\lambda^* d_1 + (1-\lambda^*)d_2 = T(\lambda^*)$ for some $\lambda^* \in [0,1]$.

Since $(R_{Marton-Sum}, R_{Marton-Sum})$ lies on this hyperplane, $\lambda^* R_{Marton-Sum} + (1-\lambda^*)R_{Marton-Sum} = T(\lambda^*)$ implies that $R_{Marton-Sum} = T(\lambda^*)$ for some $\lambda^* \in [0,1]$. Therefore

$$\min_{0\leq\lambda\leq 1} T(\lambda) \leq R_{Marton-Sum}.$$

On the other hand, for every λ, $T(\lambda) \geq R_{Marton-Sum}$. Therefore

$$\min_{0\leq\lambda\leq 1} T(\lambda) \geq R_{Marton-Sum}.$$

■

Proof of Lemma 6: Take a triple (u,v,w) such that $p(u,w)$ and $p(v,w)$ are positive. There must exist some x such that $p(u,w,x) > 0$. Since the transition matrices have positive entries and $p(u,w,y) \geq p(u,w,x)q(y|x)$, $p(u,w,y)$ will be positive for all y. A similar statement could be proved for $p(v,w,z)$. Assume that $p(u,v,w) = 0$. Take some u', v' such that $p(u',v',w) > 0$. Let us reduce $p(u',v',w)$ by ϵ and increase $p(u,v,w)$ by ϵ. Furthermore, have (u,v,w) mapped to the same x that (u',v',w) was mapped to; this ensures that the joint distribution of W and X is preserved. One can write

$$\begin{aligned}
&\lambda I(W;Y) + (1-\lambda)I(W;Z) + \\
&I(U;Y|W) + I(V;Z|W) - I(U;V|W) = \\
&\lambda I(W;Y) + (1-\lambda)I(W;Z) + \\
&H(Y|W) + H(Z|W) + \\
&H(UV|W) - H(UY|W) - H(VZ|W).
\end{aligned}$$

The only change in this expression comes from the change in $H(UV|W=w) - H(UY|W=w) - H(VZ|W=w)$. The derivative of $H(UV|W=w)$ with respect to

ϵ, at $\epsilon = 0$, will be infinity. But the derivative of $H(UY|W = w)$ and $H(VZ|W = w)$ will be finite since $p(u, y|w)$, $p(u', y|w)$, $p(v, z|w)$ and $p(v', z|w)$ are positive for all y and z. So, the first derivative of $H(UV|W = w) - H(UY|W = w) - H(VZ|W = w)$ with respect to ϵ, at $\epsilon = 0$, will be positive. This is a contradiction since $p(u, v, w, x)$ was assumed to maximize $T(\lambda)$.

■

8.3.3 Appendix

Appendix I

Suppose $p_0(u, v, w, x)$ is a joint distribution that maximizes $\lambda I(W;Y) + (1 - \lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$, and among all such joint distributions has the largest value of $I(W;Y) + I(W;Z)$. In this appendix, we prove that one can find $p(\widehat{u}, \widehat{v}, \widehat{w}, \widehat{x})$ such that

- $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$ is equal to $\lambda I(\widehat{W};\widehat{Y}) + (1-\lambda)I(\widehat{W};\widehat{Z}) + I(\widehat{U};\widehat{Y}|\widehat{W}) + I(\widehat{V};\widehat{Z}|\widehat{W}) - I(\widehat{U};\widehat{V}|\widehat{W})$,
- $I(W;Y) + I(W;Z)$ is equal to $I(\widehat{W};\widehat{Y}) + I(\widehat{W};\widehat{Z})$,
- $|\widehat{\mathcal{U}}| \leq \min(|\mathcal{X}|, |\mathcal{Y}|)$,
- $|\widehat{\mathcal{V}}| \leq \min(|\mathcal{X}|, |\mathcal{Z}|)$,
- $|\widehat{\mathcal{W}}| \leq |\mathcal{X}|$,
- $H(\widehat{X}|\widehat{U}\widehat{V}\widehat{W}) = 0$.

We begin by reducing the cardinality of W. Assume that $|\mathcal{W}| > |\mathcal{X}|$ and $p(w) \neq 0$ for all w. There must therefore exists a function $L : \mathcal{W} \to \mathbb{R}$ where

$$\mathbb{E}[L(W)|X] = 0,$$

$$\exists w : p(w) \neq 0, \quad L(w) \neq 0.$$

Let us perturb $p_0(u, v, w, x)$ along L as follows:

$$p_\epsilon(u, v, w, x, y, z) = p_0(u, v, w, x, y, z) \cdot [1 + \epsilon L(w)],$$

where ϵ is a real number in some interval $[-\overline{\epsilon}_1, \overline{\epsilon}_2]$ for some positive reals $\overline{\epsilon}_1$ and $\overline{\epsilon}_2$.

Consider the expression $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$ at $p_\epsilon(u, v, w, x, y, z)$. It can be verified that the expression is a linear function of ϵ under this perturbation. Since a maximum of this expression occurs at $\epsilon = 0$, which is a point strictly inside the interval $[-\overline{\epsilon}_1, \overline{\epsilon}_2]$, it must be the case that this expression is a constant function of ϵ. Next consider the expression $I(W;Y)+I(W;Z)$

at $p_\epsilon(u, v, w, x, y, z)$. It can be verified that the expression is a linear function of ϵ under this perturbation. Note that $p_0(u, v, w, x)$ is a joint distribution that has the largest value of $I(W;Y) + I(W;Z)$ among all joint distributions that maximize $\lambda I(W;Y)+(1-\lambda)I(W;Z)+I(U;Y|W)+I(V;Z|W)-I(U;V|W)$. Thus a maximum of $I(W;Y) + I(W;Z)$ occurs at $\epsilon = 0$, which is a point strictly inside the interval $[-\bar{\epsilon}_1, \bar{\epsilon}_2]$. But this can only happen when $I(W;Y) + I(W;Z)$ is a constant function of ϵ. Now, taking $\epsilon = -\bar{\epsilon}_1$ or $\epsilon = \bar{\epsilon}_2$ gives us a joint distribution with the same values of $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$ and $I(W;Y) + I(W;Z)$, but with a smaller support on $\mathcal{W}$. Using this argument, one can reduce the cardinality of W to $|\mathcal{X}|$.

Next, we show how one can reduce the cardinality of U to find $p(\widehat{u}, \widehat{v}, \widehat{w}, \widehat{x})$ such that

- $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$ is equal to $\lambda I(\widehat{W};\widehat{Y}) + (1-\lambda)I(\widehat{W};\widehat{Z}) + I(\widehat{U};\widehat{Y}|\widehat{W}) + I(\widehat{V};\widehat{Z}|\widehat{W}) - I(\widehat{U};\widehat{V}|\widehat{W})$,
- $I(W;Y) + I(W;Z)$ is equal to $I(\widehat{W};\widehat{Y}) + I(\widehat{W};\widehat{Z})$,
- $|\widehat{\mathcal{U}}| \leq \min(|\mathcal{X}|, |\mathcal{Y}|)$,
- $|\widehat{\mathcal{W}}| \leq |\mathcal{X}|$.

We can repeat a similar procedure to impose the constraint $|\widehat{\mathcal{V}}| \leq \min(|\mathcal{X}|, |\mathcal{Z}|)$. Imposing the extra constraint $H(\widehat{X}|\widehat{U}\widehat{V}\widehat{W}) = 0$ will be discussed at the end.

If $|\mathcal{X}| \leq |\mathcal{Y}|$, establishing the cardinality bound of $|\mathcal{X}|$ on U suffices. This cardinality bound is proved in section 7.3 using perturbations of the type $L : \mathcal{U} \times \mathcal{W} \to \mathbb{R}$ where

$$\mathbb{E}[L(U, W)|WX] = 0.$$

Note that these perturbations preserve the marginal distribution of $p(w, x)$, and thus also $I(W;Y) + I(W;Z)$. The interesting case is therefore when $|\mathcal{X}| > |\mathcal{Y}|$. Assume that $|\mathcal{U}| > |\mathcal{Y}|$. If for every $w \in \mathcal{W}$, $p(u|w) \neq 0$ for at most $|\mathcal{Y}|$ elements u, we are done, since we can relabel the elements in the range of U to ensure that only an alphabet of size at most $|\mathcal{Y}|$ is used, without affecting any of the mutual information terms in the expression of interest. There must therefore exists a function $L : \mathcal{U} \times \mathcal{W} \to \mathbb{R}$ where

$$\mathbb{E}[L(U, W)|WY] = 0,$$
$$\exists (u, w) : p_0(u, w) \neq 0, \quad L(u, w) \neq 0.$$

Let us perturb $p_0(u, v, w, x)$ along the random variable $L : \mathcal{U} \times \mathcal{W} \to \mathbb{R}$. Random variables $\widetilde{U}, \widetilde{V}, \widetilde{W}, \widetilde{X}, \widetilde{Y}, \widetilde{Z}$ are distributed according to $p_\epsilon(\widetilde{u}, \widetilde{v}, \widetilde{w}, \widetilde{x}, \widetilde{y}, \widetilde{z})$ defined as follows

$$p_\epsilon(\widetilde{u}, \widetilde{v}, \widetilde{w}, \widetilde{x}, \widetilde{y}, \widetilde{z}) = p_0(\widetilde{u}, \widetilde{v}, \widetilde{w}, \widetilde{x}, \widetilde{y}, \widetilde{z}) \cdot [1 + \epsilon L(\widetilde{u}, \widetilde{w})],$$

where ϵ is a real number in some interval $[-\bar{\epsilon}_1, \bar{\epsilon}_2]$.

The first derivative of $\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) + I(V;Z|W) - I(U;V|W)$ with respect to ϵ, at $\epsilon = 0$ should be zero. Since

$$\begin{aligned}
&\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) \\
&+ I(V;Z|W) - I(U;V|W) = \\
&\lambda\big(H(W) + H(Y) - H(WY)\big) \\
&+ (1-\lambda)\big(H(W) + H(Z) - H(WZ)\big) + \\
&H(YW) + H(ZW) - H(UYW) \\
&- H(VZW) + H(UVW) - H(W),
\end{aligned}$$

we will have:

$$\begin{aligned}
&\lambda\big(H_L(W) + H_L(Y) - H_L(WY)\big) + \\
&(1-\lambda)\big(H_L(W) + H_L(Z) - H_L(WZ)\big) \\
&+ H_L(YW) + H_L(ZW) - H_L(UYW) \\
&- H_L(VZW) + H_L(UVW) - H_L(W) = 0,
\end{aligned}$$

where $H_L(W)$ denotes $\sum_w E[L|W=w]p(w)\log\frac{1}{p(w)}$ and similarly for the other terms. Using Lemma 3 of section 7.3, we have:

$$\begin{aligned}
&\lambda I(\widetilde{W};\widetilde{Y}) + (1-\lambda)I(\widetilde{W};\widetilde{Z}) + I(\widetilde{U};\widetilde{Y}|\widetilde{W}) \\
&+ I(\widetilde{V};\widetilde{Z}|\widetilde{W}) - I(\widetilde{U};\widetilde{V}|\widetilde{W}) = \\
&\lambda I(W;Y) + (1-\lambda)I(W;Z) + I(U;Y|W) \\
&+ I(V;Z|W) - I(U;V|W) + \\
&\lambda\big(-\mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|W]\big)\big] - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|Y]\big)\big] \\
&+ \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|WY]\big)\big]\big) + \\
&(1-\lambda)\big(-\mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|W]\big)\big] - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|Z]\big)\big] \\
&+ \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|WZ]\big)\big]\big) + \\
&- \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|YW]\big)\big] - \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|ZW]\big)\big] \\
&+ \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|UYW]\big)\big] + \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|VWZ]\big)\big] \\
&- \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|UVW]\big)\big] + \mathbb{E}\big[r\big(\epsilon\cdot\mathbb{E}[L|W]\big)\big],
\end{aligned}$$

where $r(x) = (1+x)\log(1+x)$. Since $\mathbb{E}[L(U,W)|WY] = 0$, and L is a function of UW, we have:

$$\begin{aligned}
&\lambda I(\widetilde{W};\widetilde{Y}) + (1-\lambda) I(\widetilde{W};\widetilde{Z}) + I(\widetilde{U};\widetilde{Y}|\widetilde{W}) \\
&+ I(\widetilde{V};\widetilde{Z}|\widetilde{W}) - I(\widetilde{U};\widetilde{V}|\widetilde{W}) = \\
&\lambda I(W;Y) + (1-\lambda) I(W;Z) + I(U;Y|W) \\
&+ I(V;Z|W) - I(U;V|W) + \\
&(1-\lambda)\big(- \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|Z]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|WZ]\big)\big]\big) \\
&- \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|ZW]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|VWZ]\big)\big].
\end{aligned}$$

Since $r(x) = (1+x)\log(1+x)$ is a convex function, we have

$$\begin{aligned}
&- \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|Z]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|WZ]\big)\big] \geq 0, \\
&- \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|WZ]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|VWZ]\big)\big] \geq 0.
\end{aligned}$$

Therefore for any $\epsilon \in [-\overline{\epsilon}_1, \overline{\epsilon}_2]$, we have

$$\begin{aligned}
&\lambda I(\widetilde{W};\widetilde{Y}) + (1-\lambda) I(\widetilde{W};\widetilde{Z}) + I(\widetilde{U};\widetilde{Y}|\widetilde{W}) \\
&+ I(\widetilde{V};\widetilde{Z}|\widetilde{W}) - I(\widetilde{U};\widetilde{V}|\widetilde{W}) \geq \\
&\lambda I(W;Y) + (1-\lambda) I(W;Z) + I(U;Y|W) \\
&+ I(V;Z|W) - I(U;V|W).
\end{aligned}$$

This implies that $\lambda I(\widetilde{W};\widetilde{Y}) + (1-\lambda) I(\widetilde{W};\widetilde{Z}) + I(\widetilde{U};\widetilde{Y}|\widetilde{W}) + I(\widetilde{V};\widetilde{Z}|\widetilde{W}) - I(\widetilde{U};\widetilde{V}|\widetilde{W})$ is a constant function of ϵ. The maximum of $I(\widetilde{W};\widetilde{Y}) + I(\widetilde{W};\widetilde{Z})$ as a function of ϵ occurs at $\epsilon = 0$. Therefore

$$I_L(W;Y) + I_L(W;Z) = 0.$$

Using lemma 3 of section 7.3, one can observe that $[I(\widetilde{W};\widetilde{Y}) + I(\widetilde{W};\widetilde{Z})] - [I(W;Y) + I(W;Z)]$ equals

$$- \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|Z]\big)\big] + \mathbb{E}\big[r\big(\epsilon \cdot \mathbb{E}[L|WZ]\big)\big] \geq 0.$$

But this can only happen when $I(\widetilde{W};\widetilde{Y}) + I(\widetilde{W};\widetilde{Z})$ is a constant function of ϵ. Now, taking $\epsilon = -\overline{\epsilon}_1$ or $\epsilon = \overline{\epsilon}_2$ gives us auxiliary random variable $(\widetilde{U},\widetilde{W})$ with smaller support than that of (U,W). We can continue this process as long as there exists $w \in \mathcal{W}$, such that $p(u|w) \neq 0$ for more than $|\mathcal{Y}|$ elements u.

It remains to show that one can impose the extra constraint $H(\widehat{X}|\widehat{U}\widehat{V}\widehat{W}) = 0$. Fix $p(\widetilde{u},\widetilde{v},\widetilde{w})$. Consider the expressions $\lambda I(\widetilde{W};\widetilde{Y}) + (1-\lambda) I(\widetilde{W};\widetilde{Z}) + I(\widetilde{U};\widetilde{Y}|\widetilde{W}) + I(\widetilde{V};\widetilde{Z}|\widetilde{W}) - I(\widetilde{U};\widetilde{V}|\widetilde{W})$ and $I(\widetilde{W};\widetilde{Y}) + I(\widetilde{W};\widetilde{Z})$ as functions of the conditional distribution of $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$. We know that for instance that the former expression is

maximized at $p(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$. Further, the extreme points of the corresponding region for $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$ satisfy $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w}) \in \{0,1\}$. Both of the expressions are convex functions of $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$. This is because $I(\widetilde{W};\widetilde{Y})$ is convex in the conditional distribution $p(\widetilde{y}|\widetilde{w})$; similarly $I(\widetilde{U};\widetilde{Y}|\widetilde{W}=\widetilde{w})$ is convex for any fixed value of $\widetilde{w}$. The term $I(\widetilde{U};\widetilde{V}|\widetilde{W})$ that appears with a negative sign is constant since the joint distribution of $p(\widetilde{u},\widetilde{v},\widetilde{w})$ is fixed.

We can express $p(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$ as a linear combination of the extreme points of the region formed by all conditional distributions $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$. Since the maximum of $\lambda I(\widetilde{W};\widetilde{Y}) + (1-\lambda)I(\widetilde{W};\widetilde{Z}) + I(\widetilde{U};\widetilde{Y}|\widetilde{W}) + I(\widetilde{V};\widetilde{Z}|\widetilde{W}) - I(\widetilde{U};\widetilde{V}|\widetilde{W})$ occurs at some $p(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$ and the expression is convex in $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$, the maximum must also occur at all the extreme points showing up in the linear combination. One can use the convexity of $I(\widetilde{W};\widetilde{Y})+I(\widetilde{W};\widetilde{Z})$ in $r(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$ to show that the value of $I(\widetilde{W};\widetilde{Y})+I(\widetilde{W};\widetilde{Z})$ at all these extreme points must be also equal to that at $p(\widetilde{x}|\widetilde{u},\widetilde{v},\widetilde{w})$.

Appendix II

It suffices to prove the following statement:

Statement: Take an irreducible broadcast channel with positive transition matrices, and an arbitrary marginal input distribution on X, $p(x)$. Let $p(u,v,x)$ be a solution to the following maximization problem

$$\max_{UV\to X\to YZ, X\sim p(x)} I(U;Y) + I(V;Z) - I(U;V).$$

Further assume that $p(u) > 0$ for all u, and $p(v) > 0$ for all v. Further assume that $H(X|UV) = 0$. We use $x = \xi_0(u,v)$ to denote the deterministic mapping from $\mathcal{U}\times\mathcal{V}$ to $\mathcal{X}$.

Then the profile vector of the mapping ξ_0, $\overrightarrow{v_{\xi_0}}$, cannot be written as

$$\sum_{t=1}^{M} \alpha_t \overrightarrow{v_{\xi_t}},$$

where ξ_t (for $t = 1,2,3,...,M$) are deterministic mappings not equal to ξ_0, and α_t are non-negative numbers adding up to one, i.e. $\sum_{t=1}^{M}\alpha_t = 1$.

Proof of the statement: Assume that $\mathcal{U} = \{u_1,u_2,....,u_{|\mathcal{U}|}\}$ and $\mathcal{V} = \{v_1,v_2,....,v_{|\mathcal{V}|}\}$. Let $\pi_{i,j} = p(u_i,v_j)$ for $i = 1,...,|\mathcal{U}|$, $j = 1,2,3,...,|\mathcal{V}|$. The proof of Lemma 6 could be mimicked to show that $p(u,v)$ is positive for all u,v whenever $p(u) > 0$ and $p(v) > 0$ for all u,v. Therefore we must have $\pi_{i,j} > 0$ for all i and j. Let $\bar{\epsilon} = \min_{i,j}\pi_{i,j}$. Take some $\epsilon \in (0,\bar{\epsilon})$.

We prove the statement by contradiction. Assume that

$$\overrightarrow{v_{\xi_0}} = \sum_{t=1}^{M} \alpha_t \overrightarrow{v_{\xi_t}},$$

for some mappings ξ_t $(t = 1, 2, .., M)$ and non-negative numbers α_t adding up to one.

Let random variables $T_{i,j}$ (for $i = 1, ..., |\mathcal{U}|$, $j = 1, 2, 3, ..., |\mathcal{V}|$) be $M+1$-ary random variables mutually independent of each other, and of U, V, X, Y, Z satisfying:

- $p(T_{i,j} = 0) = 1 - \frac{\epsilon}{\pi_{i,j}}$,
- $p(T_{i,j} = 1) = \frac{\epsilon}{\pi_{i,j}}\alpha_1$,
- $p(T_{i,j} = 2) = \frac{\epsilon}{\pi_{i,j}}\alpha_2$,
- $p(T_{i,j} = 3) = \frac{\epsilon}{\pi_{i,j}}\alpha_3$,
- ...
- $p(T_{i,j} = M) = \frac{\epsilon}{\pi_{i,j}}\alpha_M$.

Let $\widetilde{X}$ be defined as follows:

- Under the event the pair $(U, V) = (u_i, v_j)$, let $\widetilde{X}$ be equal to $\xi_{T_{i,j}}(u_i, v_j)$. In other words, if $T_{i,j} = 0$, $\widetilde{X}$ is equal to $\xi_0(u_i, v_j)$; if $T_{i,j} = 1$, $\widetilde{X}$ is equal to $\xi_1(u_i, v_j)$, etc.

We claim that $p(\widetilde{X} = x|U = u_i) = p(X = x|U = u_i)$ for all $i = 1, 2, 3, ..., |\mathcal{U}|$ and x; and similarly $p(\widetilde{X} = x|V = v_j) = p(X = x|V = v_j)$ for all $j = 1, 2, 3, ..., |\mathcal{V}|$ and x. The reason is that

$$
\begin{aligned}
&p(\widetilde{X} = x|U = u_i) = \\
&\sum_j p(V = v_j|U = u_i)p(\widetilde{X} = x|U = u_i, V = v_j) = \\
&\sum_j p(V = v_j|U = u_i)\sum_{k=0}^{M} p(T_{i,j} = k)\mathbf{1}[\xi_k(u_i, v_j) = x] = \\
&\sum_j p(V = v_j|U = u_i)(1 - \frac{\epsilon}{\pi_{i,j}})\mathbf{1}[\xi_0(u_i, v_j) = x] + \\
&\sum_j p(V = v_j|U = u_i)\sum_{k=1}^{M} \frac{\epsilon}{\pi_{i,j}}\alpha_k\mathbf{1}[\xi_k(u_i, v_j) = x] = \\
&\sum_j p(V = v_j|U = u_i)(\frac{\pi_{i,j} - \epsilon}{\pi_{i,j}})\mathbf{1}[\xi_0(u_i, v_j) = x] + \\
&\sum_{k=1}^{M}\sum_j p(V = v_j|U = u_i)\frac{\epsilon}{\pi_{i,j}}\alpha_k\mathbf{1}[\xi_k(u_i, v_j) = x].
\end{aligned}
$$

Note that $p(V=v_j|U=u_i)=\frac{p(V=v_j,U=u_i)}{p(U=u_i)}=\frac{\pi_{i,j}}{p(U=u_i)}$. Therefore

$$\begin{aligned}
&p(\widetilde{X}=x|U=u_i)= \\
&\sum_j \frac{\pi_{i,j}-\epsilon}{p(U=u_i)}\mathbf{1}[\xi_0(u_i,v_j)=x]+ \\
&\sum_{k=1}^{M}\sum_j \frac{\epsilon}{p(U=u_i)}\alpha_k\mathbf{1}[\xi_k(u_i,v_j)=x]= \\
&\sum_j \frac{\pi_{i,j}}{p(U=u_i)}\mathbf{1}[\xi_0(u_i,v_j)=x] \\
&-\frac{\epsilon}{p(U=u_i)}\sum_j \mathbf{1}[\xi_0(u_i,v_j)=x]+ \\
&\frac{\epsilon}{p(U=u_i)}\sum_{k=1}^{M}\alpha_k\sum_j \mathbf{1}[\xi_k(u_i,v_j)=x].
\end{aligned}$$

But since

$$\overrightarrow{v_{\xi_0}}=\sum_{t=1}^{M}\alpha_t\overrightarrow{v_{\xi_t}},$$

the profiles of the i^{th} rows must also satisfy the same property:

$$\sum_j \mathbf{1}[\xi_0(u_i,v_j)=x]=\sum_{k=1}^{M}\alpha_k\sum_j \mathbf{1}[\xi_k(u_i,v_j)=x].$$

Therefore,

$$\begin{aligned}
&p(\widetilde{X}=x|U=u_i)= \\
&\sum_j \frac{\pi_{i,j}}{p(U=u_i)}\mathbf{1}[\xi_0(u_i,v_j)=x]+0-0= \\
&\sum_j \frac{\pi_{i,j}}{p(U=u_i)}\mathbf{1}[\xi_0(u_i,v_j)=x]=p(X=x|U=u_i).
\end{aligned}$$

The equation $p(\widetilde{X}=x|V=v_j)=p(X=x|V=v_j)$ for all $j=1,2,3,...,|\mathcal{V}|$ and x can be proved similarly.

Note that the above property implies that $\widetilde{X}$ and X have the same marginal distributions.

Let $\widetilde{Y}$ and $\widetilde{Z}$ be defined such that $UV(T_{i,j})_{i:1,2,..,j=1,2,..}\rightarrow\widetilde{X}\rightarrow\widetilde{Y}\widetilde{Z}$, and the conditional law of $\widetilde{y}$ and $\widetilde{z}$ given $\widetilde{x}$ is the same as $q(y,z|x)$. Here $(T_{i,j})_{i:1,2,..,j=1,2,..}$ denotes the collection of all $T_{i,j}$ for all i and j.

Without loss of generality, let us assume $\alpha_1 \neq 0$. Since the mapping $\xi_0(\cdot,\cdot)$ is not equal to $\xi_1(\cdot,\cdot)$, there must exist (i,j) such that $\xi_0(u_i,v_j) \neq \xi_1(u_i,v_j)$. Let us label the inputs symbol $\xi_0(u_i,v_j)$ by x_0, and the input symbol $\xi_1(u_i,v_j)$ by x_1. We know that the channel is irreducible. Let us then assume that there is some y such that $q(y|x_0) \neq q(y|x_1)$; the proof for the case when there is some z such that $q(z|x_0) \neq q(z|x_1)$ is similar. Let $\widetilde{U} = (U, T_{i,j})$ and $\widetilde{V} = V$.

Since $p(\widetilde{X} = x|U = u) = p(X = x|U = u)$ for all u and x, and $p(\widetilde{X} = x|V = v) = p(X = x|V = v)$ for all v and x, we have

- $I(U;\widetilde{Y}) = I(U;Y)$,
- $I(V;\widetilde{Z}) = I(V;Z)$.

Therefore $I(\widetilde{V};\widetilde{Z}) = I(V;Z)$ and $I(\widetilde{U};\widetilde{Y}) = I(U;Y) + I(T_{i,j};\widetilde{Y}|U)$. Furthermore since $T_{i,j}$ is independent of U, V, we have $I(\widetilde{U};\widetilde{V}) = I(U;V)$. Therefore

$$\begin{aligned} &I(\widetilde{U};\widetilde{Y}) + I(\widetilde{V};\widetilde{Z}) - I(\widetilde{U};\widetilde{V}) - \big(I(U;Y) + I(V;Z) - I(U;V)\big) \\ &= I(T_{i,j};\widetilde{Y}|U). \end{aligned}$$

Since $p(u,v,x)$ was maximizing $I(U;Y) + I(V;Z) - I(U;V)$ under fixed marginal distribution on x, we must have $I(T_{i,j};\widetilde{Y}|U) = 0$. Therefore $I(T_{i,j};\widetilde{Y}|U = u_i) = 0$ holds as well.

In Appendix III of this section, we prove that the following are true

$$p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 0) \neq p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 1),$$

$$p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 0) \neq p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 1).$$

But for any $x \notin \{x_0, x_1\}$,

$$p(\widetilde{X} = x|U = u_i, T_{i,j} = 0) = p(\widetilde{X} = x|U = u_i, T_{i,j} = 1).$$

Remember that we assumed that there is some y such that $q(y|x_0) \neq q(y|x_1)$. In Appendix IV of this section, we show that

$$p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0) \neq p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1).$$

This implies that $\widetilde{Y}$ and $T_{i,j}$ are not conditionally independent given $U = u_i$. Therefore $I(T_{i,j};\widetilde{Y}|U = u_i) \neq 0$ which is a contradiction.

Appendix III

Note that

$$\begin{aligned}
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0) = \\
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0, V = v_j) p(V = v_j | U = u_i, T_{i,j} = 0) \\
&+ \\
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0, V \neq v_j) p(V \neq v_j | U = u_i, T_{i,j} = 0).
\end{aligned}$$

Since under the event $(U, V) = (u_i, v_j)$ and $T_{i,j} = 0$, $\widetilde{X}$ is equal to x_0, the term $p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0, V = v_j)$ will be equal to one. Since (U, V) is independent of $T_{i,j}$, we have

$$p(V = v_j | U = u_i, T_{i,j} = 0) = p(V = v_j | U = u_i),$$

$$p(V \neq v_j | U = u_i, T_{i,j} = 0) = p(V \neq v_j | U = u_i).$$

Lastly $p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0, V \neq v_j)$ is equal to $p(\widetilde{X} = x_0 | U = u_i, V \neq v_j)$ since under the event that $(U = u_i, V \neq v_j)$, $\widetilde{X}$ will be independent of $T_{i,j}$ (note that $T_{\cdot,\cdot}$ random variables were mutually independent of each other). Therefore,

$$\begin{aligned}
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0) = \\
&p(V = v_j | U = u_i) + \\
&p(\widetilde{X} = x_0 | U = u_i, V \neq v_j) p(V \neq v_j | U = u_i).
\end{aligned} \tag{8.8}$$

Next, note that

$$\begin{aligned}
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 1) = \\
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 1, V = v_j) p(V = v_j | U = u_i, T_{i,j} = 1) + \\
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 1, V \neq v_j) p(V \neq v_j | U = u_i, T_{i,j} = 1).
\end{aligned}$$

Since under the event $(U, V) = (u_i, v_j)$ and $T_{i,j} = 1$, $\widetilde{X}$ is equal to x_1, the term $p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 1, V = v_j)$ will be equal to zero. Following an argument like above, one can show that

$$\begin{aligned}
&p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 1) = \\
&0 + p(\widetilde{X} = x_0 | U = u_i, V \neq v_j) p(V \neq v_j | U = u_i).
\end{aligned} \tag{8.9}$$

Comparing equations (8.8) and (8.9), and noting that $p(V = v_j | U = u_i) > 0$, we conclude that

$$p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 0) \neq p(\widetilde{X} = x_0 | U = u_i, T_{i,j} = 1).$$

The proof for

$$p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 0) \neq p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 1)$$

is similar.

It remains to show that for any $x \notin \{x_0, x_1\}$,

$$p(\widetilde{X} = x|U = u_i, T_{i,j} = 0) = p(\widetilde{X} = x|U = u_i, T_{i,j} = 1).$$

Note that

$$\begin{aligned}
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 1) = \\
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 1, V = v_j)p(V = v_j|U = u_i, T_{i,j} = 1)+ \\
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 1, V \neq v_j)p(V \neq v_j|U = u_i, T_{i,j} = 1) = \\
&0 + p(\widetilde{X} = x|U = u_i, V \neq v_j)p(V \neq v_j|U = u_i) = \\
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 0).
\end{aligned}$$

Appendix IV

We prove the statement by contradiction. Assume that

$$p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0) = p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1).$$

We have

$$\begin{aligned}
&p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0) = \\
&p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0, \widetilde{X} = x_0)p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 0)+ \\
&p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0, \widetilde{X} = x_1)p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 0)+ \\
&\sum_{x \in \mathcal{X}, x \notin \{x_0, x_1\}} \big(p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0, \widetilde{X} = x)\times \\
&\qquad p(\widetilde{X} = x|U = u_i, T_{i,j} = 0)\big) = \\
&p(\widetilde{Y} = y|\widetilde{X} = x_0)p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 0)+ \\
&p(\widetilde{Y} = y|\widetilde{X} = x_1)p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 0)+ \\
&\sum_{x \mathcal{X}, x \notin \{x_0, x_1\}} \big(p(\widetilde{Y} = y|\widetilde{X} = x)p(\widetilde{X} = x|U = u_i, T_{i,j} = 0)\big).
\end{aligned}$$

Similarly,

$$
\begin{aligned}
&p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1) = \\
&p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1, \widetilde{X} = x_0)p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 1)+ \\
&p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1, \widetilde{X} = x_1)p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 1)+ \\
&\sum_{x\in\mathcal{X}, x\notin\{x_0,x_1\}} \big(p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1, \widetilde{X} = x)\times \\
&\qquad\qquad p(\widetilde{X} = x|U = u_i, T_{i,j} = 1)\big) = \\
&p(\widetilde{Y} = y|\widetilde{X} = x_0)p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 1)+ \\
&p(\widetilde{Y} = y|\widetilde{X} = x_1)p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 1)+ \\
&\sum_{x\mathcal{X}, x\notin\{x_0,x_1\}} \big(p(\widetilde{Y} = y|\widetilde{X} = x)p(\widetilde{X} = x|U = u_i, T_{i,j} = 1)\big).
\end{aligned}
$$

The assumption that

$$p(\widetilde{Y} = y|U = u_i, T_{i,j} = 0) = p(\widetilde{Y} = y|U = u_i, T_{i,j} = 1),$$

therefore implies:

$$
\begin{aligned}
&p(\widetilde{Y} = y|\widetilde{X} = x_0)p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 0)+ \\
&p(\widetilde{Y} = y|\widetilde{X} = x_1)p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 0)+ \\
&\sum_{x\mathcal{X}, x\notin\{x_0,x_1\}} \big(p(\widetilde{Y} = y|\widetilde{X} = x)\times \\
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 0)\big) = \\
&p(\widetilde{Y} = y|\widetilde{X} = x_0)p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 1)+ \\
&p(\widetilde{Y} = y|\widetilde{X} = x_1)p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 1)+ \\
&\sum_{x\in\mathcal{X}, x\notin\{x_0,x_1\}} \big(p(\widetilde{Y} = y|\widetilde{X} = x)p(\widetilde{X} = x|U = u_i, T_{i,j} = 1)\big).
\end{aligned}
$$

It was shown in Appendix III of this section that

$$p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 0) \neq p(\widetilde{X} = x_0|U = u_i, T_{i,j} = 1),$$

$$p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 0) \neq p(\widetilde{X} = x_1|U = u_i, T_{i,j} = 1).$$

But for any $x \notin \{x_0, x_1\}$,

$$
\begin{aligned}
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 0) = \\
&p(\widetilde{X} = x|U = u_i, T_{i,j} = 1).
\end{aligned}
\tag{8.10}
$$

Thus, we must have

$$\begin{aligned}
&p(\widetilde{Y}=y|\widetilde{X}=x_0)p(\widetilde{X}=x_0|U=u_i,T_{i,j}=0)+\\
&p(\widetilde{Y}=y|\widetilde{X}=x_1)p(\widetilde{X}=x_1|U=u_i,T_{i,j}=0)=\\
&p(\widetilde{Y}=y|\widetilde{X}=x_0)p(\widetilde{X}=x_0|U=u_i,T_{i,j}=1)+\\
&p(\widetilde{Y}=y|\widetilde{X}=x_1)p(\widetilde{X}=x_1|U=u_i,T_{i,j}=1).
\end{aligned}$$

This implies that

$$\frac{p(\widetilde{X}=x_0|U=u_i,T_{i,j}=1)-p(\widetilde{X}=x_0|U=u_i,T_{i,j}=0)}{p(\widetilde{X}=x_1|U=u_i,T_{i,j}=0)-p(\widetilde{X}=x_1|U=u_i,T_{i,j}=1)}=\frac{p(\widetilde{Y}=y|\widetilde{X}=x_1)}{p(\widetilde{Y}=y|\widetilde{X}=x_0)}.$$

Note that the nominator and denominator are positive by what was proved in Appendix III of this section.

On the other hand, we also have by equation 8.10:

$$\begin{aligned}
&p(\widetilde{X}=x_0|U=u_i,T_{i,j}=0)+\\
&p(\widetilde{X}=x_1|U=u_i,T_{i,j}=0)=\\
&p(\widetilde{X}=x_0|U=u_i,T_{i,j}=1)+\\
&p(\widetilde{X}=x_1|U=u_i,T_{i,j}=1).
\end{aligned}$$

This implies that

$$\frac{p(\widetilde{X}=x_0|U=u_i,T_{i,j}=1)-p(\widetilde{X}=x_0|U=u_i,T_{i,j}=0)}{p(\widetilde{X}=x_1|U=u_i,T_{i,j}=0)-p(\widetilde{X}=x_1|U=u_i,T_{i,j}=1)}=1.$$

Hence,

$$\frac{p(\widetilde{Y}=y|\widetilde{X}=x_1)}{p(\widetilde{Y}=y|\widetilde{X}=x_0)}=1.$$

But we know that $p(\widetilde{Y}=y|\widetilde{X}=x_0)\neq p(\widetilde{Y}=y|\widetilde{X}=x_1)$ since the input values x_0 and x_1 are distinguishable by the Y receiver. This is a contradiction.

Appendix V

Take a broadcast channel with positive transition matrices, and let $p(u,v,w,x)$ maximize the expression $\lambda I(W;Y)+(1-\lambda)I(W;Z)+I(U;Y|W)+I(V;Z|W)-I(U;V|W)$. Fixing the joint distribution of X and W, one can see that for any w the conditional distribution $p(u,v,x|w)$ will be a solution to the following maximization problem:

$$\max_{UV\to X\to YZ, X\sim p(x|w)} H(UV)-H(UY)-H(VZ).$$

The proof relies on the following claim:

Claim. Take a broadcast channel with positive transition matrices, and an arbitrary marginal input distribution on X, $p(x)$. Let $p(u,v,x)$ be a solution to the following maximization problem

$$\max_{UV\to X\to YZ, X\sim p(x)} H(UV) - H(UY) - H(VZ).$$

Further assume that $p(u) > 0$ for all u, and $p(v) > 0$ for all v. Let the functions

$$\begin{aligned}
&\hat{f}_u : \mathcal{X} \to \mathbb{R} \text{ for every } u \in \mathcal{U},\\
&\hat{g}_v : \mathcal{X} \to \mathbb{R} \text{ for every } v \in \mathcal{V},\\
&\hat{h} : \mathcal{X} \to \mathbb{R},
\end{aligned}$$

be defined as follows:

$$\begin{aligned}
\hat{f}_u(x) &= \sum_y q(y|x) \log p(uy),\\
\hat{g}_v(x) &= \sum_z q(z|x) \log p(vz),\\
\hat{h}(x) &= \min_{u',v'} \big(\log(p(u',v')) - \hat{f}_{u'}(x) - \hat{g}_{v'}(x) \big).
\end{aligned}$$

It is then claimed that for any (u,v), we have

$$\begin{aligned}
&p(x_0|u,v) = 1 \text{ for some } x_0 \in \mathcal{X} \Rightarrow\\
&x_0 \in argmax_x \hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x),
\end{aligned}$$

and

$$\log(p(u,v)) = \max_x \hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x).$$

Proof of the claim: The proof of Lemma 6 could be mimicked to show that $p(u,v)$, $p(u,y)$ and $p(v,z)$ are positive for all u,v,y,z whenever $p(u) > 0$ and $p(v) > 0$ for all u,v. Therefore $\hat{f}_u(x)$, $\hat{g}_v(x)$ and $\hat{h}(x)$ are well-defined.

The proof begins by noting that the definition of $\hat{h}(x)$ implies that for any (u,v,x),

$$\hat{h}(x) \le \log(p(u,v)) - \hat{f}_u(x) - \hat{g}_v(x).$$

Therefore, for any (u,v,x),

$$\log(p(u,v)) \ge \hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x).$$

Thus,

$$\log(p(u,v)) \ge \max_x \big(\hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x) \big). \tag{8.11}$$

Note that the first partial derivative of $H(UV) - H(UY) - H(VZ)$ with respect to $p(u, v, x)$ is proportional to

$$\begin{aligned}
&- \log p(u, v) - 1 + \sum_y q(y|x) \log p(u, y) + 1 + \\
&\sum_z q(z|x) \log p(v, z) + 1 = \\
&- \log p(u, v) + \hat{f}_u(x) + \hat{g}_v(x) + 1.
\end{aligned}$$

Assume that the triple (u, v, x) is such that $p(u, v, x) > 0$. Take some arbitrary u' and v'. Reducing $p(u, v, x)$ by a small ϵ and increasing $p(u', v', x)$ by ϵ does not affect the marginal distribution of X and hence should not increase the expression $H(UV) - H(UY) - H(VZ)$. Therefore the first derivative of $H(UV) - H(UY) - H(VZ)$ with respect to $p(u, v, x)$ must be greater than or equal to the first derivative of $H(UV) - H(UY) - H(VZ)$ with respect to $p(u', v', x)$. Thus,

$$\begin{aligned}
&- \log p(u, v) + \hat{f}_u(x) + \hat{g}_v(x) + 1 \geq \\
&- \log p(u', v') + \hat{f}_{u'}(x) + \hat{g}_{v'}(x) + 1.
\end{aligned}$$

In other words, for any arbitrary u' and v', we have

$$\begin{aligned}
&\log p(u, v) - \hat{f}_u(x) - \hat{g}_v(x) \leq \\
&\log p(u', v') - \hat{f}_{u'}(x) - \hat{g}_{v'}(x).
\end{aligned}$$

Therefore

$$\begin{aligned}
&\log p(u, v) - \hat{f}_u(x) - \hat{g}_v(x) \leq \\
&\min_{u', v'} \log p(u', v') - \hat{f}_{u'}(x) - \hat{g}_{v'}(x) = \hat{h}(x).
\end{aligned}$$

Thus, $\log p(u, v) \leq \hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x)$ whenever $p(u, v, x) > 0$. This together with equation (8.11) imply that

$$\log(p(u, v)) = \max_x \hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x),$$

and

$$\begin{aligned}
&p(x_0|u, v) = 1 \text{ for some } x_0 \in \mathcal{X} \Rightarrow \\
&x_0 \in argmax_x \hat{f}_u(x) + \hat{g}_v(x) + \hat{h}(x).
\end{aligned}$$

Appendix VI

The proof follows from the following two statements:

Statement 1: Assume that $p^*(u,v,w,x)$ is an arbitrary joint distribution maximizing $\lambda I(W;Y)+(1-\lambda)I(W;Z)+I(U;Y|W)+I(V;Z|W)-I(U;V|W)$, and having the largest value of $I(W;Y)+I(W;Z)$ among all maximizing joint distributions. For every w, $p^*(x|w)$ must belong to the set $\mathcal{T}$ defined as follows. Let $\mathcal{T}(q(y,z|x))$ be the set of pmfs on $\mathcal{X}$, $t(x)$, such that

$$\begin{aligned}&\max_{p(u,v,w|x)t(x)q(y,z|x)} \big\{\lambda I(W;Y)+(1-\lambda)I(W;Z)\\ &\quad + I(U;Y|W)+I(V;Z|W)-I(U;V|W)\big\}\\ &\quad = \max_{p(u,v|x)t(x)q(y,z|x)} (I(U;Y)+I(V;Z)-I(U;V)),\end{aligned}$$

and $I(W;Y)=I(W;Z)=0$ for *any*[3] pmf $p(u,v,w|x)t(x)$ that maximizes the expression $\lambda I(W;Y)+(1-\lambda)I(W;Z)+I(U;Y|W)+I(V;Z|W)-I(U;V|W)$.[4]

Statement 2: Let $q(y,z|x)$ be a general broadcast channel, and $t(x)\in\mathcal{T}(q(y,z|x))$. Consider the maximization problem: $\max_{p(u,v|x)t(x)q(y,z|x)}(I(U;Y)+I(V;Z)-I(U;V))$. Assume that *a* maximum occurs at $p^*(u,v|x)$. Then the following holds for random variables $(U,V,X,Y,Z)\sim p^*(u,v|x)t(x)q(y,z|x)$:

- $I(\overline{U};Y)\geq I(\overline{U};VZ)$ for every $\overline{U}\to U\to VXYZ$.
- $I(\overline{V};Z)\geq I(\overline{V};UY)$ for every $\overline{V}\to V\to UXYZ$.

Proof of Statement 1: Assume that the marginal pmf of X given $W=w$ does not belong to $\mathcal{T}$ for some w. By the definition then, at least one of the following must hold:

Case 1: Corresponding to $p^*_{X|W=w}(x)$ is the conditional distribution $p(\widehat{u},\widehat{v},\widehat{w}|\widehat{x})$ such that

$$\begin{aligned}&I(U;Y|W=w)+I(V;Z|W=w)-I(U;V|W=w)<\\ &\lambda I(\widehat{W};\widehat{Y})+(1-\lambda)I(\widehat{W};\widehat{Z})+I(\widehat{U};\widehat{Y}|\widehat{W})\\ &\quad + I(\widehat{V};\widehat{Z}|\widehat{W})-I(\widehat{U};\widehat{V}|\widehat{W})\end{aligned}\tag{8.12}$$

where $p(\widehat{u},\widehat{v},\widehat{w},\widehat{x},\widehat{y},\widehat{z})=p(\widehat{u},\widehat{v},\widehat{w}|\widehat{x})p^*_{X|W=w}(\widehat{x})q(\widehat{y},\widehat{z}|\widehat{x})$.

Case 2: Corresponding to $p^*_{X|W=w}(x)$ is the conditional distribution $p(\widehat{u},\widehat{v},\widehat{w}|\widehat{x})$ such that

$$\begin{aligned}&I(U;Y|W=w)+I(V;Z|W=w)-I(U;V|W=w)=\\ &\lambda I(\widehat{W};\widehat{Y})+(1-\lambda)I(\widehat{W};\widehat{Z})+I(\widehat{U};\widehat{Y}|\widehat{W})\\ &\quad + I(\widehat{V};\widehat{Z}|\widehat{W})-I(\widehat{U};\widehat{V}|\widehat{W})\end{aligned}$$

[3]Note that such a pmf may not unique.

[4]We have used maximum and not supremum in the above conditions since cardinality bounds on the auxiliary random variables exist.

but $I(\widehat{W};\widehat{Y})+I(\widehat{W};\widehat{Z})>0$, where $p(\widehat{u},\widehat{v},\widehat{w},\widehat{x},\widehat{y},\widehat{z})=p(\widehat{u},\widehat{v},\widehat{w}|\widehat{x})p^*_{X|W=w}(\widehat{x})q(\widehat{y},\widehat{z}|\widehat{x})$.

Define $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$ jointly distributed with U, V, W, X, Y, Z as follows: whenever $W\neq w$, the random variables $\widetilde{U}=U$, $\widetilde{V}=V$, $\widetilde{W}=W$. For $W=w$, the Markov chain $\widetilde{U}\widetilde{V}\widetilde{W}\to X\to UVWYZ$ holds, and $p(\widetilde{u},\widetilde{v},\widetilde{w}|x)=p(\widehat{u},\widehat{v},\widehat{w}|\widehat{x})$. Next, assume that $U'=\widetilde{U}$, $V'=\widetilde{V}$, $W'=W\widetilde{W}$.

If case 1 holds, we prove that $\lambda I(W';Y)+(1-\lambda)I(W';Z)+I(U';Y|W')+I(V';Z|W')-I(U';V'|W')>\lambda I(W;Y)+(1-\lambda)I(W;Z)+I(U;Y|W)+I(V;Z|W)-I(U;V|W)$, which results in a contradiction. If case 2 holds, we prove that $\lambda I(W';Y)+(1-\lambda)I(W';Z)+I(U';Y|W')+I(V';Z|W')-I(U';V'|W')=\lambda I(W;Y)+(1-\lambda)I(W;Z)+I(U;Y|W)+I(V;Z|W)-I(U;V|W)$ but that $I(W';Y)+I(W';Z)>I(W;Y)+I(W;Z)$, which results in a contradiction.

Assume that case 1 holds. Since $W'=W\widetilde{W}$, $I(W';Y)=I(W;Y)+I(\widetilde{W};Y|W)$ and $I(W';Z)=I(W;Z)+I(\widetilde{W};Z|W)$, we need to show that

$$\begin{aligned}&\lambda I(\widetilde{W};Y|W)+(1-\lambda)I(\widetilde{W};Z|W)+I(\widetilde{U};Y|W\widetilde{W})+\\&I(\widetilde{V};Z|W\widetilde{W})-I(\widetilde{U};\widetilde{V}|W\widetilde{W})>\\&I(U;Y|W)+I(V;Z|W)-I(U;V|W)\end{aligned}$$

Remember that whenever $W\neq w$, random variables $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$ were defined to be equal to U, V, W. Therefore we need to show that

$$\begin{aligned}&p(W=w)\big[\lambda I(\widetilde{W};Y|W=w)+(1-\lambda)I(\widetilde{W};Z|W=w)+\\&I(\widetilde{U};Y|W=w,\widetilde{W})+I(\widetilde{V};Z|W=w,\widetilde{W})\\&-I(\widetilde{U};\widetilde{V}|W=w,\widetilde{W})\big]>\\&p(W=w)\big[I(U;Y|W=w)+I(V;Z|W=w)\\&-I(U;V|W=w)\big].\end{aligned}$$

On the event $W=w$, random variables $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$ were defined so that $p(\widetilde{u},\widetilde{v},\widetilde{w}|x)$ is equal to $p(\widehat{u},\widehat{v},\widehat{w}|\widehat{x})$. Furthermore the marginal distribution of $p(\widehat{x})$ is $p^*(x|W=w)$. Therefore $I(\widetilde{W};Y|W=w)=I(\widehat{W};\widehat{Y})$, $I(\widetilde{W};Z|W=w)=I(\widehat{W};\widehat{Z})$, $I(\widetilde{U};Y|W=w,\widetilde{W})=I(\widehat{U};\widehat{Y}|\widehat{W})$, etc. Thus it remains to show that

$$\begin{aligned}&\lambda I(\widehat{W};\widehat{Y})+(1-\lambda)I(\widehat{W};\widehat{Z})+I(\widehat{U};\widehat{Y}|\widehat{W})\\&+I(\widehat{V};\widehat{Z}|\widehat{W})-I(\widehat{U};\widehat{V}|\widehat{W})>\\&I(U;Y|W=w)+I(V;Z|W=w)-I(U;V|W=w).\end{aligned}$$

This holds because of equation (8.12). This concludes the proof for case 1.

Now, assume that case 2 holds. Following, the above proof for case 1, one can get

$$\begin{aligned}
&\lambda I(W';Y) + (1-\lambda) I(W';Z) + I(U';Y|W') \\
&+ I(V';Z|W') - I(U';V'|W') \geq \\
&\lambda I(W;Y) + (1-\lambda) I(W;Z) + I(U;Y|W) \\
&+ I(V;Z|W) - I(U;V|W).
\end{aligned}$$

Note that $I(W';Y) + I(W';Z) = I(W;Y) + I(\widetilde{W};Y|W) + I(W;Z) + I(\widetilde{W};Z|W)$. Thus, we need to show that $I(\widetilde{W};Y|W) + I(\widetilde{W};Z|W) > 0$. Note that

$$\begin{aligned}
&I(\widetilde{W};Y|W) + I(\widetilde{W};Z|W) = \\
&p(W=w)\big(I(\widetilde{W};Y|W=w) + I(\widetilde{W};Z|W=w)\big) \\
&= p(W=w)\big(I(\widehat{W};\widehat{Y}) + I(\widehat{W};\widehat{Z})\big) > 0.
\end{aligned}$$

Proof of Statement 2: Take an arbitrary $\overline{U}$ satisfying $\overline{U} \to U \to VXYZ$. Let $\widehat{W} = \overline{U}$, $\widehat{U} = U$, $\widehat{V} = V$. Since $t(x) \in \mathcal{T}(q(y,z|x))$, and $p^*(u,v|x)$ maximizes $I(U;Y) + I(V;Z) - I(U;V)$, we can write:

$$\begin{aligned}
&I(U;Y) + I(V;Z) - I(U;V) \geq \\
&\lambda I(\widehat{W};Y) + (1-\lambda) I(\widehat{W};Z) + I(\widehat{U};Y|\widehat{W}) + I(\widehat{V};Z|\widehat{W}) \\
&\quad - I(\widehat{U};\widehat{V}|\widehat{W}),
\end{aligned} \tag{8.13}$$

and furthermore if equality holds, we must have $I(\widehat{W};Y) = I(\widehat{W};Z) = 0$. We prove that this implies that $I(\overline{U};Y) \geq I(\overline{U};VZ)$.

We can write:

$$\begin{aligned}
&I(U;Y) + I(V;Z) - I(U;V) \geq \\
&\lambda I(\widehat{W};Y) + (1-\lambda) I(\widehat{W};Z) + I(\widehat{U};Y|\widehat{W}) + I(\widehat{V};Z|\widehat{W}) \\
&- I(\widehat{U};\widehat{V}|\widehat{W}) = \\
&\lambda I(\overline{U};Y) + (1-\lambda) I(\overline{U};Z) + I(U;Y|\overline{U}) \\
&+ I(V;Z|\overline{U}) - I(U;V|\overline{U}).
\end{aligned}$$

Therefore

$$\begin{aligned}
&I(U;Y) + I(V;Z) - I(U;V) \geq \\
&\lambda I(\overline{U};Y) + (1-\lambda) I(\overline{U};Z) + I(U;Y|\overline{U}) + I(V;Z|\overline{U}) \\
&- I(U;V|\overline{U})
\end{aligned}$$

Since $\overline{U} \to U \to VXYZ$, we have $I(U;Y) = I(\overline{U}U;Y)$ and $I(U;V) = I(\overline{U}U;V)$. This implies that

$$I(\overline{U};Y) + I(V;Z) - I(\overline{U};V) \geq$$
$$\lambda I(\overline{U};Y) + (1-\lambda)I(\overline{U};Z) + I(V;Z|\overline{U})$$

or,

$$I(\overline{U};Y) + I(V;Z) \geq \lambda I(\overline{U};Y) + (1-\lambda)I(\overline{U};Z) + I(V;Z\overline{U})$$

or,

$$(1-\lambda)I(\overline{U};Y) \geq (1-\lambda)I(\overline{U};Z) + I(V;\overline{U}|Z).$$

In other words

$$(1-\lambda)I(\overline{U};Y) \geq (1-\lambda)I(\overline{U};VZ) + \lambda I(V;\overline{U}|Z). \tag{8.14}$$

Let us consider the following two cases:

- $\lambda < 1$: In this case, equation (8.14) implies that $I(\overline{U};Y) \geq I(\overline{U};VZ) + \frac{\lambda}{1-\lambda}I(V;\overline{U}|Z)$. This inequality implies the desired inequality $I(\overline{U};Y) \geq I(\overline{U};VZ)$.
- $\lambda = 1$: In this case, equation (8.14) implies that $I(V;\overline{U}|Z) = 0$. Furthermore equation (8.13) will hold with equality. Since $t(x) \in \mathcal{T}$, we must have $I(\overline{U};Y) = I(\overline{U};Z) = 0$.
  The fact that $I(V;\overline{U}|Z) = I(\overline{U};Y) = I(\overline{U};Z) = 0$ implies that $I(\overline{U};Y) = I(\overline{U};ZV) = 0$. Therefore the inequality $I(\overline{U};Y) \geq I(\overline{U};ZV)$ also holds in this case.

In each case, we are done. The proof for the inequality $I(\overline{V};Z) \geq I(\overline{V};YU)$ is similar.

8.4 Insufficiency of Marton's coding scheme without a superposition variable

8.4.1 Statement of the result

In this section we then consider Marton's inner bound and show that, unlike in the Gaussian broadcast channel case, "Marton's coding scheme" alone is not sufficient to achieve the capacity region of the general degraded broadcast channel. Necessity of the "superposition-coding" aspect of the inner bound had previously been observed for a non-degraded broadcast channel [28].

In Marton's inner bound the auxiliary random variable W corresponds to the "superposition-coding" aspect of the bound, and the random variables U and V correspond to the "Marton-coding" aspect of the bound. When $R_0 = 0$ (private messages only) and $W = \emptyset$, Marton's inner bound reduces to the the set of non-negative rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(U;Y|Q), \tag{8.15}$$
$$R_2 \leq I(V;Z|Q), \tag{8.16}$$
$$R_1 + R_2 \leq I(U;Y|Q) + I(V;Z|Q) - I(U;V|Q) \tag{8.17}$$

for some random variables $(Q, U, V, X, Y, Z) \sim p(q)p(u, v, x|q)q(y, z|x)$.

It is known that this inner bound is tight for Gaussian broadcast channels (through dirty paper coding), implying that W is unnecessary for achieving the capacity region of this class of degraded broadcast channels. We show through an example that this is not the case in general.

Lemma 7. There are degraded broadcast channels for which Marton's private message inner bound without W is strictly contained in the capacity region of the channel.

8.4.2 Proof

Proof of Lemma 7: Consider the degraded broadcast channel $p(y, z|x) = p(y|x)p(z|y)$, where the channel from X to Y is a BSC(0.3) and the channel from Y to Z is as follows: $p_{Z|Y}(0|0) = 0.6$, $p_{Z|Y}(1|0) = 0.4$, $p_{Z|Y}(0|1) = 0$, $p_{Z|Y}(1|1) = 1$. We show that the private message capacity region for this channel is strictly larger than Marton's inner bound without W.

We first intuitively sketch outline of the proof: take a non-negative real α and consider the maximum of $R_1 + \alpha R_2$ over the pairs (R_1, R_2) in the capacity region. Since the broadcast channel is degraded, the maximum is equal to $\max_{V \to X \to YZ} I(X;Y|V) + \alpha I(V;Z)$. Since $X \to Y \to Z$, when the weight of the degraded receiver is less than or equal to 1, an optimum V will be equal to a constant (corresponding to $R_2 = 0$). As we gradually increase α beyond one, the optimum V *gradually* moves from a constant random variable to X (corresponding to $R_1 = 0$). Now, let us consider the maximum of $R_1 + \alpha R_2$ over the pairs (R_1, R_2) in Marton's inner bound without the auxiliary random variable W. The latter maximum is equal to $I(U;Y) + \alpha I(V;Z) - I(U;V)$. When $\alpha \leq 1$, it is optimum to take $U = X$, V =constant and dedicate all the rate to the stronger receiver. The simulation results however indicate that as we increase α beyond one in the problem of maximizing $I(U;Y) + \alpha I(V;Z) - I(U;V)$, $U = X$, V =constant continues to be optimal up to a threshold. Beyond this threshold, *suddenly* U =constant, $V = X$ becomes the optimizing choice, and stays as the optimizing choice afterwards. In other words, unlike the gradual transition of the maximizing V for the actual region, there is a *sharp transition* in the maximizing V for Marton's inner bound without W.

In the following, we provide a formal proof: the maximum of $R_1+2.4R_2$ over pairs (R_1, R_2) in the capacity region, is equal to $\max_{V\to X\to YZ} I(X;Y|V)+2.4I(V;Z)$. Take the joint pmf of $p(v,x)$ to be as follows: $P(V=0,X=0)=0$, $P(V=0,X=1)=0.41$, $P(V=1,X=0)=0.48$, $P(V=1,X=1)=0.11$. For this choice of $p(v,x)$, $I(X;Y|V)+2.4I(V;Z)=0.1229....$ Therefore the maximum of $R_1+2.4R_2 \geq 0.1229....$ The maximum of $R_1+2.4R_2$ over Marton's inner bound without W is equal to $\sup_{UV\to X\to YZ} I(U;V)+2.4I(V;Z)-I(U;V)$. Using the perturbation method, one can show that the supremum is indeed a minimum, and that the cardinality of U and V can be bounded from above by $|\mathcal{X}|$. Furthermore X can be assumed to be a deterministic function of (U,V). Since X is a binary random variable, we need to search over binary random variables U, V. Numerical simulations show that the maximum is equal to $0.1215... < 0.1229...$ and occurs when $X=V$ and $U=$ *constant*. Therefore Marton's inner bound without W is not tight for this broadcast channel. ■

8.5 Computation of the Nair-El Gamal outer bound

8.5.1 Statement of the result

In this section, we find bounds on the cardinalities of the auxiliary random variables appearing in the Nair-El Gamal outer bound, thus making it fully computable and generalizing an earlier result by Nair and Zizhou [45] for the case of $R_0=0$.

Theorem 13. For a general broadcast channel $q(y,z|x)$, the Nair-El Gamal outer bound $\mathcal{R}_{NE}$ is the set of non-negative rate triples (R_0,R_1,R_2) satisfying

$$R_0 \leq \min\{I(W;Y), I(W;Z)\}, \tag{8.18}$$
$$R_0+R_1 \leq I(UW;Y), \tag{8.19}$$
$$R_0+R_2 \leq I(VW;Z), \tag{8.20}$$
$$R_0+R_1+R_2 \leq \min\{I(UW;Y)+I(X;Z|UW), \; I(VW;Z)+I(X;Y|VW)\}, \tag{8.21}$$

for some random variables $(U,V,W,X,Y,Z) \sim p(w,x)p(u|w,x)p(v|w,x)q(y,z|x)$ with $|\mathcal{U}| \leq |\mathcal{X}|$, $|\mathcal{V}| \leq |\mathcal{X}|$, $|\mathcal{W}| \leq |\mathcal{X}|+6$.

Note that the above result makes the Nair-El Gamal outer bound fully computable.

8.5.2 Proof

Proof of Theorem 13: Let $\mathcal{R}_1$ denote the region given in the statement of Theorem 13. We would like to show that $\mathcal{R}_1 = \mathcal{R}_{NE}$. Our proof resembles and generalizes

the one provided by Nair and Zizhou [45] for the case of $R_0 = 0$. We first show that $\mathcal{R}_{NE} = \mathcal{R}_2$, where $\mathcal{R}_2$ consists of the set of non-negative rate triples (R_0, R_1, R_2) satisfying

$$\begin{aligned} R_0 &\leq \min\{I(W;Y), I(W;Z)\}, \\ R_0 + R_1 &\leq I(UW;Y), \\ R_0 + R_2 &\leq I(VW;Z), \\ R_0 + R_1 + R_2 &\leq \min\{I(UW;Y) + I(X;Z|UW), \\ &\qquad I(VW;Z) + I(X;Y|VW)\}, \end{aligned}$$

for some random variables $U, V, W, X, Y, Z \sim p(u,v,w,x)q(y,z|x)$.

Clearly $\mathcal{R}_{NE} \subset \mathcal{R}_2$, since in $\mathcal{R}_2$ we take the union over all $p(u,v,w,x)$, and $I(X;Z|UW) \geq I(V;Z|UW)$, $I(X;Y|VW) \geq I(U;Y|VW)$. In order to show that $\mathcal{R}_2 \subset \mathcal{R}_{NE}$, take some arbitrary $p(u,v,w,x)$. Without loss of generality assume that $\mathcal{U} = \{0,1,2,...,|\mathcal{U}|-1\}$, $\mathcal{V} = \{0,1,2,...,|\mathcal{V}|-1\}$ and $\mathcal{X} = \{0,1,2,...,|\mathcal{X}|-1\}$.

Let $\widetilde{U}$, $\widetilde{V}$, $\widetilde{X}_1$, $\widetilde{X}_2$, $\widetilde{X}_3$, $\widetilde{X}_4$ be *uniform* random variables on sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$, $\mathcal{X}$, $\mathcal{X}$, $\mathcal{X}$ respectively. We assume that $\widetilde{U}$, $\widetilde{V}$, $\widetilde{X}_1$, $\widetilde{X}_2$, $\widetilde{X}_3$ and $\widetilde{X}_4$ are *mutually independent* of each other and of U, V, W, X, Y, Z. Let us define random variables $\widehat{U}$, $\widehat{V}$, $\widehat{W}$ and $\widehat{X}$, $\widehat{Y}$ and $\widehat{Z}$ as follows:

- $\widehat{U} = (\widetilde{U} \oplus U, X \oplus \widetilde{X}_1 \oplus \widetilde{X}_4, \widetilde{X}_3)$;
- $\widehat{V} = (\widetilde{V} \oplus V, X \oplus \widetilde{X}_2 \oplus \widetilde{X}_3, \widetilde{X}_4)$;
- $\widehat{W} = (W, \widetilde{U}, \widetilde{V}, \widetilde{X}_1, \widetilde{X}_2)$;
- $\widehat{X} = X$;
- $\widehat{Y} = Y$;
- $\widehat{Z} = Z$.

It can be verified that $\widehat{U}$ is independent of $\widehat{V}$. Furthermore

- $I(W;Y) \leq I(\widehat{W};\widehat{Y})$;
- $I(W;Z) \leq I(\widehat{W};\widehat{Z})$;
- $I(UW;Y) \leq I(\widehat{U}\widehat{W};\widehat{Y})$;
- $I(VW;Z) \leq I(\widehat{V}\widehat{W};\widehat{Z})$;
- $I(UW;Y) + I(X;Z|UW) \leq I(\widehat{U}\widehat{W};\widehat{Y}) + I(\widehat{V};\widehat{Z}|\widehat{U}\widehat{W})$;
- $I(VW;Z) + I(X;Y|VW) \leq I(\widehat{V}\widehat{W};\widehat{Z}) + I(\widehat{U};\widehat{Y}|\widehat{V}\widehat{W})$.

Therefore $\mathcal{R}_2 \subset \mathcal{R}_{NE}$, and $\mathcal{R}_2 = \mathcal{R}_{NE}$. It remains to show that $\mathcal{R}_2 = \mathcal{R}_1$.

In evaluating $\mathcal{R}_2$, it does not matter if we take the union over all $p(u,v,w,x)$ or over those of the form $p(u,v,w,x) = p(w,x)p(u|w,x)p(v|w,x)$, since the expression depends only on the marginals of $p(u,w,x)$ and $p(v,w,x)$, so let us assume this is done. The last step is to establish cardinality bounds of $|\mathcal{U}| \leq |\mathcal{X}|$, $|\mathcal{V}| \leq |\mathcal{X}|$, $|\mathcal{W}| \leq |\mathcal{X}| + 6$ on the auxiliary random variables in $\mathcal{R}_2$. This would imply that $\mathcal{R}_2 = \mathcal{R}_1$.

Let us consider a six dimensional region $\mathcal{C}_{NE-I}(q(y,z|x))$ defined as the union of

$$\begin{aligned}&\Delta\big(\big\{\big(I(W;Y), I(W;Z), I(UW;Y), I(VW;Z),\\ &I(UW;Y) + I(X;Z|UW),\\ &I(VW;Z) + I(X;Y|VW)\big)\big\}\big),\end{aligned}$$

over $p(w,x)p(u|w,x)p(v|w,x)$. Here the down-set operator $\Delta(A)$ for a set $A \subset \mathbb{R}^d$ is defined as follows: $\Delta(A) = \{\overrightarrow{v} \in \mathbb{R}^d : \overrightarrow{v}$ is coordinatewise less than or equal to $\overrightarrow{w}$ for some $\overrightarrow{w} \in A\}$. Note that the region $\mathcal{C}_{NE-I}(q(y,z|x))$ specifies $\mathcal{C}_{NE}(q(y,z|x))$, since given any $p(u,v,w,x,y,z) = p(w,x)p(u|w,x)p(v|w,x)q(y,z|x)$ the corresponding vector in $\mathcal{C}_{NE-I}(q(y,z|x))$ is providing the values for the right hand side of the 6 inequalities that define the region $\mathcal{C}_{NE}(q(y,z|x))$. Therefore, it suffices to prove the cardinality bound for determining $\mathcal{C}_{NE-I}(q(y,z|x))$.

We begin by proving cardinality bounds for a weighted combination of the terms: given non-negative λ_1, λ_2, ..., λ_6, and any joint distribution $p(u,v,w,x,y,z) = p(u,v,w,x)q(y,z|x)$ on U,V,W,X,Y,Z, 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:

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

In the appendix in section 8.5.3, we verify that this is possible with a cardinality bound of $|\mathcal{X}|$ on $|\widetilde{\mathcal{U}}|$ and $|\widetilde{\mathcal{V}}|$. The cardinality of W can be reduced by fixing the conditional distribution of $p(u,v,x,y,z|w)$ and trying to change the marginal distribution of $p(w)$ so that non-zero probabilities are assigned to at most $|\mathcal{X}|$ elements of $\mathcal{W}$. Note that the above expression can be written as $\lambda_1 H(Y) + \lambda_2 H(Z) + \lambda_3 H(Y) + \lambda_4 H(Z) + \lambda_5 H(Y) + \lambda_6 H(Z)$ plus a second term that is linear in $p(w)$. In order to preserve

the first term, we preserve the marginal distribution of Y and Z by preserving the marginal distribution of X by imposing $|\mathcal{X}|-1$ linear equations on $p(w)$. There is one linear constraint $\sum_w p(w)=1$, and the inequalities $p(w)\geq 0$ for $w\in\mathcal{W}$. If we want to use the traditional Carathéodory theorem, we need to impose one more linear constraint for preserving the second linear term. The number of linear constraints will be $|\mathcal{X}|+1$. The strengthened Carathéodory theorem of Fenchel however reduces this to $|\mathcal{X}|$.

Having established cardinality bounds for a weighted combination of the terms, it remains to show that if the alphabet of W is of size greater than or equal to $|\mathcal{X}|+6$, then this guarantees the convexity of the region. We would like to show that the region defined as the union of

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

over random variables U,V,W,X,Y,Z, having the joint distribution $p(u,v,w,x,y,z)=p(u,v,w,x)q(y,z|x)$, $|\mathcal{U}|\leq|\mathcal{X}|$, $|\mathcal{V}|\leq|\mathcal{X}|$, and $|\mathcal{W}|\leq|\mathcal{X}|+6$ is convex. Note that if the constraint $|\mathcal{W}|\leq|\mathcal{X}|+6$ is relaxed, the region becomes convex by a time-sharing argument. One can then use the strengthened Carathéodory argument to reduce the cardinality of W to $|\mathcal{X}|+6$ as we would like to preserve the marginal distribution of X and the linear terms $H(Y|W)$, $H(Z|W)$, $H(Y|UW)$, $H(Z|VW)$, $I(X;Z|UW)$, $I(X;Y|VW)$.

■

8.5.3 Appendix

Claim: We claim that it suffices to find $\widetilde{W}$, $\widetilde{X}$, $\widetilde{Y}$ 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:

- $\lambda_1\cdot I(W;Y)+\lambda_2\cdot I(W;Z)+\lambda_3\cdot I(UW;Y)+\lambda_4\cdot I(VW;Z)+\lambda_5\cdot(I(UW;Y)+I(X;Z|UW))+\lambda_6\cdot(I(VW;Z)+I(X;Y|VW))$ is less than or equal to $\lambda_1\cdot I(\widetilde{W};\widetilde{Y})+\lambda_2\cdot I(\widetilde{W};\widetilde{Z})+\lambda_3\cdot I(\widetilde{U}\widetilde{W};\widetilde{Y})+\lambda_4\cdot I(\widetilde{V}\widetilde{W};\widetilde{Z})+\lambda_5\cdot(I(\widetilde{U}\widetilde{W};\widetilde{Y})+I(\widetilde{X};\widetilde{Z}|\widetilde{U}\widetilde{W}))+\lambda_6\cdot(I(\widetilde{V}\widetilde{W};\widetilde{Z})+I(\widetilde{X};\widetilde{Y}|\widetilde{V}\widetilde{W}))$,
- For any $\widetilde{w}$ where $p(\widetilde{w})>0$, $p(\widetilde{u}|\widetilde{w})\neq 0$ for at most $|\mathcal{X}|$ values of $\widetilde{u}$,
- For any $\widetilde{w}$ where $p(\widetilde{w})>0$, $p(\widetilde{v}|\widetilde{w})\neq 0$ for at most $|\mathcal{X}|$ values of $\widetilde{v}$,
- $|\widetilde{\mathcal{W}}|=|\mathcal{W}|$.

Proof of the claim: Given $\widetilde{w}\in\widetilde{\mathcal{W}}$, let $\mathcal{A}_{\widetilde{w}}$ be a subset of $\widetilde{\mathcal{U}}$ 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 $\mathcal{A}_{\widetilde{w}}=\{a_{\widetilde{w},1},a_{\widetilde{w},2},a_{\widetilde{w},3},...,a_{\widetilde{w},|\mathcal{X}|}\}$.

Similarly, let $\mathcal{B}_{\widetilde{w}}$ be a subset of $\widetilde{\mathcal{V}}$ satisfying $|\mathcal{B}_{\widetilde{w}}| = |\mathcal{X}|$, and $p(\widetilde{V} = \widetilde{v}|\widetilde{W} = \widetilde{w}) = 0$ if $\widetilde{v} \notin \mathcal{B}_{\widetilde{w}}$. Assume that $\mathcal{B}_{\widetilde{w}} = \{b_{\widetilde{w},1}, b_{\widetilde{w},2}, b_{\widetilde{w},3}, ..., b_{\widetilde{w},|\mathcal{X}|}\}$.

Define $\widetilde{U}'$ and $\widetilde{V}'$, two random variables taking values from the set $\{1, 2, 3, ..., |\mathcal{X}|\}$, and jointly distributed with $\widetilde{W}, \widetilde{X}, \widetilde{Y}$ and $\widetilde{Z}$ as follows: for any $\widetilde{w}, \widetilde{x}, \widetilde{y}$ and $\widetilde{z}$ where $p(\widetilde{W} = \widetilde{w}, \widetilde{X} = \widetilde{x}, \widetilde{Y} = \widetilde{y}, \widetilde{Z} = \widetilde{z}) > 0$, let $p(\widetilde{U}' = i, \widetilde{V}' = j|\widetilde{W} = \widetilde{w}, \widetilde{X} = \widetilde{x}, \widetilde{Y} = \widetilde{y}, \widetilde{Z} = \widetilde{z}) = p(\widetilde{U} = a_{\widetilde{w},i}|\widetilde{W} = \widetilde{w}, \widetilde{X} = \widetilde{x})p(\widetilde{V} = b_{\widetilde{w},j}|\widetilde{W} = \widetilde{w}, \widetilde{X} = \widetilde{x})$. Both $\tilde{U}'$ and $\tilde{V}'$ have alphabet of size $|\mathcal{X}|$ and furthermore $I(\widetilde{U}'; \widetilde{Y}|\widetilde{W}) = I(\widetilde{U}; \widetilde{Y}|\widetilde{W})$, $I(\widetilde{X}; \widetilde{Z}|\widetilde{U}'\widetilde{W}) = I(\widetilde{X}; \widetilde{Z}|\widetilde{U}\widetilde{W})$, $I(\widetilde{V}'; \widetilde{Z}|\widetilde{W}) = I(\widetilde{V}; \widetilde{Z}|\widetilde{W})$ and $I(\widetilde{X}; \widetilde{Y}|\widetilde{V}'\widetilde{W}) = I(\widetilde{X}; \widetilde{Y}|\widetilde{V}\widetilde{W})$. Random variables $\widetilde{U}'$, $\widetilde{V}'$, $\widetilde{W}, \widetilde{X}, \widetilde{Y}$ and $\widetilde{Z}$ have the desired properties. ■

Thus, it suffices to find $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$, $\widetilde{X}$, $\widetilde{Y}$ satisfying the properties mentioned above. We assume that random variables $\widetilde{U}$, $\widetilde{V}$, $\widetilde{W}$, $\widetilde{X}$, $\widetilde{Y}$ and $\widetilde{Z}$ are respectively defined on the alphabets 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 $I(W; Z) = I(\widetilde{W}; \widetilde{Z})$. It suffices to define $p(\widetilde{u}, \widetilde{v}|\widetilde{w}, \widetilde{x}) = p(\widetilde{u}|\widetilde{w}, \widetilde{x})p(\widetilde{v}|\widetilde{w}, \widetilde{x})$ satisfying the following properties:

- For any $w \in \mathcal{W}$, $\lambda_3 \cdot I(U; Y|W = w) + \lambda_5 \cdot (I(U; Y|W = w) + I(X; Z|UW = w))$ is less than or equal to $\lambda_3 \cdot I(\widetilde{U}; \widetilde{Y}|\widetilde{W} = w) + \lambda_5 \cdot (I(\widetilde{U}; \widetilde{Y}|\widetilde{W} = w) + I(\widetilde{X}; \widetilde{Z}|\widetilde{U}\widetilde{W} = w))$.

- For any $w \in \mathcal{W}$, $\lambda_4 \cdot I(V; Z|W = w) + \lambda_6 \cdot (I(V; Z|W = w) + I(X; Y|VW = w))$ is less than or equal to $\lambda_4 \cdot I(\widetilde{V}; \widetilde{Z}|\widetilde{W} = w) + \lambda_6 \cdot (I(\widetilde{V}; \widetilde{Z}|\widetilde{W} = w) + I(\widetilde{X}; \widetilde{Y}|\widetilde{V}\widetilde{W} = w))$.

- For any w, $p(\widetilde{U} = u|\widetilde{W} = w) \neq 0$ for at most $|\mathcal{X}|$ values of u.

- For any w, $p(\widetilde{V} = v|\widetilde{W} = w) \neq 0$ for at most $|\mathcal{X}|$ values of v.

Note that the conditions involving U and V are disjoint, because we can choose $p(\widetilde{u}, \widetilde{v}|\widetilde{w}, \widetilde{x}) = p(\widetilde{u}|\widetilde{w}, \widetilde{x})p(\widetilde{v}|\widetilde{w}, \widetilde{x})$.

Such choices of $p(\widetilde{u}|\widetilde{w}, \widetilde{x})$ and $p(\widetilde{v}|\widetilde{w}, \widetilde{x})$ exist because of the following lemma that can be proved using the strengthened Carathéodory theorem of Fenchel:

Lemma. Given any non-negative numbers α and β, a broadcast channel $q(y, z|x)$ and a fixed marginal distribution $p(x)$, consider the problem of finding the maximum of $\alpha I(U; Y) + \beta\big(I(U; Y) + I(X; Z|U)\big)$ over all $p(u|x)$ where $U, X, Y, Z \sim p(u|x)p(x)q(y, z|x)$. The cardinality of U for this problem can be reduced to $|\mathcal{X}|$. Note that $\alpha I(U; Y) + \beta\big(I(U; Y) + I(X; Z|U)\big)$ is equal to $(\alpha + \beta)H(Y)$ plus $-(\alpha + \beta)H(Y|U) + \beta I(X; Z|U)$. Since $p(x)$ is fixed, we are interested in the maximum of $-(\alpha + \beta)H(Y|U) + \beta I(X; Z|U)$ over all $p(u|x)$. A typical application of the strengthened Carathéodory theorem of Fenchel reduces the cardinality of U to $|\mathcal{X}|$.

8.6 Computation of the capacity along certain directions

8.6.1 Statement of the result

In this section we compute the capacity region along certain directions.

Lemma 8. For a broadcast channel $q(y,z|x)$ and real numbers λ_0, λ_1 and λ_2 such that $\lambda_0 \geq \lambda_1 + \lambda_2$,

$$\begin{aligned}&\max_{(R_0,R_1,R_2)\in\mathcal{C}(q(y,z|x))}(\lambda_0 R_0+\lambda_1 R_1+\lambda_2 R_2) = \\ &\max\{\max_{(R_0,R_2)\in\mathcal{C}_{d_1}(q(y,z|x))}(\lambda_0 R_0+\lambda_2 R_2), \\ &\max_{(R_0,R_1)\in\mathcal{C}_{d_2}(q(y,z|x))}(\lambda_0 R_0+\lambda_1 R_1)\},\end{aligned}$$

where $\mathcal{C}_{d_1}(q(y,z|x))$ and $\mathcal{C}_{d_2}(q(y,z|x))$ are the degraded message set capacity regions for the given channel.

Corollary 3. The above observation essentially says that if $\lambda_0 \geq \lambda_1 + \lambda_2$, then *a* maximum of $\lambda_0 R_0 + \lambda_1 R_1 + \lambda_2 R_2$ over triples (R_0, R_1, R_2) in the capacity region occurs when either $R_1 = 0$ or $R_2 = 0$.

Remark 4. Since $\mathcal{C}_{d_1}(q(y,z|x)) \cup \mathcal{C}_{d_1}(q(y,z|x)) \subset \mathcal{C}_M(q(y,z|x)) \subset \mathcal{C}(q(y,z|x))$, the above lemma implies that Marton's inner bound is tight along the direction of such $(\lambda_0, \lambda_1, \lambda_2)$, i.e.

$$\begin{aligned}&\max_{(R_0,R_1,R_2)\in\mathcal{C}(q(y,z|x))}(\lambda_0 R_0+\lambda_1 R_1+\lambda_2 R_2) = \\ &\qquad\max_{(R_0,R_1,R_2)\in\mathcal{C}_M(q(y,z|x))}(\lambda_0 R_0+\lambda_1 R_1+\lambda_2 R_2), \\ &\text{whenever } \lambda_0 \geq \lambda_1 + \lambda_2.\end{aligned}$$

Based on numerical simulations for certain broadcast channels, we conjecture that the Nair-El Gamal outer bound is also tight along the direction of any such $(\lambda_0, \lambda_1, \lambda_2)$. However if this conjecture turns out to be false, it would imply that the Nair-El Gamal outer bound is not tight.

8.6.2 Proof

Proof of Lemma 8: It suffices to show that

$$\begin{aligned}&\max_{(R_0,R_1,R_2)\in\mathcal{C}(q(y,z|x))}(\lambda_0 R_0+\lambda_1 R_1+\lambda_2 R_2) \leq \\ &\max\{\max_{(R_0,R_2)\in\mathcal{C}_{d_1}(q(y,z|x))}(\lambda_0 R_0+\lambda_2 R_2), \\ &\max_{(R_0,R_1)\in\mathcal{C}_{d_2}(q(y,z|x))}(\lambda_0 R_0+\lambda_1 R_1)\}.\end{aligned}$$

The key step is to show that if (R_0, R_1, R_2) is in the capacity region of a broadcast channel, then $(R_0 + \min\{R_1, R_2\}, R_1 - \min\{R_1, R_2\}, R_2 - \min\{R_1, R_2\})$ is also in the capacity region. Since $\lambda_0 \geq \lambda_1 + \lambda_2$, we then have that $\lambda_0(R_0 + \min\{R_1, R_2\}) + \lambda_1(R_1 - \min\{R_1, R_2\}) + \lambda_2(R_2 - \min\{R_1, R_2\}) \geq \lambda_0 R_0 + \lambda_1 R_1 + \lambda_2 R_2$, so at the maximum we must have $\min(R_1, R_2) = 0$. One can prove this property using the result of Willems [55], which shows that the *maximal* probability of error capacity region is equal to the *average* probability of error capacity region. Willems' proof, however, is rather involved. Instead, we provide a simple direct proof. Consider an arbitrary code $(M_0, M_1, M_2, X^n, \epsilon)$. We show that

$$\begin{aligned}
&\frac{\lambda_0}{n} H(M_0) + \frac{\lambda_1}{n} H(M_1) + \frac{\lambda_2}{n} H(M_2) - O(\epsilon) \leq \\
&\max\Big(\max_{(R_0,R_2) \in \mathcal{C}_{d_1}(q(y,z|x))} \lambda_0 R_0 + \lambda_2 R_2, \\
&\qquad \max_{(R_0,R_1) \in \mathcal{C}_{d_2}(q(y,z|x))} \lambda_0 R_0 + \lambda_1 R_1 \Big),
\end{aligned}$$

where $O(\epsilon)$ denotes a constant (depending only on $|\mathcal{X}|$, $|\mathcal{Y}|$, $|\mathcal{Z}|$) times ϵ.

Assume without loss of generality that $H(M_2) \leq H(M_1)$, i.e. $R_2 \leq R_1$. Let $\widehat{W} = M_0 M_2$, $\widehat{X} = X^n$, $\widehat{Y} = Y^n$, $\widehat{Z} = Z^n$. Note that $q(\widehat{y}, \widehat{z}|\widehat{x})$ is the n-fold version of $q(y, z|x)$. Let us look at $\mathcal{C}_{d_1}(q(\widehat{y}, \widehat{z}|\widehat{x}))$, evaluated at the joint pmf $p(\widehat{w}, \widehat{x})$:

$$\begin{aligned}
\widehat{R_0} &\leq I(\widehat{W}; \widehat{Z}), \\
\widehat{R_1} &\leq I(\widehat{X}; \widehat{Y}|\widehat{W}), \\
\widehat{R_0} + \widehat{R_1} &\leq I(\widehat{X}; \widehat{Y}).
\end{aligned}$$

Note that, by Fano's inequality,

$$\begin{aligned}
I(\widehat{W}; \widehat{Z}) &= I(M_0 M_2; Z^n) = H(M_0) + H(M_2) - O(n\epsilon), \\
I(\widehat{X}; \widehat{Y}|\widehat{W}) &= I(X^n; Y^n | M_0 M_2) = H(M_1) - O(n\epsilon), \\
I(\widehat{X}; \widehat{Y}) &= I(X^n; Y^n) = H(M_0) + H(M_1) - O(n\epsilon).
\end{aligned}$$

Therefore $\widehat{R_0} = H(M_0) + H(M_2) - O(n\epsilon) = n(R_0 + R_2) - O(n\epsilon)$ and $\widehat{R_1} = H(M_1) - H(M_2) = n(R_1 - R_2) - O(n\epsilon)$ is in $\mathcal{C}_{d_1}(q(\widehat{y}, \widehat{z}|\widehat{x}))$. Since $q(\widehat{y}, \widehat{z}|\widehat{x})$ is the n-fold version of $q(y, z|x)$ and $\mathcal{C}_{d_1}(q(\widehat{y}, \widehat{z}|\widehat{x}))$ is the degraded message set capacity region for $q(\widehat{y}, \widehat{z}|\widehat{x})$, we must have: $\mathcal{C}_{d_1}(q(\widehat{y}, \widehat{z}|\widehat{x})) = n \cdot \mathcal{C}_{d_1}(q(y, z|x))$, where the multiplication here is pointwise. Thus, $(\frac{\widehat{R_0}}{n}, \frac{\widehat{R_1}}{n}) \in \mathcal{C}_{d_1}(q(y, z|x))$. We can complete the proof by letting $\epsilon \to 0$, and conclude that $(R_0 + R_2, R_1 - R_2, 0) \in \mathcal{C}_{d_1}(q(y, z|x))$, and thus also in the capacity region.

■

8.7 An achievable region

8.7.1 Statement of the result

In this section we discuss an idea that may lead to a larger inner bound. Since capacity is defined in the limit of large block length, it is natural to expect that it has an invariant structure with respect to shifts in time. This suggests that it should be expressed via a formula that has a fixed-point character, namely it should involve joint distributions that are invariant under a time shift. The following theorem is a proposed inner bound along these lines.

Theorem 14. For a broadcast channel $q(y,z|x)$, consider two i.i.d. copies (U_1,V_1,W_1) and (U_2,V_2,W_2) and a conditional pmf $r(x|u_1,v_1,w_1,u_2,v_2,w_2)$. Assume that

$$U_1,V_1,W_1,U_2,V_2,W_2,X_1,X_2,Y_1,Y_2,Z_1,Z_2$$

are distributed according to

$$\begin{aligned}
&p(u_1,v_1,w_1,u_2,v_2,w_2,x_1,y_1,z_1,x_2,y_2,z_2) = \\
&r(u_1,v_1,w_1)r(u_2,v_2,w_2)\cdot \\
&r(x_2|u_1,v_1,w_1,u_2,v_2,w_2)q(y_2,z_2|x_2)\cdot \\
&\tilde{r}(x_1|u_1,v_1,w_1)q(y_1,z_1|x_1),
\end{aligned}$$

where $\tilde{r}(x|u,v,w)$ is defined as

$$\sum_{u'\in\mathcal{U},v'\in\mathcal{V},w'\in\mathcal{W}} r(x|u',v',w',u,v,w)r(u',v',w').$$

Then a rate triple (R_0,R_1,R_2) is achievable if

$$\begin{aligned}
R_0,R_1,R_2 &\geq 0,\\
R_0+R_1 &< I(U_2W_2;Y_1Y_2U_1W_1),\\
R_0+R_2 &< I(V_2W_2;Z_1Z_2V_1W_1),\\
R_0+R_1+R_2 &< I(V_2;Z_1Z_2V_1W_1|W_2)\\
&\quad + I(U_2W_2;Y_1Y_2U_1W_1) - I(U_2;V_2|W_2),\\
R_0+R_1+R_2 &< I(U_2;Y_1Y_2U_1W_1|W_2)\\
&\quad + I(V_2W_2;Z_1Z_2V_1W_1) - I(U_2;V_2|W_2),\\
2R_0+R_1+R_2 &< I(U_2W_2;Y_1Y_2U_1W_1)\\
&\quad + I(V_2W_2;Z_1Z_2V_1W_1) - I(U_2;V_2|W_2),
\end{aligned}$$

for some $U_1,V_1,W_1,U_2,V_2,W_2,X_1,X_2$ that satisfy the above conditions.

Remark 5. The above inner bound reduces to Marton's inner bound if the conditional distribution $r(x|u_1,v_1,w_1,u_2,v_2,w_2) = r(x|u_2,v_2,w_2)$, i.e. $U_1V_1W_1 \to U_2V_2W_2 \to X$ form a Markov chain.

8.7.2 Proof

Proof of Theorem 14: Consider a natural number n, and define the super symbols $\tilde{X} = X_1X_2...X_n$, $\tilde{Y} = Y_1Y_2...Y_n$, $\tilde{Z} = Z_1Z_2...Z_n$ representing n-inputs and n-outputs of the product broadcast channel

$$q^n(y_1y_2...y_n, z_1z_2...z_n|x_1x_2...x_n) = \prod_{i=1}^{n} q(y_i, z_i|x_i).$$

Since the capacity region of the product channel $q^n(\tilde{y}, \tilde{z}|\tilde{x})$ is n times the capacity region of $q(y, z|x)$, we have $\frac{1}{n}\mathcal{C}_M(q^n(y_1y_2...y_n, z_1z_2...z_n|x_1x_2...x_n)) \subset \mathcal{C}(q(y, z|x))$. Given an *arbitrary* joint pmf $p(u^n, v^n, w^n, x^n)$, one can then show that the following region is an inner bound to $\mathcal{C}(q(y, z|x))$:

$$\begin{aligned}
R_0, R_1, R_2 &\geq 0, \\
R_0 + R_1 &\leq \frac{1}{n} I(U^nW^n; Y^n), && (8.22)\\
R_0 + R_2 &\leq \frac{1}{n} I(V^nW^n; Z^n), && (8.23)\\
R_0 + R_1 + R_2 &\leq \frac{1}{n}\big[I(U^nW^n; Y^n) + I(V^n; Z^n|W^n) \\
&\qquad - I(U^n; V^n|W^n)\big], && (8.24)\\
R_0 + R_1 + R_2 &\leq \frac{1}{n}\big[I(U^n; Y^n|W^n) + I(V^nW^n; Z^n) \\
&\qquad - I(U^n; V^n|W^n)\big], && (8.25)\\
2R_0 + R_1 + R_2 &\leq \frac{1}{n}\big[I(U^nW^n; Y^n) + I(V^nW^n; Z^n) \\
&\qquad - I(U^n; V^n|W^n)\big], && (8.26)
\end{aligned}$$

where $U^n, V^n, W^n, X^n, Y^n, Z^n$ are distributed according to $p(u^n, v^n, w^n, x^n)q(y^n, z^n|x^n)$. Clearly if we assume that (U^n, V^n, W^n, X^n) is n i.i.d. copies of $p(u, v, w, x)$ we get back the one-letter version of Marton's inner bound. Assume that

$$p(u^n, v^n, w^n) = \prod_{i=1}^{n} r(u_i, v_i, w_i).$$

Note that U_i, V_i, W_i are i.i.d. copies of (U, V, W) distributed according to $r(u, v, w)$. We further use the given conditional law $r(x|u_1, v_1, w_1, u_2, v_2, w_2)$ to define the joint distribution of X^n given U^n, V^n, W^n as

$$\begin{aligned}
&p(x_2^n|u^n, v^n, w^n) = \prod_{i=2}^{n} r(x_i|u_{i-1}, v_{i-1}, w_{i-1}, u_i, v_i, w_i), \\
&X_1 = \textit{constant}.
\end{aligned}$$

We then have

$$I(U^nW^n;Y^n) = H(U^nW^n) - H(U^nW^n|Y^n) =$$
$$\sum_{i=1}^{n} H(U_iW_i) - H(U_iW_i|U^{i-1}W^{i-1}Y^n) =$$
$$\sum_{i=1}^{n} I(U_iW_i;U^{i-1}W^{i-1}Y^n) \geq \sum_{i=2}^{n} I(U_iW_i;U_{i-1}W_{i-1}Y_iY_{i-1})$$
$$= (n-1)I(U_2W_2;Y_1Y_2U_1W_1).$$

Similarly $I(V^nW^n;Z^n) \geq (n-1)I(V_2W_2;V_1W_1Z_1Z_2)$. Next, note that

$$I(V^n;Z^n|W^n) = H(V^n|W^n) - H(V^n|W^nZ^n) =$$
$$\sum_{i=1}^{n} H(V_i|W_i) - H(V_i|V^{i-1}W^nZ^n) =$$
$$\sum_{i=1}^{n} I(V_i;V^{i-1}W^nZ^n|W_i) \geq$$
$$\sum_{i=2}^{n} I(V_i;V_{i-1}W_{i-1}Z_iZ_{i-1}|W_i) =$$
$$(n-1)I(V_2;V_1W_1Z_2Z_1|W_2).$$

Similarly, $I(U^n;Y^n|W^n) \geq (n-1)I(U_2;Y_1Y_2U_1W_1|W_2)$. Lastly, note that $I(U^n;V^n|W^n) = n \cdot I(U;V|W)$. We obtain the desired result by substituting these values into equations (8.22)-(8.26), and letting $n \to \infty$.

■

Appendix A

Appendices

A.1 Lower bound on secret key rate

A.1.1 Source Model

The essentially best known lower bound on the source model secrecy capacity, proved using random binning arguments, is due to Ahlswede and Csiszár [1]: the maximum of $\sup_{V\to U\to X_1\to X_2Z}\big(I(U;X_2|V)-I(U;Z|V)\big)$ and $\sup_{V\to U\to X_2\to X_1Z}\big(I(U;X_1|V)-I(U;Z|V)\big)$. [1]

Roughly speaking our new lower bound in the source model is proved by following the interactive communication stage by stage, however we have to do some careful bookkeeping of the buildup of the secret-key rate by controlling the amount of reduction of secret key rate built up in earlier stages due to the communication in later stages. The lower bound in the source model is exploited for deriving a new lower bound on the secret key capacity in the channel model. After the submission of [23], the authors were informed about the existence of a related result in [54] in which a two-way key agreement protocol for binary random variables (in the context of the quantum key distribution) is discussed.

Theorem 15. $S(X_1;X_2;...;X_u;(X_{u+1})^{(s)};...;(X_m)^{(s)}\|Z)$ is bounded below by
$\sum_{j=a}^{b}[\min_{1\le r\le m} I(U_j;X_r|U_{1:j-1}) - I(U_j;Z|U_{1:j-1})]$
for all natural numbers $a\le b$, and finite random variables $U_1,U_2,...,U_b$ satisfying the following constraints:

[1] Maurer provided a different technique for deriving lower bounds on the secret key capacity in [39]. He proved, for instance, that even when the maximum of the two one-way secret key capacities vanishes, the secret key capacity may still be positive. This technique however seems to give us a rather low secret key rate in this case. A generally applicable single letter form of a lower bound based on the ideas in [39] is not known.

- $$p(U_1, U_2, ..., U_b|X_1, X_2, X_3, ..., X_m, Z) = \prod_{k=1}^{b} p(U_k|U_{1:k-1}X_{j_k}),$$

  where $1 \leq j_k \leq m$ is such that $j_k = k$ modulo m;

- $U_k = 0$ whenever $u + 1 \leq j_k \leq m$ where j_k is defined as above.

This lower bound strictly improves what is essentially the currently best known lower bound, namely the maximum of the two one-way secret key capacities.

Discussion: The first property that $(U_1, ..., U_b)$ should satisfy is equivalent to the following condition:

$I(U_k; X_{[m]-\{j_k\}}|U_{1:k-1}X_{j_k}) = 0$.

Intuitively, assuming that all the X_i's and Z have learnt $U_{1:k-1}$, the j_k-th terminal can create U_k. The individual terms in the lower bound can be understood from the form of the one-way secret key capacity. ■

Proof

Proof of Theorem 15: It is enough to prove the lower bound for the special case of $a = 1$. This is because $S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ can be bounded below by

$$S\big(X_1U_{1:a-1}; ...; X_uU_{1:a-1}; (X_{u+1}U_{1:a-1})^{(s)}; ... \\ ...; (X_mU_{1:a-1})^{(s)} \| ZU_{1:a-1}\big)$$

since the m terminals can collaboratively create *i.i.d.* repetitions of $U_{1:a-1}$. Here we are using the following inequality for $k = 1, 2, ..., a - 2$:

$$S\big(X_1U_{1:k-1}; ...; X_uU_{1:k-1}; (X_{u+1}U_{1:k-1})^{(s)}; ... \\ ...; (X_mU_{1:k-1})^{(s)} \| ZU_{1:k-1}\big) \\ \geq S\big(X_1U_{1:k}; ...; X_uU_{1:k}; (X_{u+1}U_{1:k})^{(s)}; ... \\ ...; (X_mU_{1:k})^{(s)} \| ZU_{1:k}\big).$$

We proceed with the assumption $a = 1$.

For any sequence $(s_1, s_2, ..., s_l)$, let $(s_1, s_2, ..., s_{i-1}, \overbrace{s_i}, s_{i+1}, ..., s_l)$ refer to the subsequence in which s_i is removed. Apply Lemma A3.1 mentioned at the end of this section to the $m + 1$-tuple:

$$(U_i, X_1U_{1:i-1}, ..., X_{j_{i-1}}U_{1:i-1}, \overbrace{X_{j_i}U_{1:i-1}}, X_{j_{i+1}}U_{1:i-1}, \\ ..., X_mU_{1:i-1}, ZU_{1:i-1})$$

for $i = 1, 2, ..., b$ where j_i is defined as the natural number $1 \leq j_i \leq m$ satisfying $j_i = i$ modulo m. The lemma implies the existence of a natural number n and random variables $C_{1:b}$ satisfying the following four properties (here we use $U^n_{1:i-1}$ as a shorthand for $U^n_1 U^n_2 U^n_3 ... U^n_{i-1}$, n i.i.d repetitions of $U_1 U_2 ... U_{i-1}$):

- C_i is a function of U^n_i, $i = 1, 2, 3..., b$;
- U^n_i could be reconstructed from C_i and $X^n_j U^n_{1:i-1}$ for all j with probability $1 - \epsilon$ for $i = 1, 2, 3..., b$;
- $\frac{1}{n} I(C_i; Z^n U^n_{1:i-1}) < \epsilon + \max[0, I(U_i; Z U_{1:i-1}) - \min_j I(U_i; X_j U_{1:i-1})] = \epsilon + \max[0, I(U_i; Z|U_{1:i-1}) - \min_j I(U_i; X_j|U_{1:i-1})]$;
- $\frac{1}{n} H(U^n_i | C_i Z^n U^n_{1:i-1}) \geq \max[0, \min_j I(U_i; X_j U_{1:i-1}) - I(U_i; Z U_{1:i-1})] - \epsilon = \max[0, \min_j I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})] - \epsilon$.

Assume that the m terminals observe n i.i.d repetitions of their random variables. At the i-th stage, U^n_i and C_i are created by the j_i-th terminal. C_i is then communicated to the other terminals and thereby enabling the other $m-1$ terminals to create U^n_i with probability $1 - \epsilon$. The probability that after b stages all the m terminals cannot agree on the common randomness $U^n_1 U^n_2 U^n_3 ... U^n_b$ will therefore be at most $(m-1)b\epsilon$. In other words, if we let G_i represent the i-th terminal's guess of $U^n_{1:b}$, we will have:

$P(G_1 = \cdots = G_m = U^n_{1:b}) \geq 1 - (m-1)b\epsilon$.

We can bound $S(X_1; X_2; ...; X_u; X^{(s)}_{u+1}; ...; X^{(s)}_m \| Z)$ from below by

$$\frac{1}{n} S(G_1; G_2; ...; G_u; G^{(s)}_{u+1}; ...; G^{(s)}_m \| C_{1:b} Z^n) \geq$$
$$\frac{1}{n} [H(G_1|C_{1:b}Z^n) - \sum_{i=2}^{m} H(G_1|G_i)].$$

The last inequality was derived using property 4 of Theorem 1. Since

$$P(G_1 = \cdots = G_m = U^n_{1:b}) \geq 1 - (m-1)b\epsilon,$$

we can work out the last expression as follows:

$$\frac{1}{n} [H(G_1|C_{1:b}Z^n) - \sum_{i=2}^{m} H(G_1|G_i)] \geq$$
$$\frac{1}{n} [H(U^n_{1:b}|C_{1:b}Z^n) - H(U^n_{1:b}|G_1) - \sum_{i=2}^{m} H(G_1|G_i)] \geq$$
$$\frac{1}{n} H(U^n_{1:b}|C_{1:b}Z^n)$$
$$- m\big(h((m-1)b\epsilon) + (m-1)b\epsilon \log \prod_{i=1}^{b} |\mathcal{U}_i|\big),$$

where $h(.)$ is the binary entropy function.

We prove that $\frac{1}{n}H(U_{1:b}^n|C_{1:b}Z^n)$ is at least
$\sum_{i=1}^{b}[\min_{1\leq j\leq m} I(U_i;X_j|U_{1:i-1}) - I(U_i;Z|U_{1:i-1})] - 2b\epsilon$.

If we can show this, the proof would be finished by letting ϵ tend to zero.

$$H(U_{1:b}^n|C_{1:b}Z^n) = \sum_{i=1}^{b} H(U_i^n|C_{1:b}Z^nU_{1:i-1}^n) =$$
$$\sum_{i=1}^{b} H(U_i^n|C_{1:i}Z^nU_{1:i-1}^n) -$$
$$\sum_{i=1}^{b-1} I(U_i^n;C_{i+1:b}|C_{1:i}Z^nU_{1:i-1}^n) =$$
$$\sum_{i=1}^{b} H(U_i^n|C_iZ^nU_{1:i-1}^n) -$$
$$\sum_{i=1}^{b-1} I(U_i^n;C_{i+1:b}|C_{1:i}Z^nU_{1:i-1}^n).$$

Starting with the second term,

$$\sum_{i=1}^{b-1} I(U_i^n;C_{i+1:b}|C_{1:i}Z^nU_{1:i-1}^n) =$$
$$\sum_{1\leq i<j\leq p} I(U_i^n;C_j|C_{1:j-1}Z^nU_{1:i-1}^n) =$$
$$\sum_{j=2}^{b} I(U_{1:j-1}^n;C_j|C_{1:j-1}Z^n) \leq$$
$$\sum_{j=2}^{b} I(U_{1:j-1}^nC_{1:j-1}Z^n;C_j) =$$
$$\sum_{j=2}^{b} I(U_{1:j-1}^nZ^n;C_j) \leq$$

$$\sum_{j=2}^{b} n\big(\epsilon + \max[0, I(U_j;Z|U_{1:j-1}) - \min_r I(U_j;X_r|U_{1:j-1})]\big),$$

where we have used the third above-mentioned property of the C_j in the last step.

The first term in the above expansion of $H(U_{1:b}^n|C_{1:b}Z^n)$ can be bounded below

using the fourth property of the C_i.

$$\sum_{i=1}^{b} H(U_i^n|C_i Z^n U_{1:i-1}^n) \geq$$

$$n\sum_{i=1}^{b}\big(\max[0, \min_j I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})] - \epsilon\big).$$

Therefore

$$H(U_{1:b}^n|C_{1:b}Z^n) \geq$$

$$n\sum_{i=1}^{b}\big(\max[0, \min_j I(U_i; X_j|U_{1:i-1}) - I(U_i; Z|U_{1:i-1})]\big) -$$

$$n\sum_{i=2}^{b}\big(\max[0, I(U_i; Z|U_{1:i-1}) - \min_j I(U_i; X_j|U_{1:i-1})]\big) - 2nb\epsilon.$$

Since, for every real number r, $\max[0, r] - \max[0, -r] \geq r$, we can conclude:

$$\frac{1}{n}H(U_{1:b}^n|C_{1:b}Z^n) \geq$$

$$\sum_{j=1}^{b}[\min_{1\leq r\leq m} I(U_j; X_r|U_{1:j-1}) - I(U_j; Z|U_{1:j-1})] - 2b\epsilon.$$

It remains to prove that, in the case of two terminals, the new lower bound strictly improves the maximum of the two one-way secret key capacities. Since $m = 2$, for simplicity we use the notation X, Y instead of X_1 and X_2 for the rest of the proof. We note that for any arbitrary random variables V_1 and V_2 satisfying the Markov chain $V_1 \to V_2 \to X \to YZ$, the choice of $a = b = 3$ and $U_1 = V_1$, $U_2 = 0$, $U_3 = V_2$ would achieve $I(V_2; Y|V_1) - I(V_2; Z|V_1)$. Therefore the new lower bound is no worse than the maximum of the two one-way secret key capacities. We use the example and proof technique provided by Ahlswede and Csiszár in [1] to show that there is at least one example in which the new lower bound outperforms the maximum of the two one-way secret key capacities. Assume that X_1 and X_2 are independent binary random variables. The joint conditional distribution of Y_1, Y_2, Z_1, Z_2 given X_1 and X_2 is defined in Figure A.1. Let $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$, $Z = (Z_1, Z_2)$. Assume further that X_1 has a uniform distribution.

The upper bound $I(X; Y|Z) = I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2)$ is also a lower bound on $S(X; Y\|Z)$. This is because the above expression is achievable with the choice of $U_1 = X_1$, $U_2 = Y_2$. But this cannot be achieved by either of the one-way secret key capacities. As pointed out in [1], the one-way secret key capacity $S(X; Y^{(s)}\|Z)$ depends only on $p(x, y)$ and $p(x, z)$. But $p((x_1, x_2), (y_1, y_2))$ is the same as $p((x_1, x_2), (y_1, t_2))$. Further $(X_1, X_2) \to (Y_1, T_2) \to (Z_1, Z_2)$ forms a Markov chain. Therefore $S(X; Y^{(s)}\|Z) =$

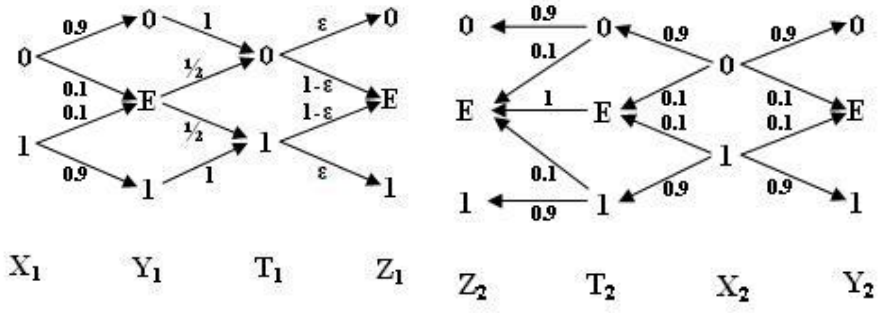

Figure A.1: The conditional distribution of (Y_1, Y_2, Z_1, Z_2) given X_1 and X_2

$I(X_1; Y_1|Z_1) + I(X_2; T_2|Z_2) < I(X_1; Y_1|Z_1) + I(X_2; Y_2|Z_2)$. The last inequality is because $I(Y_2; Z_2) = 0.9I(X_2; Z_2) < I(X_2; Z_2)$.

Similarly, $S(X^{(s)}; Y\|Z) < I(X; Y|Z)$ because $p((y_1, y_2), (x_1, x_2))$ is the same as $p((y_1, y_2), (t_1, x_2))$ as X_1 has a uniform distribution, and also because $I(X_1; Z_1) < I(Y_1; Z_1)$. The latter inequality is valid because $H(Z_1|X_1) = h(0.95\epsilon, 1-\epsilon, 0.05\epsilon) > H(Z_1|Y_1) = 0.9h(\epsilon, 1-\epsilon) + 0.1h(0.5\epsilon, 1-\epsilon, 0.5\epsilon)$.

■

Lemma A3.1 For any random variables $X_1, X_2, ..., X_m$ and Z taking values in finite sets, and for any $\epsilon > 0$, there exists a natural number M such that for any $n \geq M$, there exists random variable C such that:

- $H(C|X_1^n) = 0$;
- X_1^n could be reconstructed from C and X_j^n for all j with probability $1 - \epsilon$;
- $\frac{1}{n} I(C; Z^n) < \epsilon + \max(0, I(X_1; Z) - \min_j I(X_1; X_j))$;
- $\frac{1}{n} H(X_1^n|CZ^n) \geq \max[0, \min_j I(X_1; X_j) - I(X_1; Z) - \epsilon]$.

Proof: Let $\mathcal{X}_1$ denote the alphabet of X_1. We will find a mapping $f : \mathcal{X}_1^n \mapsto \{1, 2, 3, ..., 2^{n(\max_j H(X_1|X_j) + c\epsilon)}\}$ such that $C = f(X_1^n)$ satisfies the required properties. $c < 1$ is a small constant that will be specified during the proof.

We consider two cases: in the first case we assume $I(X_1; Z) - \min_j I(X_1; X_j) \geq 0$. In other words, $\max_j H(X_1|X_j) \geq H(X_1|Z)$. Consider the scenario in which the first terminal wants to enable the terminals X_2, X_3, ..., X_m and Z to recover his message with probability at least $1 - c\epsilon$. Slepian-Wolf tells us that there is a natural number M such that for any $n \geq M$ there exists random variable $C = f(X_1^n)$ of entropy $n[\max_j H(X_1|X_j) + c\epsilon]$ that would work. Among the four properties that C has to satisfy, all but the third one are trivial. Regarding the third inequality one can write:

$$I(X_1^n; Z^n) = I(C; Z^n) + I(X_1^n; Z^n|C) =$$
$$I(C; Z^n) + H(X_1^n|C) - H(X_1^n|CZ^n).$$

According to the Fano inequality, $H(X_1^n|CZ^n)$ is of order $n(h(c\epsilon) + c\epsilon \log |\mathcal{X}_1|)$ since X_1^n can be recovered from CZ^n with probability $1 - c\epsilon$ and the logarithm of the support set of these random variables is of order n. The constant c can be chosen so that $h(c\epsilon) + c\epsilon \log |\mathcal{X}_1| \leq \epsilon$.

We get the desired bound on $I(C; Z^n)$ by noting that

$$H(X_1^n|C) = H(X_1^n) - H(C) =$$
$$n[H(X_1) - \max_j H(X_1|X_j)] = n \cdot \min_j I(X_1; X_j).$$

For the second case, we assume that $I(X_1; Z) - \min_j I(X_1; X_j) < 0$, or in other words

$$\max_j H(X_1|X_j) < H(X_1|Z).$$

Slepian-Wolf shows the existence of a natural number M such that for any $n \geq M$ there are random variables $C = f(X_1^n)$ of entropy $n[\max_j H(X_1|X_j) + c\epsilon]$, and $C' = g(X_1^n)$ of entropy $n[H(X_1|Z) - \max_j H(X_1|X_j) + c\epsilon]$ such that X_1^n is recoverable from (C, C', Z^n) with probability $1 - c\epsilon$, and from (C, X_j^n) for any j with probability $1 - c\epsilon$. Now,

$$I(X_1^n; CC'Z^n) = I(X_1^n; Z^n) + H(CC'|Z^n).$$

On the other hand,

$$I(X_1^n; CC'Z^n) = H(X_1^n) - H(X_1^n|CC'Z^n) =$$
$$H(X_1^n) - n(h(c\epsilon) + c\epsilon \cdot \log |\mathcal{X}_1|).$$

The constant c can be chosen so that $h(c\epsilon) + c\epsilon \cdot \log |\mathcal{X}_1| = \epsilon$. Therefore $H(CC'|Z^n) = H(X_1^n) - I(X_1^n; Z^n) - n\epsilon \geq H(C) + H(C') - n\epsilon$. In the last inequality we have used the fact that the values of $H(C)$ and $H(C')$ are known.

But since $H(CC'|Z^n) = H(C|Z^n) + H(C'|CZ^n)$, we can conclude $\frac{1}{n} I(C; Z^n) + \frac{1}{n} I(C'; CZ^n) = \epsilon$. This proves the third property that C has to satisfy, i.e. $\frac{1}{n} I(C; Z^n) \leq \epsilon$. The fourth property can be proved by noting that

$$\frac{1}{n} H(X_1^n|CZ^n) \geq \frac{1}{n} H(C'|CZ^n) \geq$$
$$\frac{1}{n}[H(C') - I(C'; CZ^n)] \geq \min_j I(X_1; X_j) - I(X_1; Z) - \epsilon.$$

■

A.1.2 Channel Model

In the channel model, for the case of $m = 2$, the best known upper bound explicitly mentioned in the literature, as far as we are aware, is

$$\min[\sup_{p(x_1)} I(X_1; X_2), \sup_{p(x_1)} I(X_1; X_2|Z))],$$

which was proposed by Maurer [39]. This can however be easily generalized to

$$\inf_{\overline{Z} \to Z \to X_1 X_2} [\sup_{p(x_1)} I(X_1; X_2|\overline{Z})].$$

The essentially best know lower bound, as far as we are aware, is

$$\sup_{p(x_1)} \max \big\{ \sup_{V \to U \to X_1 \to X_2 Z} [I(U; X_2|V) - I(U; Z|V)], \\ \sup_{V \to U \to X_2 \to X_1 Z} [I(U; X_1|V) - I(U; Z|V)] \big\}, \tag{A.1}$$

which one can find in [12], [39]. Recently, Csiszár and Narayan have derived new sufficient conditions for tight upper bounds [13].

In this section, we derive a new lower on the secrecy capacity. An example is provided to show that the new bound represents a strict improvement over the previously best known bound.

Theorem 16. Assume that $a \leq b$ are two arbitrary natural numbers and $(U_1, U_2, ..., U_b)$ are arbitrary finite random variables satisfying the following constraints:

- $$p(U_1, U_2, ..., U_b|X_1, X_2, X_3, ..., X_m, Z) = \\ \prod_{k=1}^{b} p(U_k|U_{1:k-1} X_{j_k}),$$

  where $1 \leq j_k \leq m$ is such that $j_k = k$ modulo m;

- $U_k = 0$ whenever $u + 1 \leq j_k \leq m$ where j_k is defined as above.[2]

$C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$ is then bounded from below by

$$\sup_{p(x_1)} \sum_{j=a}^{b} [\min_{1 \leq r \leq m} I(U_j; X_r|U_{1:j-1}) - I(U_j; Z|U_{1:j-1})],$$

[2]By $U_k = 0$, we mean $P(U_k = 0) = 1$, in effect meaning that the alphabet for U_k is of size one.

where random variables $X_1, X_2, ..., X_m, Z, U_1, ..., U_b$ inside the supremum are jointly distributed as

$$p(x_1)\mathrm{q}(x_2, ...x_m, z|x_1)p(u_1, u_2, ..., u_b|x_1, x_2, ..., x_m, z).$$

In the case of $m = 2$, the new lower bound on $C_{CH}(2, \mathrm{q}(x_2, z|x_1))$ derived by taking supremum over all valid $(a, b, U_1, U_2, ..., U_b)$ strictly improves the

$$\sup_{p(x_1)}[\max(S(X_1; X_2^{(s)}\|Z), S(X_1^{(s)}; X_2\|Z))]$$

lower bound, where in this expression, $S(X_1; X_2^{(s)}\|Z)$ is the source model one-way secret key capacity from X_1 to X_2 in the presence of Z.

Discussion: $C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$ is bounded from below by

$$\sup_{p(x_1)} S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}\|Z),$$

because given any $p(x_1)$ and a source model key generation scheme for

$$S(X_1; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}\|Z),$$

one can simulate the scheme in the channel model [39]. More specifically, let SK(n, ϵ, S_1, S_2, S_3, ..., S_m, $\mathbf{C}$) denote a source model secret key generation scheme. This scheme can be simulated in the channel model by having the first terminal insert i.i.d. copies of X_1 at the input of the DMBC for n stages, and letting the first $n-1$ public discussions $\mathbf{C}_1$, $\mathbf{C}_2$, ..., $\mathbf{C}_{n-1}$ be vacuous, and $\mathbf{C}_n$ to be equal to the source model discussion $\mathbf{C}$. The same secret keys S_1, S_2, S_3, ..., S_m are then created at the end of the scheme.

We can then apply Theorem 15 of section A.1.1 to bound

$$S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)}\|Z)$$

from below by

$$\sum_{j=a}^{b}[\min_{1\le r\le m} I(U_j; X_r|U_{1:j-1}) - I(U_j; Z|U_{1:j-1})].$$

The proof will establish that, in the case of $u = m = 2$, this new lower bound represents a strict improvement over the

$$\sup_{p(x_1)}[\max(S(X_1; X_2^{(s)}\|Z), S(X_1^{(s)}; X_2\|Z))]$$

lower bound. ■

Proof of Theorem 16: $C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$ is bounded from below by

$$\sup_{p(x_1)} S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z).$$

This is argued in the discussion following the statement of Theorem 16. We apply Theorem 15 of section A.1.1 to bound

$S(X_1; X_2; ...; X_u; X_{u+1}^{(s)}; ...; X_m^{(s)} \| Z)$ from below by

$\sum_{j=a}^{b} [\min_{1 \le r \le m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]$. Therefore $C_{CH}(u, \mathrm{q}(x_2, x_3, ...x_m, z|x_1))$ is bounded from below by

$$\sup_{p(x_1)} [\sum_{j=a}^{b} [\min_{1 \le r \le m} I(U_j; X_r | U_{1:j-1}) - I(U_j; Z | U_{1:j-1})]]. \tag{A.2}$$

For the case of $u = m = 2$, for simplicity, we use the notation X, Y instead of X_1 and X_2 for the rest of the proof. We first prove that the new lower bound on $C_{CH}(2, \mathrm{q}(y, z|x))$ is always greater than or equal to

$$\sup_{p(x)} [\max(S(X; Y^{(s)} \| Z), S(X^{(s)}; Y \| Z))].$$

Take some arbitrary $p(x)$, and consider random variables X, Y and Z having the joint distribution $p(x)\mathrm{q}(y, z|x)$. Take arbitrary random variables V_1 and V_2 satisfying the Markov chain $V_2 \to V_1 \to X \to YZ$. Specializing equation (A.2) to $a = b = 3$, the chosen $p(x)$, and $(U_1, U_2, U_3) = (V_2, 0, V_1)$[3], one can show that $C_{CH}(2, \mathrm{q}(y, z|x)) \ge I(V_2; Y|V_1) - I(V_2; Z|V_1)$. Therefore the new lower bound is always greater than or equal to $\sup_{p(x)} S(X; Y^{(s)} \| Z)$. By symmetry, it is greater than or equal to $\sup_{p(x)} S(X; Y^{(s)} \| Z)$. Thus,

$$C_{CH}(2, \mathrm{q}(y, z|x)) \ge$$
$$\sup_{p(x)} [\max(S(X; Y^{(s)} \| Z), S(X^{(s)}; Y \| Z))].$$

Next, we construct an example to show that there is at least one case in which the new lower bound outperforms $\sup_{p(x)} [\max(S(X; Y^{(s)} \| Z), S(X^{(s)}; Y \| Z))]$. Our example is in part motivated by the example and the proof technique of Ahlswede and Csiszár in [1].

Assume that $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$, $Z = (Z_1, Z_2)$. The conditional distribution of (Y_1, Y_2, Z_1, Z_2) given X_1 and X_2 is defined in Figure A.1 in terms of a parameter $\epsilon \in [0, 1]$. We prove that the new lower bound and the upper

[3]By $U_2 = 0$, we mean that the finite random variable U_2 takes on the value 0 with probability one.

bound $\sup_{p(x)} I(X;Y|Z)$ match for this broadcast channel. This would imply that $C_{CH}(2, \mathrm{q}(y,z|x)) = \sup_{p(x)} I(X;Y|Z)$. On the other hand, we show that

$$\sup_{p(x)} I(X;Y|Z) > \sup_{p(x)}[\max(S(X;Y^{(s)}\|Z), S(X^{(s)};Y\|Z))], \tag{A.3}$$

meaning that the previously known lower bound does not close the gap.

We begin by showing that the supremum $\sup_{p(x)} I(X;Y|Z)$ is *uniquely* achieved at the uniform distribution on X, i.e. when $p(x) = \frac{1}{4}$ for all $x = (x_1, x_2) \in \{0,1\} \times \{0,1\}$. In other words, the supremum is uniquely achieved when X_1 and X_2 are independent uniform binary random variables. In appendix of section A.1.2, with reference to Figure A.1 with $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$ and $Z = (Z_1, Z_2)$, it is shown that for any $0 < \epsilon < 1$, $I(X;Y|Z)$ *strictly increases* when

- X_1 and X_2 are not independent and we replace $p(X_1, X_2)p(Y, Z|X)$ with $p(X_1)p(X_2)p(Y, Z|X)$, i.e. replacing the joint distribution of X_1, X_2 with the product of their marginal distributions;
- we change the marginal distribution of X_1 to a uniform distribution if X_1 and X_2 are independent, but X_1 is not uniform;
- we change the marginal distribution of X_2 to a uniform distribution if X_1 and X_2 are independent, but X_2 is not uniform.

Therefore the supremum $\sup_{p(x)} I(X;Y|Z)$ is uniquely achieved when X_1 and X_2 are independent uniform binary random variables.

When X_1 and X_2 are independent, the pairs (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) will become independent. In this case, $I(X;Y|Z)$ will be equal to $I(X_1;Y_1|Z_1)+I(X_2;Y_2|Z_2)$. Since the Markov chains $X_1 \to Y_1 \to Z_1$ and $Y_2 \to X_2 \to Z_2$ hold, the sum $I(X_1;Y_1|Z_1)+I(X_2;Y_2|Z_2)$ will be equal to $I(X_1;Y_1)-I(X_1;Z_1)+I(Y_2;X_2)-I(Y_2;Z_2)$. The latter secrecy rate is achievable by the choice of $a = 1$, $b = 2$, $(U_1, U_2) = (X_1, Y_2)$ in equation (A.2).

Now, we will prove equation (A.3). Since

$$\forall p(x), \quad I(X;Y|Z) \geq \max(S(X;Y^{(s)}\|Z), S(X^{(s)};Y\|Z)),$$

and the supremum $\sup_{p(x)} I(X;Y|Z)$ is *uniquely* achieved when X_1 and X_2 are independent uniform binary random variables, it suffices to show that

$$I(X;Y|Z) > \max(S(X;Y^{(s)}\|Z), S(X^{(s)};Y\|Z))$$

for independent uniform binary random variables X_1 and X_2. In the proof of Theorem 15 of section A.1.1, we have considered exactly the same joint distribution on X, Y and Z, and showed that $I(X;Y|Z)$ strictly exceeds $\max(S(X;Y^{(s)}\|Z), S(X^{(s)};Y\|Z))$. In order to avoid duplication, the argument is not repeated here.

■

Appendix I

In this appendix, we show that with reference to Figure A.1 with $X = (X_1, X_2)$, $Y = (Y_1, Y_2)$ and $Z = (Z_1, Z_2)$, for any $0 < \epsilon < 1$, $I(X;Y|Z)$ *strictly increases* when

- X_1 and X_2 are not independent and we replace $p(X_1, X_2)p(Y, Z|X)$ with $p(X_1)p(X_2)p(Y, Z|X)$, i.e. replace the joint distribution of X_1, X_2 with the product of their marginal distributions;
- we change the marginal distribution of X_1 to a uniform distribution if X_1 and X_2 are independent, but X_1 is not uniform;
- we change the marginal distribution of X_2 to a uniform distribution if X_1 and X_2 are independent, but X_2 is not uniform.

Case 1:

$$\begin{aligned} &I(X;Y|Z) = \\ &I(X_1X_2;Y_1Y_2|Z_1Z_2) = \\ &H(Y_1Y_2|Z_1Z_2) - H(Y_1Y_2|Z_1Z_2X_1X_2). \end{aligned}$$

Since $Y_1Z_1 \to X_1 \to X_2 \to Y_2Z_2$, we can work out the second term as:

$$\begin{aligned} &H(Y_1Y_2|Z_1Z_2X_1X_2) = \\ &H(Y_1|Z_1Z_2X_1X_2) + H(Y_2|Z_1Z_2X_1X_2Y_1) = \\ &H(Y_1|Z_1X_1) + H(Y_2|X_2Z_2). \end{aligned}$$

The first term can be bounded from above as follows:

$$\begin{aligned} &H(Y_1Y_2|Z_1Z_2) = H(Y_2|Z_1Z_2) + H(Y_1|Z_1Z_2Y_2) \leq \\ &H(Y_2|Z_2) + H(Y_1|Z_1). \end{aligned}$$

Therefore $I(X;Y|Z) \leq I(X_1;Y_1|Z_1) + I(X_2;Y_2|Z_2)$. This would mean that if we replace
$p(X_1, X_2)p(Y, Z|X)$ with $p(X_1)p(X_2)p(Y, Z|X)$, the term $I(X;Y|Z)$ does not decrease.

We prove that $I(X;Y|Z)$ strictly increases by contradiction. Assume $I(X;Y|Z)$ does not increase. In this case, $H(Y_1|Z_1Z_2Y_2)$ must be equal to $H(Y_1|Z_1)$, implying that $I(Y_1;Y_2|Z_1) = 0$. Since $Z_1 \to Y_1 \to Y_2$ is a Markov chain, the $I(Y_1;Y_2|Z_1) = 0$ constraint implies that $I(Y_2;Z_1) = I(Y_2;Y_1)$. But since

$$I(Y_2;Y_1) \geq I(Y_2;T_1) \geq I(Y_2;Z_1),$$

we get $I(Y_2;T_1) = I(Y_2;Z_1)$.

$$I(Y_2;Z_1) = I(Y_2;Z_1,\mathbf{1}[Z_1 = E]) =$$
$$I(Y_2;\mathbf{1}[Z_1 = E]) + I(Y_2;Z_1|\mathbf{1}[Z_1 = E]) = 0 + \epsilon \cdot I(Y_2;T_1).$$

Since $\epsilon < 1$, $I(Y_2;T_1) = I(Y_2;Z_1)$ can hold only when $I(Y_2;T_1) = I(Y_2;Z_1) = I(Y_2;Y_1) = 0$.

$$0 = I(Y_2;Y_1) = I(Y_2,\mathbf{1}[Y_2 = E];Y_1,\mathbf{1}[Y_1 = E]) \geq$$
$$I(Y_2;Y_1|\mathbf{1}[Y_2 = E],\mathbf{1}[Y_1 = E]) \geq$$
$$p(Y_2 \neq E).p(Y_1 \neq E).I(Y_2;Y_1|Y_2 \neq E, Y_1 \neq E) =$$
$$0.81I(X_1;X_2).$$

Therefore $I(X_1;X_2) = 0$, meaning that X_1 and X_2 are independent. This is a contradiction. ■

Case 2:

$I(X_1;Y_1|Z_1) = I(X_1;Y_1) - I(X_1;Z_1) = H(Y_1) - H(Y_1|X_1) - H(Z_1) + H(Z_1|X_1)$ can be thought of as a function of $p(X_1 = 0) = a$. $H(Y_1|X_1)$ and $H(Z_1|X_1)$ are constant not depending on a. The marginal distribution of Z_1 equals $(\epsilon \cdot (0.9a + 0.05), 1 - \epsilon, \epsilon \cdot (-0.9a + 0.95))$, and the marginal distribution of Y_1 equals $(0.9a, 0.1, 0.9 - 0.9a))$. Therefore it is enough to show that $H(Y_1) - H(Z_1)$ uniquely reaches its maximum at $a = 0.5$. This can be seen by noting that the derivative of $\frac{1}{0.9}(H(Y_1) - H(Z_1))$ with respect to a equals $\log \frac{0.5-(a-0.5)}{0.5+(a-0.5)} - \epsilon \log \frac{0.5-0.9(a-0.5)}{0.5+0.9(a-0.5)}$, which is zero only at $a = 0.5$. ■

Case 3:

$$I(X_2;Y_2|Z_2) = I(X_2;(Y_2,\mathbf{1}[Y_2 = E])|Z_2) =$$
$$I(X_2;\mathbf{1}[Y_2 = E]\big|Z_2) + I(X_2;Y_2\big|\mathbf{1}[Y_2 = E],Z_2) =$$
$$0 + P(Y_2 = E) * 0 + P(Y_2 \neq E) \cdot H(X_2|Z_2) =$$
$$0.9H(X_2|Z_2).$$

But

$$H(X_2|Z_2) =$$
$$P(Z_2 = 0) * 0 + P(Z_2 = 1) * 0 + P(Z_2 = E) * H(X_2).$$

Therefore

$$I(X_2;Y_2|Z_2) = 0.9 * 0.19H(X_2).$$

We are done by noting that $H(X_2)$ strictly increases when the distribution of X_2 is changed to the uniform distribution.

Bibliography

[1] R. Ahlswede and I. Csiszár, "Common Randomness in Information Theory and Cryptography. Part I: Secret sharing", *IEEE Trans. IT*, 39 (4), pp. 1121 -1132 (1993).

[2] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger, "Network coding for computing", *Proceedings of the 46th Annual Allerton Conference on Communications, Control and Computing*, Urbana, Illinois, September 23 -26, pp. 1-6 (2008).

[3] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "The secrecy capacity of the wiretap channel with rate-limited feedback," *IEEE Trans. IT*, 55 (12), pp. 53535361 (2009).

[4] Y. Cao, B. Chen, J. Zhang, "A New Achievable Rate Region for Interference Channels with Common Information," *Wireless Communications and Networking Conference*, pp. 2069 - 2073 (2007).

[5] M. Christandl, R. Renner and S. Wolf, "A property of the intrinsic mutual information", *Proceedings of the International Symposium on Information Theory (ISIT)*, 2003, p. 258.

[6] M. H. M. Costa and A. El Gamal, "The capacity region of the discrete memoryless interference channel with strong interference", *IEEE Trans. IT*, vol. 33 (5), pp. 710-711 (1987).

[7] T. M. Cover, A. El Gamal, and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Trans. IT*, 26(6), pp. 648-657 (1980).

[8] T. Cover, "An achievable rate region for the broadcast channel," IEEE Trans. IT, 21 (4), pp. (399-404) (1975).

[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.

[10] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic, 1982.

[11] I. Csiszár and J. Korner, "Broadcast Channels with Confidential Messages", *IEEE Trans. IT*, 24 (3), pp. 339-348 (1978).

[12] I. Csiszár and P. Narayan, "Secrecy Capacities for Multiple Terminals", *IEEE Trans. IT*, 50 (12), pp. 3047-3061 (2004).

[13] I. Csiszár and P. Narayan, "Secrecy Capacities for Multiterminal Channel Models", *IEEE Trans. IT*, 54 (6), pp. 2437-2452 (2008).

[14] I. Csiszár, "Almost independence and secrecy capacity" (in. Russian), *Problems of Information Transmission (PPI)*, 32 (1), pp. 48-57 (1996).

[15] A. El Gamal and Y.-H. Kim, *Lecture Notes on Network Information Theory* , 2010, imprint available at http://arxiv.org/abs/1001.3404.

[16] P. Gács and J, Körner, "Common information is much less than mutual information," *Probl. Contr. Inf. Theory*, 150 (2), pp. 149-162 (1973).

[17] M. Gastpar, "Cut-set Arguments For Source-Channel Networks," *Proceedings of the International Symposium on Information Theory (ISIT)*, 34, (2004).

[18] S. I. Gelfand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Inf. Transm.*, 16 (1), pp. 17-25 (1980).

[19] A. Giridhar and P. R. Kumar, "Computing and communicating functions over sensor networks," *IEEE Journal on Selected Areas in Communications*, 23(4), pp. 755-764 (2005).

[20] A. A. Gohari and V. Anantharam, "Communication for Omniscience by a Neutral Observer and Information-Theoretic Key Agreement of Multiple Terminals", *Proceedings of the International Symposium on Information Theory (ISIT)*, 2007, pp. 2056-2060.

[21] A. A. Gohari and V. Anantharam, "An outer bound to the admissible source region of broadcast channels with arbitrarily correlated sources and channel variations", *Proceedings of the 46th Annual Allerton Conference on Communications, Control and Computing,*, 2008, pp. 301-308.

[22] A. A. Gohari and V. Anantharam, "A Generalized Cut-Set Bound", *Proceedings of the International Symposium on Information Theory (ISIT)*, 2009, pp. 99-103.

[23] A. A. Gohari and V. Anantharam, "Information-Theoretic Key Agreement of Multiple Terminals – Part I: Source Model," accepted for publication in *IEEE Trans. IT*. Available at http://www.eecs.berkeley.edu/∼aminzade/SourceModel.pdf

[24] A. A. Gohari and V. Anantharam, "Information-Theoretic Key Agreement of Multiple Terminals – Part II: Channel Model," accepted for publication in *IEEE Trans. IT*. Available at http://www.eecs.berkeley.edu/∼aminzade/ChannelModel.pdf

[25] D. Gündüz, E. Erkip, A. Goldsmith, H. V. Poor, "Source and Channel Coding for Correlated Sources Over Multiuser Channels," *IEEE Trans. IT*, 55 (9), pp. 3927-3944 (2009).

[26] B. E. Hajek and M. B. Pursley, "Evaluation of an achievable rate region for the broadcast channel," *IEEE Trans. IT*, 25 (1), pp. 36-46 (1979).

[27] T. Han, M. Costa, "Broadcast Channels with Arbitrarily Correlated Sources," *IEEE Trans. IT* 33(5), pp. 641- 650 (1987)

[28] V. Jog and C. Nair, "An information inequality for the BSSC channel," *Proceedings of the ITA workshop*, San Diego, pp. 1-8, 2010.

[29] W. Kang and S. Ulukus, "A new data processing inequality and its applications in distributed source and channel coding," submitted to *IEEE Trans. IT*.

[30] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. IT*, 23 (1), pp. 60-64 (1977).

[31] G. Kramer, Y. Liang and S. Shamai (Shitz), "Outer bounds on the admissible source region for broadcast channels with dependent sources," *Inform. Theory and Applications Workshop*, pp. 162-179 (2009).

[32] G. Kramer and S. A. Savari, "Cut sets and information flow in networks of two-way channels," *Proceedings of the International Symposium on Information Theory (ISIT)*, 33, (2004).

[33] Y, Liang, G. Kramer, "Rate regions for relay broadcast channels," *IEEE Trans. IT*, 53 (10), pp. 3517-3535 (2007).

[34] Y. Liang, G. Kramer, and S. Shamai (Shitz), "Capacity outer bounds for broadcast channels," *IEEE Inf. Theory Workshop*, Porto, Portugal, May 5-9, pp. 2-4 (2008).

[35] 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).

[36] I. Maric, R. D. Yates and G. Kramer, "The Capacity Region of the Strong Interference Channel with Common Information", *Asilomar Conference On Signals, Systems and Computers*, Pacific Grove, CA, pp. 1737-1741 (2005).

[37] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. IT*, 25 (3), pp. 306-311 (1979).

[38] U. M. Maurer, R. Renner and S. Wolf, "Unbreakable Keys from Random Noise", *Security with Noisy Data*, Springer-Verlag, 2007, pp. 21-44.

[39] U. M. Maurer, "Secret Key Agreement by Public Discussion From Common Information", *IEEE Trans. IT*, 39(3), pp. 733-742 (1993).

[40] U. M. Maurer and S. Wolf, "The Intrinsic Conditional Mutual Information and Perfect Secrecy", *Proceedings of the International Symposium on Information Theory (ISIT)*, 1997, p. 88.

[41] U. M. Maurer and S. Wolf, "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information", *IEEE Trans. IT*, 45 (2), pp. 499-514 (1999).

[42] U. M. Maurer and S. Wolf, "From Weak to Strong Information-Theoretic Key Agreement", *Proceedings of the International Symposium on Information Theory (ISIT)*, 2000, p. 18.

[43] P. Minero and Y.-H. Kim, "Correlated Sources over Broadcast Channels," *Proceedings of the International Symposium on Information Theory (ISIT)*, South Korea, pp. 2780 - 2784 (2009).

[44] C. Nair, "An outer bound for 2-receiver discrete memoryless broadcast channels," Available at http://chandra.ie.cuhk.edu.hk/pub/papers/outerbound.pdf

[45] 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, pp. 226-229 (2008).

[46] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," *IEEE Trans. IT*, 53 (1), pp. 350-355 (2007).

[47] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Trans. IT*, 53(10), pp. 3498-3516 (2007).

[48] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. IT*, 47 (3), pp. 903-917 (2001).

[49] S. S. Pradhan, S. Choi and K. Ramchandran, "A graph-based framework for transmission of correlated sources over multiple access channels," *IEEE Trans. IT*, 53 (12), pp. 4583-4604 (2007).

[50] R. Pulikkoonattu, E. Perron and S. Diggavi, "Xitip Information Theoretic Inequalities Prover," available at http://xitip.epfl.ch/

[51] R. Renner and S. Wolf, "New Bounds in Secret-Key Agreement: The Gap Between Formation and Secrecy Extraction", *Proceedings of EUROCRYPT 2003*, LNCS, Springer-Verlag, Vol. 2656, May 2003, pp. 562-577.

[52] C.E. Shannon, "Communication Theory of Secrecy", *Bell System Technical Journal*, Vol. 28, Oct. 1949, pp. 656-715.

[53] E. C. van der Meulen, "Random coding theorems for the general discrete memoryless broadcast channel," *IEEE Trans. IT*, 21 (2), pp. 180-190 (1975).

[54] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication" , *Phys. Rev. A*, 76 (3), pp. 032312-1-7 (2007).

[55] F. M. J. Willems, "The maximal-error and average-error capacity region of the broadcast channel are identical," *Problems of Control and Information Theory*, 19 (4), pp. 339-347 (1990).

[56] A. D. Wyner, "The Wiretap Channel", *Bell System Technical Journal*, 54 (8), pp. 1355-1387 (1975).

[57] H. Yamamoto, "Wyner-Ziv theory for a general function of the correlated sources," *IEEE Trans. IT*, 28 (5), pp. 803-807 (1982).

[58] R. Yeung and Y. Yan, "ITIP - Information Theoretic Inequality Prover," available at http://user-www.ie.cuhk.edu.hk/ ITIP/