Computing a Function of Correlated Sources

Milad Sefidgaran and Aslan Tchamkerten

Abstract

A receiver wants to compute a function \( f \) of two correlated sources \( X \) and \( Y \) and side information \( Z \). What is the minimum number of bits that needs to be communicated by each transmitter?

In this paper, we derive inner and outer bounds to the rate region of this problem which coincide in the cases where \( f \) is partially invertible and where the sources are independent given the side information. From the former case we recover the Slepian-Wolf rate region and from the latter case we recover Orlitsky and Roche’s single source result.

I. Introduction

Given two sources \( X \) and \( Y \) separately observed by two transmitters, we consider the problem of finding the minimum number of bits that needs to be sent by each transmitter to a common receiver, who has access to side information \( Z \), and wants to compute a given function \( f(X, Y, Z) \) with high probability\(^1\).

The first result on this problem was obtained by Körner and Marton [8] who derived the rate region for the case where \( f \) is the sum modulo two of binary \( X \) and \( Y \) and where \( p(x, y) \) is symmetric (no side information is available at the receiver). Interestingly, this result came before Orlitsky and Roche’s general result for the single source case [13], which provides a closed form expression on the minimum number of bits needed to be transmitted to compute \( f(X, Z) \) at the receiver, for arbitrary \( f \) and \( p(x, z) \)\(^2\).

However, the Körner and Marton’s arguments appear to be difficult to generalize to other functions and probability distributions (for an extension of [8] to sum modulo \( p \) and symmetric distributions see [5]).

More recently, Doshi, Shah, and Médard [4] derived conditions under which a rate pair can be achieved for fixed code length and error probability. These conditions do not, however, provide a single letter characterization for the rate region.

This work was supported in part by a “Future et Rupture” grant from the Institut Telecom, and by an Excellence Chair Grant from the French National Research Agency (ACE project).

M. Sefidgaran and A. Tchamkerten are with the Department of Communications and Electronics, Telecom ParisTech, 46 Rue Barrault, 75634 Paris Cedex 13, France. Emails: {sefidgaran,aslan.tchamkerten}@telecom-paristech.fr.

Part of this work will be presented at ISIT 2011.

\(^1\)Alternatively, zero error probability has been variously investigated (see, e.g., [7], [11], [12], [13], [21]).

\(^2\)Their result has been generalized for two round communication [13], and \( K \) round communication [9] in a point-to-point channel. Also, coding schemes and converses established in [13] have been used in other network configurations, such as cascade networks [3], [17].
A more general setting has been investigated by Nazer and Gastpar [10], who considered the problem of function computation over a multiple access channel, thereby introducing potential interference between transmitters.

Function computation has also been studied in more general networks, such as in the context of network coding [1] and decentralized decision making and computation [15].

In this paper first we provide an inner bound and an outer bound for partially invertible functions, e.g., when $X$ or $Y$ is a function of both $f(X, Y, Z)$ and $Z$. These bounds are tight in the case where $f$ is partially invertible with respect to one of the sources. As a corollary, we recover the Slepian-Wolf rate region, which corresponds to the case where $f$ is invertible with respect to both sources. From the outer bound for partially invertible functions, we derive a general outer bound which is tight with the inner bound when the sources are independent given the side information. As a corollary, we recover the rate region for a single source [13]. Finally, a second general outer bound is derived using results from rate distortion for correlated sources. In general, these two outer bounds can’t be derived from each other.

For a single source $X$ and side information $Z$, the minimum number of bits needed for computing a function $f(x, z)$ is the solution of an optimization problem defined over the set of all independent sets with respect to a characteristic graph defined by $X$, $Z$, and $f$. Indeed, Orlitsky and Roche showed that, for a single source, allowing for multisets of independent sets doesn’t yield any improvement on achievable rates (see proof of [13, Theorem 2]). In contrast, our inner and outer bounds are the solutions to optimization problems defined over multisets of all independent sets with respect to similar characteristic graphs. Allowing for multisets may indeed increase the set of achievable rate pairs. This is shown via simulation in an example of a partially invertible function where inner and outer bounds are tight.

An outline of the paper is as follows. In Section II we formally state the problem and provide some background material and definitions. Section III contains our results, and Section IV is devoted to the proofs.

II. PROBLEM STATEMENT AND PRELIMINARIES

Let $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, and $\mathcal{F}$ be finite sets, and $f : \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} \to \mathcal{F}$. Let $\{(x_i, y_i, z_i)\}_{i=1}^{\infty}$ be independent instances of random variables $(X, Y, Z)$ taking values over $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ and distributed according to $p(x, y, z)$.

**Definition 1** (Code). A $(n, R_X, R_Y)$ code consists of two encoding functions

$$\varphi_X : \mathcal{X}^n \to \{1, 2, \ldots, 2^{nR_X}\},$$

$$\varphi_Y : \mathcal{Y}^n \to \{1, 2, \ldots, 2^{nR_Y}\},$$
and a decoding function

\[ \psi : \{1, 2, ..., 2^{nR_X}\} \times \{1, 2, ..., 2^{nR_Y}\} \times \mathcal{Z}^n \rightarrow \mathcal{F}^n. \]

The error probability of a code is defined as

\[ P(\psi(\varphi_X(X), \varphi_Y(Y), Z) \neq f(X, Y, Z)), \]

where \( X \overset{\text{def}}{=} X_1, \ldots, X_n \) and

\[ f(X, Y, Z) \overset{\text{def}}{=} \{ f(X_1, Y_1, Z_1), \ldots, f(X_n, Y_n, Z_n) \}. \]

**Definition 2** (Rate Region). A rate pair \((R_X, R_Y)\) is achievable if, for any \( \epsilon > 0 \) and all \( n \) large enough, there exists a \((n, R_X, R_Y)\) code whose error probability is no larger than \( \epsilon \). The rate region is the closure of the set of achievable \((R_X, R_Y)\).

The problem we consider in this paper is to characterize the rate region for given \( f \) and \( p(x, y, z) \).

Below we remind definitions and properties of conditional characteristic graphs [18], [7], which play a key role in coding for computing.

**Definition 3** (Conditional Characteristic Graph). Given \((X, Y) \sim p(x, y)\) and \( f(X, Y) \), the conditional characteristic graph \( G_{X|Y} \) of \( X \) given \( Y \) is the (undirected) graph whose vertex set is \( \mathcal{X} \) and whose edge set \( E(G_{X|Y}) \) consists of the set of all \((x_i, x_j)\) for which there exists \( y \in \mathcal{Y} \) such that

i. \( p(x_i, y) \cdot p(x_j, y) > 0 \),
ii. \( f(x_i, y) \neq f(x_j, y) \).

**Notation.** Given two random variables \( X \) and \( V \), where \( X \) ranges over \( \mathcal{X} \) and \( V \) over subsets of \( \mathcal{X} \), we write \( X \in V \) whenever \( P(X \in V) = 1 \).

Recall that an independent set of a graph \( G \) is a subset of vertices no two of which are connected. A maximal independent set is an independent set that is not included in any other independent set. The set of independent sets of \( G \) and the set of maximal independent sets of \( G \) are denoted by \( \Gamma(G) \) and \( \Gamma^*(G) \), respectively.

Given a finite set \( \mathcal{S} \), we use \( M(\mathcal{S}) \) to denote the collection of all multisets of \( \mathcal{S} \). (Recall that a multiset of a set \( \mathcal{S} \) is a collection of elements from \( \mathcal{S} \) possibly with repetitions, e.g., if \( \mathcal{S} = \{0, 1\} \), then \( \{0, 1, 1\} \) is a multiset.)

\(^3\)I.e., a sample of \( V \) is a subset of \( \mathcal{X} \).
**Definition 4** (Conditional Graph Entropy [13]). The conditional entropy of a graph is defined as

\[ H_{G_{X|Y}}(X|Y) \overset{\text{def}}{=} \min_{V-X-Y \in \Gamma(G_{X|Y})} I(V; X|Y) = \min_{V-X-Y \in M(\Gamma(G_{X|Y}))} I(V; X|Y). \]

The second equality in the above expression was established in [13].

We now extend the definition of conditional characteristic graph to allow conditioning on variables that take values over independent sets.

**Definition 5** (Generalized Conditional Characteristic Graph). Given \((X,Y,W,Z) \sim p(x,y,w,z)\) and \(f(X,Y,Z)\) such that \(Y \in W \in \Gamma(G_{Y|X,Z})\) \(^5\) let \(\tilde{f}_Y(x,w,z) = f(x,y,z)\) for \(x \in X, z \in Z, y \in w \in \Gamma(G_{Y|X,Z}),\) and \(p(x,y,w,z) > 0.\) The generalized conditional characteristic graph of \(X\) given \(W\) and \(Z,\) denoted by \(G_{X|W,Z}\), is the conditional characteristic graph of \(X\) given \((W,Z)\) with respect to the marginal distribution \(p(x,w,z)\) and \(\tilde{f}_Y(X,W,Z)\).

**Example 1.** Let \(X\) and \(Y\) to be random variables defined over the alphabets \(\mathcal{X}\) and \(\mathcal{Y},\) respectively, with \(\mathcal{X} = \mathcal{Y} = \{1, 2, 3, 4\}\), and with probability distribution \(p(X = Y) = 0\) and uniform over the pairs \((i,j) \in \mathcal{X} \times \mathcal{Y}\) that \(i \neq j.\) The receiver wants to decide whether \(X > Y\) or \(Y > X,\) i.e., compute the function \(f(X,Y)\) defined as

\[ f(x,y) = \begin{cases} 0, & \text{if } x < y, \\ 1, & \text{if } x > y. \end{cases} \]  

(1)

Fig. 1(a) depicts \(G_{X|Y}\) which is equal to \(G_{Y|X}\) by symmetry. Hence,

\[ \Gamma(G_{X|Y}) = \Gamma(G_{Y|X}) = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{2, 3\}, \{3, 4\}\}. \]

\[ \Gamma^*(G_{X|Y}) = \Gamma^*(G_{Y|X}) = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}. \]

\(^4\)We use the notation \(U - V - W\) whenever random variables \((U,V,W)\) form a Markov chain.

\(^5\)By definition \(\Gamma(G_{Y|X,Z}) = \Gamma(G_{Y|(X,Z)}).\)
An example of random variable $W$ that satisfies
\[ Y \in W \in \Gamma(G_{X|Y}), \tag{2} \]
is one whose support set is
\[ \mathcal{W} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}\}. \]

For such a $W$, the generalized conditional characteristic graph $G_{X|W}$ is depicted in Fig. [I(b)] and we have
\[ \Gamma(G_{X|W}) = \{\{1\}, \{2\}, \{3\}, \{4\}, \{2, 3\}, \{3, 4\}\}. \]

Another example of random variable $W$ that satisfies (2) is one whose support set is
\[ \mathcal{W} = \{\{2\}, \{4\}, \{1, 2\}, \{2, 3\}\}. \]

For such a $W$, the generalized conditional characteristic graph $G_{X|W}$ is depicted in Fig. [I(c)] and we have
\[ \Gamma(G_{X|W}) = \{\{1\}, \{2\}, \{3\}, \{4\}, \{3, 4\}\}. \]

Note that, in general,
\[ E(G_{X|Y,Z}) \subseteq E(G_{X|W,Z}) \]
whenever
\[ Y \in W \in \Gamma(G_{X|Y,Z}). \]

The following lemma provides sufficient conditions under which generalized conditional characteristic graph and conditional characteristic graph are the same, i.e., for which
\[ E(G_{X|Y,Z}) = E(G_{X|W,Z}). \]

**Lemma 1.** Given $(V, X, Y, Z) \sim p(v, x, y, z)$ and $f(X, Y, Z)$, we have
\[ G_{Y|V,Z} = G_{Y|X,Z}, \]
for all $V$ such that $X \in V \in \Gamma(G_{X|Y,Z})$, in each of the following cases:

a. $p(x, y, z) > 0$ for all $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$;

b. $G_{X|Y,Z}$ is a complete graph or equivalently $\Gamma(G_{X|Y,Z})$ consists only of singletons;
c. \(X\) and \(Y\) are independent given \(Z\).

We use the following definition in the Analysis and Appendix sections.

**Definition 6** (Support set of a random variable). Given \((V, X) \sim p(v, x)\), the support set of \(V\) with respect to \(X\) is the set valued random variable

\[
S_X(V) = \{x : p(V, x) > 0\}
\]

whenever there is a one-to-one correspondence between \(v\) and \(\{x : p(v, x) > 0\}\).

If \(v\) and \(\{x : p(v, x) > 0\}\) are not in one-to-one correspondence, \(S_X(V)\) is defined as follows. First, label \(\{x : p(v, x) > 0\}\) with different indices for all \(v\)'s. \(S_X(V)\) is then defined as in the one-to-one correspondence case, but with respect to this labeling.

Note that, by definition, \(V\) and \(S_X(V)\) are in one-to-one correspondence.

### III. Results

Our results are often stated in terms of certain random variables \(V\) and \(W\) which can usefully be interpreted as auxiliaries used to construct the codebooks for transmitter \(X\) and transmitter \(Y\), respectively. This interpretation is consistent with the proofs of the results.

Propositions \(\square\) provides a general inner bound to the rate region:

**Proposition 1** (Inner bound). \((R_X, R_Y)\) is achievable whenever

\[
R_X \geq I(V; X|W, Z),
\]

\[
R_Y \geq I(Y; W|V, Z),
\]

\[
R_X + R_Y \geq I(V; X|Z) + I(Y; W|V, Z),
\]

for some \(V\) and \(W\) that satisfy

\[
V - X - (Y, W, Z),
\]

\[
(V, X, Z) - Y - W,
\]

and either

\[
X \in V \in M(\Gamma(G_X|Y, Z))
\]

\[
Y \in W \in M(\Gamma(G_Y|V, Z)),
\]
or, equivalently,

\[ Y \in W \in M(\Gamma(G_Y|X,Z)) \]

\[ X \in V \in M(\Gamma(G_X|W,Z)). \]

Note that when there is no side information at the decoder, i.e., when \( Z \) is a constant, the two Markov chain constraints in Proposition 1 are equivalent to the single long Markov chain

\[ V - X - Y - W, \]

which imply that the sum rate inequality of Proposition 1 becomes

\[ R_X + R_Y \geq I(X,Y;V,W). \]

The next result provides an outer bound to the rate region when the function is partially invertible with respect to \( X \) (with respect to \( Y \), respectively), i.e., when \( X \) (\( Y \), respectively) is a deterministic function of both \( f(X,Y,Z) \) and \( Z \). Interestingly, this bound implies a general outer bound to the rate region (see Corollary 2 below).

**Proposition 2** (Outer Bound - Partially Invertible Function). If \( f \) is partially invertible with respect to \( X \), then \((R_X, R_Y)\) satisfies

\[ R_X \geq H(X|W,Z), \]

\[ R_Y \geq I(Y;W|X,Z), \]

\[ R_X + R_Y \geq H(X|Z) + I(Y;W|X,Z), \]

for some \( W \) that satisfies

\[ (X,Z) - Y - W, \]

\[ Y \in W \in W \subset M(\Gamma(G_Y|X,Z)), \]

with

\[ |W| \leq |Y| + 2. \]

Propositions 1 with \( V = X \) together with Proposition 2 yields the following result:

**Theorem 1** (Rate Region - Partially Invertible Function). If \( f \) is partially invertible with respect to \( X \),
then the rate region is the closure of rate pairs \((R_X, R_Y)\) that satisfy the conditions of Propositions \(^2\).

In Section IV, we provide an alternative proof for Theorem 1 using the canonical theory developed in [6]. This alternative proof, however, doesn’t establish the cardinality bound \(|\mathcal{W}| \leq |\mathcal{Y}| + 2\).

**Example 2.** Consider the situation with no side information given by \(f(x, y) = (-1)^y \cdot x\), with \(\mathcal{X} = \mathcal{Y} = \{0, 1, 2\}\), and

\[
p(x, y) = \begin{bmatrix}
.21 & .03 & .12 \\
.06 & .15 & .16 \\
.03 & .12 & .12 
\end{bmatrix}.
\]

Since \(f(X, Y)\) is partially invertible with respect to \(X\), we can use Theorem 1 to numerically evaluate the rate region. The obtained region is given by the union of the three shaded areas in Fig. 2. These areas are discussed later, after Example 4.

To numerically evaluate the rate region, we would need to consider the set of all conditional distributions \(p(w|y), y \in \mathcal{Y}, w \in \mathcal{M}(\Gamma(G_{Y|X}))\). Since \(|\mathcal{W}| \leq 5\), \(\mathcal{M}(\Gamma(G_{Y|X}))\) consists of multisets of

\[
\Gamma(G_{Y|X}) = \{\{0\}, \{1\}, \{2\}, \{0, 2\}\}
\]

whose cardinalities are bounded by 5.

However, as we now show, among all possible \(4^5 = 1024\) multisets with cardinality at most 5, considering just the multiset \(\{\{1\}, \{0, 2\}, \{0, 2\}, \{0, 2\}, \{0, 2\}\}\) gives the rate region.

Consider a multiset with cardinality at most 5.

1. If the multiset does not contain sample \(\{1\}\), then the condition \(\sum_{w \in \mathcal{W}} p(w|Y = 1) = 1\), hence the condition \(Y \in W\), cannot be satisfied. Therefore this multiset is not admissible, and we can ignore it.

2. If the multiset contains two samples \(w_1 = \{1\}\) and \(w_2 = \{1\}\) with conditional probabilities \(p(w_1|Y = 1)\) and \(p(w_2|Y = 1)\), respectively, replacing them by one sample \(w = \{1\}\) whose conditional probability is \(p(w|Y = 1) = p(w_1|Y = 1) + p(w_2|Y = 1)\), gives the same terms \(H(X|W)\) and \(I(Y; W|X)\), hence the same rate pairs. Therefore, without loss of optimality we can consider only multisets which contain a unique sample of \(\{1\}\).

3. If the multiset contains a sample \(w_1 = \{0\}\) with arbitrary conditional probability \(p(w_1|Y = 0)\), replacing it with sample \(w_2 = \{0, 2\}\) whose conditional probabilities are \(p(w_2|Y = 0) = p(w_1|Y = 0)\) and \(p(w_2|Y = 2) = 0\) gives the same rate pairs. (The same argument holds for a sample \(w_1 = \{2\}\).

From 1., 2., and 3., multisets with one sample of \(\{1\}\) and multiple copies of \(\{0, 2\}\) gives the rate
4. If the multiset has cardinality $k < 5$, adding $5 - k$ samples $\{0, 2\}$ with zero conditional probabilities, gives the same rate pairs.

It follows that the rate region can be obtained by considering the unique multiset

$$\{w_1 = \{1\}, w_2 = \{0, 2\}, w_3 = \{0, 2\}, w_4 = \{0, 2\}, w_5 = \{0, 2\}\}$$

and by optimizing over the conditional probabilities $\{p(w|y)\}$ that satisfy

$$p(w_1|Y = 1) = 1,$$

$$p(w_1|Y = j) = 0, j \in \{0, 2\},$$

$$\sum_{i=2}^{5} p(w_i|Y = 0) = 1,$$

$$\sum_{i=2}^{5} p(w_i|Y = 2) = 1,$$

$$p(w_i|Y = 1) = 0, i \in \{2, 3, 4, 5\}.$$ 

Notice that this optimization has only six degrees of freedom.

When $f$ is invertible, i.e., when $(X, Y)$ is a function of both $f(X, Y, Z)$ and $Z$, Theorem 1 reduces to the Slepian-Wolf rate region [14]:

**Corollary 1 (Rate Region - Invertible Function).** If $f$ is invertible, then the rate region is the closure of
rate pairs \( (R_X, R_Y) \) such that

\[
R_X \geq H(X|Y, Z), \\
R_Y \geq H(Y|X, Z), \\
R_X + R_Y \geq H(X, Y|Z).
\]

**Example 3.** Let \( X = Y = \{1, 2, 3, 5, 7\} \), \( Z = \{1, 2, 3\} \), let \( p(x, y, z) \) be such that

\[
p(x, y, z) \cdot p(y, x, z) = 0,
\]

for any \( x, y, z \) with \( x \neq y \), and let

\[
f(x, y, z) = x \cdot y \cdot z.
\]

Since \( f(X, Y, Z) \) is invertible, the rate region is the Slepian-Wolf rate region given by Corollary 1.

**Proof of Corollary 7.** To deduce Corollary 1 from Theorem 1, suppose \( f \) is invertible and suppose \( (X, Y, W, Z) \) satisfy the conditions of Proposition 2 for given \( (R_X, R_Y) \). Note first that \( H(X|W, Z) \geq H(X|Y, Z) \) by Markovity, hence the first inequality in Proposition 2 gives

\[
R_X \geq H(X|Y, Z). \tag{3}
\]

Further, knowledge of \( (W, X, Z) \) implies knowledge of \( f(X, Y, Z) \), by property of \( W \). Hence,

\[
H(Y|W, X, Z) = H(Y|W, X, Z, f(X, Y, Z)) = 0
\]

since the function is invertible. Therefore, the second and third inequalities in Proposition 2 yield

\[
R_Y \geq H(Y|X, Z) \\
R_X + R_Y \geq H(X, Y|Z). \tag{4}
\]

Since the bound given by inequalities (3) and (4) is achievable by letting \( W = Y \) in Proposition 2, Corollary 1 follows.

The following result is a consequence of Proposition 2:
Corollary 2 (General Outer Bound 1). If \((R_X, R_Y)\) is achievable then

\[
R_X \geq H_{G_{X|Y,Z}}(X|Y, Z), \\
R_Y \geq H_{G_{Y|X,Z}}(Y|X, Z), \\
R_X + R_Y \geq H_{G_{X,Y|Z}}(X,Y|Z).
\]

Proof of Corollary 2: Corollary 2 is obtained by reducing the multi-source computation problem to a single source computation problem, and, as such, can also be derived from [13, Theorem 1].

To obtain Corollary 2 from Proposition 2 we proceed as follows. For the first inequality in Corollary 2, note that if \((R_X, R_Y)\) is achievable when computing \(f(X, Y, Z)\) with side information \(Z\), then \((0, R_Y)\) is achievable when computing the function

\[
g(X, Y, Z) = (f(X, Y, Z), X)
\]

with side information \((X, Z)\). Since \(g(X, Y, Z)\) is partially invertible with respect to \(X\), from Proposition 2 we get

\[
R_Y \geq I(Y; W|X, Z),
\]

where \(W\) satisfies

\[
(X, Z) - Y - W;
\]

\[
Y \in W \in M(\Gamma(G_{Y|X,Z})).
\]

The second inequality in Corollary 2 then follows from Definition 4. The first inequality in Corollary 2 is obtained similarly, by swapping the roles of \(X\) and \(Y\).

Finally, if \((R_X, R_Y)\) is achievable with side information \(Z\), then \(R_X + R_Y\) is clearly achievable for a single source \((X, Y)\) and side information \(Z\). By applying the first inequality in Corollary 2 to this single source one deduces the third inequality.

The inner and outer bounds given by Proposition 1 and Corollary 2 are tight for independent sources, hence also for the single source computation problem\(^6\) for which we recover [13, Theorem 1].

Corollary 3 (Rate Region - Independent Sources). If \(X\) and \(Y\) are independent given \(Z\), the rate region

\(^6\)A single source can be seen as two sources with one of them being constant.
is the closure of rate pairs \((R_X, R_Y)\) such that

\[ R_X \geq H_{G_{X|Y,Z}}(X|Y, Z), \]
\[ R_Y \geq H_{G_{Y|X,Z}}(Y|X, Z). \]

Hence, if \(Y\) is constant, \(R_X\) is achievable if and only if \(R_X \geq H_{G_{X|Z}}(X|Z)\).

Proof of Corollary 3: For the converse of Corollary 3 note that the two inequalities in the corollary correspond to the first two inequalities of Corollary 2.

For achievability, suppose \(V\) and \(W\) satisfy the conditions of Proposition 1 i.e.,

\[ X \in V \in M(\Gamma(G_{X|Y,Z})) \]
\[ Y \in W \in M(\Gamma(G_{Y|V,Z})) \]

and

\[ V - X - (Y, W, Z), \]
\[ (V, X, Z) - Y - W. \]

From these two Markov chains and the fact that \(X\) and \(Y\) are independent given \(Z\), we deduce the long Markov chain

\[ V - X - Z - Y - W. \]

It then follows that

\[ I(V; X|W, Z) = I(V; X|Y, Z) \]

and

\[ I(Y; W|V, Z) = I(Y; W|X, Z). \]

Using Proposition 1 we deduce that the rate pair \((R_X, R_Y)\) given by

\[ R_X = I(V; X|Y, Z) \]

and

\[ R_Y = I(Y; W|X, Z) \]
is achievable. Now, since $X$ and $Y$ are independent given $Z$, $G_{Y|V,Z} = G_{Y|X,Z}$ by Claim c. of Lemma 1. This allows to minimize the above two mutual information terms separately, which shows that the rate pair

$$R_X = \min_{X \in V \in \mathcal{M}(\Gamma(G_{X|Y,Z}))} I(V; X|Y, Z)$$

$$R_Y = \min_{Y \in W \in \mathcal{M}(\Gamma(G_{Y|X,Z}))} I(Y; W|X, Z)$$

is achievable (Notice that $I(V; X|Y, Z)$ is a function of the joint distribution $p(v, x, y, z)$ only, thus the minimization constraint $V - X - (Y, Z, W)$ reduces to $V - X - (Y, Z)$. A similar comment applies to the minimization of $I(Y; W|X, Z)$.) The result then follows from Definition 4.

**Example 4.** Let $Z \in \{1, 2, 3\}$, let $U$ and $V$ be independent uniform random variables over $\{-1, 0, 1\}$ and $\{0, 1, 2\}$, respectively, and let $X = Z + U$ and $Y = Z + V$. The receiver wants to decide if $X$ is equal to $Y$, i.e., compute the function $f(X, Y)$ defined as

$$f(x, y) = \begin{cases} 
0, & \text{if } x \neq y, \\
1, & \text{if } x = y.
\end{cases} \quad (5)$$

Since $X$ and $Y$ are independent given $Z$, the rate region is given by Corollary 3. It can be checked that

$$\Gamma^*(G_{X|Y,Z}) = \{\{0, 2\}, \{0, 3\}, \{0, 1, 4\}\}$$

$$\Gamma^*(G_{Y|X,Z}) = \{\{2, 5\}, \{3, 5\}, \{1, 4, 5\}\},$$

and a numerical evaluation of conditional graph entropy gives

$$H(G_{X|Y,Z}) = H(G_{Y|X,Z}) \simeq 1.28.$$ 

Hence the rate region is given by the set of rate pairs satisfying

$$R_X \gtrsim 1.28,$$

$$R_Y \gtrsim 1.28.$$ 

For a single source, Orlitsky and Roche [13] showed that $H_{G_{X|Z}}(X|Z)$ (see Definition 4) is achieved by some $V$ taking values over maximal independent sets $\Gamma^*(G_{X|Z})$. In contrast, for two sources, the restriction to maximal independent sets may induce a loss of optimality. Fig. 2 in Example 2 shows the
rate region for a partially invertible function, when restricting $V$ and $W$ to be over maximally independent sets (gray area), all independent sets (gray and light areas), and multisets of independent sets (union of gray, light gray, and black areas). Denoting these areas by $\mathcal{R}(\Gamma^\ast)$, $\mathcal{R}(\Gamma)$, and $\mathcal{R}(\mathcal{M}(\Gamma))$ respectively, we thus numerically get the strict sets inclusions

$$\mathcal{R}(\Gamma^\ast) \subset \mathcal{R}(\Gamma) \subset \mathcal{R}(\mathcal{M}(\Gamma)).$$

Numerical evidence suggests that the small difference between $\mathcal{R}(\Gamma)$ and $\mathcal{R}(\mathcal{M}(\Gamma))$ is unrelated to the specificity of the probability distribution $p(x, y)$ in the example (i.e., by choosing other distributions the difference between $\mathcal{R}(\Gamma)$ and $\mathcal{R}(\mathcal{M}(\Gamma))$ remains small).

We now provide a second rate region outer bound which is derived using results from rate distortion for correlated sources [16]:

**Proposition 3 (General Outer Bound 2).** If $(R_X, R_Y)$ is achievable, then

\[
\begin{align*}
R_X &\geq I(X,Y;V|W,Z), \\
R_Y &\geq I(X,Y;W|V,Z), \\
R_X + R_Y &\geq I(X,Y;V,W|Z),
\end{align*}
\]

for some random variables $(V, W)$ that satisfy $H(f(X,Y,Z)|V,W,Z) = 0$ and

\[
\begin{align*}
V - X - (Y,Z), \\
(X,Z) - Y - W.
\end{align*}
\]

Using Lemma 3 in the Appendix, one can show that had the above two Markov chain constraints been

\[
\begin{align*}
V - X - (Y,W,Z) \\
(V,X,Z) - Y - W,
\end{align*}
\]

the outer bound given by Proposition 3 would be equal to the inner bound given by Proposition 1. However, since this inner bound is not tight in general, as we show in the coming subsection, these hypothetical Markov chains don’t hold in general.

Finally note that it may be difficult to extract an explicit outer bound from Proposition 3 since it is

\footnote{With $|\mathcal{M}(\Gamma)| \leq 5$.}
implicitly characterized by random variables \((V,W)\) that should (in part) satisfy
\[
H(f(X,Y,Z)|V,W,Z) = 0.
\]

**Gap between upper and lower bounds**

In general, Proposition 1 and Corollary 2 need not be tight, such as for the sum modulo 2 of binary \(X\) and \(Y\) (no side information) with symmetric distribution, i.e.,
\[
p(x,y) = \begin{bmatrix}
\frac{p}{2} & \frac{1-p}{2} \\
\frac{1-p}{2} & \frac{p}{2}
\end{bmatrix}.
\]
Assuming \(p \in (0,1)\), \(\Gamma(G_X|Y)\) and \(\Gamma(G_Y|X)\) both consists of singletons. This implies that the achievable region given by Proposition 1 reduces to
\[
R_X \geq H(X|W),
R_Y \geq H(Y|V),
R_X + R_Y \geq H(X) + H(Y|V).
\] (6)
since
\[
H(X|V) = H(Y|W) = 0
\]
for all \((V,X,Y,W)\) that satisfy
\[
X \in V \in M(\Gamma(G_X|Y)),
Y \in W \in M(\Gamma(G_Y|V)).
\]
Note that since \(\Gamma(G_Y|V)\) (which is equal to \(\Gamma(G_Y|X)\) according to Lemma 1 Claim a.) consists of singletons,
\[
H(X|W) = H(X|Y, W) \leq H(X|Y).
\] (7)
Furthermore, because of the Markov chain constraint
\[
(V,X) - Y - W,
\]
we have

\[ H(X|W) \geq H(X|Y), \quad (8) \]

by the data processing inequality. Hence, (7) and (8) yields

\[ H(X|W) = H(X|Y), \]

and, from the same argument,

\[ H(Y|V) = H(Y|X). \]

Inequalities (6) thus become

\[ R_X \geq H(X|Y), \]
\[ R_Y \geq H(Y|X), \]
\[ R_X + R_Y \geq H(X,Y). \quad (9) \]

Therefore the achievable region given by Proposition 1 reduces to the Slepian-Wolf rate region. This achievable region isn’t maximal since the rate region is given by the set of rate pairs that satisfy the only two constraints

\[ R_X \geq H(X|Y) \]
\[ R_Y \geq H(Y|X) \]

as shown by Körner and Marton [8].

IV. ANALYSIS

Proof of Lemma 1: Suppose \( X \in V \subseteq \Gamma(G_{X|Y,Z}) \). For all claims, we show that \( E(G_{Y|V,Z}) \subseteq E(G_{Y|X,Z}) \) i.e., if two nodes are connected in \( G_{Y|V,Z} \), then they are also connected in \( G_{Y|X,Z} \). The opposite direction, \( E(G_{Y|X,Z}) \subseteq E(G_{Y|V,Z}) \), follows from the definition of generalized conditional characteristic graph.

Suppose nodes \( y_1 \) and \( y_2 \) are connected in \( G_{Y|V,Z} \). This means that there exist \( v \in \mathcal{V} \), \( x_1, x_2 \in v \) and \( z \in \mathcal{Z} \) such that

\[ p(x_1, y_1, z) \cdot p(x_2, y_2, z) > 0, \]

\(^8 E(G) \) is the set of edges of graph \( G \).
and

\[ f(x_1, y_1, z) \neq f(x_2, y_2, z). \]

If \( x_1 = x_2 \), then \( y_1 \) and \( y_2 \) are also connected in \( G_{Y|X,Z} \) according to the definition of conditional characteristic graph. We now assume \( x_1 \neq x_2 \) and prove Claims a., b., and c.

a. Since all probabilities are positive we have \( p(x_1, y_2, z) > 0 \), hence

\[ p(x_1, y_1, z) \cdot p(x_1, y_2, z) > 0, \]

and \( x_1, x_2 \in v \in \Gamma(G_{X|Y,Z}) \) yields

\[ f(x_1, y_2, z) = f(x_2, y_2, z) \neq f(x_1, y_1, z), \]

which implies that \( y_1 \) and \( y_2 \) are also connected in \( G_{Y|X,Z} \).

b. \( \Gamma(G_{X|Y,Z}) \) consists of singletons, so \( x_1, x_2 \in v \in \Gamma(G_{X|Y,Z}) \) yields \( x_1 = x_2 \), and thus \( y_1 \) and \( y_2 \) are also connected in \( G_{Y|X,Z} \) as we showed above.

c. From independence of \( X \) and \( Y \) given \( Z \) we have

\[ p(x, y, z) = p(z) \cdot p(x|z) \cdot p(y|z). \]

Hence, since

\[ p(x_1, y_1, z) \cdot p(x_2, y_2, z) > 0, \]

we have

\[ p(z) \cdot p(x_1|z) \cdot p(y_2|z) > 0, \]

i.e. \( p(x_1, y_2, z) > 0 \). The rest of the proof is the same as Claim a..

\[ \blacksquare \]

**Proof of Proposition 1** We consider a coding scheme similar to the Berger-Tung rate distortion coding scheme \[16\].

Note that rate distortion achievability results do not, in general, provide a direct way for establishing achievability results for coding for computing problems. Indeed, for rate distortion problems one usually considers average distortion between the source and the reconstruction block whereas in computation problems one usually considers the more stringent block distortion criterion \[19\], \[2\].

We consider a two-step coding procedure; a compression phase followed by a Slepian-Wolf coding \[14\].
of the compressed sequences.

Pick $V$ and $W$ such that

$$V - X - (Y, W, Z)$$

$$(V, X, Z) - Y - W,$$

and

$$X \in V \in M(\Gamma(G_{X|Y,Z}))$$

$$Y \in W \in M(\Gamma(G_{Y|V,Z})).$$

Assume these random variables together with $X, Y, Z$ are distributed according to some $p(v, x, y, w, z)$.

For $v \in \Gamma(G_{X|Y,Z})$ and $w \in \Gamma(G_{Y|V,Z})$, define $\tilde{f}(v, w, z)$ to be equal to $f(x, y, z)$ for $x \in v$ and $y \in w$ such that $p(x, y, z) > 0$ (Notice that all such $(x, y)$ gives the same $f(x, y, z)$). Further, for $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$ let

$$\tilde{f}(v, w, z) \overset{\text{def}}{=} \{\tilde{f}(v_1, w_1, z_1), \ldots, \tilde{f}(v_n, w_n, z_n)\}.$$

Randomly generate $2^{nI(V;X)}$ independent sequences

$$v^{(i)} = (v_1^{(i)}, v_2^{(i)}, \ldots, v_n^{(i)}), i \in \{1, 2, \ldots, 2^{nI(V;X)}\},$$

in an i.i.d. manner according to the marginal distribution $p(v)$, and randomly and uniformly bin these sequences into $2^{nR_X}$ bins. Similarly, randomly generate $2^{nI(Y;W)}$ independent sequences

$$w^{(i)} = (w_1^{(i)}, w_2^{(i)}, \ldots, w_n^{(i)}), i \in \{1, 2, \ldots, 2^{nI(Y;W)}\},$$

in an i.i.d. manner according to $p(w)$, and randomly and uniformly bin them into $2^{nR_Y}$ bins. Reveal the bin assignments $\phi_X$ and $\phi_Y$ to the encoders and to the decoder.

**Encoding:** The $X$-transmitter finds a sequence $v$ that is jointly robust typical with source sequence $x$, and sends the index of the bin that contains $v$, i.e., $\phi_X(v)$.

Recall that $(v, x)$ are jointly $\delta$-robust typical [13], if

$$|\tilde{p}_{v,x}(v, x) - p(v, x)| \leq \delta \cdot p(v, x),$$
for all \((v, x) \in V \times X\), where

\[
\tilde{p}_{v, x}(v, x) \overset{\text{def}}{=} \frac{|\{i : (v_i, x_i) = (v, x)\}|}{n}.
\]

Note that if \((v, x)\) are jointly robust typical, then \(\forall i, p(v_i, x_i) > 0\), i.e. \(\forall i, x_i \in v_i\).

The \(Y\)-transmitter proceeds similarly sends \(\phi_Y(w)\). If a transmitter doesn’t find such an index it declares an errors, and if there are more than one indices, the transmitter selects one of them randomly and uniformly.

**Decoding:** Given \(z\) and the index pair \((i_X, i_Y)\), declare \(f(\hat{v}, \hat{w}, z)\) if there exists a unique jointly robust typical \((\hat{v}, \hat{w}, z)\) such that \(\phi_X(\hat{v}) = i_X\) and \(\phi_Y(\hat{w}) = i_Y\), and such that \(f(\hat{v}, \hat{w}, z)\) is defined. Otherwise declare an error.

**Probability of Error:** There are two types of error. The first type of error occurs when no \(v\)’s, respectively \(w\)’s, is jointly robust typical with \(x\), respectively with \(y\). The probability of each of these two errors is shown to be negligible in [13] for \(n\) large enough. Hence, the probability of the first type of error can be made arbitrary small by taking \(n\) large enough.

The second type of error refers to the Slepian-Wolf coding procedure. By symmetry of the encoding and decoding procedures, the probability of error of the Slepian-Wolf coding procedure, averaged over sources outcomes, over \(v\)’s and \(w\)’s, and over the binning assignments, is the same as the average error probability conditioned on the transmitters selecting \(V^{(1)}\) and \(W^{(1)}\). Note that whenever \((\hat{V}, \hat{W}) = (V^{(1)}, W^{(1)})\), there is no error, i.e., \(f(X, Y, Z) = \tilde{f}(V^{(1)}, W^{(1)}, Z)\) by definition of robust typicality and by the definitions of \(V\) and \(W\). We now compute the probability of the event \((\hat{V}, \hat{W}) \neq (V^{(1)}, W^{(1)})\).

Define event \(E(i, j)\) as

\[
E(i, j) = \{(V^{(i)}, W^{(j)}, Z) \in \mathcal{T}, \phi_X(V^{(i)}) = \phi_X(V^{(1)}), \phi_Y(W^{(j)}) = \phi_Y(W^{(1)})\}
\]

where \(\mathcal{T}\) denotes the \((\delta\text{-})\) jointly robust typical set with respect to distribution \(p(v, w, z)\). The probability
of the second type of error is upper bounded as

\[
P((\hat{V}, \hat{W}) \neq (V^{(1)}, W^{(1)}))
\]

\[
= P(\mathcal{E}^c(1, 1) \cup (\bigcup_{(i,j) \neq (1,1)} \mathcal{E}(i, j)))
\]

\[
\leq P(\mathcal{E}^c(1, 1)) + \sum_{i \neq 1} P(\mathcal{E}(i, 1))
\]

\[
+ \sum_{j \neq 1} P(\mathcal{E}(1, j)) + \sum_{i \neq 1, j \neq 1} P(\mathcal{E}(i, j)).
\]  

(10)

According to the properties of jointly robust typical sequences [13], we have

\[
P(\mathcal{E}^c(1, 1)) \leq \varepsilon
\]

\[
P(\mathcal{E}(i, 1)) \leq 2^{-n(R_X + I(V;W,Z))} + \varepsilon
\]

\[
P(\mathcal{E}(1, j)) \leq 2^{-n(R_Y + I(V,Z;W))} + \varepsilon
\]

\[
P(\mathcal{E}(i, j)) \leq 2^{-n(R_X + R_Y + I(V;W) + I(V,W;Z))} + \varepsilon
\]  

(11)

for any \(\varepsilon > 0\) and \(n\) large enough. Hence, from (10) and (11)

\[
P((\hat{V}, \hat{W}) \neq (V^{(1)}, W^{(1)})) \leq \varepsilon + 2^n I(V;X) 2^{-n(R_X + I(V;W,Z))}
\]

\[
+ 2^n I(Y;W) 2^{-n(R_Y + I(V,Z;W))}
\]

\[
+ 2^n (I(V;X) + I(Y;W)) 2^{-n(R_X + R_Y + I(V;W) + I(V,W;Z))}.
\]

The error probability of the second type is thus negligible whenever

\[
R_X \geq I(V;X) - I(V;W,Z)
\]

\[
= H(V|W,Z) - H(V|X)
\]

\[
\overset{(a)}{=} I(V;X|W,Z),
\]

\[
R_Y \geq I(Y;W) - I(V,Z;W)
\]

\[
= H(W|V,Z) - H(W|Y)
\]

\[
\overset{(b)}{=} I(Y;W|V,Z),
\]
\[ R_X + R_Y \geq I(V; X) + I(Y; W) - I(V; W) - I(V, W; Z) \]
\[ = (H(V|Z) - H(V|X)) + (H(W|V, Z) - H(W|Y)) \]
\[ \overset{(c)}{=} I(V; X|Z) + I(Y; W|V, Z), \]
(12)

where \((a)\) and \((b)\) follow from the Markov chains \(V - X - (W, Z)\) and \((V, Z) - Y - W\), respectively, and where \((c)\) follows from the Markov chains \(V - X - Z\) and \((V, Z) - Y - W\).

We end the proof by showing the equivalence of the conditions

\[ X \in V \in M(\Gamma(G_{X|Y,Z})), \]
\[ Y \in W \in M(\Gamma(G_{Y|V,Z})), \]

and

\[ Y \in W \in M(\Gamma(G_{Y|X,Z})), \]
\[ X \in V \in M(\Gamma(G_{X|W,Z})). \]

We prove one direction, the proof for the other direction is the same. Assume

\[ X \in V \in M(\Gamma(G_{X|Y,Z})), \]
\[ Y \in W \in M(\Gamma(G_{Y|V,Z})), \]

holds. To prove that \(W \in M(\Gamma(G_{Y|X,Z}))\), we show that for any \(w \in W\), \(y_1, y_2 \in w, x \in \mathcal{X}, \) and \(z \in \mathcal{Z}\) such that

\[ p(x, y_1, z) \cdot p(x, y_2, z) > 0, \]

we have

\[ f(x, y_1, z) = f(x, y_2, z). \]

Since \(P(X \in V) = 1\), there exists \(v \in V\) such that \(p(v|x) > 0\), hence, by definition of generalized conditional characteristic graph \(G_{Y|V,Z}\), we have\[10\]

\[ f(x, y_1, z) = \tilde{f}_X(v, y_1, z) = \tilde{f}_X(v, y_2, z) = f(x, y_2, z). \]

\[9\] \(W\) is the alphabet of random variable \(W\).

\[10\] \(\tilde{f}_X(v, y, z)\) is defined in the same way as \(\tilde{f}_Y(x, w, z)\) in Definition\[5\].
To prove that $V \in M(\Gamma(G_{X|W,Z}))$, note that for any $w \in W$, $y_1, y_2 \in w$, $v \in V$, $x_1, x_2 \in X$, and $z \in Z$ such that $p(x, y_1, z) \cdot p(x, y_2, z) > 0$,

i) if $y_1 = y_2 = y$, then $f(x_1, y, z) = f(x_2, y, z)$, since $V \in M(\Gamma(G_X|Y,Z))$.

ii) if $y_1 \neq y_2$, then

$$f(x_1, y_1, z) = \hat{f}_X(v, y_1, z) = \hat{f}_X(v, y_2, z) = f(x_2, y_2, z),$$

since $W \in M(\Gamma(G_Y|V,Z))$.

Hence $V \in M(\Gamma(G_{X|W,Z}))$ for both cases i) and ii).

Proof of Proposition 2: Assume the received messages from the transmitters are $C_X = \varphi_X(X)$ and $C_Y = \varphi_Y(Y)$. Since the rate pair $(R_X, R_Y)$ is achievable, there exist a decoding function

$$\psi(C_X, C_Y, Z) = U,$$

such that

$$P(U \neq f(X, Y, Z)) \rightarrow 0 \text{ as } n \rightarrow \infty. \quad (13)$$

Also, since $f$ is partially invertible with respect to $X$, i.e $X$ is a function of $f(X, Y, Z)$ and $Z$, there exist a function

$$g(C_X, C_Y, Z) = (\hat{X}_1, ..., \hat{X}_n) = \hat{X},$$

such that

$$P(\hat{X} \neq X) \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Define the distortion measures

$$d_X(x, \hat{x}) = \begin{cases} 0, & \text{if } x = \hat{x} \\ 1, & \text{otherwise.} \end{cases} \quad (14)$$

$$d_Y(x, y, z, u) = \begin{cases} 0, & \text{if } u = f(x, y, z) \\ 1, & \text{otherwise.} \end{cases} \quad (15)$$

Since

$$P(U \neq f(X, Y, Z)) \geq P(U_i \neq f(X_i, Y_i, Z_i)),$$
we have

\[ P(U \neq f(X, Y, Z)) \geq \frac{1}{n} \sum_{i=1}^{n} p(U_i \neq f(X_i, Y_i, Z_i)) \]

\[ \triangleq d_Y(X, Y, Z, U) \quad (16) \]

From (13) and (16), \( d_Y(X, Y, Z, T) \to 0 \) as \( n \to \infty \). With the same argument one shows that

\[ d_X(X, \hat{X}) \triangleq \frac{1}{n} \sum_{i=1}^{n} d_X(X_i, \hat{X}_i) \to 0 \text{ as } n \to \infty. \]

According to [2, Theorem 1], it follows that there exist random variable \( W' \) and functions \( g_1(X, W', Z) \) and \( g_2(X, W', Z) \) such that\(^{11}\)

\[ \mathbb{E} d_X(X, g_1(X, W', Z)) = 0, \]

\[ \mathbb{E} d_Y(X, Y, Z, g_2(X, W', Z)) = 0, \]

\[ (X, Z) = Y - W', \]

and

\[ R_X \geq H(X|W', Z), \]

\[ R_Y \geq I(Y; W'|X, Z), \]

\[ R_X + R_Y \geq H(X|Z) + I(Y; W'|X, Z). \]

(17)

Notice that since the distortion \( \mathbb{E} d_Y(X, Y, Z, g_2(X, W', Z)) \) is equal to zero, for any \( (x, y_1, w', z) \) and

\( (x, y_2, w', z) \) that satisfy

\[ p(x, y_1, w', z) \cdot p(x, y_2, w', z) > 0, \]

we should have

\[ f(x, y_1, z) = g_2(x, w', z) = f(x, y_2, z). \]

This according to Lemma [2] in the Appendix, is equivalent to

\[ H( f(X, Y, Z) | X, W', Z) = 0. \]

\(^{11}\)There is one caveat in applying the converse arguments of [3, Theorem 1]. In our case we need the distortion measures to be defined over functions of the sources. More precisely, we need Hamming distortion for source \( X \) and Hamming distortion for a function defined over both sources \( (X, Y) \) and side information \( Z \). However, it is straightforward to extend the converse of [3, Theorem 1] to handle this setting (same as [20] which shows that Wyner and Ziv’s result [19] can be extended to the case where the distortion measure is defined over a function of the source and the side information.).
Since \( H(f(X, Y, Z)|X, W', Z) = 0 \) and since \((X, Z) - Y - W'\) holds, using Corollary 4 in the Appendix yields

\[
Y \in S_Y(W') \in M(\Gamma(G_Y|X, Z)),
\]

and

\[
(X, Z) - Y - S_Y(W').
\]

Also, by definition of \( S_Y(W') \) (Definition 6) we have

\[
\begin{align*}
H(X|W', Z) &= H(X|S_Y(W'), Z), \\
I(Y; W'|X, Z) &= I(Y; S_Y(W')|X, Z), \\
H(X|Z) + I(Y; W'|X, Z) &= H(X|Z) + I(Y; S_Y(W')|X, Z).
\end{align*}
\]

Taking \( W = S_Y(W') \) and using (17) and (18) completes the proof. ■

**Alternative Proof of Theorem 1, without cardinality bound:**

We present a proof that establishes Theorem 1 except for the cardinality bound \(|W| \leq |Y| + 2\) (see Proposition 2), using the canonical theory developed in [6]. Suppose there is a third transmitter who knows \( U = f(X, Y, Z) \) and sends some information with rate \( R_U \) to the receiver. For this problem, the rate region is the set of achievable rate pairs \((R_X, R_Y, R_U)\). By intersecting this rate region with \( R_U = 0 \), we obtain the rate region for our two-transmitter computation problem.

Consider the three-transmitter setting as above. Since \( f(X, Y, Z) \) is partially invertible, we can equivalently assume that the goal for the receiver is to obtain \((X, U)\). This corresponds to \((M, J, L) = (3, 2, 0)\) in the Jana-Blahut notation, and, using [6, Theorem 6], the rate region is given by the set of all \((R_X, R_Y, R_U)\) such that

\[
\begin{align*}
R_X &\geq H(X|W', Z, U) \\
R_Y &\geq I(Y; W'|X, Z, U) \\
R_U &\geq H(U|X, W', Z) \\
R_X + R_Y &\geq I(X, Y; X, W'|Z, U)
\end{align*}
\]
For some $W'$ that satisfies

$$(X, Z, U) - Y - W'. $$

Due to this Markov chain we have

$$I(U; W'|X, Y, Z) = I(U; X, W'|X, Y, Z) = 0. $$

(21)

Intersecting with $R_U = 0$, from (19) we derive that

$$H(U|X, W', Z) = 0. $$

(22)

Hence, using (21) and (22), the last three inequalities in (20) become

$$R_X + 0 \geq H(X|W', Z) \geq H(X|W', Z, U)$$

$$R_Y + 0 \geq I(Y; W'|X, Z)$$

$$= H(W'|X, Z) - H(W'|X, Y, Z)$$

$$= H(W'|X, Z) - H(W'|X, Y, Z, U)$$

$$\geq H(W'|X, Z, U) - H(W'|X, Y, Z, U) = I(Y; W'|X, Z, U)$$

$$R_X + R_Y + 0 \geq I(X, Y; X, W'|Z) = H(X|Z) + I(Y; W'|X, Z)$$

$$\geq H(X|Z, U) + I(Y; W'|X, Z, U) = I(X, Y; X, W'|Z, U),$$

which also imply the first three inequalities in (20).

Therefore, when the three last inequalities of (20) hold and when $H(U|X, W', Z) = 0$, all other inequalities are satisfied. The rate region for the two transmitter problem thus becomes the set of rate
pairs \((R_X, R_Y)\) that satisfy

\[
R_X \geq H(X|W', Z) \\
R_Y \geq I(Y; W'|X, Z) \\
R_X + R_Y \geq I(X, Y; X, W'|Z)
\]

for some \(W'\) that satisfies \((X, Z) - Y - W'\) and \(H(U|X, W', Z) = 0\). Now, according to Corollary \([4]\) we have

\[
Y \in S_Y(W') \in M(\Gamma(G_Y|X, Z)),
\]

and

\[
(X, Z) - Y - S_Y(W'').
\]

Taking \(W = S_Y(W')\) completes the proof.

\textbf{Proof of Proposition 3} Assume the received messages from transmitters are \(C_X = \varphi_X(X)\) and \(C_Y = \varphi_Y(Y)\). Since the rate pair \((R_X, R_Y)\) is achievable, there exists a decoding function

\[
\psi(C_X, C_Y, Z) = U,
\]

such that

\[
P(U \neq f(X, Y, Z)) \to 0 \text{ as } n \to \infty.
\]

Define the distortion function

\[
d(x, y, z, u) = \begin{cases} 0, & \text{if } u = f(x, y, z), \\ 1, & \text{otherwise.} \end{cases}
\]

From a similar argument as in the proof of Proposition \([2]\) we have

\[
d(X, Y, Z, U) \to 0 \text{ as } n \to \infty.
\]

Hence assuming the same distortion for both sources, \((R_X, R_Y) \in R_D(0, 0)\)\(^{12}\) and, according to \([16, \text{Theorem 5.1}]\), there exist random variables \(V\) and \(W\) and a function \(g(V, W, Z)\) such that

\[
\mathbb{E}d(X, Y, Z, g(V, W, Z)) = 0,
\]

\(^{12}\)\(R_D(D_X, D_Y)\) is the rate distortion region for correlated source \(X\) and \(Y\) with distortion criteria \(D_X\) and \(D_Y\), respectively.
\[ V - X - (Y, Z) \]
\[ (X, Z) - Y - W, \]

and
\[ R_X \geq I(X, Y; V|W, Z) \]
\[ R_Y \geq H(X, Y; W|V, Z) \]
\[ R_X + R_Y \geq I(X, Y; V, W|Z). \]

It remains to show that \((V, W)\) satisfy \(H(f(X, Y, Z)|V, W, Z) = 0\).

Since the distortion is equal to 0, for any \((v, x_1, y_1, w, z)\) and \((v, x_2, y_2, w, z)\) that satisfy
\[ p(v, x_1, y_1, w, z) \cdot p(v, x_2, y_2, w, z) > 0, \]
we should have
\[ f(x_1, y_1, z) = g(v, w, z) = f(x_2, y_2, z). \]

This implies that \(H(f(X, Y, Z)|V, W, Z) = 0\) by Lemma 2.

\section*{References}

[1] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger. Network coding for computing: Cut-set bounds. \textit{Information Theory, IEEE Transactions on}, 57(2):1015 –1030, February 2011.

[2] T. Berger and R. W. Yeung. Multiterminal source encoding with one distortion criterion. \textit{Information Theory, IEEE Transactions on}, 35(2):228 –236, March 1989.

[3] P. Cuff, Han-I Su, and A. El Gamal. Cascade multiterminal source coding. In \textit{Information Theory, 2009. ISIT 2009. IEEE International Symposium on}, pages 1199 –1203, 2009.

[4] V. Doshi, D. Shah, M. Médard, and S. Jaggi. Distributed functional compression through graph coloring. In \textit{Proceedings of the Data Compression Conference}, pages 93–102, 2007.

[5] T. S. Han and K. Kobayashi. A dichotomy of functions \(f(x,y)\) of correlated sources \((x,y)\) from the viewpoint of the achievable rate region. \textit{Information Theory, IEEE Transactions on}, 33:69–76, January 1987.

[6] S. Jana and R. Blahut. Canonical description for multiterminal source coding. In \textit{Information Theory, 2008. ISIT 2008. IEEE International Symposium on}, pages 697 –701, July 2008.

[7] J. Körner. Coding of an information source having ambiguous alphabet and the entropy of graphs. In \textit{Transactions, 6th Prague Conference on Information Theory}, 1973.

[8] J. Körner and K. Marton. How to encode the modulo-two sum of binary sources (corresp.). \textit{Information Theory, IEEE Transactions on}, 25(2):219 –221, March 1979.

[9] N. Ma, P. Ishwar, and P. Gupta. Information-theoretic bounds for multiround function computation in collocated networks. In \textit{Proceedings of ISIT - Volume 4}, pages 2306–2310, 2009.
APPENDIX

In this appendix we show random variables $V$ and $W$ that satisfy $H(f(X,Y,Z)|V,W,Z) = 0$, in certain cases, can be characterized as random variables defined over the multiset of independent sets of the (generalized) conditional characteristic graph.

Lemma 2. Let

$$(V,X,Y,W,Z) \in \mathcal{V} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{W} \times \mathcal{Z},$$

be distributed according to $p(v,x,y,w,z)$. The two following statements are equivalent:

a) $H(f(X,Y,Z)|V,W,Z) = 0$.

b) For all

$$(x_1,y_1,z),(x_2,y_2,z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z},$$

$$(v,w) \in \mathcal{V} \times \mathcal{W},$$

that satisfy

$$p(v,x_1,y_1,w,z) \cdot p(v,x_2,y_2,w,z) > 0,$$
we have
\[ f(x_1, y_1, z) = f(x_2, y_2, z). \]

**Proof:** For showing the equivalence notice that \( H(f(X, Y, Z)|V, W, Z) = 0 \) if and only if there exist a function \( g(v, w, z) \) such that
\[ f(X, Y, Z) = g(V, W, Z), \]
which is the same as b.

**Lemma 3.** Given \((X, Y, Z) \sim p(x, y, z)\) and \( f(X, Y, Z), (V, W) \) satisfy
\[ H(f(X, Y, Z)|V, W, Z) = 0, \]
and
\[ V - X - (Y, W, Z) \]
\[ (V, X, Z) - Y - W, \]
if and only if they satisfy
\[ X \in S_X(V) \in M(\Gamma(G_X|Y, Z)) \]
\[ Y \in S_Y(W) \in M(\Gamma(G_Y|S_X(V), Z)), \]
and
\[ S_X(V) - X - (Y, S_Y(W), Z) \]
\[ (S_X(V), X, Z) - Y - S_Y(W). \]

In a special case of above Lemma for \( V = X \) we derive the following lemma.

**Corollary 4.** Given \((X, Y, Z) \sim p(x, y, z)\) and \( f(X, Y, Z), W \) satisfies
\[ H(f(X, Y, Z)|X, W, Z) = 0, \]
and
\[ (X, Z) - Y - W, \]
if and only if
\[ Y \in S_Y(W) \in M(\Gamma(G_Y|X, Z)), \]
and
\[ (X, Z) - Y - S_Y(W). \]
Proof of Lemma 3: The lemma is a direct consequence of the following four claims, proved thereafter:

a. \( X \in S_X(V) \) and \( Y \in S_Y(W) \) always hold.

b. 
\[
\begin{align*}
V &- X - (Y, W, Z) \\
(V, X, Z) &- Y - W,
\end{align*}
\]

if and only if
\[
\begin{align*}
S_X(V) &- X - (Y, S_Y(W), Z) \\
(S_X(V), X, Z) &- Y - S_Y(W).
\end{align*}
\]

Further, when these Markov chains hold, Claims c. and d. below hold:

C. \((V, W)\) satisfy
\[
H(f(X, Y, Z)|V, W, Z) = 0,
\]

if and only if for all \(x_1, x_2 \in S_X(v)\) and \(y_1, y_2 \in S_Y(w)\) such that
\[p(x_1, y_1, z) \cdot p(x_2, y_2, z) > 0,\]

it holds that
\[f(x_1, y_1, z) = f(x_2, y_2, z).\]

d. 
\[
\begin{align*}
S_X(V) &\in M(\Gamma(G_X|Y,Z)) \\
S_Y(W) &\in M(\Gamma(G_Y|S_X(V), Z)),
\end{align*}
\]

if and only if for all \(x_1, x_2 \in S_X(v)\) and \(y_1, y_2 \in S_Y(w)\) that
\[p(x_1, y_1, z) \cdot p(x_2, y_2, z) > 0,\]

it holds that
\[f(x_1, y_1, z) = f(x_2, y_2, z).\]

Claims a. and b. come directly from the Definition 6.

c. Notice that due to the Markov chains
\[
\begin{align*}
V &- X - (Y, W, Z) \\
(V, X, Z) &- Y - W,
\end{align*}
\]
we can write
\[ p(v, x, y, w, z) = p(x, y, z) \cdot p(v|x) \cdot p(w|y). \]

Hence
\[ p(v, x_1, y_1, w, z) \cdot (v, x_2, y_2, w, z) > 0, \]

if and only if
\[ p(x_1, y_1, z) \cdot p(x_2, y_2, z) \cdot p(v, x_1) \cdot p(v, x_2) \cdot p(y_1) \cdot p(y_2) > 0, \]

which is equivalent to constraints
\[ x_1, x_2 \in S_X(v), \]
\[ y_1, y_2 \in S_Y(w), \]
\[ p(x_1, y_1, z) \cdot p(x_2, y_2, z) > 0. \]

Using the Lemma 2 completes the proof of the claim.

d. The proof for converse part is straightforward from the definition of (generalized) conditional characteristic graph.

To prove the direct part, for \( x_1, x_2 \in S_X(v), y_1, y_2 \in S_Y(w) \) such that
\[ p(x_1, y_1, z) \cdot p(x_2, y_2, z) > 0, \]

we show that
\[ f(x_1, y_1, z) = f(x_2, y_2, z). \]

i. If \( y_1 = y_2 \), then since
\[ S_X(v) \in M(\Gamma(G_X|Y,Z)), \]

for \( x_1, x_2 \in S_X(v), f(x_1, y_1, z) = f(x_2, y_2, z) \) (The same argument is valid if \( x_1 = x_2 \).

ii. If \( x_1 \neq x_2, y_1 \neq y_2 \), then from
\[ S_Y(w) \in M(\Gamma(G_Y|S_X(v),Z)), \]

we have\[ f(x_1, y_1, z) = \tilde{f}_X(S_X(v), y_1, z) = \tilde{f}_X(S_X(v), y_2, z) = f(x_2, y_2, z). \]

\[ \tilde{f}_X(v, y, z) \text{ is defined in the same way as } \tilde{f}_Y(x, w, z) \text{ in Definition 5.} \]