Encoding of Functions of Correlated Sources

Saravanan Vijayakumaran

February 1, 2008

Abstract

In this correspondence, we describe the achievable rate region for reliably recovering deterministic functions of correlated sources which have a finite alphabet. The method of proof is almost the same as that used to prove the Slepian-Wolf theorem.

1 Introduction

Consider the problem of recovering a function $F(X,Y)$ of two correlated sources $(X,Y)$ by encoding the sources separately (see Fig. 1). A problem of this class was first considered in [1], where the exact rate region for the modulo-two adder source network was derived. In [2], necessary and sufficient conditions were derived, for the achievable rate region for recovering functions of correlated sources to coincide with the Slepian-Wolf region [3].

In this correspondence, we describe the achievable rate region for reliably recovering deterministic functions of correlated sources which have a finite alphabet. The method of proof is almost the same as that used to prove the Slepian-Wolf theorem [3], [4].

2 System Model

The system model is essentially the same as the one described in [2]. We repeat it here for convenience and notational clarity. Let $X$ and $Y$ be a pair of correlated random variables defined on finite sample spaces $\mathcal{X}$ and $\mathcal{Y}$, respectively. Denote their joint probability distribution by

$$p_{XY}(x,y) = \Pr[X = x, Y = y], \quad x \in \mathcal{X}, y \in \mathcal{Y}. \quad (1)$$

Conforming with the usual convention, we will use uppercase letters to denote random variables and lowercase letters to denote fixed values the random variables may take. Let $(X,Y) = (X^n,Y^n) = ((X_1,Y_1),(X_2,Y_2),\ldots,(X_n,Y_n))$ be a sequence of $n$ independent realizations of the pair of random variables $(X,Y)$. The distribution of $(X,Y)$ is given by

$$p_{XY}(x,y) = \Pr[X = x, Y = y] = \prod_{i=1}^{n} p_{XY}(x_i,y_i), \quad x \in \mathcal{X}^n, y \in \mathcal{Y}^n. \quad (2)$$

The number of coordinates in $(X,Y)$ or $(x,y)$ will be clear from context.

---

*This work was supported in part by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322, and by a University of Florida Alumni Fellowship (2001-2005).

†The author is with the Laboratory for Computer Communications and Applications, Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland.
Let $F : \mathcal{X} \times \mathcal{Y} \mapsto \mathcal{Z}$ be an arbitrary deterministic function. We will denote the sequence $(F(X_1, Y_1), F(X_2, Y_2), \ldots, F(X_n, Y_n))$ by $F(X, Y)$. We will sometimes find it convenient to denote the random variable $F(X, Y)$ by $Z$. Then $Z = Z^n = F(X, Y)$.

The sequence $(X_1, X_2, \ldots)$ is available at node $A$ and the sequence $(Y_1, Y_2, \ldots)$ is available at node $B$. We wish to reliably recover the sequence $(Z_1, Z_2, \ldots)$ at node $C$, under the condition that there is no communication between nodes $A$ and $B$. This situation is illustrated in Fig. 1.

The channels from node $A$ to node $B$ and node $A$ to node $C$ are assumed to be noiseless. So we have a distributed source coding problem where the goal is to simultaneously minimize the required rates $R_1$ and $R_2$, which allow reliable recovery of the sequence $(Z_1, Z_2, \ldots)$ at node $C$.

We now present some definitions similar to ones presented in [4, Section 14.4].

**Definition:** A distributed source code $C_n(F)$ for the random variable $F(X, Y)$ is a triplet of functions $(f_1, f_2, g)$,

\[
\begin{align*}
  f_1 & : \mathcal{X}^n \mapsto \{1, 2, \ldots, 2^{nR_1}\} \\
  f_2 & : \mathcal{Y}^n \mapsto \{1, 2, \ldots, 2^{nR_2}\} \\
  g & : \{1, 2, \ldots, 2^{nR_1}\} \times \{1, 2, \ldots, 2^{nR_2}\} \mapsto \mathcal{X}^n
\end{align*}
\]

where $f_1, f_2$ correspond to the encoding functions and $g$ corresponds to the decoding function. Here $R_1, R_2$ are nonnegative real numbers and $n$ is a positive integer.

**Definition:** For a particular distributed source code $C_n(F)$, the probability of error is defined as

\[
P^{(n)}_e = \Pr[g(f_1(X), f_2(Y)) \neq F(X, Y)]. \tag{3}
\]

**Definition:** A rate pair $(R_1, R_2)$ is said to be achievable for a function $F$ if there exists a sequence of distributed source codes $\{C_n(F) : n \in \mathbb{N}\}$ with corresponding probabilities of error $P^{(n)}_e$ such that $P^{(n)}_e \to 0$ as $n \to \infty$.

**Definition:** For a particular function $F$, the achievable rate region $\mathcal{R}(F)$ is the closure of the set of all achievable rate pairs.

### 3 Main Result

The following is the main result of this correspondence.
Theorem: The achievable rate region for a function $F$ of correlated random variables $(X,Y)$ is given by

$$\mathcal{R}(F) = \{(R_1, R_2) : R_1 \geq H(F(X,Y)|Y), R_2 \geq H(F(X,Y)|X), R_1 + R_2 \geq H(F(X,Y))\}.$$ 

The proof of this result is a simple application of the techniques used to prove the Slepian-Wolf theorem in [H]. So we shamelessly adopt the conventions and notation in [H Chapter 14], if not for any other reason but to illustrate the simplicity of the proof. We need to borrow the following notation\(^1\) before we proceed with the proof.

Let $(U_1, U_2, \ldots, U_k)$ be a finite collection of discrete random variables with a fixed joint distribution, $p(u_1, u_2, \ldots, u_n), (u_1, u_2, \ldots, u_n) \in \mathcal{U}_1 \times \mathcal{U}_2 \times \cdots \times \mathcal{U}_k$. The set of $\epsilon$-typical $n$-sequences will be denoted by $A(J)(U_1, U_2, \ldots, U_k)$. We will denote the set of $U_i$ $n$-sequences that are jointly $\epsilon$-typical with a particular $U_j$ $n$-sequence, $u_j$, by $A(J)(U_i|u_j)$.

Proof of Achievability: For each $x \in \mathcal{X}^n$, set $f_1(x)$ to a value chosen from the set \(\{1, 2, \ldots, 2^{nR_1}\}\) according to a uniform distribution. Similarly, for each $y \in \mathcal{Y}^n$ set $f_2(y)$ to a value chosen from the set \(\{1, 2, \ldots, 2^{nR_2}\}\) according to a uniform distribution. The encoding functions are revealed to the corresponding encoder and the decoder, i.e., the decoder needs to know both $f_1$ and $f_2$ while encoder $i$ needs to know only $f_i$, $i = 1, 2$.

The encoding operation consists of encoder 1 and encoder 2 sending the values of $f_1(X)$ and $f_2(Y)$, respectively, to the decoder. Given the encoder outputs $(f_1(X), f_2(Y)) = (i_0, j_0)$, the decoder outputs its estimate of $F(X, Y)$, $\hat{Z}$, to be $z$ if there exists a unique sequence $x, \hat{x}, y, \hat{y} \in A(J)(Z, X, Y)$ such that $(x, y, \hat{x}, \hat{y}) \in A(J)(Z, X, Y)$ for some $(x, y) \in \mathcal{X}^n \times \mathcal{Y}^n$ such that $f_1(x) = i_0$ and $f_2(y) = j_0$. Note that the pair $(x, y)$ need not be unique.

The decoder operation is where the current coding scheme differs from Slepian-Wolf coding scheme. Of course, if $F$ is the identity function, i.e., $F(x, y) = (x, y), \forall (x, y) \in \mathcal{X} \times \mathcal{Y}$, then the above decoder coincides with the decoder in the Slepian-Wolf coding scheme.

We now proceed with the analysis of the probability of error averaged over all possible encoder choices $f_1, f_2$. Let $E = \{\hat{Z} \neq Z\}$ denote the decoding error event. Then we have $E = E_0 \cup E_1 \cup E_2 \cup E_{12}$ where

$$E_0 = \left\{ \exists \text{ no } z \in \mathcal{Z}^n : (z, x', y') \in A(J)(Z, X, Y) \text{ for some } (x', y') \ni f_1(x') = f_1(x), f_1(y') = f_1(y) \right\},$$

$$E_1 = \left\{ \exists z \in \mathcal{Z}^n : (z, x', y) \in A(J)(Z, X, Y) \text{ for some } x' \ni f_1(x') = f_1(x), z = F(x', Y), z \neq F(X, Y) \right\},$$

$$E_2 = \left\{ \exists z \in \mathcal{Z}^n : (z, x, y') \in A(J)(Z, X, Y) \text{ for some } y' \ni f_1(y') = f_1(y), z = F(X, y'), z \neq F(X, Y) \right\},$$

$$E_{12} = \left\{ \exists z \in \mathcal{Z}^n : (z, x', y') \in A(J)(Z, X, Y) \text{ for some } (x', y') \ni f_1(x') = f_1(x), f_1(y') = f_1(y), z = F(x', y') \neq F(X, Y) \right\}.$$

From the definition of jointly typical sequences, it is easy to see that

$$\Pr[E_0] \leq \Pr((z, x', y') \in \mathcal{Z}^n \times \mathcal{X}^n \times \mathcal{Z}^n : (z, x', y') \notin A(J)(Z, X, Y)) < \epsilon, \quad (4)$$

\(^1\)See [H Section 14.2] for definitions and properties.
for sufficiently large $n$. We bound $\Pr[E_1]$ in the following manner.

$$
\Pr[E_1] = \Pr[\exists z \in \mathcal{X}^n : (z, x', y) \in A^{(n)}(Z, X, Y) \text{ for some } x' \ni f_1(x') = f_1(X), z = F(x', Y) \neq F(X, Y)]
$$

(a) $\leq \Pr[\exists z \in \mathcal{X}^n : (z, x, y) \in A^{(n)}(Z, Y), \text{ for some } x' \ni f_1(x') = f_1(X), z = F(x', y) \neq F(X, y)]$

$$
= \sum_{x, y} p_{XY}(x, y) \Pr[\exists z \in \mathcal{X}^n : (z, y) \in A^{(n)}(Z, Y) \text{ for some } x' \ni f_1(x') = f_1(x), z = F(x', y) \neq F(x, y)]
$$

(b) $\leq \sum_{x, y} p_{XY}(x, y) \Pr[(z, y) \in A^{(n)}(Z, Y) : \text{For some } x' \neq x, f_1(x') = f_1(x)]$

$$
\leq 2^{-nR_1} 2^{n(H(Z|Y) + 2\epsilon)},
$$

where

(a) follows from the fact that for any $(z, x', y) \in \mathcal{X}^n \times \mathcal{X}^n \times \mathcal{Y}^n$, $(z, x', y) \in A^{(n)}(Z, X, Y) \Rightarrow (z, y) \in A^{(n)}(Z, Y)$,

(b) follows from the fact that we are averaging over all possible encoder choices for $f_1$ and the property that for a fixed $y \in \mathcal{Y}^n$, $|\{(z, y) \in A^{(n)}(Z, Y)\}| = |A^{(n)}(Z|y)|$.

(c) follows from the fact that $|A^{(n)}(Z|y)| \leq 2^{n(H(Z|Y) + 2\epsilon)}$ [Theorem 14.2.2].

The final bound on $\Pr[E_1]$ tends to zero as $n \to \infty$ if $R_1 > H(Z|Y) + 2\epsilon$. Thus for sufficiently large $n$, $\Pr[E_1] < \epsilon$. Similarly, we can show that $\Pr[E_2] < \epsilon$ for sufficiently large $n$ if $R_2 > H(Z|X) + 2\epsilon$.

Note that $E_1 \subset E_{12}$ and $E_2 \subset E_{12}$. It then follows that $E = E_0 \cup E_1 \cup E_2 \cup E_{12} = E_0 \cup E_1 \cup E_2 \cup (E_{12} \cap E_1 \cap E_2)$. We will find it easier to bound $E_{12} \cap E_1 \cap E_2$ rather than bound $E_{12}$ directly. We bound $\Pr[E_{12} \cap E_1 \cap E_2]$ in the following manner.

$$
\Pr[E_{12} \cap E_1 \cap E_2] = \Pr[\exists z \in \mathcal{X}^n : (z, x', y') \in A^{(n)}(Z, X, Y) \text{ for some } x' \neq X, y' \neq Y \ni f_1(x') = f_1(X), f_2(y') = f_2(Y), z = F(x', y') \neq F(X, Y)]
$$

(a) $\leq \Pr[\exists z \in \mathcal{X}^n : z \in A^{(n)}(Z) \text{ for some } x' \neq X, y' \neq Y \ni f_1(x') = f_1(X), f_2(y') = f_2(Y), z = F(x', y') \neq F(X, Y)]$

$$
= \sum_{x, y} p_{XY}(x, y) \Pr[\exists z \in \mathcal{X}^n : z \in A^{(n)}(Z) \text{ for some } x' \neq x, y' \neq y \ni f_1(x') = f_1(x), f_2(y') = f_2(y), z = F(x', y') \neq F(x, y)]
$$

(b) $\leq \sum_{x, y} p_{XY}(x, y) \Pr[z \in A^{(n)}(Z) : \text{For some } x' \neq x, y' \neq y, f_1(x') = f_1(x), f_2(y') = f_2(y)]$

$$
\leq 2^{-nR_1 - nR_2} 2^{nH(Z)} \leq 2^{-n(R_1 + R_2 + \epsilon)},
$$

where
(a) follows from the fact that for any \((z, x', y') \in \mathcal{Z}^n \times \mathcal{X}^n \times \mathcal{Y}^n\), \((z, x', y') \in A^{(n)}(Z, X, Y) \Rightarrow z \in A^{(n)}(Z)\).

(b) follows from the fact that we are averaging over all possible encoder choices \(f_1, f_2\) and from the definition of \(A^{(n)}(Z)\).

(c) follows from the fact that \(|A^{(n)}(Z)| \leq 2^n \log (\mathbb{E} + \epsilon)\).

The final bound on \(\Pr[E_1 \cap E_2] \leq 4\epsilon\) can be made smaller than \(\epsilon\) for sufficiently large \(n\) if \(R_1 + R_2 > H(Z) + \epsilon\).

Thus, we have \(\Pr[E] \leq \Pr[E_0] + \Pr[E_1] + \Pr[E_2] + \Pr[E_{12} \cap E_1^c \cap E_2^c] < 4\epsilon\) for sufficiently large \(n\). Since the probability of error averaged over all codes is less than \(4\epsilon\), there exists at least one code \(\mathcal{C}^{(n)}(F)\) for which the average probability of error is less than \(4\epsilon\). Since \(\epsilon\) was arbitrary, we can construct a sequence of codes such that \(P_e^{(n)} \to 0\) as \(n \to \infty\). The arbitrary choice of \(\epsilon\) also implies that any rate pair \((R_1, R_2)\) satisfying \(R_1 > H(F(X, Y)|Y), R_2 > H(F(X, Y)|X), R_1 + R_2 > H(F(X, Y))\) is achievable. Since the achievable rate region is the closure of all achievable rates, we have

\[
\mathcal{A}(F) \supset \{(R_1, R_2) : R_1 \geq H(F(X, Y)|Y), R_2 \geq H(F(X, Y)|X), R_1 + R_2 \geq H(F(X, Y))\}.
\]

This completes the proof of the achievability.

\textbf{Proof of Converse:} This proof is once again very similar to the proof of the converse to the Slepian-Wolf theorem [4, Section 14.4.2].

Let \((R_1, R_2)\) be an achievable rate pair. By definition, there exists a sequence of distributed source codes \(\{\mathcal{C}_n(F) : n \in \mathbb{N}\}\) and hence a sequence of function triplets \(\{(f_1^{(n)}, f_2^{(n)}, g^{(n)}) : n \in \mathbb{N}\}\), with \(P_e^{(n)} = \Pr[g(f_1(X), f_2(Y)) \neq F(X, Y)]\) such that \(P_e^{(n)} \to 0\) as \(n \to \infty\).

For notational convenience, define \(I_0^{(n)} = f_1^{(n)}(X)\) and \(J_0^{(n)} = f_2^{(n)}(Y)\). By Fano’s inequality, we have

\[
H(F(X, Y)|I_0^{(n)}, J_0^{(n)}) \leq P_e^{(n)} \log |\mathcal{Z}^n| + 1 = P_e^{(n)} n \log |\mathcal{Z}| + 1 = n \delta_n, \tag{5}
\]

where \(\delta_n = P_e^{(n)} \log |\mathcal{Z}|\). We know that \(\delta_n \to 0\) as \(n \to \infty\). Since conditioning reduces entropy, we also have

\[
H(F(X, Y)|Y, I_0^{(n)}, J_0^{(n)}) \leq n \delta_n, \tag{6}
\]

\[
H(F(X, Y)|X, I_0^{(n)}, J_0^{(n)}) \leq n \delta_n. \tag{7}
\]

Following the notation in [4], we will write \(U \to V \to W\) for some random variables \(U, V, W\) to mean that \(U\) and \(W\) are conditionally independent given \(V\). For the problem under consideration, we have the following relations,

\[
(I_0^{(n)}, J_0^{(n)}) \to (X, Y) \to F(X, Y), \quad I_0^{(n)} \to (X, Y) \to (F(X, Y), Y), \quad J_0^{(n)} \to (X, Y) \to (F(X, Y), X).
\]

Application of the data processing inequality to each of the above relations and simple manipulations yield the following respective inequalities.

\[
H(I_0^{(n)}, J_0^{(n)}|X, Y) \leq H(I_0^{(n)}, J_0^{(n)}|F(X, Y)) \tag{8}
\]

\[
H(I_0^{(n)}|X, Y) \leq H(I_0^{(n)}|F(X, Y), Y) \tag{9}
\]

\[
H(J_0^{(n)}|X, Y) \leq H(J_0^{(n)}|F(X, Y), X) \tag{10}
\]
Then we have a chain of inequalities

\[
\begin{align*}
n(R_1 + R_2) & \geq H(I_0^{(n)}, J_0^{(n)}) = I(F(X, Y); I_0^{(n)}, J_0^{(n)}) + H(I_0^{(n)}, J_0^{(n)}|F(X, Y)) \\
& \geq I(F(X, Y); I_0^{(n)}, J_0^{(n)}) + H(I_0^{(n)}, J_0^{(n)}|X, Y) \\
& = H(F(X, Y)) - H(F(X, Y)|I_0^{(n)}, J_0^{(n)}) \\
& \geq nH(F(X, Y)) - n\delta_n,
\end{align*}
\]

where

(a) follows from \ref{eq:chain_rule},
(b) follows from the fact that \((I_0^{(n)}, J_0^{(n)})\) is a function of \((X, Y),
(c) follows from the chain rule and the fact that \(F(X, Y)\) consists of i.i.d. components, and from \ref{eq:referee_7}.

Similarly, we can write

\[
\begin{align*}
nR_1 & \geq H(I_0^{(n)}) \geq H(I_0^{(n)}|Y) \\
& = I(F(X, Y); I_0^{(n)}|Y) + H(I_0^{(n)}|F(X, Y), Y) \\
& \geq I(F(X, Y); I_0^{(n)}|Y) + H(I_0^{(n)}|X, Y) \\
& = H(F(X, Y)|Y)) - H(F(X, Y)|Y, I_0^{(n)}, J_0^{(n)}) \\
& \geq nH(F(X, Y)|Y) - n\delta_n,
\end{align*}
\]

where

(a) follows from \ref{eq:referee_7},
(b) follows from the fact that \(I_0^{(n)}\) is a function of \(X,
(c) follows from the chain rule and the fact that \(H(F(X, Y)|Y) = H(F(X, Y)|Y)\) for \(i = 1, 2, \ldots, n,\) and from \ref{eq:referee_7}.

Using similar techniques, we also get \(nR_2 \geq nH(F(X, Y)|X) - n\delta_n\) by using \ref{eq:referee_7} and \ref{eq:referee_7}.

Thus, for any \(n\), we have \(R_1 \geq H(F(X, Y)|Y) - \delta_n, R_2 \geq H(F(X, Y)|X) - \delta_n\) and \(R_1 + R_2 \geq H(F(X, Y)) - \delta_n\). Since \(\delta_n \to 0\) as \(n \to \infty\), we have that any rate pair is achievable only if \(R_1 \geq H(F(X, Y)|Y), R_2 \geq H(F(X, Y)|X)\) and \(R_1 + R_2 \geq H(F(X, Y))\). Thus,

\[\mathcal{B}(F) \subset \{(R_1, R_2) : R_1 \geq H(F(X, Y)|Y), R_2 \geq H(F(X, Y)|X), R_1 + R_2 \geq H(F(X, Y))\} .\]

This completes the proof of the converse.

\section{Concluding Remarks}

We have found the exact achievable rate region for the problem of reliably recovering a function of correlated sources by separate encoding of the sources. The proof turns out to be a simple plug-and-play of the techniques in \ref{eq:referee_7}. It is obvious that the achievable rate region found here reduces to the Slepian-Wolf region when \(F\) is the identity function. Although less obvious, it is not difficult to see that the result derived in this correspondence conforms with the results of \ref{eq:referee_7}, \ref{eq:referee_7}.
References

[1] J. Körner and K. Marton, “How to encode the modulo-two sum of binary sources,” *IEEE Trans. Inform. Theory*, vol. 25, pp. 219–221, Mar 1979.

[2] 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,” *IEEE Trans. Inform. Theory*, vol. 33, Jan 1987.

[3] D. Slepian and J. K. Wolf, “Noiseless coding of correlated information sources,” *IEEE Trans. Inform. Theory*, vol. 19, pp. 471–480, July 1973.

[4] T. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.