STRONG CONVERSE FOR GEL'FAND-PINSKER CHANNEL

Pierre Moulin

Beckman Inst., Coord. Sci. Lab and ECE Department
University of Illinois at Urbana-Champaign, USA

ABSTRACT

A strong converse for the Gel'fand-Pinsker channel is established in this paper. The method is then extended to a multiuser scenario. A strong converse is established for the multiple-access Gel'fand-Pinsker channel under the maximum error criterion, and the capacity region is determined.

1. INTRODUCTION

The Gel'fand-Pinsker (GP) channel [1] and its variants have attracted considerable interest in the information theory literature. Applications include coding in the presence of a known interference at the transmitter, and watermarking [2]. This paper derives a strong converse for the GP channel. In addition to strengthening the classical weak converse [1], the derivation provides new insights into the problem and in particular into the role of the auxiliary random variable. These insights are particularly useful for the multiple-access version of the GP channel, for which an outer rate region can be derived using a weak converse based on Fano's inequality, but that region does not coincide with the achievable region identified in [3]. We prove that in fact the maximum error probability tends to 1 for any rate pair outside the region of [3], thereby determining the capacity region of the multiple-access GP channel. The proof does not require the wringing methods of [4] that were used to prove the strong converse for the multiple-access channel without side information (SI) under the average error criterion. Also note that: (i) according to Ahlswede [5, 6], the maximum error criterion is more natural in multiuser communications than the average error criterion because the latter guarantees a small error probability only if the users choose their message with uniform probability; and (ii) capacity regions under the max error criterion are generally smaller than capacity regions under the average error criterion [6]. These capacity regions coincide if stochastic encoders are allowed [7, pp. 284,285]. This holds *a fortiori* if common randomness between encoders and receiver is allowed.

2. GEL'FAND-PINSKER CHANNEL

Consider the GP channel $p(y|x,s)$ with input alphabet $\mathcal{X}$, output alphabet $\mathcal{Y}$, and channel state $S \in \mathcal{S}$ distributed according to a pmf p_S [1]. A message M drawn uniformly from $\mathcal{M}_N \triangleq \{1, \cdots, 2^{NR}\}$ is to be sent over the channel using a length-N code. The channel state sequence $\mathbf{S} = (S_1, \cdots, S_N) \in \mathcal{S}^N$ is iid p_S, independent of M, and available to the encoder. The transmitted sequence is denoted by $f_N(M, \mathbf{S}) \in \mathcal{X}^N$ and the decoding rule by $g_N(\mathbf{Y}) \in \mathcal{M}_N$. Gel'fand and Pinsker established the capacity formula

$$C = \max_{p_{XU|S}} [I(U;Y) - I(U;S)] \tag{1}$$

where U is an auxiliary random variable taking values in an alphabet $\mathcal{U}$ of cardinality $|\mathcal{U}| \leq |\mathcal{S}|\,|\mathcal{X}|+1$, and $U \to (S,X) \to Y$ forms a Markov chain. The maximum over $p_{X|US}$ is achieved by a deterministic pmf: $p_{X|US} = \mathbb{1}\{X = f(U,S)\}$ for some function $f : \mathcal{U} \times \mathcal{S} \to \mathcal{X}$.

The direct part of the theorem was proven using a random binning technique, where an arbitrarily small number $\epsilon > 0$ is chosen, and codewords $\mathbf{u}(l,m)$, $1 \leq l \leq 2^{N[I(U;S)+\epsilon]}$, $1 \leq m \leq 2^{NR}$ are drawn iid from the marginal p_U associated with the capacity-achieving distribution $p_{XU|S}$, and a "virtual memoryless channel" $p_{Y|U}$ is created from U to Y. The transmitted sequence is given by $x_t = f(u_t(m,\mathbf{s}), s_t)$ for $t = 1, \cdots, N$. Decoding of the codeword $\mathbf{u}(l,m)$ selected by the encoder is successful if $I(U;S) + R \leq I(U;Y) - 2\epsilon$.

The (weak) converse part of the theorem was proved using a telescoping formula. In this derivation, $U = (M, S_{T+1}^N, Y_1^{T-1}, T)$ (where T is a time-sharing random variable) does not admit an obvious coding interpretation since $\mathbf{Y}$ is not available at the encoder.

In this paper, we establish a strong converse. The notion of a virtual channel $p_{Y|U}$ appears clearly in this derivation, and the construction of U does not involve feedback from the decoder. The source and channel coding aspects of the problem arise from the tension between providing the decoder with information about $\mathbf{S}$ and M, respectively, and are also apparent in the derivation. Our main result is stated below.

Theorem 2.1 *Assume that* $H(S) > 0$ *and* $\min_{y,x,s} p_{Y|XS}(y|x,s) > 0$. *For any sequence of length-*N *codes* (f_N, g_N) *with rate* $R > C$, *the average error probability* $P_e(f_N, g_N)$ *for the GP channel tends to 1 as* $N \to \infty$.

Extended sketch of the proof. Assume without loss of generality (wlog) that $\min_s p_S(s) \geq \epsilon$ and $\min_{y,x,s} p_{Y|XS}(y|x,s) \geq$

ϵ, for some arbitrarily small $\epsilon > 0$.

Step 1. Assume wlog that the codewords are given by the following two-step procedure:

- An alphabet $\mathcal{U}$ of arbitrarily large cardinality, a function $f : \mathcal{U} \times \mathcal{S} \to \mathcal{X}$, and a codebook with codewords $\mathbf{u}(m, \mathbf{s}) \in \mathcal{V}^N$ are defined;
- Each channel input symbol is obtained as

$$x_t = f(u_t(m, \mathbf{s}), s_t), \quad 1 \le t \le N.$$

Since this construction contains the choice

$$\mathcal{U} = \mathcal{X}, \quad \mathbf{u}(m, \mathbf{s}) \equiv \mathbf{x}(m, \mathbf{s}), \quad f(x, s) = x$$

as a special case, there is no loss of generality in making the above assumption. Moreover, it can be shown that capacity is not reduced if, instead of $\mathbf{S}$, a slightly degraded version of $\mathbf{S}$ is available to the encoder (output of an R/D code with vanishing Hamming distortion for each $m \in \mathcal{M}_N$) and so we may restrict our attention to codes that satisfy property (P1) below. Such codes may be thought of as including an elementary amount of binning, since for each m, many (albeit not necessarily exponentially many) sequences $\mathbf{s}$ map to the same codeword $\mathbf{u}(m, \mathbf{s})$.

Let $d_H(\mathbf{s}, \mathbf{s}')$ denote Hamming distance between two sequences $\mathbf{s}$ and $\mathbf{s}'$ and Ω the set of pairs $(m, \mathbf{s})$ such that

$$\mathbf{u}(m, \mathbf{s}) = \mathbf{u}(m, \mathbf{s}'), \quad \forall \mathbf{s}' : d_H(\mathbf{s}, \mathbf{s}') \le 1. \tag{2}$$

In other words, given m, arbitrarily changing any one sample s_t of the sequence $\mathbf{s}$ does not change the value of the codeword $\mathbf{u}(m, \mathbf{s})$. Denote by $\Sigma(m) \triangleq \{\mathbf{s} : (m, \mathbf{s}) \in \Omega\}$ the sections of Ω along the m direction. Also denote by $p_{\mathbf{s}}$ the type of the sequence $\mathbf{s}$ (and empirical pmf over $\mathcal{S}$), by $\mathcal{T}_\epsilon = \{\mathbf{s} : \max_{s \in \mathcal{S}} |p_{\mathbf{s}}(s) - p_S(s)| \le \epsilon\}$ the strong ϵ-typical set, and by $\Sigma_\epsilon(m) \triangleq \Sigma(m) \cap \mathcal{T}_\epsilon$ its intersection with $\Sigma(m)$.

(P1). For each $m \in \mathcal{M}_N$, the set $\Sigma_\epsilon(m)$ has probability

$$P_S^N(\Sigma_\epsilon(m)) \ge 1 - o(1). \tag{3}$$

Step 2. Define the random variables $U_t = u_t(M, \mathbf{S}) \in \mathcal{U}$ and $Q_t = \{S_j,\, j \ne t\} \in \mathcal{S}^{N-1}$ (note Q_t is independent of S_t) for $1 \le t \le N$. The equivalence relation $\mathbf{s} = (s_t, q_t)$ holds for each $1 \le t \le N$. Let T be a time-sharing random variable uniformly distributed over $\{1, 2, \cdots, N\}$ and independent of all other random variables. Let $S = S_T$, $Q = Q_T$, $X = X_T$, $U = U_T$, and $Y = Y_T$. For each $1 \le t \le N$, the joint pmf of $(\mathbf{S}, M, U_t, X_t, Y_t)$ is given by

$$\begin{aligned} p(\mathbf{s}, m, u_t, x_t, y_t) &= p_S^N(\mathbf{s})\, p_M(m)\, \mathbb{1}\{u_t = \mathbf{u}(m, \mathbf{s})\} \\ &\quad \times \mathbb{1}\{x_t = f(u_t, s_t)\}\, p_{Y|XS}(y_t|x_t, s_t). \end{aligned}$$

Hence the joint pmf of (T, S, Q, U, X, Y) is $p_T\, p_S\, p_Q\, p_{U|SQT}\, \mathbb{1}\{X = f(V, S)\}\, p_{Y|XS}$. Note that $V \to (S, X) \to Y$ forms a Markov chain. The distribution of $\mathbf{Y}$ given $m, \mathbf{s}$ is the product pmf $p_{Y|US}^N(\mathbf{y}|\mathbf{u}(m, \mathbf{s}), \mathbf{s})$. Denote by $\mathcal{D}_m$ the decoding region for message m, i.e.,

$$\mathbf{y} \in \mathcal{D}_m \quad \Leftrightarrow \quad g_N(\mathbf{y}) = m, \quad m \in \mathcal{M}_N.$$

The decoding regions form a partition of $\mathcal{Y}^N$. The probability of *correct decoding* of message $m \in \mathcal{M}_N$ is given by

$$\begin{aligned} P_c(f_N, g_N, m) &= Pr[g_N(\mathbf{Y}) = m] \\ &= \sum_{\mathbf{y} \in \mathcal{D}_m} \sum_{\mathbf{s} \in \mathcal{S}^N} p_S^N(\mathbf{s})\, p_{Y|US}^N(\mathbf{y}|\mathbf{u}(m, \mathbf{s}), \mathbf{s}). \end{aligned} \tag{4}$$

The average probability of correct decoding is given by

$$P_c(f_N, g_N) = 2^{-NR} \sum_{m \in \mathcal{M}_N} P_c(f_N, g_N, m).$$

Step 3. For each $m \in \mathcal{M}_N$ and $\mathbf{s} \in \mathcal{S}^N$, denote by $\lambda = \lambda(m, \mathbf{s}) \in \mathscr{P}_{U|S}^{[N]}$ the conditional type of $\mathbf{u}(m, \mathbf{s})$ given $\mathbf{s}$ (empirical conditional pmf, implicitly dependent on $(m, \mathbf{s})$). The quadruple $(p_S, \lambda, f, p_{Y|XS})$ induces a joint pmf on $\mathcal{S} \times \mathcal{U} \times \mathcal{X} \times \mathcal{Y}$:

$$\lambda_{SUXY}(s, u, x, y) = p_S(s)\, \lambda(u|s)\, \mathbb{1}\{X = f(V, S)\}\, p_{Y|XS}(y|x, s).$$

Thus $U \to (X, S) \to Y$ forms a Markov chain for each λ, f. We denote by $\lambda_Y, \lambda_{S|U}$, etc. the various marginals and conditional marginals associated with λ_{SUXY} and therefore induced by (λ, f). Consider the conditional mutual informations

$$\begin{aligned} I_\lambda(U; S) &= \sum_{s,u} p_S(s)\, \lambda(u|s)\, \log \frac{\lambda_{S|U}(s|u)}{p_S(s)} \\ I_{\lambda,f}(U; Y) &= \sum_{s,u,y} p_S(s)\, \lambda_{YU|S}(y, u|s)\, \log \frac{\lambda_{Y|U}(y|u)}{\lambda_Y(y)} \end{aligned}$$

which will be viewed as functions of λ and f. Also define the empirical conditional self-informations

$$\hat{I}_\lambda(U; S) = \alpha(m, \mathbf{s}) \triangleq \frac{1}{N} \sum_{t=1}^N \log \frac{\lambda_{S|U}(s_t|u_t(m, \mathbf{s}))}{p_S(s_t)}, \tag{5}$$

$$\hat{I}_\lambda(U; Y) = \hat{\beta}(m, \mathbf{s}, \mathbf{y}) \triangleq \frac{1}{N} \sum_{t=1}^N \log \frac{\lambda_{Y|U}(y_t|u_t(m, \mathbf{s}))}{\lambda_Y(y_t)},$$

$$\begin{aligned} \check{I}_{\lambda,f}(U; Y) = \beta(m, \mathbf{s}) &\triangleq \frac{1}{N} \sum_{t=1}^N \sum_{y_t \in \mathcal{Y}} p_{Y|US}(y_t|u_t(m, \mathbf{s}), s_t) \\ &\quad \times \log \frac{\lambda_{Y|U}(y_t|u_t(m, \mathbf{s}))}{\lambda_Y(y_t)} \\ &= \mathbb{E}_{\mathbf{Y}|M,\mathbf{S}}\, [\hat{\beta}(m, \mathbf{s}, \mathbf{Y})]. \end{aligned} \tag{6}$$

These quantities do not coincide with $I_\lambda(U; S)$ and $I_{\lambda,f}(U; Y)$ because the type of $\mathbf{s}$ does not coincide with p_S in general.

However for strongly typical $\mathbf{s} \in \mathcal{T}_\epsilon$ we have

$$\begin{aligned} |\hat{I}_\lambda(U;S) - I_\lambda(U;S)| &\leq \epsilon \log|\mathcal{S}| \\ |\breve{I}_{\lambda,f}(U;Y) - I_{\lambda,f}(U;Y)| &\leq \epsilon \log|\mathcal{Y}|. \end{aligned} \quad (7)$$

Also the following inequality holds for all $(m,\mathbf{s}) \in \Omega$ and $\mathbf{s}'$ differing from $\mathbf{s}$ in position t:

$$\max_{s_t' \in \mathcal{S}} [-\alpha(m,\mathbf{s}')] \leq \min_{s_t' \in \mathcal{S}} [-\alpha(m,\mathbf{s})] + \frac{2\log 2/\epsilon}{N}. \quad (8)$$

Step 4. Define the following subsets of $\mathcal{Y}^N$, indexed by $m, \mathbf{s}$:

$$\mathcal{B}_\epsilon(m,\mathbf{s}) \triangleq \left\{ \mathbf{y} : \hat{\beta}(m,\mathbf{s},\mathbf{y}) \leq \beta(m,\mathbf{s}) + \epsilon \right\} \quad (9)$$

For all $m \in \mathcal{M}_N$, $\mathbf{s} \in \mathcal{S}^N$, the probability

$$Pr[\mathbf{Y} \notin \mathcal{B}_\epsilon(m,\mathbf{s}) \,|\, M = m, \mathbf{S} = \mathbf{s}] \leq \frac{\log^2 \epsilon}{N\epsilon^2} \quad (10)$$

vanishes as $N \to \infty$. This follows from Chebyshev's inequality and the fact that $Y_t, 1 \leq t \leq N$, are conditionally independent given $(m,\mathbf{s})$.

Step 5. The probability of correct decoding for m may be upper-bounded as

$$\begin{aligned} P_c(f_N, g_N, m) &\leq Pr[\mathbf{Y} \notin \mathcal{B}_\epsilon(m,\mathbf{S}) \,|\, M = m] \\ &\quad + Pr[\mathbf{S} \notin \Sigma_\epsilon(m)] + \underline{P}_c(f_N, g_N, m) \end{aligned} \quad (11)$$

where the first two terms in the right side were upper-bounded in (3) and (10) respectively, and

$$\begin{aligned} &\underline{P}_c(f_N, g_N, m) \\ &\triangleq Pr[g_N(\mathbf{Y}) = m\,, \mathbf{S} \in \Sigma_\epsilon(m),\ \mathbf{Y} \in \mathcal{B}_\epsilon(m,\mathbf{S}) \,|\, M = m] \\ &= \sum_{\mathbf{s} \in \Sigma_\epsilon(m)} \sum_{\mathbf{y} \in \mathcal{D}_m \cap \mathcal{B}_\epsilon(m,\mathbf{s})} p_S^N(\mathbf{s})\, p_{Y|US}^N(\mathbf{y}|\mathbf{u}(m,\mathbf{s}),\mathbf{s}). \end{aligned} \quad (12)$$

Define the disjoint events

$$\mathcal{E}(m,\lambda) \triangleq \{\mathbf{S} \in \Sigma_\epsilon(m),\ \lambda(m,\mathbf{S}) = \lambda,\ \mathbf{Y} \in \mathcal{D}_m \cap \mathcal{B}_\epsilon(m,\mathbf{S})\}$$

for all $m \in \mathcal{M}_N$ and $\lambda \in \mathscr{P}_{U|S}^{[N]}$, and write (12) as

$$\begin{aligned} &\underline{P}_c(f_N, g_N, m) \\ &= \sum_\lambda \sum_{\mathbf{s} \in \mathcal{S}^N} \sum_{\mathbf{y} \in \mathcal{Y}^N} p_S^N(\mathbf{s})\, p_{Y|US}^N(\mathbf{y}|\mathbf{u}(m,\mathbf{s}),\mathbf{s})\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &\overset{(a)}{=} \sum_\lambda \sum_{\mathbf{s} \in \mathcal{S}^N} \sum_{\mathbf{y} \in \mathcal{Y}^N} 2^{-N\alpha(m,\mathbf{s})}\, \lambda_{S|U}^N(\mathbf{s}|\mathbf{u}(m,\mathbf{s})) \\ &\qquad \times p_{Y|US}^N(\mathbf{y}|\mathbf{u}(m,\mathbf{s}),\mathbf{s})\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &= \sum_\lambda \sum_{\mathbf{y} \in \mathcal{Y}^N} \prod_{t=1}^N \sum_{s_t \in \mathcal{S}} 2^{-\alpha(m,\mathbf{s})}\, \lambda_{S|U}(s_t|u_t(m,\mathbf{s})) \\ &\qquad \times p_{Y|US}(y_t|u_t(m,\mathbf{s}),s_t)\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &\overset{(b)}{\leq} \sum_\lambda \sum_{\mathbf{y} \in \mathcal{Y}^N} \prod_{t=1}^N \sum_{s_t \in \mathcal{S}} 2^{-\alpha(m,\mathbf{s}) + \frac{2\log 2/\epsilon}{N}}\, w(s_t|y_t) \\ &\qquad \times \lambda_{Y|U}(y_t|u_t(m,\mathbf{s}))\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &= \frac{16}{\epsilon^4} \sum_\lambda \sum_{\mathbf{y} \in \mathcal{Y}^N} \sum_{\mathbf{s} \in \mathcal{S}^N} 2^{-N\alpha(m,\mathbf{s})} w^N(\mathbf{s}|\mathbf{y}) \\ &\qquad \times \lambda_{Y|U}^N(\mathbf{y}|\mathbf{u}(m,\mathbf{s}))\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &\overset{(c)}{\leq} \frac{16}{\epsilon^4} \sum_\lambda \sum_{\mathbf{y} \in \mathcal{Y}^N} \sum_{\mathbf{s} \in \mathcal{S}^N} 2^{N[\beta(m,\mathbf{s}) - \alpha(m,\mathbf{s}) + \epsilon]} w^N(\mathbf{s}|\mathbf{y}) \\ &\qquad \times \lambda_Y^N(\mathbf{y})\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &\overset{(d)}{\leq} \sum_\lambda 2^{N[I_{\lambda,f}(U;Y) - I_\lambda(U;S) + \epsilon']} \\ &\qquad \sum_{\mathbf{y} \in \mathcal{Y}^N} \sum_{\mathbf{s} \in \mathcal{S}^N} w^N(\mathbf{s}|\mathbf{y})\, \lambda_Y^N(\mathbf{y})\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \end{aligned} \quad (13)$$

where $\epsilon' = \epsilon \log(2|\mathcal{S}|\,|\mathcal{Y}|)$. Equality (a) follows from (5). In (b) the conditional pmf $w(s|y)$ is arbitrary. There we have used the property (P1) which implies that given any $m \in \mathcal{M}_N$, $\mathbf{s} \in \Sigma(m)$ and $1 \leq t \leq N$, $u_t(m,\mathbf{s})$ is independent of s_t. Similarly $\mathcal{B}_\epsilon(m,\mathbf{s})$ is independent of s_t; and by (8), $\alpha(m,\mathbf{s})$ is "almost independent" of s_t. Inequality (c) follows from (9) and (6), and inequality (d) from (7). Averaging (13) over $m \in \mathcal{M}_N$, we obtain

$$\begin{aligned} &\underline{P}_c(f_N, g_N) \\ &= 2^{-NR} \sum_{m \in \mathcal{M}_N} \underline{P}_c(f_N, g_N, m) \\ &\leq 2^{-NR} \sum_{m,\lambda} 2^{N[I_{\lambda,f}(U;Y) - I_\lambda(U;S) + \epsilon']} \\ &\qquad \sum_{\mathbf{s} \in \mathcal{S}^N} \sum_{\mathbf{y} \in \mathcal{Y}^N} w^N(\mathbf{s}|\mathbf{y})\, \lambda_Y^N(\mathbf{y})\, \mathbb{1}\{\mathcal{E}(m,\lambda)\} \\ &\leq \sup_{|\mathcal{V}|} \max_{\lambda,f} 2^{-N[R - I_{\lambda,f}(U;Y) + I_\lambda(U;S) - \epsilon']} \\ &\qquad \underbrace{\sum_{\mathbf{s} \in \mathcal{S}^N} \sum_{\mathbf{y} \in \mathcal{Y}^N} w^N(\mathbf{s}|\mathbf{y})\, \lambda_Y^N(\mathbf{y}) \sum_{m,\lambda} \mathbb{1}\{\mathcal{E}(m,\lambda)\}}_{\leq 1} \\ &\overset{(a)}{\leq} 2^{-N[R - \sup_{|\mathcal{V}|} \max_{\lambda,f} (I_{\lambda,f}(U;Y) - I_\lambda(U;S)) - \epsilon']} \\ &= 2^{-N[R - C - \epsilon']} \end{aligned} \quad (14)$$

where (a) holds because the events $\mathcal{E}(m,\lambda)$ are disjoint.

Step 6. Combining (3), (10), (12), and (14) yields

$$P_c(f_N, g_N) \leq o(1) + \frac{\log^2 \epsilon}{N\epsilon^2} + 2^{-N(R - C - \epsilon')}. \quad (15)$$

Hence $P_c(f_N, g_N)$ vanishes for all sequences of codes (f_N, g_N) of rate $R > C + \epsilon'$. Since this inequality holds for arbitrarily small $\epsilon > 0$, we conclude that $P_c(f_N, g_N)$ vanishes for all $R > C$. This concludes the proof. □

3. MULTIPLE-ACCESS GEL'FAND-PINSKER CHANNEL

Consider the multiple-access GP channel $p(y|x_1, x_2, s)$ with alphabets $\mathcal{S}, \mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}$ and message sets $\{1, \cdots, 2^{NR_1}\}$ and

$\{1, \cdots, 2^{NR_2}\}$. The channel state sequence $\mathbf{S} \in \mathcal{S}^N$ is iid p_S and is known to both encoders. The encoders transmit sequences $f_N^1(m_1, \mathbf{s}) \in \mathcal{X}_1^N$ and $f_N^2(m_2, \mathbf{s}) \in \mathcal{X}_2^N$ respectively, where M_1 and M_2 are independent of $\mathbf{S}$ and are drawn uniformly and independently from their respective message sets. Given the channel output sequence $\mathbf{y} \in \mathcal{Y}^N$, the decoder outputs $(\hat{m}_1, \hat{m}_2) = g_N(\mathbf{y})$. Somekh-Baruch and Merhav [3] have shown that the following rate region $\mathscr{R}$ is achievable. For a pmf P of the form $p_S\, p_T\, p_{X_1V_1|ST}\, p_{X_2V_2|ST}\, p_{Y|X_1X_2S}$, let $\mathscr{R}(L, P)$ be the region of rate pairs (R_1, R_2) that satisfy

$$\begin{aligned} R_1 &< I(V_1; Y|V_2, T) - I(V_1; S|V_2, T) \\ R_2 &< I(V_2; Y|V_1, T) - I(V_2; S|V_1, T) \\ R_1 + R_2 &< I(V_1, V_2; Y|T) - I(V_1, V_2; S|T) \quad (16) \end{aligned}$$

where the alphabets for the auxiliary random variables V_1 and V_2 have cardinality L. Let $\mathscr{R}$ denote the closure of $\cup_{L,P} \mathscr{R}(L, P)$. Rate pairs in $\mathscr{R}(L, P)$ are achieved using a time-shared binning scheme with codeword arrays $\{\mathbf{u}_1(l_1, m_1)\}$ and $\{\mathbf{u}_2(l_2, m_2)\}$. Each transmitter selects the row index so that the corresponding codeword is jointly typical with $\mathbf{s}$.

Attempts to find a outer rate region for this problem by deriving a weak converse (based on Fano's inequality and the telescoping formula) have met only partial success. We have derived a rate region of the form (16), but the maximization is over a larger set of distributions, with the distribution of (X_1, V_1, X_2, V_2) given (S, T) given by $p_{X_1|ST}\, p_{X_2|ST}\, p_{V_1V_2|X_1X_2ST}$ instead of $p_{X_1V_1|ST}\, p_{X_2V_2|ST}$. (See [9] for a related problem, and [8] for a similar mismatch in the case of SI causally available to the encoders.) Apparently the resulting outer region is strictly larger than the inner region $\mathscr{R}$ of (16). However, using a strong converse we have established the following result.

Theorem 3.1 *Assume that $H(S) > 0$ and $\min_{y,x_1,x_2,s} p_{Y|X_1X_2S}(y|x_1, x_2, s) > 0$. For any sequence of length-N codes with rate pair $(R_1, R_2) \notin \mathscr{R}$, the maximum error probability (over all pairs of messages m_1, m_2) tends to 1 as $N \to \infty$. Furthermore, in the definition of $\mathscr{R}$, it suffices to consider conditional pmfs $p_{X_iV_i|ST}$ of the form $p_{V_i|ST}\, \mathbb{1}\{X_i = f_i(V_i, S)\}$ where f_i is a mapping from $\mathcal{V}_i \times \mathcal{S}$ to $\mathcal{X}$, for each $i = 1, 2$.*

Sketch of the proof. The proof extends the methods from Sec. 2, however our derivation does not make use of types (presumably wringing methods would have to be used to show that certain correlated types have low probability). Define the decoding regions $\mathcal{D}(m_1, m_2)$ which form a partition of $\mathcal{Y}^N$. As in Step 2 of the proof of Theorem 1, assume the codewords are given by the following two-step procedure:

- Define for $i = 1, 2$ an alphabet $\mathcal{V}_i$ of arbitrarily large cardinality, a function $f_i : \mathcal{V}_i \times \mathcal{S} \to \mathcal{X}_i$, and a codebook with codewords $\mathbf{v}_i(m_i, \mathbf{s}) \in \mathcal{V}_i^N$;
- Each channel input symbol is obtained as

$$x_{it} = f_i(v_{it}(m_i, \mathbf{s}), s_t), \quad i = 1, 2,\ 1 \le t \le N.$$

Observe that the channel from $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{s})$ to $\mathbf{y}$ is time-invariant and memoryless, where

$$p_{Y|V_1V_2S}(y|v_1, v_2, s) = p_{Y|X_1X_2S}(y|f_1(v_1, s), f_2(v_2, s), s).$$

Define the random variables $V_{it} = v_{it}(M_i, \mathbf{S}) \in \mathcal{V}_i$ for $i = 1, 2$, and $Q_t = \{S_j,\, j \ne t\} \in \mathcal{S}^{N-1}$ (again note Q_t is independent of S_t) for $1 \le t \le N$. The equivalence relation $\mathbf{s} = (s_t, q_t)$ holds for each $1 \le t \le N$. Let T be a time-sharing random variable uniformly distributed over $\{1, 2, \cdots, N\}$ and independent of all other random variables. Let $S = S_T$, $Q = Q_T$, $X_1 = X_{1T}$, $V_1 = V_{1T}$, $X_2 = X_{2T}$, $V_2 = V_{2T}$, and $Y = Y_T$. For each $1 \le t \le N$, the joint pmf of $(\mathbf{S}, M, V_{1t}, X_{1t}, V_{2t}, X_{2t}, Y_t)$ is given by

$$\begin{aligned} p(\mathbf{s}, m, v_{1t}, x_{1t}, v_{2t}, x_{2t}, y_t) &= p_S^N(\mathbf{s})\, p_M(m) \\ &\times \prod_{i=1}^{2} \left(\mathbb{1}\{v_{it} = v_{it}(m_i, \mathbf{s})\}\, \mathbb{1}\{x_{it} = f_i(v_{it}, s_t)\}\right) \\ &\times p_{Y|X_1X_2S}(y_t|x_{1t}, x_{2t}, s_t). \end{aligned}$$

The joint pmf of $T, S, Q, V_1, V_2, X_1, X_2, Y$ is given by

$$\begin{aligned} &p_T\, p_S\, p_Q\, p_{V_1|SQT}\, p_{V_2|SQT}\, \mathbb{1}\{X_1 = f_1(V_1, S)\} \\ &\times \mathbb{1}\{X_2 = f_2(V_2, S, T)\}\, p_{Y|X_1X_2S}. \end{aligned}$$

The probability of correct decoding for (m_1, m_2) is given by

$$\begin{aligned} P_c(f_N^1, f_N^2, g_N, m_1, m_2) = &\sum_{\mathbf{y} \in \mathcal{D}(m_1, m_2)} \\ &\sum_{\mathbf{s} \in \mathcal{S}^N} p_S^N(\mathbf{s})\, p_{Y|V_1V_2S}^N(\mathbf{y}|\mathbf{v}_1(m_1, \mathbf{s}), \mathbf{v}_2(m_2, \mathbf{s}), \mathbf{s}). \end{aligned}$$

Under the maximal error criterion we have

$$P_c(f_N^1, f_N^2, g_N, m_1, m_2) \ge 1 - \delta, \quad \forall m_1, m_2$$

where δ is the maximum error probability.

Denote by Ω the set of triples $(m_1, m_2, \mathbf{s})$ such that $\mathbf{v}_i(m_i, \mathbf{s}) = \mathbf{v}_i(m_i, \mathbf{s}'), \quad i = 1, 2,\ \forall \mathbf{s}' :\ d_H(\mathbf{s}, \mathbf{s}') \le 1$.

As in (2), for $(m_1, m_2, \mathbf{s}) \in \Omega$, arbitrarily changing any one sample s_t of the sequence $\mathbf{s}$ does not change the value of the codewords $\mathbf{v}_1(m_1, \mathbf{s})$ and $\mathbf{v}_2(m_2, \mathbf{s})$. Denote by $\Sigma(m_1, m_2) \triangleq \{\mathbf{s} :\ (m_1, m_2, \mathbf{s}) \in \Omega\}$ and $\mathcal{M}_N(\mathbf{s}) \triangleq \{(m_1, m_2) :\ (m_1, m_2, \mathbf{s}) \in \Omega\}$ the sections of Ω along the (m_1, m_2) and $\mathbf{s}$ directions.

Choose an arbitrarily small $\epsilon > 0$. Similarly to (P1), without loss of optimality, we restrict our attention to codes that satisfy the following property.

(P2). For each m_1, m_2, the set $\Sigma(m_1, m_2)$ has probability

$$P_S^N(\Sigma(m_1, m_2)) \ge 1 - o(1). \quad (17)$$

Hence the sets

$$\begin{aligned} \Sigma_\epsilon &\triangleq \{\mathbf{s} :\ |\mathcal{M}_N(\mathbf{s})| \ge (1 - \epsilon) 2^{N(R_1 + R_2)}\}, \\ \Sigma_\epsilon(m_1, m_2) &\triangleq \Sigma(m_1, m_2) \cap \Sigma_\epsilon \end{aligned}$$

have probabilities $P_S^N(\cdot) \ge 1 - o(1)$.

Step 2. Define three conditional self-informations:

$$\frac{1}{N}\sum_{t=1}^{N}\hat{I}(V_{1t}V_{2t};S_t|Q_t=q_t)=\alpha^{(3)}(m_1,m_2,\mathbf{s})\triangleq\frac{1}{N}\sum_{t=1}^{N}\sum_{s'_t}p_S(s'_t)\log\frac{p_{S_t|V_{1t}V_{2t}Q_t}(s'_t|v_{1t}(m_1,\mathbf{s}),v_{2t}(m_2,\mathbf{s}),q_t)}{p_{S_t|Q_t}(s'_t|q_t)}$$

and for $j=1,2$, $\alpha^{(j)}(m_1,m_2,\mathbf{s})$ is defined similarly, using log ratios $p_{S_t|V_{1t}V_{2t}Q_t}/p_{S_t|V_{|1-j|,t}Q_t}$. For any sequence $\mathbf{s}\in\Sigma(m_1,m_2)$, $1\le t\le N$, and $j=1,2,3$, the quantity $\alpha^{(j)}(m_1,m_2,\mathbf{s})$ does not depend on s_t. We also define the following three conditional self-informations:

$$\frac{1}{N}\sum_{t=1}^{N}\hat{I}(V_{1t}V_{2t};Y_t|Q_t=q_t)=\beta^{(3)}(m_1,m_2,\mathbf{s})\triangleq\frac{1}{N}\sum_{t=1}^{N}\sum_{s'_t}\sum_{y_t\in\mathcal{Y}}p_{Y|V_1V_2S}(y_t|v_{1t}(m_1,\mathbf{s}),v_{2t}(m_2,\mathbf{s}),s'_t)\times\log\frac{p_{Y_t|V_{1t}V_{2t}Q_t}(y_t|v_{1t}(m_1,\mathbf{s}),v_{2t}(m_2,\mathbf{s}),q_t)}{p_{Y_t|Q_t}(y_t|q_t)}.$$

and for $j=1,2$, $\beta^{(j)}(m_1,m_2,\mathbf{s})$ is defined similarly, using log ratios $p_{Y_t|V_{1t}V_{2t}Q_t}/p_{Y_t|V_{|1-j|,t}Q_t}$. Define

$$\begin{aligned}\tilde{R}_{1t}(q_t)&=I(V_{1t};Y_t|V_{2t},Q_t=q_t)-I(V_{1t};S_t|V_{2t},Q_t=q_t)\\ \tilde{R}_{2t}(q_t)&=I(V_{2t};Y_t|V_{1t},Q_t=q_t)-I(V_{2t};S_t|V_{1t},Q_t=q_t)\\ \tilde{R}_{3t}(q_t)&=I(V_{1t}V_{2t};Y_t|Q_t=q_t)-I(V_{1t}V_{2t};S_t|Q_t=q_t).\end{aligned}$$

It may be shown that, for $j=1,2,3$ and $\mathbf{s}\in\Sigma_\epsilon$,

$$(1-\epsilon)\mathbb{E}[\beta^{(j)}(M_1,M_2,\mathbf{s})-\alpha^{(j)}(M_1,M_2,\mathbf{s})]\le\frac{1}{N}\sum_{t=1}^{N}\tilde{R}_{jt}(q_t)+\epsilon'. \quad (18)$$

Similarly to (9), 3 high-probability subsets $\mathcal{B}_\epsilon^{(j)}(m_1,m_2,\mathbf{s})$ of $\mathcal{Y}^N$ are also defined. 3 cond'l reference pmf's are defined: $r^{(1)}(\mathbf{y}|\mathbf{v}_2,\mathbf{s})$, $r^{(2)}(\mathbf{y}|\mathbf{v}_1,\mathbf{s})$, and $r^{(3)}(\mathbf{y}|\mathbf{s})\triangleq\prod_{t=1}^{N}p_{Y_t|Q_t}(y_t|q_t)$.

Step 3. Three upper bounds are evaluated for the probability of correct decoding for m_1,m_2:

$$\begin{aligned}1-\delta&\le P_c(f_N^1,f_N^2,g_N,m_1,m_2)\\ \Rightarrow\ 1-\delta-\epsilon&\le\underline{P}_c^{(j)}(f_N^1,f_N^2,g_N,m_1,m_2),\quad j=1,2,3\end{aligned}$$

where

$$\underline{P}_c^{(j)}(f_N,g_N,m_1,m_2)\triangleq Pr[g_N(\mathbf{Y})=(m_1,m_2),\mathbf{S}\in\Sigma_\epsilon(m_1,m_2),\mathbf{Y}\in\mathcal{B}_\epsilon^{(j)}(m_1,m_2,\mathbf{S})\,|\,M_1=m_1,M_2=m_2]. \quad (19)$$

Step 4. The case $j=3$ yields an upper bound on the sum rate $R_3=R_1+R_2$. Define the "good" event

$$\mathcal{E}^{(3)}(m_1,m_2)=\{\mathbf{S}\in\Sigma_\epsilon(m_1,m_2),\mathbf{Y}\in\mathcal{D}(m_1,m_2)\cap\mathcal{B}_\epsilon^{(3)}(m_1,m_2,\mathbf{S})\}.$$

Analogously to (14), we derive

$$\begin{aligned}1-\delta-\epsilon&\le\underline{P}_c^{(3)}(f_N,g_N,m_1,m_2)\\ &\le\sum_{\mathbf{y}\in\mathcal{Y}^N}\sum_{\mathbf{s}\in\mathcal{S}^N}2^{N[\beta^{(3)}(m_1,m_2,\mathbf{s})-\alpha^{(3)}(m_1,m_2,\mathbf{s})+\epsilon]}p_S^N(\mathbf{s})\,r^{(3)}(\mathbf{y}|\mathbf{s})\,\mathbb{1}\{\mathcal{E}^{(3)}(m_1,m_2)\}. \quad (20)\end{aligned}$$

Now, since the average value of $\beta^{(3)}(m_1,m_2,\mathbf{s})-\alpha^{(3)}(m_1,m_2,\mathbf{s})$ over m_1,m_2 satisfies (18) for all $\mathbf{s}\in\Sigma_\epsilon$, there must exist a large set $\Gamma_3(\mathbf{s})$ of pairs m_1,m_2 for which

$$\begin{aligned}&\beta^{(3)}(m_1,m_2,\mathbf{s})-\alpha^{(3)}(m_1,m_2,\mathbf{s})\\ &\le\ \mathbb{E}[\cdot|\mathbf{s}]+\epsilon\le\frac{1}{N}\sum_{t=1}^{N}\tilde{R}_{3t}(q_t)+2\epsilon.\end{aligned}$$

It is easily shown that $|\Gamma_3(\mathbf{s})|\ge\epsilon'\,2^{NR_3}$ where $\epsilon'=\frac{\epsilon}{\epsilon+\log|\mathcal{Y}|}$. Averaging (20) over $(m_1,m_2)\in\Gamma_3(\mathbf{s})$, we obtain

$$\frac{1}{N}\log\frac{\epsilon(1-\delta-\epsilon)}{\epsilon+\log|\mathcal{Y}|}\le-R_3+\max_{\{q_t\}}\frac{1}{N}\sum_{t=1}^{N}\tilde{R}_{3t}(q_t)+2\epsilon. \quad (21)$$

In the cases $j=1$ and $j=2$, the decoder uses a helper who reveals one message and the corresponding codeword $\mathbf{v}_i(m_i,\mathbf{s})$ (but not $\mathbf{s}$). This leads to the same inequality (21), with R_j and $\tilde{R}_{jt}$ in place of R_3 and $\tilde{R}_{3t}$, respectively.

Step 5. Let $W=(T,S,V_1,V_2,X_1,X_2,Y)$ and define $\overline{R}_j(p_{WQ})=\frac{1}{N}\sum_{t=1}^{N}\sum_{q_t}p_{Q_t}(q_t)\tilde{R}_{jt}(q_t)$ for $j=1,2,3$. We obtain

$$\frac{1}{N}\log\frac{\epsilon(1-\delta-\epsilon)}{\epsilon+\log|\mathcal{Y}|}\le\min_{j=1,2,3}[-R_j+\max_{p_Q}\overline{R}_j(p_{W|Q}\,p_Q)]+2\epsilon. \quad (22)$$

Taking $\epsilon\downarrow 0$, we conclude that for (22) to hold for all $0\le\delta\le 1$, there must exist a pmf $P=p_{WQJ}$ of the form $p_S\,p_{QJT}\,p_{V_1|SQJT}\,p_{V_2|SQJT}\,\mathbb{1}\{X_1=f_1(V_1,S)\}\,\mathbb{1}\{X_2=f_2(V_2,S)\}\,p_{Y|X_1X_2S}$ such that (16) holds with (Q,J,T) in place of T. □

4. REFERENCES

[1] S. I. Gel'fand and M. S. Pinsker, "Coding for Channel with Random Parameters," *Probl. Contr. Info. Th.*, Vol. 9, No. 1, pp. 19—31, 1980.

[2] G. Keshet, Y. Steinberg, and N. Merhav, "Channel Coding in the Presence of Side Information: Subject Review," *Foundations and Trends in Communications and Information Theory*, 2007.

[3] A. Somekh-Baruch and N. Merhav, "On the Random Coding Error Exponents of the Single-User and the Multiple-Access Gel'fand-Pinsker Channels," *Proc. ISIT*, p. 448, Chicago, IL, June-July 2004.

[4] R. Ahlswede, "An Elementary Proof of the Strong Converse Theorem for the Multiple-Access Channel," *J. Combinatorics, Information and System Sciences*, Vol. 7, No. 3, pp. 216—230, 1982.

[5] R. Ahlswede, "On Two-Way Communication Channels and a Problem by Zarankiewicz," *6th Prague Conf. on Information Theory, Statistical Decision Functions, and Random Processes*, Prague, 1971.

[6] G. Dueck, Maximal Error Capacity Regions Are Smaller than Average Error Capacity Regions for Multi-User Channels, *Problems Control and Information Theory*, Vol. 7, No. 1, pp. 11—19, 1978.

[7] I. Csiszár and J. Körner, *Information Theory: Coding Theory for Discrete Memoryless Systems*, Academic Press, NY, 1981.

[8] S. Sigurjónsson and Y.-H. Kim, "On Multiple User Channels with State Information at the Transmitters," *Proc. ISIT* 2005.

[9] Y. Wang and P. Moulin, "Blind Fingerprinting," arXiv:0803.0265v1 [cs.IT], March 2008.