On Information Rates for Mismatched Decoders

Neri Merhav, *Senior Member, IEEE*, Gideon Kaplan, *Member, IEEE*, Amos Lapidoth, and Shlomo Shamai (Shitz), *Fellow, IEEE*

***Abstract*— Reliable transmission over a discrete-time memoryless channel with a decoding metric that is not necessarily matched to the channel (mismatched decoding) is considered. It is assumed that the encoder knows both the true channel and the decoding metric. The lower bound on the highest achievable rate found by Csiszár and Körner and by Hui for DMC's, hereafter denoted C_{LM}, is shown to bear some interesting information-theoretic meanings. The bound C_{LM} turns out to be the highest achievable rate in the random coding sense, namely, the random coding capacity for mismatched decoding. It is also demonstrated that the ϵ-capacity associated with mismatched decoding cannot exceed C_{LM}. New bounds and some properties of C_{LM} are established and used to find relations to the generalized mutual information and to the generalized cutoff rate. The expression for C_{LM} is extended to a certain class of memoryless channels with continuous input and output alphabets, and is used to calculate C_{LM} explicitly for several examples of theoretical and practical interest. Finally, it is demonstrated that in contrast to the classical matched decoding case, here, under the mismatched decoding regime, the highest achievable rate depends on whether the performance criterion is the bit error rate or the message error probability and whether the coding strategy is deterministic or randomized.**

***Index Terms*—Channel capacity, mismatched decoding, generalized cutoff rate, generalized mutual information, random coding, exponential families, sphere packing.**

I. Introduction

The subject of mismatched decoding has been of interest since the 1970's (see, e.g., [15], [27]). A coded communication system operates over a discrete-time memoryless channel with a sequence transition probability $W(\boldsymbol{y} \mid \boldsymbol{x})$, whereas the decoder employs maximum-likelihood (ML) decoding with an additive metric $\ln V(\boldsymbol{y} \mid \boldsymbol{x})$. The encoder, in turn, knows both W and V and strives to optimize performance in terms of the achievable reliable information rate. This is a realistic model for time-varying channels, or when implementation constraints dictate a given decoding metric. As an example, consider the common decoder chip which employs integer metrics [29] and is designed for the quantized additive white Gaussian channel (AWGN), operating under fading, jamming, or noisy phase conditions. Theoretically, one can employ universal decoding [13], [37]; however, in many applications, it is ruled out by complexity considerations.

The generalized cutoff rate (GCR) has been the commonly used performance measure for such a scenario (see, e.g., [15], [27], [29]). It is considered to be a practically achievable reliable rate for a discrete memoryless channel (DMC) with mismatched decoding, although it has been recently shown [25] that the GCR may behave very differently from the maximum achievable rate. In [6], a similar treatment is presented for a channel with a finite memory. In [23], a condition for the strict positivity of the GCR was stated. In [21], the Gallager upper bound on the average message error probability for DMC's under the random coding regime was employed to account for mismatched decoding, and the generalized mutual information (GMI), which is viewed as an extension of [16], was defined.

In [12] and [20], coding theorems for a mismatched DMC were introduced independently. Hui [20] used standard random coding and combinatorial considerations associated with strong typicality of sequences to obtain a single-letter expression for a lower bound on the highest achievable rate. It was also conjectured by Hui that this lower bound on the mismatched capacity is indeed the maximal rate of reliable communication under mismatched conditions, that is, the mismatched capacity. Csiszár and Körner [12] established an error exponent for random coding with fixed composition codes, and a decoder using an arbitrary decoding rule, by invoking a graph decomposition theorem. The lower bounds on mismatched capacity of [12] and [20] coincide, and they are designated hereafter as C_{LM}, where the subscript LM stands for a lower bound on the mismatched capacity C_M.

While Hui's conjecture has been reported true for binary input channels by Balakirsky [3], it has been recently refuted in the general case by Csiszár and Narayan [14] by Ahlswede et al. [1], and by Lapidoth [24], [25]. The counterexample described in [14] is based on formulating

Manuscript received April 1, 1993; revised March 16, 1994. The work of N. Merhav, G. Kaplan and S. Shamai was partially supported by the S. Neaman Institute (Technion) in the framework of the Israeli consortium for satellite communications. The work of A. Lapidoth was supported in part by NSF Grant NCR-9205663 and ARPA Contract J-FBI-91-218. This paper was presented in part at the 1993 IEEE International Symposium on Information Theory, San Antonio, TX, January 1993.

N. Merhav and S. Shamai (Shitz) are with the Department of Electrical Engineering, Technion—Israel Institute of Technology, Haifa 32000, Israel.

G. Kaplan was with the Department of Electrical Engineering, Technion—Israel Institute of Technology, Haifa 32000, Israel. He is now with Gilat Satellite Networks, Ltd., 24a Habarzel St., Tel Aviv 69710, Israel.

A. Lapidoth was with the Department of Electrical Engineering, Technion—Israel Institute of Technology, Haifa 32000, Israel. He is now with the Department of Electrical Engineering, Information Systems Laboratory, Stanford University, Stanford, CA 94305.

IEEE Log Number 9406225.

0018-9448/94$04.00 © 1994 IEEE

a zero-error capacity problem as a mismatched decoding problem and showing that random coding does not achieve the zero-error capacity. The example given in [24], [25] is that of minimum Euclidean distance decoding of the additive noise vector Gaussian channel (see Example 6 in Section VI below). Csiszár and Narayan [14] have also shown that, in general, for any $k > 1$, one can improve on the rate C_{LM} through a random coding argument applied to the superalphabet corresponding to k-length input blocks. They conjectured that as $k \to \infty$, the rates achievable by random coding applied to the superchannel approach C_M. Lapidoth [25] obtained a single-letter lower bound on C_M which is, in general, tighter than C_{LM}. His techniques are based on random product codes. The improved bound which he has obtained can, of course, be applied to the superchannel as well. Interesting connections between the erasures-only capacity and the mismatched capacity have been described in [14] and [1].

In this paper, we further study some properties of C_{LM} in its single-letter definition. Although it is not the exact mismatched capacity in general, we show that it does bear some other interesting information-theoretic meanings. Specifically, we show in Section III that under a random coding regime, C_{LM} is not only a lower bound, but also an upper bound on the highest achievable rate, and hence it is the exact expression of the random coding capacity for mismatched decoding. Another feature of C_{LM}, demonstrated in Section IV, is that it serves as an upper bound on the ϵ-capacity [19], [28], [36] under mismatched decoding. This means that for an information rate exceeding C_{LM}, there must be at least one codeword for which the size of its decision region is exponentially equivalent to the total size of its intersection with decision regions corresponding to other codewords.

In Section V, several novel properties of the lower bound on the mismatched capacity are addressed, along with some interesting examples. One of the results (reported also in [21]) is that C_{LM} is never smaller than the GMI, which in turn upper bounds the GCR. The former inequality indicates that the converse theorem stated in [18] for Fischer's expression [16] does not seem to hold since it is never larger than the GMI.

In Section VI, we extend the achievable rate theorem to more general memoryless channels with possibly continuous input and output alphabets satisfying certain conditions. This extension includes as special cases DMC's, Gaussian channels, and the Poisson channel. It also facilitates broadening the scope to certain channels of practical interest, and studying more closely their behavior under mismatched decoding. Several examples of theoretical and practical interest are worked out.

Finally, in Section VII, we demonstrate that the properties of reliable communication under a mismatched decoding regime might be considerably different from their well-known counterparts in the classical matched case. For example, unlike in the matched case, the coding capacity defined with respect to the bit error probability might differ from that of the block error probability. Another example shows that while under optimal (matched) decoding conditions the best random coding strategy is *deterministic*, in the mismatched case, a randomized encoding mechanism may outperform any deterministic code. Thus, if the mismatched capacity is defined with respect to the bit error probability and/or with respect to randomized encoders, it turns out that rates higher than C_{LM} and even C_M might be achievable.

II. Notation, Definitions, and Preliminaries

Throughout this paper, we adopt the convention that a (scalar) random variable is denoted by a capital letter (e.g., X), a specific value it may take is denoted by the respective lower case letter (x), and its alphabet is denoted by the respective script letter ($\mathcal{X}$). As for vectors, a boldface capital letter ($\boldsymbol{X}$) will denote an n-dimensional random vector $(X_1,\cdots,X_n)$, a boldface lower case letter ($\boldsymbol{x}$) will denote a specific vector value $(x_1,\cdots,x_n)$, and the respective superalphabet, which is the nth Cartesian power of the single-letter alphabet, will be denoted by the corresponding script letter with the superscript n ($\mathcal{X}^n$). The cardinality of a set will be denoted by $|\cdot|$, e.g., $|\mathcal{X}|$ is the size of the alphabet of X.

Since the method of types [10], [13] will be used throughout this paper, we next describe some notational conventions associated with types. For a given sequence $\boldsymbol{x} \in \mathcal{X}^n$, $\mathcal{X}$ being a finite alphabet, the empirical probability mass function (EPMF) is the vector $p_{\boldsymbol{x}} = \{p_{\boldsymbol{x}}(x), x \in \mathcal{X}\}$ where $p_{\boldsymbol{x}}(x) = n_{\boldsymbol{x}}(x)/n$, $n_{\boldsymbol{x}}(x)$ being the number of occurrences of the letter $x \in \mathcal{X}$ in the sequence $\boldsymbol{x}$. The set of all EPMF's of sequences $\boldsymbol{x}$ in $\mathcal{X}^n$, i.e., rational probability mass functions (PMF's) with denominator n, will be denoted by $\mathcal{P}_n$. The type $T_{\boldsymbol{x}}$ of a sequence $\boldsymbol{x}$ is the set of all sequences $\boldsymbol{x}' \in \mathcal{X}^n$ such that $p_{\boldsymbol{x}'} = p_{\boldsymbol{x}}$. The empirical entropy associated with $\boldsymbol{x}$ is the entropy associated with its EPMF $p_{\boldsymbol{x}}$, i.e.,

$$H_{\boldsymbol{x}}(X) = -\sum_{x\in\mathcal{X}} p_{\boldsymbol{x}}(x)\ln p_{\boldsymbol{x}}(x). \tag{1}$$

Hereafter, the notations "$a_n \doteq b_n$" and "$a_n \mathrel{\dot{\geq}} b_n$" mean that $\lim_{n\to\infty} n^{-1}\log a_n/b_n$ is zero and nonnegative, respectively. For instance, it is well known [13] that $|T_{\boldsymbol{x}}| \doteq e^{nH_{\boldsymbol{x}}(X)}$. A somewhat different notion of a type that will be used throughout the sequel is that of an ϵ-type w.r.t. a memoryless source $p = \{p(x), x \in \mathcal{X}\}$. We shall denote by $T_\epsilon(p)$ the set of all sequences $\boldsymbol{x} \in \mathcal{X}^n$ such that $|p_{\boldsymbol{x}}(x) - p(x)| < \epsilon$ for every $x \in \mathcal{X}$. Similar definitions and notations will be used for the type of sequences $\boldsymbol{y} \in \mathcal{Y}^n$ and ϵ-types associated with these sequences, with the appropriate substitution of symbols.

Similarly, for sequence pairs $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{X}^n \times \mathcal{Y}^n$, the joint EPMF $p_{\boldsymbol{xy}}$ is the matrix $\{p_{\boldsymbol{xy}}(x,y)\}_{x\in\mathcal{X}, y\in\mathcal{Y}}$ where $p_{\boldsymbol{xy}}(x,y) = n_{\boldsymbol{xy}}(x,y)/n$, $n_{\boldsymbol{xy}}(x,y)$ being the joint count of $x_i = x$ and $y_i = y$ along the pair sequence $(\boldsymbol{x}, \boldsymbol{y})$. The joint type $T_{\boldsymbol{xy}}$ is the set of all pairs $(\boldsymbol{x}', \boldsymbol{y}')$ with the same joint EPMF as $(\boldsymbol{x}, \boldsymbol{y})$. The empirical joint entropy $H_{\boldsymbol{xy}}(X,Y)$ associated with $(\boldsymbol{x}, \boldsymbol{y})$ is the entropy associated with the joint EPMF $p_{\boldsymbol{xy}}$. A time average of a function of x and y, e.g., $n^{-1}\sum_{i=1}^{n} g(x_i, y_i)$, will sometimes be viewed as an expectation of $g(X,Y)$ w.r.t. the joint EPMF p_{xy}, and hence will be denoted by $E_{xy}g(X,Y)$.

The conditional type $T_{x|y}$ for a given y is the set of all sequences $x' \in \mathcal{X}^n$ such that $(x', y) \in T_{xy}$. The conditional PMF $p_{x|y}$ is the matrix $\{p_{x|y}(x \mid y)\}_{x\in\mathcal{X}, y\in\mathcal{Y}}$, where $p_{x|y}(x \mid y)$ is defined as $p_{xy}(x,y)/p_y(y)$ if $p_y(y) > 0$, and as zero otherwise. The empirical conditional entropy of X given Y associated with the pair sequence (x, y) is given by

$$H_{x|y}(X \mid Y) = H_{xy}(X,Y) - H_y(Y)$$
$$= -\sum_{x\in\mathcal{X}, y\in\mathcal{Y}} p_{xy}(x,y)\ln p_{x|y}(x \mid y). \quad (2)$$

It is well known [13] that $|T_{x|y}| \doteq e^{nH_{x|y}(X|Y)}$. The empirical mutual information associated with the pair of sequences (x, y) is defined as the mutual information associated with their joint EPMF p_{xy}, or, equivalently,

$$I_{xy}(X;Y) = H_x(X) - H_{x|y}(X \mid Y). \quad (3)$$

A DMC is fully characterized by a transition probability matrix $\{W(y \mid x)\}_{x\in\mathcal{X}, y\in\mathcal{Y}}$, where $\mathcal{X}$ and $\mathcal{Y}$ designate finite input and output alphabets, respectively. The conditional probability $\Pr\{Y = y \mid X = x\}$ will be denoted by $W(y \mid x)$, which for a DMC is given by $\prod_{i=1}^{n} W(y_i \mid x_i)$.

A rate R block code of size n is a set of $M = e^{nR}$ equiprobable n-dimensional vectors (codewords), $x_i = (x_1^i, \cdots, x_n^i) \in \mathcal{X}^n$, $1 \le i \le M$ to be transmitted over the channel. The decoder, upon receiving a vector $Y = (Y_1, \cdots, Y_n) \in \mathcal{Y}^n$ at the channel output, estimates the index i of the transmitted codeword as the one that maximizes $\ln V(y \mid x_i)$, henceforth referred to as the *decoding metric*, where $V(y \mid x) = \prod_{i=1}^{n} V(y_i \mid x_i)$, and unless specified otherwise, it is not necessary that $\sum_{y\in\mathcal{Y}} V(y \mid x) = 1$ for every $x \in \mathcal{X}$. If the decoding metric V is not equivalent to that of the optimal ML decoder W in the sense of yielding an identical decision rule, we say that the decoder is *mismatched.* An achievable rate for a DMC W and a mismatched decoding metric V is a rate R such that for every $\epsilon > 0$, there exists a large enough n and a rate R block code of size n such that the probability of error when decoding with the metric V is less than ϵ. The capacity of a DMC W with a mismatched decoding metric V, i.e., the *mismatched capacity* C_M, is the supremum of all achievable rates in the above definition.

Now, let

$$I(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x)f(y \mid x)\ln\frac{f(y \mid x)}{\sum_{x'\in\mathcal{X}} p(x')f(y \mid x')} \quad (4)$$

denote the mutual information for some DMC $f = \{f(y \mid x)\}$ with an input PMF $p = \{p(x)\}_{x\in\mathcal{X}}$. Let

$$I'(X;Y) = \min_f I(X;Y) \quad (5)$$

where the minimization is over all channels f satisfying

$$\sum_{x\in\mathcal{X}} p(x)f(y \mid x) = \sum_{x\in\mathcal{X}} p(x)W(y \mid x) \triangleq q(y), \qquad \forall y \in \mathcal{Y}$$

and (6)

$$\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x)f(y \mid x)\ln V(y \mid x) \ge \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x)W(y \mid x)\ln V(y \mid x) \triangleq -D.$$

Finally, C_{LM} is defined as

$$C_{LM} = \max_p I'(X;Y). \quad (7)$$

In [20, Theorem 4.1] (see also [12, Lemma 3]) it has been proved by a random coding argument that C_{LM} is an achievable rate for W when the decoding metric is V, and hence serves as a lower bound on the mismatched capacity. In other words, the average message error probability over the ensemble of randomly chosen block codes is guaranteed to vanish as $n \to \infty$ provided that $R < C_{LM}$.

III. A Converse Theorem for Random Coding

We next show that C_{LM} is also an upper bound on the highest rate for which the random coding error probability still tends to zero, i.e., C_{LM} is the highest achievable rate in the random coding sense. The significance of this statement will be further emphasized in Section VII, in view of some interesting examples for which one can derive other coding strategies achieving reliable rates higher than C_{LM} or even C_M.

Consider a codebook of $e^{nR} + 1$ n-dimensional vectors where each vector is generated at random with a memoryless PMF $p = \{p(x), x \in \mathcal{X}\}$ and independently of all other vectors. Let $\bar{P}_e$ denote the average error probability w.r.t. the ensemble of randomly chosen codes. Under mismatched decoding, we have the following result.

Theorem 1: Assume that there exists a channel f that satisfies the two constraints of (6) with a strict inequality in the second constraint. Then, for any memoryless random coding PMF p, $R > C_{LM}$ implies $\lim_{n\to\infty} \bar{P}_e = 1$.

Two comments are in order.

1) A similar statement, with only minor modifications in the proof, can be made for a random coding distribution that is *uniform* within the type that is most likely under p.

2) A sufficient condition for the existence of a channel f that satisfies the conditions of the theorem is that there exist two distinct input letters $a, a' \in \mathcal{X}$ and two distinct output letters $b, b' \in \mathcal{Y}$ such that $p(a)$, $p(a')$, $W(b \mid a')$, and $W(b' \mid a)$ are all strictly positive, and at the same time $V(b \mid a)V(b' \mid a') > V(b \mid a')V(b' \mid a)$ (see Appendix A). This sufficient condition is easy to check and fairly mild, although it may rule out some channels for which $C_{LM} > 0$.

The remaining part of this section is devoted to the proof of Theorem 1.

Proof: Fix $\epsilon > 0$, and let $T_\epsilon(p)$ and $T_\epsilon(q)$ denote the ϵ-types associated with the input and output marginals, respectively. Similarly, fix $\delta > 0$, and let $T_\delta^- = \{(x, y) : \ln V(y \mid x) \le n(-D + \delta)\}$. The average probability of correct message decoding can be upper bounded as follows:

$$\begin{aligned}1 - \bar{P}_e &= \Pr\left\{V(\boldsymbol{y} \mid \boldsymbol{x}_j) < V(\boldsymbol{y} \mid \boldsymbol{x}_i) \qquad \text{for all } j \neq i\right\}\\ &\leq \Pr\left\{V(\boldsymbol{y} \mid \boldsymbol{x}_j) < V(\boldsymbol{y} \mid \boldsymbol{x}_i)\right.\\ &\qquad\qquad \left.\text{for all } j \neq i, (\boldsymbol{x}_i, \boldsymbol{y}) \in T_\delta^-, \boldsymbol{y} \in T_\epsilon(q)\right\}\\ &\quad + \Pr\{\boldsymbol{y} \in T_\epsilon^c(q)\} + \Pr\left\{(\boldsymbol{x}_i, \boldsymbol{y}) \in [T_\delta^-]^c\right\}. \quad (8)\end{aligned}$$

Now, the two last terms on the rightmost side vanish as $n \to \infty$ by the weak law of large numbers (WLLN), so it remains to upper bound the first term, henceforth denoted by A, by a vanishing quantity as well. Note that

$$\begin{aligned}A &\leq \Pr\left\{\ln V(\boldsymbol{y} \mid \boldsymbol{x}_j) \leq n(-D + \delta)\right.\\ &\qquad\qquad \left.\text{for all } j \neq i, \boldsymbol{y} \in T_\epsilon(q)\right\}\\ &= \sum_{\boldsymbol{y} \in T_\epsilon(q)} q(\boldsymbol{y})[1 - h(\boldsymbol{y})]^{e^{nR}} \qquad (9)\end{aligned}$$

where $h(\boldsymbol{y}) = \sum_{\boldsymbol{x}: \ln V(\boldsymbol{y} \mid \boldsymbol{x}) > n(-D+\delta)} p(\boldsymbol{x})$. Next, observe that

$$\begin{aligned}A &\leq \sum_{\boldsymbol{y} \in T_\epsilon(q)} q(\boldsymbol{y}) \exp\{-h(\boldsymbol{y}) e^{nR}\}\\ &\leq \exp\left\{-\min_{\boldsymbol{y} \in T_\epsilon(q)} h(\boldsymbol{y}) e^{nR}\right\} \qquad (10)\end{aligned}$$

where we have used the fact that $1 - \alpha \leq e^{-\alpha}$ for every real α. To complete the proof, we need to show that for every $\boldsymbol{y} \in T_\epsilon(q)$, $h(\boldsymbol{y})$ is exponentially no smaller than $e^{-nI'(X;Y)}$ when ϵ vanishes, and hence for every $R > I'(X;Y)$, A is essentially less than $\exp\{-e^{n(R - I'(X;Y))}\} \to 0$. To this end, let us further lower bound $h(\boldsymbol{y})$. First, note that for every $\boldsymbol{y} \in T_\epsilon(q)$,

$$h(\boldsymbol{y}) = \sum_{T_{\boldsymbol{x} \mid \boldsymbol{y}} \subseteq \{\boldsymbol{x}: \ln V(\boldsymbol{y} \mid \boldsymbol{x}) \geq n(-D+\delta)\}} |T_{\boldsymbol{x} \mid \boldsymbol{y}}| \cdot p(\boldsymbol{x}) \qquad (11)$$

where we have used the facts that the set $\{\boldsymbol{x} : \ln V(\boldsymbol{y} \mid \boldsymbol{x}') > n(-D + \delta)\}$ is a union of conditional types $\{T_{\boldsymbol{x} \mid \boldsymbol{y}}\}$, and that for a given conditional type, all sequences $\boldsymbol{x}$ have the same probability. Now, let

$$T = \{\boldsymbol{x} : \ln V(\boldsymbol{y} \mid \boldsymbol{x}') > n(-D + \delta)\} \cap T_\epsilon(p), \qquad (12)$$

and note that for every $\boldsymbol{x} \in T_\epsilon(p)$, $p(\boldsymbol{x}) \geq \exp\{-n[H_{\boldsymbol{x}}(X) + \epsilon']\}$ where $\epsilon' = \epsilon \cdot |\mathscr{X}| \ln[1/p_{\min}]$, $p_{\min}$ being the smallest letter probability. Therefore,

$$\begin{aligned}h(\boldsymbol{y}) &\geq \sum_{T_{\boldsymbol{x} \mid \boldsymbol{y}} \subseteq T} |T_{\boldsymbol{x} \mid \boldsymbol{y}}| \cdot p(\boldsymbol{x})\\ &\geq \max_{T_{\boldsymbol{x} \mid \boldsymbol{y}} \subseteq T} |T_{\boldsymbol{x} \mid \boldsymbol{y}}| \cdot p(\boldsymbol{x})\\ &\geq \max_{T_{\boldsymbol{x} \mid \boldsymbol{y}} \subseteq T} e^{n[H_{\boldsymbol{x} \mid \boldsymbol{y}}(X \mid Y) - \zeta_n]} \cdot e^{-n[H_{\boldsymbol{x}}(X) + \epsilon']}\\ &= \exp\left[-n \cdot \left(\min I_{\boldsymbol{x}\boldsymbol{y}}(X;Y) + \epsilon' + \zeta_n\right)\right] \qquad (13)\end{aligned}$$

where $\zeta_n = O(\log n/n)$ and the minimum is over all empirical joint PMF's $p_{\boldsymbol{x}\boldsymbol{y}}$ of sequence pairs $(\boldsymbol{x}, \boldsymbol{y})$ such that $\boldsymbol{x} \in T$. By definition, these pairs of sequences satisfy the following constraints: $|p_{\boldsymbol{x}}(x) - p(x)| < \epsilon$ for every $x \in \mathscr{X}$, $|p_{\boldsymbol{y}}(y) - q(y)| < \epsilon$ for every $y \in \mathscr{Y}$, and $E_{\boldsymbol{x}\boldsymbol{y}} \ln V(Y \mid X) > -D + \delta$. Note that these constraints on the EPMF $p_{\boldsymbol{x}\boldsymbol{y}}$ are exactly the same as those of (6), except that the input and output marginal PMF's are not exactly p and q, but within ϵ close, and the last constraint is similar to the inequality of (6) where $-D$ is replaced by $-D + \delta$. Since the subset $B_{\epsilon,\delta}$ of *all* joint PMF's m satisfying $\max_{x \in \mathscr{X}} |m(x) - p(x)| < \epsilon$, $\max_{y \in \mathscr{Y}} |m(y) - q(y)| < \epsilon$, and $E_m \ln V(Y \mid X) > -D + \delta$ (E_m being the expectation w.r.t. m) is open and nonempty for some $\delta > 0$ by the assumption of the theorem, and since the set of rational joint PMF's with denominator n becomes dense in the continuum of PMF's as $n \to \infty$, then the infimum over $B_{\epsilon,\delta}$ of the mutual information induced by m, denoted by $I'_{\delta,\epsilon}(X;Y)$, can be approached (from above) by a rational PMF with denominator n, as $n \to \infty$. Now, since $I'(X;Y)$ is continuous in p and W (see [14, Lemma 1]), $\lim_{\epsilon \to 0} I'_{\delta,\epsilon}(X;Y) = I'_\delta(X;Y)$ where $I'_\delta(X;Y)$ is defined similarly as $I'_{\delta,\epsilon}(X;Y)$, but the infimum being defined over a set B_δ of PMF's m whose marginals are constrained to coincide *exactly* with p and q, respectively, and the third constraint is unchanged. Thus, to complete the proof, we need to show that $\lim_{\delta \to 0} I'_\delta(X;Y) = I'(X;Y)$. Equivalently, we need to show that the function $R(d) = \inf I(X;Y)$ where the infimum is over the set of all joint PMF's m such that $m(x) = p(x)$, $m(y) = q(y)$, and $-E_m \ln V(Y \mid X) < -d$ is continuous at $d = D$. This, in turn, follows from a simple consideration: the function $R(d)$ is well defined on the interval $[D - \delta, -E_{p \times q} \ln V(Y \mid X)]$. Since, $R(d)$ is a convex function (similarly as the rate-distortion function), then it must be continuous at least on $(D - \delta, -E_{p \times q} \ln V(Y \mid X))$, and hence also at D, which is an inner point of this interval. This completes the proof of Theorem 1. □

IV. Sphere Packing Arguments

Another notion of capacity is associated with the maximum number of *disjoint* "decoding spheres" that one can pack in the space of channel output sequences. This is often referred to as the ϵ-capacity [19], [28], [36]. In this section, it is shown that the ϵ-capacity associated with mismatched decoding cannot exceed C_{LM}.

Let

$$S_d(\boldsymbol{x}) \triangleq \{\boldsymbol{y} \in T_\epsilon(q) : -\ln V(\boldsymbol{y} \mid \boldsymbol{x}) \leq n \cdot d\} \qquad (14)$$

designate decoding "spheres" for a threshold decoder.

Given that $\boldsymbol{x}_i$ is transmitted, the output sequence that satisfies the above will be typically found near the surface of a "sphere" with a normalized radius $d = D$ where D is defined as in (6).

Lemma 1: If there exist e^{nR} disjoint spheres $\{S_D(\boldsymbol{x}_i)\}$ in $T_\epsilon(q)$, then $R < C_{LM}$.

Proof: Since there are e^{nR} codewords and the number of types $|\mathscr{P}_n|$ is polynomial, there must be at least one type $T_{\boldsymbol{x}}$ that is populated by a number of codewords that is exponentially equivalent to e^{nR}. Thus, without loss of generality, we can restrict our attention to fixed composition codes, i.e., codes for which all codewords are from the same type, characterized by an empirical input PMF $p = \{p(x), x \in \mathscr{X}\}$. For the spheres $\{S_D(\boldsymbol{x}_i)\}_{i=1}^{e^{nR}}$ to be disjoint, one must have

$$e^{n[H(Y)+\xi(\epsilon)]} \doteq |T_\epsilon(q)| \geq \sum_{i=1}^{e^{nR}} |S_D(\boldsymbol{x}_i)| \tag{15}$$

where $H(Y) = -\sum_{y \in \mathscr{Y}} q(y) \ln q(y)$ is the marginal output entropy, and $\xi(\epsilon)$ is an infinitesimal correction term defined as $H'(Y) - H(Y)$ where $H'(Y)$ is the maximum entropy over all measures $q' = \{q'(y), y \in \mathscr{Y}\}$ such that $|q'(y) - q(y)| \leq \epsilon$ for all $y \in \mathscr{Y}$. Now, since $S_D(\boldsymbol{x}_i)$ is a union of conditional types $\{T(\boldsymbol{y} \mid \boldsymbol{x}_i)\}$, and since the total number of conditional types is polynomial in n,

$$|S_D(\boldsymbol{x}_i)| = \sum_{T_{y|x_i} \subseteq S_D(\boldsymbol{x}_i)} |T_{y|x_i}| \doteq \max_{T_{y|x_i} \subseteq S_D(\boldsymbol{x}_i)} |T_{y|x_i}|$$

$$\doteq \exp\left\{n \cdot \max_{p_{xy} \in B(D)} H_{y|x}(Y \mid X)\right\} \tag{16}$$

where

$$B(D) \triangleq \left\{p_{xy} : p_x = p, \ -E_{xy} \ln V(Y \mid X) \leq D, \right.$$
$$\left. \max_{y \in \mathscr{Y}} |p_y(y) - q(y)| \leq \epsilon \right\}.$$

Now, let

$$F(D) \triangleq \max_{p_{xy} \in B(D)} H_{y|x}(Y \mid X). \tag{17}$$

Then, it follows from (16) that for (15) to be satisfied, a necessary condition is that

$$R < H(Y) - F(D) + \xi(\epsilon), \tag{18}$$

which for D as defined in (6), tends to $I'(X;Y)$ as $n \to \infty$ and $\epsilon \to 0$ from continuity arguments similar to those of Section III. Again, $I'(X;Y)$ can be maximized by optimizing the input PMF p. □

It is interesting to note that even if R only slightly exceeds C_{LM}, not only do the decoding spheres start to intersect, but there is at least one codeword for which the cardinality of the intersection with other decoding spheres is exponentially equivalent to the size of its decoding sphere itself. This is stated formally in the next lemma.

Lemma 2: Let $R = C_{LM} + \epsilon$ for some $\epsilon > 0$. Then, for at least one codeword $\boldsymbol{x}_i$,

$$\left| S_D(\boldsymbol{x}_i) \cap \left[\bigcup_{j \neq i} S_D(\boldsymbol{x}_j) \right] \right| \geq e^{-n\epsilon/2} |S_D(\boldsymbol{x}_i)|. \tag{19}$$

Proof: Suppose, conversely, that (19) is violated for *all* $M = e^{nR}$ codewords. Then, from Lemma 1 and under this assumption,

$$\begin{aligned} e^{nH'(Y)} &\doteq |T_\epsilon(q)| \\ &\geq \sum_{i=1}^{e^{nR}} |S_D(\boldsymbol{x}_i)| - \sum_{i=1}^{e^{nR}} \left| S_D(\boldsymbol{x}_i) \cap \left[\bigcup_{j \neq i} S_D(\boldsymbol{x}_j) \right] \right| \\ &\stackrel{.}{\geq} e^{nR} \cdot e^{nF(D)} - e^{-n\epsilon/2} \cdot e^{nR} \cdot e^{nF(D)} \\ &\doteq e^{n[H'(Y)+\epsilon]} - e^{n[H'(Y)+\epsilon/2]} \\ &\doteq e^{n[H'(Y)+\epsilon]}, \end{aligned} \tag{20}$$

which is a contradiction. □

This, however, does *not* imply that the error probability (given that $\boldsymbol{x}_i$ is transmitted) is large. To see this, consider the joint PMF $p^*_{x,y}$ that achieves $F(D)$. Clearly, the conditional type $T_{p^*_{y|x}}$ induced by $p^*_{x,y}$ is exponentially the dominant type in the sense of possessing at least a polynomial fraction of the sequences in $S_D(\boldsymbol{x}_i)$. Thus, (19) also implies that a polynomial fraction of $T_{p^*_{y|x}}$ intersects with other spheres $S_D(\boldsymbol{x}_j)$. However, $T_{p^*_{y|x}}$ is not necessarily dominant in the sense of possessing a large *probability* unless $p^*_{y|x}$ happens to coincide with W as is the case with matched decoding where $V = W$. Nevertheless, for binary-input channels operating above C_{LM}, Balakirsky [3] was able to prove that a nonexponential fraction of output sequences that are typical to W fall in a typical sphere corresponding to some incorrect codeword, and thus the error probability cannot decay exponentially. In other words, the maximum rate for which an exponentially vanishing error probability is achievable (referred to as the E-capacity in [2]) cannot exceed C_{LM}. This still does *not* imply that the capacity, as defined in the usual sense, is never larger than C_{LM}; however, it is stated in [3] that the proof can be extended so as to obtain the converse theorem in the binary input case.

V. Properties of $I'(X;Y)$ and Examples

In [20], some properties of $I'(X;Y)$ have been investigated. The most important one (Theorem 4.3.3 therein) is that $I'(X;Y)$ is convex (∪) in $\{m(x,y)\} = \{p(x)W(y \mid x)\}$ when $\{p(x)\}$ and $\{q(y)\}$ are held fixed. In this section, we study several additional properties of $I'(X;Y)$.

Proposition 1: Let $f^*(y \mid x)$ be the channel that minimizes $I(X;Y)$ in (5), and hence its matched capacity is C_{LM}. Then, the mismatched capacity of $f^*(y \mid x)$ with a decoding metric $\ln V(y \mid x)$ is also C_{LM}.

This proposition, whose proof is evident from [20, Theorem 4.1], tells us that mismatched decoding with $\ln V(y \mid x)$ does not damage the *maximum* achievable rate (i.e., capacity) of $f^*(y \mid x)$. The following proposition provides a lower bound on $I'(X;Y)$, and hence another lower bound on the mismatched capacity.

Proposition 2:

$$I'(X;Y) \geq I(X;Y) - \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x)W(y \mid x)$$
$$\cdot \ln \frac{W(y \mid x)}{q_*(y \mid x)} + \sum_{y \in \mathscr{Y}} q(y) \ln \frac{q(y)}{q_*(y)} \tag{21}$$

where $I(X;Y)$ is the mutual information associated with W,

$$q_*(y \mid x) = \frac{V^S(y \mid x)}{a(x)b(y)},$$

$$q_*(y) = \sum_{x \in \mathscr{X}} p(x) q_*(y \mid x),$$

and where S, $\{a(x)\}_{x \in \mathscr{X}}$, and $\{b(y)\}_{y \in \mathscr{Y}}$ are positive numbers.

Of course, the tightest lower bound is obtained by maximizing the right-hand side of (21) w.r.t. S, $\{a(x)\}_{x \in \mathscr{X}}$, and $\{b(y)\}_{y \in \mathscr{Y}}$. This inequality is stronger than the following inequalities (proved in [21]):

$$I'(X;Y) \geq GMI(X;Y) \geq \tilde{R}_0 \tag{22}$$

where

$$GMI(X;Y) \triangleq \max_{S \geq 0} \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x) W(y \mid x) \cdot \ln \frac{V^S(y \mid x)}{\sum_{x' \in \mathscr{X}} p(x') V^S(y \mid x')} \tag{23}$$

is the GMI which is based on the Gallager bound [21], and $\tilde{R}_0$ is the GCR [27]. The GMI equals the right-hand side of (21) when $a(x) = b(y) = 1$ for all $x \in \mathscr{X}$, $y \in \mathscr{Y}$. Thus, in [21], the only free parameter for maximization of (23) is S. For $S = 1$, the GMI degenerates to Fischer's expression [16].

The proof of this proposition relies on exploiting the conditions for the $f(y \mid x)$ of [20, Theorem 4.1] and appears in Appendix B, along with the expressions for the optimum $\{a(x)\}$ and $\{b(y)\}$. (Note that C_{LM} is invariant if instead of $V(y \mid x)$ one uses $V(y \mid x)/[a(x)b(y)]$ for arbitrary positive $\{a(x)\}$ and $\{b(y)\}$ [3].)

It should be noted that the right-hand side of (21) is tight under the optimization of $\{a(x)\}$, $\{b(y)\}$ (detailed in Appendix B), and S (see also [14, Lemma 2]). For a DMC, the channel f that achieves $I'(X;Y)$ in (5) has the exact form as $\{q_*(y \mid x)\}$ (see [5]), where $\{a(x)\}$, $\{b(y)\}$, and S are defined so as to satisfy the constraints, and where the inequality constraint (6) is assumed to hold with equality (which is the case when $I'(X;Y) > 0$). Now, it is easy to see that the optimal $\{a(x)\}$ and $\{b(y)\}$ in Appendix B happen to satisfy these constraints. Therefore, $I'(X;Y)$ is actually given by the right-hand side of (21) under a further optimization over S.

A Rate-Distortion Interpretation: $I'(X;Y)$ can be viewed as a constrained rate distortion function, at a specified average distortion level D [defined as in (6)], where the distortion measure is $d(x,y) = -\ln V(y \mid x)$. This means that

$$\sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x) f(y \mid x) d(x,y) \leq D. \tag{24}$$

The additional constraint is the specification of the output marginal $q(y)$, $\forall y \in \mathscr{Y}$. This is a direct result of the basic definition in (5), (6).

For the case where the input and the output alphabets are such that there is a definition of a subtraction operation $(y - x)$, we use the above interpretation to derive lower bounds on I' for $d(x,y) = -\ln V(y \mid x) = \rho(y - x)$, i.e., for a difference metric corresponding to an additive channel. By the data processing theorem for the divergence [7],

$$\mathscr{D}(\{p(x)f(y \mid x)\} \parallel \{p(x)q(y)\}) \geq \mathscr{D}(\{m(y-x)\} \parallel \{m_I(y-x)\}) \tag{25}$$

where $m(y-x)$ is the PMF of $(y-x)$ that is induced by the joint PMF $p(x)f(y \mid x)$ and $m_I(y-x)$ is the PMF of $(y-x)$ that is induced by $p(x)q(y)$. The left-hand side of the above equation is the mutual information as defined in (4), and we are interested in obtaining the minimum over f to evaluate $I'(X;Y)$. Thus, we examine

$$\min_m \sum_z m(z) \ln \frac{m(z)}{m_I(z)} \tag{26}$$

where $z = y - x$, under the constraint

$$\sum_z m(z) \cdot \rho(z) \leq D \tag{27}$$

where the constraint that $m(y-x)$ is induced by a PMF $m(x,y)$ with fixed input and output marginals, p and q, has been relaxed. The solution is readily obtained as

$$m(z) = C_1 \cdot m_I(z) e^{\lambda \rho(z)} \tag{28}$$

where C_1 is a normalization constant and λ is chosen to satisfy (27). This further leads to the bound

$$I'(X;Y) \geq \ln C_1 + \lambda D. \tag{29}$$

This result calls for an extension to channels with continuous input and output alphabets (see Section VI), where the notions of additivity and a difference metric emerge naturally.

The following examples of memoryless channels with mismatched decoding are addressed:

Example 1—Combined BSC and Erasure Channel: The true channel W is depicted in Fig. 1(a), and the channel V associated with mismatched decoder is specified in Fig. 1(b). It is a model for error and erasure mismatched decoding. Assuming $1 - w_1 - w_2 > w_2$ and $1 - v_1 - v_2 > v_2$, one readily finds that $I'(X;Y) = I(X;Y)$. This is commensurate with the insight that the decoder has only to *count* erasures and errors, and the metric is not important as long as it does not inflict confusion of "1" to "0" and vice versa. If, on the other hand, $1 - w_1 - w_2 > w_2$ while $1 - v_1 - v_2 < v_2$, then the channel f that achieves $I'(X;Y)$ is equal to q, and hence $I'(X;Y) = 0$.

Example 2—Binary Input, 4-ary Output, Symmetric Channel: The true channel W is depicted in Fig. 2(a), and the channel V associated with the mismatched decoder is presented in Fig. 2(b). Assuming that $w_1 > w_2$, the mismatched metric V turns the channel into a useless one (in the sense that $I'(X;Y) = 0$) if both the relations

$$v_2 > v_1 \quad \text{and} \quad (v_2/v_1) > (v_0/v_3)^{(w_0 - w_3)/(w_1 - w_2)}$$

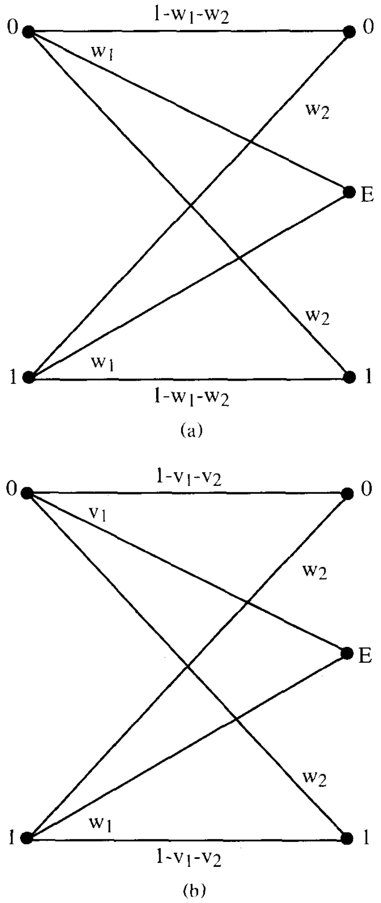

Fig. 1. A combined BSC and erasure channel. (a) True channel W. (b) Channel V corresponding to mismatched decoder.

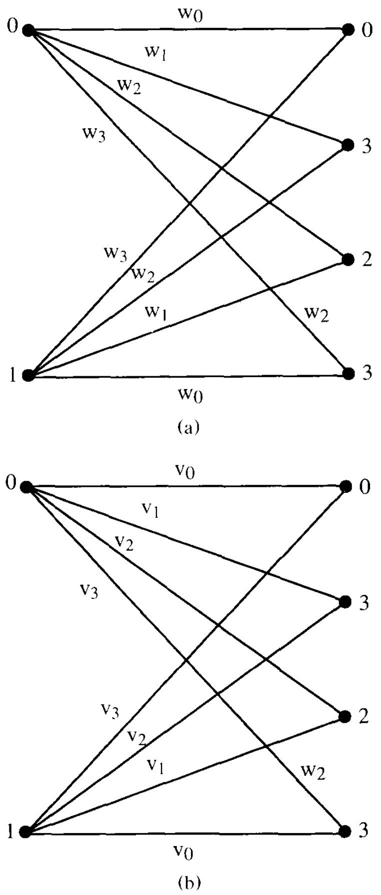

Fig. 2. A binary-input, 4-ary output symmetric channel. (a) True channel W. (b) Channel V corresponding to mismatched decoder.

hold. Otherwise, the channel f that achieves $I'(X;Y)$ is symmetric and satisfies

$$f_0 = (w_0 + w_3) \cdot \frac{v_3^\lambda}{v_0^\lambda + v_3^\lambda}$$

$$f_1 = (w_1 + w_2) \cdot \frac{v_2^\lambda}{v_1^\lambda + v_2^\lambda} \tag{30}$$

where $f_0 = f(0 \mid 0)$, $f_1 = f(1 \mid 0)$, and

$$f_0 + f_3 = w_0 + w_3, \qquad f_1 + f_2 = w_1 + w_2$$

where $\lambda \geq 0$ is chosen to satisfy the inequality constraint (6) with equality.

One notes the structure of the above expression, which is readily generalized to the general binary-input, M-ary output symmetric channel (see [3]). From the form of $f^*(y \mid x)$ in this case, and the formula for the $GMI(X;Y)$, one concludes the following result.

Proposition 3: For a binary-input, output symmetric channel with a correspondingly symmetric decoding metric, $GMI(X;Y) = I'(X;Y)$.

VI. Extension to Continuous Alphabet Channels

Theorem 4.1 of [20] is extended here to a wider class of memoryless channels where the input and output alphabets $\mathscr{X}$ and $\mathscr{Y}$ may be finite, countable (like in the Poisson channel [4]), or uncountable. Several examples will be discussed later.

Consider a memoryless channel characterized by the single-letter conditional probability density function (pdf) $W(y \mid x)$, $x \in \mathscr{X}$, $y \in \mathscr{Y}$, where $\mathscr{X}$ and $\mathscr{Y}$ designate the input and the output alphabets, respectively. Hereafter, the integral sign will be used as a generic symbol, where for the finite and countable alphabet case, it should be understood as a summation. Let $p(x)$, $x \in \mathscr{X}$ denote the single-letter marginal of a memoryless channel input pdf (i.e., a random coding pdf), and let $q(y)$, $y \in \mathscr{Y}$ denote the induced output marginal pdf, i.e., $q(y) = \int_{\mathscr{X}} p(x)W(y \mid x)\,dx$.

Let $\phi(x)$, $x \in \mathscr{X}$ denote a k-dimensional vector function $(\phi_1(x),\cdots,\phi_k(x))$ such that for every component j, $E\phi_j(X) \triangleq \int_{\mathscr{X}} dx \cdot p(x)\phi_j(x)$ is finite and the WLLN holds, i.e., $\Pr\{|n^{-1}\sum_{i=1}^n \phi_j(X_i) - E\phi_j(X)| \geq \epsilon\}$ tends to zero for every $\epsilon > 0$, where the probability is w.r.t. the n-fold power of p. Similarly, let $\psi(y)$, $y \in \mathscr{Y}$ denote an l-dimensional vector function $(\psi_1(y),\cdots,\psi_l(y))$ having finite expectations and satisfying the WLLN w.r.t. q. Next, define the parametric family of joint pdf's,

$$\mu_\theta(x,y) = \exp[a \cdot \phi(x) + b \cdot \psi(y) + c \ln V(y \mid x) - K(\theta)] \quad (31)$$

where $a = (a_1,\cdots,a_k)$ is a k-dimensional parameter vector, $b = (b_1,\cdots,b_l)$ is an l-dimensional parameter vector, $a \cdot \phi(x)$ and $b \cdot \psi(y)$ are the inner products, c is a scalar, θ is the $(k+l+1)$-dimensional concatenated vector (a,b,c), and $e^{-K(\theta)}$ is a normalization constant, where θ takes on values in an open bounded subset Θ of the set

$$\Theta_0 = \left\{\theta : \int_{\mathscr{X}\times\mathscr{Y}} dx\,dy \cdot \exp[a \cdot \phi(x) + b \cdot \psi(y) + c \ln V(y \mid x)] < \infty\right\}. \quad (32)$$

To establish the achievability result, we need some additional definitions. Let

$$h(X) \triangleq -\int_{\mathscr{X}} dx \cdot p(x) \ln p(x) \quad (33)$$

and

$$h(Y) \triangleq -\int_{\mathscr{Y}} dy \cdot q(y) \ln q(y) \quad (34)$$

denote the input differential entropy and the output differential entropy, respectively. Similarly, let

$$h_\theta(X,Y) = -E_\theta \ln \mu_\theta(x,y) \quad (35)$$

where E_θ denotes expectation w.r.t. μ_θ. We shall make the following assumptions throughout this section.

A1: There exists a positive number δ such that for every $-\delta < \gamma < \delta$,

$$\int_{\mathscr{X}\times\mathscr{Y}} dx\,dy \cdot p(x)q(y)V^\gamma(y \mid x) < \infty.$$

A2: The input differential entropy $h(X)$ is finite and $n^{-1} \ln p(X) \rightarrow h(X)$ in probability w.r.t. p. Similarly, $h(Y)$ is finite and $n^{-1} \ln p(Y) \rightarrow h(Y)$ in probability w.r.t. q. Finally, $D \triangleq -E \ln V(Y \mid X)$, where E denotes expectation w.r.t. $p \times W$ is finite and $n^{-1} \ln V(Y \mid X) \rightarrow -D$ in probability w.r.t. $p \times W$.

A3: The set $B = \{\theta \in \Theta : E_\theta\phi(X) = E\phi(X), E_\theta\psi(Y) = E\psi(Y), E_\theta \ln V(Y \mid X) \geq -D\}$ is nonempty.

It is easy to see that for every $\theta \in B$, we have

$$h_\theta(X;Y) = K(\theta) - a \cdot E\phi(X) - b \cdot E\psi(Y) - cE_\theta \ln V(Y \mid X). \quad (36)$$

Now, let

$$\begin{aligned} I'(X;Y) &= h(X) + h(Y) - \sup_{\theta\in B} h_\theta(X,Y) \\ &= h(X) + h(Y) + \inf_{\lambda \geq -D} \sup_{\theta' \in \Theta} \\ &\quad [a' \cdot E\phi(X) + b' \cdot E\psi(Y) + c'\lambda - K(\theta')] \end{aligned} \quad (37)$$

where $\theta' = (a',b',c')$. The following theorem is an extension of [12, Lemma 3] and [20, Theorem 4.1] to general memoryless channels.

Theorem 2: Assume that conditions A1–A3 are met. Then, for the memoryless channel W and the decoding metric V, every rate below $I'(X;Y)$ is achievable.

The proof appears in Appendix C.

Note that $I'(X;Y)$ is a nondecreasing function of k and l; that is, if one adds more input and output moment constraints, the bound improves. If the vector functions ϕ and ψ are chosen appropriately, then in the limit as k and l tend to infinity, these moment constraints may pose constraints on the marginals of μ_θ to be very close, in some sense, to p and q, respectively. For instance, if $\mathscr{X} = \mathscr{Y} = \mathbb{R}$ and if the components of ϕ and ψ are indicator functions of nonoverlapping narrow intervals whose union covers $\mathbb{R}$, then the equality constraints of B are interpreted as a requirement that the quantized versions of the marginals of μ agree with the corresponding quantized versions of p and q, respectively.

Another observation that should be made is that if the inequality constraint of B is satisfied with equality (as is the case when $I'(X;Y) > 0$), then $I'(X;Y)$ can be interpreted as the infimum of $I(X;Y)$ over *all* joint pdf's $\mu(x,y)$ whose marginals satisfy the moment constraints and $E_\mu \ln V(Y \mid X) \geq -D$, and not only all pdf's from the parametric form of μ_θ. This is true because the minimum-achieving pdf subject to moment equality constraints associated with $\phi(x)$, $\psi(y)$, and $\ln V(y \mid x)$ has the form of μ_θ (see also Proposition 2 and the comments thereafter). If, in addition, the input pdf is from the exponential family [26]

$$p(x) = \exp\{\alpha \cdot \phi(x) - K_x(\alpha)\} \quad (38)$$

where $\alpha \in \mathbb{R}^k$ and $e^{-K_x(\alpha)}$ is a normalization constant, and if the output marginal pdf's associated with both $p \times W$ and μ_θ are from the exponential family

$$q(y) = \exp\{\beta \cdot \psi(y) - K_y(\beta)\} \quad (39)$$

where, similarly, $\beta \in \mathbb{R}^l$ and $e^{-K_y(\beta)}$ is the normalization constant, then $I'(X;Y)$ may be interpreted as the infimum of $I(X;Y)$ over all joint pdf's $\mu(x,y)$ whose marginals *entirely* coincide with p and q, respectively, and $E_\mu \ln V(Y \mid X) = -D$. This is true because for exponential families, the expectations of the sufficient statistics ϕ and ψ dictate the parameter values. Finally, C_{LM} can be now defined as the supremum of $I'(X;Y)$ over all input pdf's p in a certain class.

It is easy to see that these conditions, as well as conditions A1–A3, are met for DMC's with memoryless inputs (as detailed in Appendix D), and therefore [20, Theorem

4.1] is obtained as a special case. Similarly, it is not difficult to verify that these conditions hold as well for Gaussian channels fed by Gaussian inputs, where the decoding metric is a possibly mismatched Euclidean metric.

We next discuss several examples that we believe provide some additional insight on the more general expression of C_{LM}.

Example 3—A Continuous Additive Noise Channel with a Euclidean Decoding Metric: Here, the channel model is $y_i = x_i + w_i$ where $\{w_i\}$ is an i.i.d. noise source with a symmetric marginal pdf around the origin. For any noise pdf that corresponds to a channel W that satisfies the above conditions, it is readily shown that for the Euclidean decoding, $I'(X;Y) > 0$ as long as $I(X;Y) > 0$. Moreover, it is easy to show that for a Gaussian codebook, $GMI(X;Y)$ coincides with the capacity of the additive white Gaussian channel with the same noise power. In fact, it has been shown by Thomas and Hughes [32] that the Gaussian capacity is achievable with a Gaussian codebook and Euclidean distance decoding for any bounded energy interference (see also [11]). Lapidoth [25] has recently shown that irrespective of the noise pdf, no rate above the Gaussian capacity can be achieved using random coding according to the Gaussian distribution in conjunction with a minimum Euclidean distance decoder.

Example 4—An AWGN Channel with an Unknown Signal Level: The channel model is $y_i = ax_i + w_i$, where $\{w_i\}$ is a zero-mean Gaussian white noise with variance σ^2, $\{x_i\}$ are zero-mean Gaussian memoryless inputs with variance σ_x^2, and $a > 0$ is an unknown constant. The mismatched decoder performs ML decoding based on $a = 1$. Following the formulation of a memoryless channel as above, one finds that

$$C_{LM} = \frac{1}{2}\ln\left(1 + \frac{a^2\sigma_x^2}{\sigma^2}\right) = C \tag{40}$$

regardless of the value of a. This is the expected result, since if one uses codewords having a constant energy (namely, $\sum_{j=1}^{n} x_{ij}^2 = E$, for all i), then there is no difference between the matched and mismatched ML metrics in this case; and it is known that capacity is achievable in the matched case using constant-energy codewords [30]. Note that in this case, it is readily shown that $GMI(X,Y) \le I(X;Y)$, and the difference between these quantities increases as the value of the parameter a decreases (below 1).

Example 5—A Two-Dimensional AWGN Channel with a Phase Offset: Here, the channel input is a two-dimensional, zero-mean Gaussian random vector, with variance of σ_x^2 per dimension. A circular-complex additive Gaussian noise with a variance of σ^2 in each of its statistically independent dimensions accompanies the signal. The mismatch, in this case, stems from an (unknown) phase offset ω (modeling, for example, inaccurate phase training). Equivalently, instead of the matched ML metric $\sum_{i=1}^{n}\|y_i - x_i\|^2$, the mismatched decoder uses $\sum_{i=1}^{n}\|y_i - e^{j\omega}x_i\|^2$. The minimization leading to $I'(X;Y)$ has been carried out, and after some algebraic manipulations, omitted here for the sake of brevity, one obtains

$$I'(X;Y) = \begin{cases} \ln\left[1 + \dfrac{\sigma_x^2\cos^2\omega}{\sigma_n^2 + \sigma_x^2(1-\cos^2\omega)}\right], \\ \qquad |\omega| \le \dfrac{\pi}{2}(\operatorname{mod} 2\pi) \\ 0, \qquad \text{otherwise.} \end{cases} \tag{41}$$

This expression shows an attenuation of $\cos^2\omega$ for the desired in-phase signal, and an excess noise of the cross-quadrature interference term $\sigma_x^2\sin^2\omega$. Thus, the familiar behavior of uncoded communications in the presence of a phase error ω is duplicated here as well. In view of the fact that the phase offset is fixed throughout the message interval, one might wonder whether this is indeed the highest achievable rate. This question will be addressed, among others, in the next section.

Example 6—The Vector Memoryless Gaussian Channel: Here, the so-called vector (or block) memoryless Gaussian channel [17] is analyzed, where the mismatched decoder is unaware of the noise autocorrelation matrix within each block and employs the common squared Euclidean distance metric. It is shown that the matched capacity can be achieved, as outlined below.

According to this model, a K-dimensional vector channel (column vectors are used throughout) has output vector $\boldsymbol{y}_i$, at discrete time i, given by

$$\boldsymbol{y}_i = \boldsymbol{x}_i + \boldsymbol{w}_i \tag{42}$$

where the input vector at time i is designated by $\boldsymbol{x}_i$, and the additive Gaussian noise vector $\boldsymbol{w}_i$ has possibly correlated components, although vectorwise $\boldsymbol{w}_i$ and $\boldsymbol{w}_j$ $(i \neq j)$ are statistically independent and identically distributed. Suppose ψ_i, $i \in 1,\cdots,K$ is an orthonormal basis for the $(K \times K)$ covariance matrix $\Gamma = E(\boldsymbol{w}\boldsymbol{w}^T)$ of the noise samples (of each block) where superscript T denotes the transpose. That is, $\Gamma = \Psi^T\Lambda\Psi$ where Ψ is the $K \times K$ orthonormal matrix specified by the column $\{\psi_i\}$ and Λ the associated diagonal eigenvalue matrix. The input vectors, constrained by an average power limitation, are formed (at the transmitter) by the well-known method [8], [22], [33], [34] of projecting the input symbols on Ψ, that is,

$$\boldsymbol{x}_i = \sum_{j=1}^{K} a_{ij}\psi_j \tag{43}$$

where $\{a_{ij}\}$ are the inputs of the jth virtual orthogonal subchannel, and have their energies determined according to the "water-pouring" principle [8], [17], [22], [33], [34]. Note that the above projection is power conserving, as

$$E\left[\boldsymbol{x}_i^T \cdot \boldsymbol{x}_i\right] = \sum_{j=1}^{K} a_{ij}^2.$$

A codeword, in this scheme, is composed of N uses [that is, $i \in 1,\cdots,N$ in (42)] of the vector channel. The code employed is a product of K independent subcodes (one for each subchannel), where the subcode for the jth channel is $\{a_{1j},\cdots,a_{Nj}\}$.

The optimal (matched) receiver correlates the received vector $\boldsymbol{x}_i$ with each of the $\{\psi_j\}$ vectors to obtain a separation of the vector channel to K independent scalar Gaussian (sub) channels [22], [33], [34]. It then performs ML decoding according to the metric

$$\boldsymbol{m} \triangleq \{m_j\} = \left\{\min \sum_{i=1}^{N} |y_{ij} - a_{ij}|^2, \qquad j \in 1,\cdots,K\right\} \quad (44)$$

where the minimization is carried over all the $\boldsymbol{a}$ sequences in the codebook and since a product code is employed the minimization is done for each subchannel $j = 1,2,\cdots,K$ separately. The observables y_{ij} are given by projecting $\boldsymbol{y}_i$ on the orthonormal basis $\{\psi_j\}$, that is, $y_{ij} = (\boldsymbol{y}_i, \psi_j)$, and clearly,

$$\boldsymbol{y}_i = \sum_{j=1}^{N} y_{ij}\psi_j.$$

The mismatched receiver adheres to the Euclidean-distance decoding, and is assumed to lack the knowledge of the set $\{\psi_j\}$, but does possess the set of possible $\boldsymbol{x}_i$, $i = 1,2,\cdots,N$ vectors, and also the mapping from the codewords $\{\boldsymbol{x}_i\}$ $i = 1,\cdots,N$ to the corresponding user messages.

Thus, the mismatched decoder performs the metric

$$m' = \min \sum_{i=1}^{N} |\boldsymbol{y}_i - \boldsymbol{x}_i|^2 = \min \sum_{i=1}^{N} \left| \sum_{j=1}^{K} (y_{ij} - a_{ij})\psi_j \right|^2 \quad (45)$$

where the minimization in the expression above is carried out over all the legitimate codewords $\{\boldsymbol{x}_i\}_{i=1}^{N}$. By Parseval's Theorem, m' is *equivalent* to

$$m' = \min \sum_{i=1}^{N} \sum_{j=1}^{K} |y_{ij} - a_{ij}|^2$$

where the minimization is (virtually) performed over the set of legitimate a sequences. As the code employed over the channel is a product code, the virtual m' above is equivalent to m'', where

$$m'' = \sum_{j=1}^{K} \min_{j} \sum_{i=1}^{N} |y_{ij} - a_{ij}|^2 \quad (46)$$

which is exactly the matched metric [see (44)].

Since the (matched) capacity of this channel can be achieved by a product code [7], [8], [22], [33], [34] as employed in this example, this capacity also remains unchanged in case of the Euclidean distance mismatched decoder. In contrast, Lapidoth [24] has shown recently that for the vector Gaussian channel considered here, classical random coding techniques fail to assess the true mismatched capacity, that is, C_{LM} for this case is *not* a tight bound. This serves as another counterexample to Hui's conjecture, which is practically encountered more frequently than the counterexample of [14] and [1].

The vector Gaussian channel considered in this example can serve as a model for decoding a pulse amplitude modulated (PAM) sequence in the presence of colored noise, assuming that the autocorrelation sequence of the noise samples has a finite support, and that appropriate guard times are used in the transmission.

The conclusion also holds for the case where the noise process does not have an autocorrelation function of finite support, but rather posses an autocorrelation function which decays with time such that the noise entropy is finite (that is, the integral of the related log spectrum is defined and finite). This can be shown by invoking the arguments which are used in the well-known treatments of the matched decoder with stationary, correlated inputs and sample-independent additive Gaussian noise [8], [22], [34].

The analogy to the standard intersymbol interference (ISI) Gaussian channels treated in [8], [22], [33], [34] is established by examining a block (K-component) channel, and orthogonalizing the noise by a linear information lossless operation which yields an equivalent block-ISI channel with independent Gaussian noise samples. The result follows by taking $K \to \infty$, and under the mild restrictions specified above, the effect of the intervector dependence on the capacity monotonically vanishes [8], [22], [34] as $K \to \infty$.

Lapidoth [24] has recently extended the above results to a class of ISI channels with i.i.d. Gaussian noise, where the receiver ignores the intersymbol interference and simply chooses the codeword which is of least Euclidean distance from the received sequence.

VII. Discussion: Other Notions of Mismatched Capacity

So far, we have considered only deterministic encoders and the message error probability criterion. Another underlying assumption is that the transmitter *is* aware of the mismatch, for otherwise, the meaning of the maximization in $C_{LM} = \max_p I'(X;Y)$ is questionable, at least for cases where the maximizing input assignment $\{p(x)\}$ depends on the mismatch; also, recall that the achievable rate depends on both W and V. In this section, a few examples are examined in which coding strategies *motivated by the nature of the mismatch* are employed. It is shown that the properties of achievable rates in the mismatched decoding regime might differ considerably from those of the classical matched one.

First, we focus on capacity w.r.t. the bit error probability as opposed to the one defined w.r.t. the block error probability. Consider a clean BSC [i.e., $w_1 = w_2 = 0$ in Fig. 1(a)], while the decoder assumes $v_1 = 0$ and $v_2 > 0.5$ [Fig. 1(b)]. It is easy to check that, here, $C_{LM} = 0$ [20], and hence also $C_M = 0$ [14]. However, suppose a variant of differential encoding as presented in Table I is employed. The first transmitted symbol is equal to the first information bit, and thereon the transmitted symbol changes from

TABLE I
A DIFFERENTIAL-TYPE CODE FOR THE BSC

Message	Transmitted codeword
000	000
001	001
010	011
011	010
100	111
101	110
110	100
111	101

TABLE II
A RANDOMIZED CODE FOR THE BSC

Message	Transmitted codeword
00	000, 111
01	001, 110
10	010, 101
11	011, 100

“0” to “1” or vice versa if the information bit is a “1”; otherwise, the symbol transmitted is identical to the previous one. The receiver performs the inverse mapping to the transmitter's, after the operation of channel ML decoding. Even if there is a confusion of 1's to 0's (and vice versa) in the decoder, the receiver will be able to recover the transmitted bits reliably except for the *first* bit (which will always be wrong in this case). Thus, the message (block) error probability tends to unity while the bit error probability goes to zero as $n \to \infty$. Observe, though, that the latter does not have an exponential behavior; rather, it goes to zero as fast as $1/n$. For any $w_2 < 0.5$, a positive rate less than C is achievable w.r.t. the bit error probability by using asymptotically large codewords. Similar arguments can be applied to the complex Gaussian channel with a phase offset of $\pi/2$ (Example 5 of Section VI) when the same differential-type code is used.

For the latter channel, note that we *ruled out* the possibility that the transmitter shifts the transmitted symbol phases (in order to compensate for the phase offset) while the decoder is unaware of this operation; for in this case, the codeword to transmitted signal mapping is *not* identical to the receiver mapping (of received signal to received codeword). Another class of interesting mismatched problems emerges when the transmitter is allowed to change its strategy to mitigate the receiver's mismatch degradation. In the above example, it is clear that by deshifting the phase, the transmitter absolutely compensates for this mismatch. It is readily seen that for a general DMC, the transmitter may introduce any supplementary DMC in tandem in an effort to maximize the overall achievable rate, although it is clear that the matched capacity cannot be increased with this strategy. It readily follows that maximizing C_{LM} over all input permutations (that is, the supplementary DMC is the noiseless permuting channel) is also an achievable rate. The argument extends to multiletter interpretations.

Next, it will be shown that some forms of *randomized* encoding–decoding strategies are capable of achieving rates higher than C_{LM} w.r.t. block error probability. Let us reconsider the clean BSC with the mismatched decoder that assumes $v_1 = 0$ and $v_2 > 0.5$, and suppose that a randomized strategy, as outlined in Table II, is employed. This means, for example, that the two-bit message “00” is transmitted by randomly choosing between either $\boldsymbol{x}_1$ = “000” or $\boldsymbol{x}_2$ = “111.” The receiver, being fully aware of this strategy, uses a metric $\ln[\frac{1}{2}V(\boldsymbol{y} \mid \boldsymbol{x}_1) + \frac{1}{2}V(\boldsymbol{y} \mid \boldsymbol{x}_2)]$. Clearly, one is able to communicate reliably employing this method, with a rate of $2/3$ bits per channel use, while $C_{LM} = C_M = 0$. Moreover, by creating codewords of length n using the same idea, it is possible to achieve a rate of $(n-1)/n$ bits per channel use. As a side remark, a decoder that uses the metric $\ln V(\boldsymbol{y} \mid \boldsymbol{x})$ and *then* performs the inverse mapping, after the decision on a sequence (e.g., “000” → “00,” “111” → “00”), would be inferior to the decoder described above, but will still be able to cope with the mismatch. Again, for $w_1 = 0$ and $0 < w_2 < 0.5$, rates close to the capacity are achievable by using sufficiently long codewords based on the above method.

Such a randomized strategy can be adapted to the complex Gaussian channel with a phase offset (Example 5 above) in the following manner. For any (complex) input vector $\boldsymbol{x}$, the transmitter selects among four options $\boldsymbol{x}$, $\boldsymbol{x}e^{j\pi/2}$, $\boldsymbol{x}e^{j\pi}$, $\boldsymbol{x}e^{j3\pi/2}$. The receiver has the reversed table in tandem to the decoder. Clearly, one can achieve reliable communications with rate $R > 0$, for any phase offset, while $I'(X;Y)$ (and hence, C_{LM}) become negligibly small for ω in the vicinity of $\pi/2$. Recall that strictly employing random coding would *not* achieve a reliable rate larger than C_{LM}.

In the above example, subtle mappings between the information source and the encoder (as well as between the decoder and the receiving destination) were allowed to improve the achievable rates for a given channel, encoder, and a given metric. One may further argue that another class of cases is established when the communication engineer optimizes over all modulation/coding options under a given mismatched channel. As an example, for a channel with a possibly large phase offset, one may use *noncoherent* communication. It is well known that such a scheme can achieve the matched Shannon capacity asymptotically as $n \to \infty$ in the presence of a random phase [9]. As another example, for a mismatched binary input/output channel, use the common differential encoding/decoding mechanism. In these cases, one may degrade the performance of a matched channel in some sense (e.g., the exponential behavior of P_e), but gain considerably in a “worse case” mismatched channel. One may also consider the case of time-varying channels, where one may optimize the worst case $I'(X;Y)$. (Recall the idea of optimizing the decoder metric for a class of unknown channels [31].) These cases hint at the connection of our subject to the analysis of compound and arbitrarily varying channels [13], [35] as is further elaborated in [14].

The above examples demonstrate another interesting fact for mismatched channels: "data processing"-type arguments [17] do not necessarily hold. Consider the BSC with $w_2 < 0.5$ and a decoder using $v_2 > 0.5$ on which a randomized encoding mechanism is employed: the fact that the actual transmitted sequence is *not* disclosed to the receiver actually *improves* the performance in this case.

Returning to the common case of deterministic encoder/decoder mapping strategies, the mismatched capacity C_M has not yet been determined, and it has been conjectured in [14] that for a DMC, it equals the limit as $k \to \infty$ of C_{LM}^k, which is defined as C_{LM} but w.r.t. k-letter alphabet extensions of the channel and the mismatched metric.

Appendix A

Let $\epsilon > 0$ and $\delta > 0$ satisfy $\epsilon p(a) = \delta p(a')$. Let f be identical to W, except for the entries corresponding to a, a', b, and b', where $f(b \mid a) = W(b \mid a) + \epsilon$, $f(b' \mid a') = W(b' \mid a') + \delta$, $f(b \mid a') = W(b \mid a') - \delta$, and $f(b' \mid a) = W(b' \mid a) - \epsilon$, and where δ and ϵ are chosen sufficiently small so that all the entries of f remain in [0, 1]. Now,

$$\begin{aligned}\sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} & p(x) f(y \mid x) \ln V(y \mid x) \\ &- \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x) W(y \mid x) \ln (y \mid x) \\ &= p(a)\epsilon \ln V(b \mid a) + p(a')\delta \ln V(b' \mid a') \\ &\quad - p(a)\epsilon \ln V(b' \mid a) - p(a')\delta \ln V(b \mid a') \\ &= p(a)\epsilon[\ln V(b \mid a) + \ln V(b' \mid a') \\ &\quad - \ln V(b' \mid a) - \ln V(b \mid a')], \qquad (A.1)\end{aligned}$$

which is positive by the assumption on the positivity of the expression in the brackets. Similarly, it is easy to see that the above f satisfies the output marginality constraint of (6).

Appendix B

Proof of Proposition 2

Using the conditions on the transition probability matrix f w.r.t. the channel and the mismatched metric (6), one has

$$\begin{aligned}- \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} & p(x) f(y \mid x) \log \frac{V^S(y \mid x)}{a(x) b(y)} \\ &\le - \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x) W(y \mid x) \log \frac{V^S(y \mid x)}{a(x) b(y)} \qquad (B.1)\end{aligned}$$

for any $S \ge 0$ and $a(x)$, $b(x)$ nonnegative functions (absolutely continuous w.r.t. $V(y \mid x)$). Let

$$q_*(y \mid x) \triangleq \frac{V^S(y \mid x)}{a(x) \cdot b(y)},$$

multiply and divide the argument of the logarithm on the left-hand side of (B.1) by $f(y \mid x)$, and the right-hand side of (B.1) by $W(y \mid x)$ to obtain

$$\begin{aligned}H'(Y \mid X) &+ \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x) f(y \mid x) \log \frac{f(y \mid x)}{q_*(y \mid x)} \\ &\le H(Y \mid X) + \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} p(x) W(y \mid x) \log \frac{W(y \mid x)}{q_*(y \mid x)} \qquad (B.2)\end{aligned}$$

where $H(Y \mid X)$ and $H'(Y \mid X)$ designate the conditional entropies for the channels with $W(y \mid x)$ and $f(y \mid x)$, respectively. One readily realizes (see, e.g., the proof of Theorem 4.3.6 in [7]) that the second term on the left-hand side of (B.2) is lower bounded by

$$\begin{aligned}\sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} & p(x) f(y \mid x) \log \frac{f(y \mid x)}{q_*(y \mid x)} \\ &\ge \sum_{y \in \mathscr{Y}} q(y) \log \frac{q(y)}{q_*(y)} \qquad (B.3)\end{aligned}$$

where $q_*(y) = \sum_{x \in \mathscr{X}} p(x) q_*(y \mid x)$.

From (B.2) and (B.3), the relation (21) follows immediately. To optimize this lower bound on $I'(X;Y)$, let $b(y) = [\sum_{x \in \mathscr{X}} V^S(y \mid x)/a(x)]/q(y)$, and the optimum $\{a(x)\}$ is obtained as $a(x) = [\sum_{y \in \mathscr{Y}} V^S(y \mid x)]/b(y)$. By standard optimization methods, it is realized that $\{q_*(y \mid x)\}$ with the above optimized parameters achieves $I'(X;Y)$ whenever it is positive. See also [3] and [14].

Appendix C

I. Proof of Theorem 2

The proof involves a technique similar to that of [20], where rather than upper bounding cardinalities of sets of typical finite-alphabet sequences by combinatorial techniques, we bound *volumes* of types of continuous alphabet sequences using probabilistic arguments. For the sake of completeness, the pertinent results of [12] and [20] will be rederived here.

Consider a randomly chosen codebook, where each codeword $\boldsymbol{x}_i \in \mathscr{X}^n$ is drawn independently from $p(\boldsymbol{x}) = \prod_{i=1}^n p(x_i)$ with the requirement that it will be typical, i.e., it falls in ϵ-type:

$$T_\epsilon^x(p) = \left\{ \boldsymbol{x} \in \mathscr{X}^n : \left| -\frac{1}{n} \ln p(\boldsymbol{x}) - h(X) \right| < \epsilon, \right.$$
$$\left. \max_{1 \le j \le k} \left| \frac{1}{n} \sum_{i=1}^n \phi_j(x_i) - E\phi_j(X) \right| < \epsilon \right\}. \qquad (C.1)$$

In other words, if a randomly drawn codeword $\boldsymbol{x}$ happens to be atypical, we randomly select a new codeword, check whether it is typical, and so on, until it turns out to be typical. Note that the overall probability of $\boldsymbol{x}$ being a codeword is

$$p(\boldsymbol{x} \mid T_\epsilon^x(p)) = \frac{p(\boldsymbol{x})}{p(T_\epsilon^x(p))} \le \frac{p(\boldsymbol{x})}{1 - \delta} \qquad (C.2)$$

where by the WLLN, $\delta > 0$ can be made arbitrarily small for every $\epsilon > 0$ provided that n is sufficiently large. Consider next an auxiliary threshold decoder which decodes $\boldsymbol{x}_i$ as the transmitted message if and only if the received $\boldsymbol{y}$ falls in the ϵ-type of the output sequences,

$$T_\epsilon^y(q) = \left\{ \boldsymbol{y} \in \mathscr{Y}^n : \left| -\frac{1}{n} \ln q(\boldsymbol{y}) - h(Y) \right| < \epsilon, \right.$$

$$\left. \max_{1 \le j \le l} \left| \frac{1}{n} \sum_{i=1}^{n} \psi_j(y_i) - E\psi_j(Y) \right| < \epsilon \right\}, \quad \text{(C.3)}$$

and $\boldsymbol{x}_i$ is the *only* message that together with $\boldsymbol{y}$ falls in the set

$$T_\epsilon^+ = \left\{ (\boldsymbol{x}, \boldsymbol{y}) : \frac{1}{n} \ln V(\boldsymbol{y} \mid \boldsymbol{x}) > -D - \epsilon \right\}; \quad \text{(C.4)}$$

otherwise, an error is declared. Let P_e denote the probability of error associated with the ML decoder that assumes a channel V, and let $\tilde{P}_e$ denote the probability of error associated with the auxiliary threshold decoder defined above. Then, clearly, $\tilde{P}_e$ is never smaller than P_e because whenever the threshold decoder does not reject, its output is identical to that of the mismatched decoder under consideration. Hence, it is sufficient to overbound $\tilde{P}_e$. From symmetry of the random coding mechanism, it is clear that the conditional error probability given that message i has been transmitted is the same for all $1 \le i \le M$, and hence equal to the overall error probability. Thus,

$$\begin{aligned} \tilde{P}_e &= \Pr\{\boldsymbol{y} \notin T_\epsilon^y(q) \text{ or } (\boldsymbol{x}_i, \boldsymbol{y}) \notin T_\epsilon^+ \\ &\qquad \text{or } \{\boldsymbol{y} \in T_\epsilon^y(q) \text{ and } \exists j \ne i : (\boldsymbol{x}_j, \boldsymbol{y}) \in T_\epsilon^+\}\} \\ &\overset{(a)}{\le} \Pr\{\boldsymbol{y} \notin T_\epsilon^y(q)\} + \Pr\{(\boldsymbol{x}, \boldsymbol{y}) \notin T_\epsilon^+\} \\ &\qquad + (M-1) \int_{T_\epsilon^+ \cap (T_\epsilon^x(p) \times T_\epsilon^y(q))} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x} \mid T_\epsilon^x(p)) q(\boldsymbol{y}) \\ &\overset{(b)}{\le} 2\delta + \frac{e^{nR}}{1-\delta} \int_{T_\epsilon^+ \cap (T_\epsilon^x(p) \times T_\epsilon^y(q))} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \qquad \text{(C.5)} \end{aligned}$$

where we have used the union bound and the WLLN for the two terms after (a) (Assumption A2), and where the third term after (a) results because, for the random coding scheme $\boldsymbol{x}_j (j \ne i)$ and the received vector $\boldsymbol{y}$, given $\boldsymbol{x}_i$ is transmitted, are independent. Thus, the proof will be complete if we show that the integral in the last term is exponentially less than $e^{-nI'(X;Y)}$.

Let C be an arbitrarily large number, and define the sets $G = \{(\boldsymbol{x}, \boldsymbol{y}) : |\ln V(\boldsymbol{y} \mid \boldsymbol{x})| \le C \cdot n\}$, $E = G \cap T_\epsilon^+ \cap (T_\epsilon^x(p) \times T_\epsilon^y(q))$, and

$$T_\epsilon(\lambda) = \left\{ (\boldsymbol{x}, \boldsymbol{y}) : \left| \frac{1}{n} \sum_{i=1}^{n} \ln V(y_i \mid x_i) - \lambda \right| \le \epsilon \right\}. \quad \text{(C.6)}$$

The last term on the right-hand side of (C.5) can be overbounded as follows:

$$\begin{aligned} &\int_{T_\epsilon^+ \cap (T_\epsilon^x(p) \times T_\epsilon^y(q))} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \\ &\qquad \le \int_E d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) + \int_{G^c} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}). \qquad \text{(C.7)} \end{aligned}$$

It is shown in Section II of this Appendix that under Assumption A1, if C is chosen sufficiently large,

$$\int_{G^c} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \le e^{-n(R+\epsilon)} \quad \text{(C.8)}$$

for all large n, and hence this term has a vanishingly small contribution in (C.7). As for the first term on the right-hand side of (C.7), the integration domain which is a subset of G can be covered by less than $N = 2C/\epsilon$ sets $\{T_\epsilon(\lambda_i)\}_{i=1}^N$, corresponding to a sufficiently dense grid of numbers $\lambda_i \in [-C, C]$. Therefore, this term can be overbounded as follows:

$$\begin{aligned} &\int_E d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \\ &\qquad \le e^{-n[h(X)-\epsilon]} e^{-n[h(Y)-\epsilon]} \sum_{i=1}^{N} \int_{T_\epsilon(\lambda_i) \cap E} d\boldsymbol{x}\, d\boldsymbol{y} \qquad \text{(C.9)} \end{aligned}$$

where we have used the fact $\boldsymbol{x}$ and $\boldsymbol{y}$ are typical in the integration domain. It is shown in Section III of this Appendix, invoking a technique similar to [10, Theorem 9.2.2], that

$$\int_{T_\epsilon(\lambda) \cap E} d\boldsymbol{x}\, d\boldsymbol{y} \le \exp[n(\hat{h}(\lambda) + L \cdot \epsilon)] \quad \text{(C.10)}$$

for some constant $L > 0$, where $\hat{h}(\lambda) = \inf_{\theta' \in \Theta} \hat{h}(\theta', \lambda)$,

$$\hat{h}(\theta', \lambda) \triangleq K(\theta') - a' \cdot E\phi(X) - b' \cdot E\psi(Y) - c'\lambda,$$

and $\theta' = (a', b', c')$. Thus,

$$\begin{aligned} &\int d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \\ &\qquad \le e^{-n[h(X)+b(Y)-2\epsilon]} \left(\frac{2C}{\epsilon} \right) \max_i \exp\{n[\hat{h}(\lambda_i) + L\epsilon]\} \\ &\qquad \le \exp\left\{ -n \left[h(X) + h(Y) - \sup_{\lambda \ge -D-\epsilon} \hat{h}(\lambda) - \delta \right] \right\} \\ &\qquad\qquad \text{(C.11)} \end{aligned}$$

where $\delta = (L+2)\epsilon + n^{-1} \ln(2C/\epsilon)$. Thus, for $R < I'(X;Y) - \delta$, the average probability of error tends to zero. Finally, by letting $n \to \infty$, $\epsilon \to 0$ (and hence also $\delta \to 0$), one readily sees that every rate below $I'(X;Y)$ is achievable by random coding w.r.t. p. This completes the proof of Theorem 2.

II. Proof of (C.8)

Let us partition G^c into $G_+^c = \{(\boldsymbol{x}, \boldsymbol{y}) : \ln V(\boldsymbol{y} \mid \boldsymbol{x}) \ge Cn\}$ and $G^c = \{(\boldsymbol{x}, \boldsymbol{y}) : \ln V(\boldsymbol{y} \mid \boldsymbol{x}) \le -Cn\}$. Since

$$\begin{aligned} &\int_{G^c} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \\ &\qquad = \int_{G_+^c} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) + \int_{G_-^c} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}), \qquad \text{(C.12)} \end{aligned}$$

it is sufficient to show that each one of the terms on the right-hand side of (C.12) can be made exponentially less than e^{-nR} for a sufficiently large C. Let $\gamma > 0$ be sufficiently small such that Assumption A2 holds. Then, by the Chernoff bound,

$$\begin{aligned} &\int_{G_+^c} d\boldsymbol{x}\, d\boldsymbol{y} p(\boldsymbol{x}) q(\boldsymbol{y}) \\ &\qquad \le e^{-Cn\gamma} \left[\int_{\mathscr{X}} \int_{\mathscr{Y}} dx\, dy \cdot p(x) q(y) V^\gamma(y \mid x) \right]^n. \qquad \text{(C.13)} \end{aligned}$$

It is now readily seen that by choosing C larger than $\gamma^{-1}\{R + \ln[\int_{\mathscr{X}} \int_{\mathscr{Y}} dx\, dy \cdot p(x) q(y) V^\gamma(y \mid x)]\}$, the probability of G_+^c under the product measure $p \times q$ can be made exponentially less than e^{-nR}. A similar argument holds for G_-^c with $\gamma < 0$ and C replaced by $-C$. This completes the proof of (C.8).

III. Proof of (C.10)

For every parameter value $\theta' = (a', b', c') \in \Theta$,

$$
\begin{aligned}
1 &\geq \mu_{\theta'}\{T_\epsilon(\lambda) \cap E\} \\
&= \int_{T_\epsilon(\lambda)\cap E} dx\,dy \exp\left\{n\left[a' \cdot \frac{1}{n}\sum_{i=1}^{n} \phi(x_i) + b' \right.\right. \\
&\qquad \left.\left. \cdot \frac{1}{n}\sum_{i=1}^{n} \psi(y_i) + c' \cdot \frac{1}{n}\sum_{i=1}^{n} \ln V(y_i \mid x_i) - K(\theta')\right]\right\} \\
&\geq \int_{T_\epsilon(\lambda)\cap E} dx\,dy \exp\{n[a' \cdot E\phi(X) + b' \\
&\qquad \cdot E\psi(Y) + c'\lambda - K(\theta') - \zeta]\} \\
&= \exp\{n[a' \cdot E\phi(X) + b' \cdot E\psi(Y) + c'\lambda \\
&\qquad - K(\theta') - \zeta]\} \cdot \int_{T_\epsilon(\lambda)\cap E} dx\,dy
\end{aligned}
\tag{C.14}
$$

where $\zeta = \zeta(\epsilon) = \epsilon(\Sigma_{j=1}^{k}|a_j| + \Sigma_{j=1}^{l}|b_j| + |c|)$. Thus,

$$
\begin{aligned}
\int_{T_\epsilon(\lambda)\cap E} dx\,dy \leq \exp\{n[K(\theta') - a' \cdot E\phi(X) - b' \\
\cdot E\psi(Y) - c'\lambda + \zeta(\epsilon)]\}.
\end{aligned}
\tag{C.15}
$$

Since this holds for every θ', the tightest upper bound is obtained by minimizing the right-hand side of (C.15) over Θ. Since Θ is assumed a bounded set, then $\zeta < L\epsilon$ for some constant L, and hence this minimization is equivalent to the minimization of $\hat{h}(\theta', \lambda)$ which yields $\hat{h}(\lambda)$, i.e.,

$$\int_{T_\epsilon(\lambda)\cap E} dx\,dy \leq \exp\{n[\hat{h}(\lambda) + L\epsilon]\}. \tag{C.16}$$

This completes the proof of (C.10).

Appendix D

We first show that a memoryless source is from an exponential family (see also [26, p. 28]). For a finite alphabet $\mathscr{X}$, the number of *free* parameters (letter probabilities) is $k = |\mathscr{X}| - 1$. Therefore, $p(x)$ can be represented by (38) if we assume, without loss of generality, that $\mathscr{X} = \{0, 1, \cdots, k\}$, define $\alpha = (\alpha_1, \cdots, \alpha_k)$, where $\alpha_i = \ln[p(i)/p(0)]$, $1 \leq i \leq k$, $\phi(x) = (\phi_1(x), \cdots, \phi_k(x))$, where $\phi_i(x)$, $i, x \in \{1, \cdots, k\}$ is the indicator function of $x = i$, and finally, let $K_x(\alpha) = -\ln[1 + \Sigma_{i=1}^{k} e^{\alpha_i}]$.

The output pdf q induced by a discrete memoryless source p and a DMC W is again memoryless, and hence also a source from an exponential family. Any joint PMF of the form corresponding to μ_θ is again a memoryless source for pair letters. Assumption A1 holds trivially whenever $V(y \mid x)$ is bounded. Assumption A2 holds as well as by the WLLN for memoryless processes. The set B corresponds to the constraints in (6). The minimization of $\hat{h}(\theta', \lambda)$ over θ' for a given λ yields the joint empirical entropy $H_{xy}(X, Y)$ because it is equivalent to ML estimation for the exponential family

$$\ln m(x, y) \equiv -n[H_{xy}(X, Y) - \mathscr{D}(p_{xy} \,\|\, m)] \tag{D.1}$$

where the maximum is attained when $\mathscr{D}(p_{xy} \,\|\, m) = 0$, and only the term of the empirical entropy remains. Therefore, $I'(X; Y)$ becomes the minimum mutual information over all joint PMF's for which the input and output marginals are given (and hence also the corresponding marginal entropies), and $E_{xy} \ln V(Y \mid X) \geq E \ln V(Y \mid X)$.

Acknowledgment

The authors are grateful to I. Csiszár, P. Narayan, T. Cover, E. Ordentlich, and R. Wesel for stimulating discussions, and to S. Verdú whose comments have greatly contributed to the lucidity of the presentation and driven us to further generalize the results on continuous alphabet channels.

References

[1] R. Ahlswede, N. Cai, and Z. Zhang, "Erasure, list and detection zero-error capacities for low noise and a relation to identification," Univ. Bielefeld, Tech. Rep. 93-068, Nov. 1993.

[2] M. E. Arutyunyan, "Bounds on E-capacity of a channel with a random parameter," *Probl. Inform. Transmission*, vol. 27, pp. 14–23, Jan.–Mar. 1991.

[3] V. B. Balakirsky, "Coding theorem for discrete memoryless channels with given decision rules," in *Lecture Notes in Comput. Sci. 573, Proc. 1st French–Soviet Workshop Algebraic Coding*, July 1991, pp. 142–150.

[4] D. Ben-Eli, Y. E. Dallal, and S. Shamai (Shitz), "Performance bounds and cut-off rates of quantum limited OOK with optical amplification," to appear in *IEEE J. Select. Areas Commun.* Also, in *Proc. 1994 Int. Symp. Inform. Theory*, p. 78, Trondheim, Norway, June 1994.

[5] T. Berger, *Rate Distortion Theory.* Englewood Cliffs, NJ: Prentice-Hall, 1971.

[6] L. Biederman, J. K. Omura, and P. C. Jain, "Decoding with approximate channel statistics," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 697–708, Nov. 1981.

[7] R. E. Blahut, *Principles and Practice of Information Theory.* Reading, MA: Addison-Wesley, 1987.

[8] L. H. Brandenburg and A. D. Wyner, "Capacity of the Gaussian channel with memory: The multivariate case," *Bell Syst. Tech. J.*, vol. 53, pp. 745–778, May–June 1974.

[9] S. A. Butman, I. Bar-David, B. K. Levitt, R. F. Lyon, and M. J. Klass, "Design criteria for noncoherent Gaussian channels with MFSK signaling and coding," *IEEE Trans. Commun.*, vol. COM-24, pp. 1078–1088, Oct. 1976.

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

[11] I. Csiszár, "Arbitrarily varying channel with general alphabets and states," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1725–1742, Nov. 1992.

[12] I. Csiszár and J. Körner, "Graph decomposition: A new key to coding theorems," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 5–12, Jan. 1981.

[13] ——, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* New York: Academic, 1981.

[14] I. Csiszár and P. Narayan, "Channel capacity for a given decoding metric," to appear in *IEEE Trans. Inform. Theory*. See also *Proc. 1994 Int. Symp. Inform. Theory*, p. 378, Trondheim Norway, June 1994.

[15] D. Divsalar, "Performance of mismatched receivers on bandlimited channels," Ph.D. dissertation, Univ. California, Los Angeles, Dec. 1978.

[16] T. R. M. Fischer, "Some remarks on the role of inaccuracy in Shannon's theory of information transmission," in *Proc. 8th Prague Conf. Inform. Theory*, 1971, pp. 211–226.

[17] R. G. Gallager, *Information Theory and Reliable Communications.* New York: Wiley, 1968.

[18] E. Geraniotis, "Minimax robust coding for channels with uncertain statistics," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 802–811, Nov. 1985.

[19] M. L. Honig, S. P. Boyd, B. Gopinath, and E. Rantapaa, "On optimal signal sets for digital communications with finite precision and amplitude constraints," *IEEE Trans. Commun.*, vol. 39, pp. 249–255, Feb. 1991.

[20] J. Y. N. Hui, "Fundamental issues of multiple accessing," Ph.D. dissertation, M.I.T., ch. IV, 1983.

[21] G. Kaplan and S. Shamai (Shitz), "Information rates of compound channels with application to antipodal signaling in a fading environment," *AËU*, vol. 47, no. 4, pp. 228–239, 1993. (Also, in G. Kaplan, "Reliable communication over compound and mis-

matched channels," Ph.D. dissertation, Technion—I.I.T., May 1993.)

[22] S. Kasturia, J. T. Aslanis, and J. M. Cioffi, "Vector coding for partial response channels," *IEEE Trans. Inform. Theory*, vol. 36, pp. 741–762, July 1990.

[23] D. Kazakos, "Upper and lower bounds for noisy channel coding under mismatch," in *Proc. 1981 Conf. Inform. Sci. Syst.*, Johns Hopkins Univ., Mar. 1981, pp. 37–42.

[24] A. Lapidoth, "On information rates for mismatched decoders," in *Proc. 2nd Int. Winter Meeting on Coding and Inform. Theory*, Essen, Germany, Dec. 1993.

[25] ——, "Mismatched decoding and the multiple access channel," in *Proc. Int. Symp. Inform. Theory*, Trondheim, Norway, June 1994.

[26] E. L. Lehmann, *Theory of Point Estimation.* New York: Wiley, 1983.

[27] J. K. Omura and B. K. Levitt, "Coded error probability evaluation for antijam communication systems," *IEEE Trans. Commun.*, vol. COM-30, pp. 896–903, May 1982.

[28] W. L. Root, "Estimates of ϵ-capacity for certain linear communication channels," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 361–369, May 1968.

[29] J. Salz and E. Zehavi, "Decoding under integer metrics constraints," to appear in *IEEE Trans. Commun.*

[30] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Syst. Tech. J.*, vol. 38, pp. 611–656, May 1959.

[31] I. G. Stiglitz, "A coding theorem for a class of unknown channels," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 217–220, Apr. 1967.

[32] T. G. Thomas and B. Hughes, "Exponential error bounds for random codes on Gaussian arbitrarily varying channels," *IEEE Trans. Inform. Theory*, vol. 37, pp. 643–649, May 1991.

[33] B. S. Tsybakov, "Capacity of a vector Gaussian channel without memory," *Probl. Peredach. Inform.*, vol. 1, pp. 26–40, 1965.

[34] ——, "Capacity of a discrete-time Gaussian channel with a filter," *Probl. Peredach. Inform.*, vol. 6, pp. 78–82, 1970.

[35] J. Wolfowitz, *Coding Theorems of Information Theory.* Englewood Cliffs, NJ: Springer-Verlag, 1978.

[36] A. D. Wyner, "A bound on the number of distinguishable functions which are time-limited and approximately band-limited," *SIAM J. Appl. Math.*, vol. 27, pp. 289–297, May 1973.

[37] J. Ziv, "Universal decoding for finite-state channels," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 453–460, July 1985.