# Cooperative multi-sensor detection under variable-length coding

Mustapha Hamad, Michèle Wigger, Mireille Sarkiss

# Cooperative Multi-Sensor Detection under Variable-Length Coding

Mustapha Hamad
*LTCI, Telecom Paris, IP Paris*
91120 Palaiseau, France
mustapha.hamad@telecom-paris.fr

Michèle Wigger
*LTCI, Telecom Paris, IP Paris*
91120 Palaiseau, France
michele.wigger@telecom-paris.fr

Mireille Sarkiss
*SAMOVAR, Telecom SudParis, IP Paris*
91011 Evry, France
mireille.sarkiss@telecom-sudparis.eu

***Abstract*—We investigate the testing-against-independence problem over a cooperative MAC with two sensors and a single detector under an average rate constraint on the sensors-detector links. For this setup, we design a variable-length coding scheme that maximizes the achievable type-II error exponent when the type-I error probability is limited to $\epsilon$. Similarly to the single-link result, we show here that the optimal error exponent depends on $\epsilon$ and that variable-length coding allows to increase the rates over the optimal fixed-length coding scheme by the factor $(1-\epsilon)^{-1}$.**

***Index Terms*—Distributed Hypothesis Testing, Cooperative MAC, Variable-Length Coding, Error Exponent**

## I. Introduction

Motivated by the broadly emerging Internet of Things (IoT) applications, distributed hypothesis testing problems gained increasing attention recently. In such problems, sensors send information about their observations to one or multiple decision centers. Then, the decision centers attempt to detect the joint distributions underlying the data observed at all the terminals including their own observations.

Our focus is on binary hypothesis testing with a null hypothesis and an alternative hypothesis. We are interested in maximizing the exponential decay (in the number of observed samples) of the probability of error under the alternative hypothesis, given a constraint on the probability of error under the null hypothesis. The study of such a Stein setup has a long history in the information theoretic literature, see e.g., [1]–[8] which study point-to-point, interactive, cascaded, and multi-sensor and/or multi-detector systems. All these works constrain the *maximum* rate of communication between terminals, and a fixed-length communication scheme is obviously optimal. Recently, the authors of [9] proposed to only constrain the *average* rate of communication, and they presented a variable-length coding scheme that under this weaker constraint improves the maximum achievable error exponent. The present work is the first extension of the point-to-point average-rate scenario in [9] and the corresponding variable-length coding scheme to systems with multiple sensors.

Specifically, we consider the two-sensors single-detector system in Fig. 1, where the first sensor communicates over a shared link to the second sensor and the detector, and after receiving this message, also the second sensor communicates with the detector. The two sensors observe the sequences $X_1^n$ and $X_2^n$, respectively, and the detector observes $Y^n$, where we assume that the following Markov chain holds both under the null hypothesis $\mathcal{H}=0$ as well as under the alternative hypothesis $\mathcal{H}=1$:

$$X_1^n \leftrightarrow X_2^n \leftrightarrow Y^n \tag{1}$$

We consider the *testing-against-independence* scenario where under the alternative hypothesis $\mathcal{H}=1$ the observations at the two sensors are independent of the observations at the detector. We further assume that the sensors' observations $X_1^n, X_2^n$ follow the same *joint* distribution and the decision center's observation $Y^n$ follows the same *marginal* distribution under both hypotheses.

The focus of this paper is on the maximum achievable error exponents under the alternative hypothesis when the error probability under the null hypothesis is not allowed to exceed a given $\epsilon>0$, and the rates of communication from the first and the second sensors are constrained by $R_1$ and $R_2$, respectively. Under *maximum rate constraints*, this optimal error exponent $\theta^*_{\epsilon,\text{Fix}}(R_1,R_2)$ was characterized in [10] even without Markov chain (1) in the limit $\epsilon\to 0$.[1] In this paper, we establish the corresponding *strong converse* under the Markov chain (1), by proving the same result on $\theta^*_{\epsilon,\text{Fix}}(R_1,R_2)$ for any $\epsilon>0$.

The main result of the paper is the maximum achievable error exponent $\theta^*_\epsilon(R_1,R_2)$ under *expected rate constraints*, which depends on $\epsilon$ and can be charcterized as:

$$\theta^*_\epsilon(R_1,R_2)=\theta^*_{\epsilon,\text{Fix}}\Big(R_1\cdot(1-\epsilon)^{-1},R_2\cdot(1-\epsilon)^{-1}\Big). \tag{2}$$

Thus, through variable-length coding we can increase all available rates in the network by the factor $(1-\epsilon)^{-1}$. A similar observation was already made for the point-to-point setup studied in [9]. In this sense, the current paper extends the conclusion to multiple links, and it shows in particular that the rate-increase can be attained on all links simultaneously.

*Notation:* We follow the notation in [11] and [9]. In particular, we use sans serif font for bit-strings: e.g., $\mathsf{m}$ for a deterministic and $\mathsf{M}$ for a random bit-string. We let $\text{string}(m)$ denote the shortest bit-string representation of a positive integer $m$, and for any bit-string $\mathsf{m}$ we let $\text{len}(\mathsf{m})$

[1] In the converse proof of [10, Theorem 2], the second line in the lower bound to $R_1$ relies on the identity $H(X_{1,i}X_{2,i}|M_1X_1^{i-1}X_2^{i-1}) = H(X_{1,i}X_{2,i}|M_1X_1^{i-1}X_{2,i+1}^n)$ which does not necessarily hold. In fact, the "$=$" has to be replaced with "$\geq$" and in some cases the inequality is strict.

and $\mathrm{dec}(\mathsf{m})$ denote its length and its corresponding positive integer. We use $h_{\mathrm{b}}(\cdot)$ for the binary entropy function.

## II. System Model

Consider the distributed hypothesis testing problem in Fig. 1 in the special case of testing against independence where

$$\text{under } \mathcal{H}=0: (X_1^n, X_2^n, Y^n) \sim \text{i.i.d. } P_{X_1X_2}\cdot P_{Y|X_2}; \quad (3)$$

$$\text{under } \mathcal{H}=1: (X_1^n, X_2^n, Y^n) \sim \text{i.i.d. } P_{X_1X_2}\cdot P_{Y}. \quad (4)$$

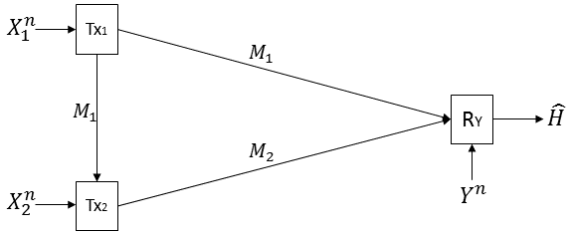


Fig. 1: Cooperative MAC Setup with 2 transmitters and 1 receiver.

Specifically, the system consists of two transmitters ($T_{X_1}$ and $T_{X_2}$) and a receiver ($R_Y$). $T_{X_1}$ observes the source sequence $X_1^n$ and sends its bit-string message $\mathsf{M}_1=\phi_1^{(n)}(X_1^n)$ to both $T_{X_2}$ and $R_Y$, where the encoding function is of the form $\phi_1^{(n)}: \mathcal{X}_1^n \to \{0,1\}^\star$ and satisfies the rate constraint

$$\mathbb{E}\left[\mathrm{len}\left(\mathsf{M}_1\right)\right] \le nR_1. \quad (5)$$

$T_{X_2}$ observes the source sequence $X_2^n$ and with the message $\mathsf{M}_1$ received from $T_{X_1}$, it computes the bit-string message $\mathsf{M}_2=\phi_2^{(n)}\left(X_2^n, \mathsf{M}_1\right)$ using some encoding function $\phi_2^{(n)}: \mathcal{X}_2^n\times\{0,1\}^\star\to\{0,1\}^\star$ satisfying the rate constraint

$$\mathbb{E}\left[\mathrm{len}\left(\mathsf{M}_2\right)\right] \le nR_2. \quad (6)$$

$T_{X_2}$ sends message $\mathsf{M}_2$ to $R_Y$ which decides on the hypothesis $\mathcal{H}=\{0,1\}$ based on the messages $\mathsf{M}_1$ and $\mathsf{M}_2$ and its own observation $Y^n$. That means, using a decoding function $g^{(n)}: \mathcal{Y}^n\times\{0,1\}^\star\times\{0,1\}^\star\to\{0,1\}$, it produces:

$$\hat{\mathcal{H}}=g^{(n)}\left(\mathsf{M}_1,\mathsf{M}_2,Y^n\right)\ \in\{0,1\}. \quad (7)$$

The goal is to design encoding and decision functions such that their type-I error probability

$$\alpha_n \triangleq \Pr[\hat{\mathcal{H}}=1|\mathcal{H}=0] \quad (8)$$

stays below a given threshold and the type-II error probability

$$\beta_n \triangleq \Pr[\hat{\mathcal{H}}=0|\mathcal{H}=1] \quad (9)$$

decays to 0 exponentially fast.

*Definition 1:* Error exponent $\theta\ge 0$ is called *$\epsilon$-achievable* if there exists a sequence of encoding and decision functions $\{\phi_1^{(n)},\phi_2^{(n)},g^{(n)}\}$ satisfying

$$\alpha_n \le \epsilon, \quad (10)$$

$$\varliminf_{n\to\infty}\frac{1}{n}\log\frac{1}{\beta_n} \ge \theta. \quad (11)$$

The supremum over all $\epsilon$-achievable error exponents is called the *optimal error exponent* and is denoted $\theta_\epsilon^*(R_1,R_2)$.

*Remark 1:* The setup in [10] is similar to our setup here, except that it imposes the more stringent constraints

$$\mathrm{len}\left(\mathsf{M}_i\right)\le nR_i, \quad i\in\{1,2\}, \quad (12)$$

and it allows for a general $P_{Y|X_1X_2}$ distribution in (3).

## III. Main Results

*Theorem 1:* There exist auxiliary random variables $U_1$ and $U_2$ such that the optimal error exponent is given by:

$$\theta_\epsilon^*\left(R_1,R_2\right)= \max_{\substack{P_{U_1|X_1},P_{U_2|U_1X_2}:\\ R_1\ge(1-\epsilon)I(U_1;X_1)\\ R_2\ge(1-\epsilon)I(U_2;X_2|U_1)\\ U_1\leftrightarrow X_1\leftrightarrow(X_2,Y)\\ U_2\leftrightarrow(X_2,U_1)\leftrightarrow(X_1,Y)}} I\left(U_1U_2;Y\right) \quad (13)$$

where mutual information quantities are calculated according to the joint pmf $P_{U_1U_2X_1X_2Y}\triangleq P_{U_1|X_1}P_{U_2|U_1X_2}P_{X_1X_2}P_{Y|X_2}$.

*Proof:* Achievability is proved in Section IV and the converse in Section V. ∎

*Lemma 1:* In Theorem 1, it suffices to choose $U_1$ and $U_2$ over alphabets of sizes $|\mathcal{U}_1|\le|\mathcal{X}_1|+2$ and $|\mathcal{U}_2|\le|\mathcal{U}_1||\mathcal{X}_2|+1$.

*Proof:* Omitted. It follows by standard applications of Carathéodory's theorem, see [11, Appendix C]. ∎

### A. Comparing Variable-Length with Fixed-Length Coding

For comparison, we also present the optimal error exponent under fixed-length coding.

*Remark 2:* Under fixed-length coding, i.e., under rate constraints (12), the optimal error exponent $\theta_{\epsilon,\mathrm{Fix}}^*\left(R_1,R_2\right)$ is:

$$\theta_{\epsilon,\mathrm{Fix}}^*\left(R_1,R_2\right)= \max_{\substack{P_{U_1|X_1},P_{U_2|U_1X_2}:\\ R_1\ge I(U_1;X_1)\\ R_2\ge I(U_2;X_2|U_1)\\ U_1\leftrightarrow X_1\leftrightarrow(X_2,Y)\\ U_2\leftrightarrow(X_2,U_1)\leftrightarrow(X_1,Y)}} I\left(U_1U_2;Y\right), \quad (14)$$

where mutual informations are calculated according to the joint probability mass function (pmf) $P_{U_1U_2X_1X_2Y}\triangleq P_{U_1|X_1}P_{U_2|U_1X_2}P_{X_1X_2}P_{Y|X_2}$.

*Proof:* Achievability can be proved as described in Section IV when the set $\mathcal{S}_n$ is replaced by an empty set. The converse can be shown as in Section V if inequality (40), i.e., $H(\tilde{\mathsf{M}}_i)\le\frac{nR_i}{\Delta_n}\left(1+h_b\left(\frac{\Delta_n}{nR_i}\right)\right)$, is replaced by the trivial inequality $H(\tilde{\mathsf{M}}_i)\le nR_i$. ∎

We examine the gain provided by variable-length coding on the cooperative MAC at hand of an example.

*Example 1:* Let $X_1,S,T$ be independent Bernoulli random variables of parameters $p_{X_1}=0.4, p_S=0.8, p_T=0.8$ and set $X_2=X_1\oplus T$ and $Y=X_2\oplus S$. For this example, Fig. 2 shows the optimal error exponents of variable-length and fixed-length coding, $\theta_\epsilon^*(R_1,R_2)$ and $\theta_{\epsilon,\mathrm{Fix}}^*(R_1,R_2)$, when $\epsilon=0.05$ and both links are of same rates $R_1=R_2$. Fig. 2 also presents the optimal variable-length error exponent $\theta_\epsilon^*(R_1=0,R_2)$ when $R_1=0$, i.e., when the first sensor is not present or cannot communicate. The figure thus illustrates the benefits of variable length coding (the gap between the solid blue line and the dash-dotted red line) and of the first sensor $T_{X_1}$ (the gap between the dashed green line and the solid blue line).

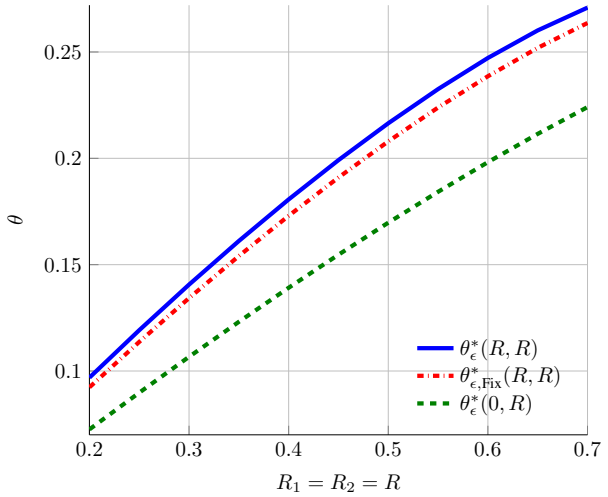


Fig. 2: Optimal exponents of variable-length and fixed-length coding for Example 1 when $\epsilon = 0.05$.

## IV. Achievability Proof

Fix a large blocklength $n$, a small number $\mu \in (0, \epsilon)$, and conditional pmfs $P_{U_1|X_1}$ and $P_{U_2|U_1,X_2}$ such that:

$$R_1 = (1 - \epsilon + \mu)\left(I(U_1; X_1) + 2\mu\right) \tag{15}$$

$$R_2 = (1 - \epsilon + \mu)\left(I(U_2; X_2|U_1) + 2\mu\right) \tag{16}$$

where mutual informations are meant with respect to

$$P_{U_1U_2X_1X_2Y} \triangleq P_{U_1|X_1} \cdot P_{U_2|U_1X_2} \cdot P_{X_1X_2} \cdot P_{Y|X_2}. \tag{17}$$

Randomly generate a codebook

$$C_{U_1} \triangleq \left\{u_1^n(m_1) : m_1 \in \left\{1, \cdots, 2^{n(I(U_1;X_1)+\mu)}\right\}\right\} \tag{18}$$

by drawing all entries i.i.d. according to the marginal pmf $P_{U_1}$. For each codeword $u_1^n(m_1)$, generate a codebook

$$C_{U_2}(m_1) \triangleq \left\{u_2^n(m_2|m_1) : m_2 \in \left\{1, \cdots, 2^{n(I(U_2;X_2|U_1)+\mu)}\right\}\right\}, \tag{19}$$

by drawing the $j$-th entry of each codeword according to $P_{U_2|U_1}$. Also choose a set $\mathcal{S}_n$,

$$\mathcal{S}_n \subseteq \mathcal{T}_\mu^{(n)}(P_{X_1}) : \ \Pr\left[X_1^n \in \mathcal{S}_n\right] = \epsilon - \mu, \tag{20}$$

with $\mathcal{T}_\mu^{(n)}(P_{X_1})$ the strongly-typical set [12, Definition 2.8].

Transmitter 1: Assume it observes the sequence $X_1^n = x_1^n$. If $x_1^n \notin \mathcal{S}_n$, it looks for indices $m_1 \geq 1$ satisfying $(u_1^n(m_1), x^n) \in \mathcal{T}_\mu^n(P_{U_1X_1})$, randomly picks one of these indices, and sends its corresponding bit-string $\mathsf{M}_1 = \text{string}(m_1)$ both to Transmitter 2 and the Receiver. Otherwise, it sends the single-bit string $\mathsf{M}_1 = [0]$.

Transmitter 2: Assume it observes the sequence $X_2^n = x_2^n$ and receives the bit-string message $\mathsf{M}_1 = \mathsf{m}_1$ from Transmitter 1. If $\mathsf{m}_1 = [0]$, then it sends the bit-string message $\mathsf{M}_2 = [0]$. Else, if $m_1 = \text{dec}(\mathsf{m}_1) \geq 1$, it looks for an index $m_2 \geq 1$ satisfying $(u_1^n(m_1), u_2^n(m_2|m_1), x_2^n) \in \mathcal{T}_\mu^n(P_{U_1U_2X_2})$. It randomly picks one of these indices and sends its corresponding bit-string $\mathsf{M}_2 = \text{string}(m_2)$ to the Receiver. Otherwise, it sends $\mathsf{M}_2 = [0]$.

Receiver: Assume it observes the sequence $Y^n = y^n$ and receives messages $\mathsf{M}_1 = \mathsf{m}_1$ and $\mathsf{M}_2 = \mathsf{m}_2$. If any of the bit-strings $\mathsf{m}_1$ or $\mathsf{m}_2$ equals $[0]$, it declares $\hat{\mathcal{H}} = 1$. Else, it sets $m_i = \text{dec}(\mathsf{m}_i)$, for $i = 1, 2$, and checks if $(u_1^n(m_1), u_2^n(m_2|m_1), y^n) \in \mathcal{T}_\mu^n(P_{U_1U_2Y})$. It declares $\hat{\mathcal{H}} = 0$ if the condition is verified, and $\hat{\mathcal{H}} = 1$ otherwise.

The error probability and message length analysis are omitted here but can be found in the full version [13]. ■

## V. Converse Proof to Theorem 1

Notice first that it suffices to show

$$\theta^*_\epsilon(R_1, R_2) \leq \max_{\substack{p(u_1|x_1)p(u_2|u_1,x_2): \\ R_1 \geq (1-\epsilon)I(U_1;X_1) \\ R_2 \geq (1-\epsilon)I(U_2;X_2|U_1) \\ U_1 \leftrightarrow X_1 \leftrightarrow (X_2,Y) \\ U_2 \leftrightarrow (X_2,U_1) \leftrightarrow Y}} I(U_1U_2; Y), \tag{21}$$

i.e., the Markov chain $U_2 \leftrightarrow (U_1, X_2) \leftrightarrow (X_1, Y)$ in Theorem 1 can be replaced by the weaker Markov chain $U_2 \leftrightarrow (U_1, X_2) \leftrightarrow Y$, because the right-hand side of (21) does not depend on the joint pmf of $U_2$ and $X_1$. A more formal proof of this sufficiency can be found in [13].

Fix $\theta < \theta^*_\epsilon(R_1, R_2)$, a sequence of encoding and decision functions satisfying the type-I and type-II error constraints, a blocklength $n$, and a small number $\eta \geq 0$. Define:

$$\mathcal{B}_n(\eta) \triangleq \{(x_1^n, x_2^n) : \Pr[\hat{\mathcal{H}} = 0 | X_1^n = x_1^n, X_2^n = x_2^n, \mathcal{H} = 0] \geq \eta\}, \tag{22}$$

$$\mu_n \triangleq n^{-\frac{1}{3}}, \tag{23}$$

$$\mathcal{D}_n(\eta) \triangleq T^n_{\mu_n}(P_{X_1X_2}) \cap \mathcal{B}_n(\eta). \tag{24}$$

By constraint (10) on the type-I error probability, we have:

$$1 - \epsilon \leq P_{X_1^nX_2^n}(\mathcal{B}_n(\eta)) + \eta(1 - P_{X_1^nX_2^n}(\mathcal{B}_n(\eta))) \tag{25}$$

$$\Rightarrow P_{X_1^nX_2^n}(\mathcal{B}_n(\eta)) \geq \frac{1 - \epsilon - \eta}{1 - \eta}. \tag{26}$$

Moreover, by [12, Remark to Lemma 2.12],

$$P^n_{X_1X_2}\left(\mathcal{T}^{(n)}_{\mu_n}(P_{X_1X_2})\right) \geq 1 - \frac{|\mathcal{X}_1||\mathcal{X}_2|}{4\mu_n^2 n}, \tag{27}$$

and thus by (24) and (26),

$$P_{X_1^nX_2^n}(\mathcal{D}_n(\eta)) \geq \frac{1 - \epsilon - \eta}{1 - \eta} - \frac{|\mathcal{X}_1||\mathcal{X}_2|}{4\mu_n^2 n} \triangleq \Delta_n. \tag{28}$$

We define the random variables $(\tilde{\mathsf{M}}_1, \tilde{\mathsf{M}}_2, \tilde{X}_1^n, \tilde{X}_2^n, \tilde{Y}^n)$ as the restriction of the random variables $(\mathsf{M}_1, \mathsf{M}_2, X_1^n, X_2^n, Y^n)$ to $(X_1^n, X_2^n) \in \mathcal{D}_n(\eta)$.

The probability distribution of the former tuple is given by:

$$P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2\tilde{X}_1^n\tilde{X}_2^n\tilde{Y}^n}(\mathsf{m}_1, \mathsf{m}_2, x_1^n, x_2^n, y^n) \triangleq P_{X_1^nX_2^nY^n}(x_1^n, x_2^n, y^n) \cdot \frac{\mathbb{1}\{x_1^n, x_2^n \in \mathcal{D}_n(\eta)\}}{P_{X_1^nX_2^n}(\mathcal{D}_n(\eta))} \cdot \mathbb{1}\{\phi_1(x_1^n) = \mathsf{m}_1\} \cdot \mathbb{1}\{\phi_2(x_2^n, \phi_1(x_1^n)) = \mathsf{m}_2\}, \tag{29}$$

leading to the following inequalities:

$$P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2}(\mathsf{m}_1, \mathsf{m}_2) \leq P_{\mathsf{M}_1\mathsf{M}_2}(\mathsf{m}_1, \mathsf{m}_2)\Delta_n^{-1}, \tag{30}$$

$$P_{\tilde{Y}^n}(y^n) \le P_Y^n(y^n)\Delta_n^{-1}, \tag{31}$$

$$D(P_{\tilde{X}_1^n\tilde{X}_2^n}||P_{X_1X_2}^n) \le \log \Delta_n^{-1}. \tag{32}$$

Define the following random variables:

$$\tilde{L}_i \triangleq \mathrm{len}(\tilde{\mathsf{M}}_i), \qquad i=1,2. \tag{33}$$

By the rate constraints (5) and (6), we have for $i=1,2$:

$$\begin{aligned} nR_i &\ge \mathbb{E}[L_i] \ge \mathbb{E}[L_i|(X_1^n,X_2^n)\in\mathcal{D}_n(\eta)]P_{X_1^nX_2^n}(\mathcal{D}_n(\eta)) \\ &\ge \mathbb{E}[\tilde{L}_i]\Delta_n, \end{aligned} \tag{34}$$

where the last inequality follows by (28). Moreover, by definition, $\tilde{L}_i$ is a function of $\tilde{\mathsf{M}}_i$, for $i=1,2$, so we can upper bound the entropy of $\tilde{\mathsf{M}}_i$ as follows:

$$\begin{aligned} H(\tilde{\mathsf{M}}_i) &= H(\tilde{\mathsf{M}}_i,\tilde{L}_i) && (35)\\ &= \sum_{l_i}\Pr[\tilde{L}_i=l_i]H(\tilde{\mathsf{M}}_i|\tilde{L}_i=l_i)+H(\tilde{L}_i) && (36)\\ &\le \sum_{l_i}\Pr[\tilde{L}_i=l_i]l_i + H(\tilde{L}_i) && (37)\\ &= \mathbb{E}[\tilde{L}_i]+H(\tilde{L}_i) && (38)\\ &\le \frac{nR_i}{\Delta_n}+\frac{nR_i}{\Delta_n}h_b\left(\frac{\Delta_n}{nR_i}\right) && (39)\\ &= \frac{nR_i}{\Delta_n}\left(1+h_b\left(\frac{\Delta_n}{nR_i}\right)\right), && (40) \end{aligned}$$

where (39) holds by (34) and since the maximum possible entropy of $\tilde{L}_i$ is obtained by a geometric distribution of mean $\mathbb{E}[\tilde{L}_i]$, which is further bounded by $\frac{nR_i}{\Delta_n}$ [14, Theorem 12.1.1].

On the other hand, we lower bound the entropy of $\tilde{\mathsf{M}}_1$ as:

$$\begin{aligned} H(\tilde{\mathsf{M}}_1) &\ge I(\tilde{\mathsf{M}}_1;\tilde{X}_1^n\tilde{X}_2^n)+D(P_{\tilde{X}_1^n\tilde{X}_2^n}||P_{X_1X_2}^n)+\log\Delta_n && (41)\\ &= H(\tilde{X}_1^n\tilde{X}_2^n)+D(P_{\tilde{X}_1^n\tilde{X}_2^n}||P_{X_1X_2}^n) \\ &\quad -H(\tilde{X}_1^n\tilde{X}_2^n|\tilde{\mathsf{M}}_1)+\log\Delta_n && (42)\\ &\ge n[H(\tilde{X}_{1,T}\tilde{X}_{2,T})+D(P_{\tilde{X}_{1,T}\tilde{X}_{2,T}}||P_{X_1X_2})] \\ &\quad -\sum_{t=1}^n H(\tilde{X}_{1,t}\tilde{X}_{2,t}|\tilde{U}_{1,t})+\log\Delta_n && (43)\\ &= n[H(\tilde{X}_{1,T}\tilde{X}_{2,T})+D(P_{\tilde{X}_{1,T}\tilde{X}_{2,T}}||P_{X_1X_2})] \\ &\quad -nH(\tilde{X}_{1,T}\tilde{X}_{2,T}|\tilde{U}_{1,T},T)+\log\Delta_n && (44)\\ &= n[H(\tilde{X}_1\tilde{X}_2)+D(P_{\tilde{X}_1\tilde{X}_2}||P_{X_1X_2})] \\ &\quad -nH(\tilde{X}_1\tilde{X}_2|U_1)+\log\Delta_n && (45)\\ &\ge n\left[I(U_1;\tilde{X}_1)+\frac{1}{n}\log\Delta_n\right]. && (46) \end{aligned}$$

Here, (41) holds by (32); (43) holds by the super-additivity property in [15, Proposition 1], by the chain rule, and by defining $\tilde{U}_{1t}\triangleq(\tilde{\mathsf{M}}_1,\tilde{X}_1^{t-1},\tilde{X}_2^{t-1})$; (44) by defining $T$ uniform over $\{1,\ldots,n\}$ independent of all other random variables; and (45) by defining $U_1\triangleq(\tilde{U}_{1T},T)$, $\tilde{X}_1\triangleq\tilde{X}_{1,T}$, and $\tilde{X}_2\triangleq\tilde{X}_{2,T}$.

Similarly,

$$\begin{aligned} H(\tilde{\mathsf{M}}_2) &\ge I(\tilde{\mathsf{M}}_2;\tilde{X}_1^n\tilde{X}_2^n|\tilde{\mathsf{M}}_1) && (47)\\ &= \sum_{t=1}^n I(\tilde{U}_{2,t};\tilde{X}_{1,t}\tilde{X}_{2,t}|\tilde{U}_{1,t}) && (48)\\ &= nI(\tilde{U}_{2,T}T;\tilde{X}_{1,T}\tilde{X}_{2,T}|\tilde{U}_{1,T}T) && (49)\\ &\ge nI(U_2;\tilde{X}_2|U_1). && (50) \end{aligned}$$

Here, (47) holds since $\tilde{\mathsf{M}}_2$ is function of $\tilde{X}_2^n$ and $\tilde{\mathsf{M}}_1$; (48) holds by the chain rule, the definition of $\tilde{U}_{1t}$, and by defining $\tilde{U}_{2t}\triangleq\tilde{\mathsf{M}}_2$; and (50) holds by defining $U_2\triangleq(\tilde{U}_{2T},T)$.

Combining (40) with (46) and (50), yields:

$$R_1 \ge \frac{I(U_1;\tilde{X}_1)+\frac{1}{n}\log\Delta_n}{\left(1+h_b\left(\frac{\Delta_n}{nR_1}\right)\right)}\cdot\Delta_n \tag{51}$$

$$R_2 \ge \frac{I(U_2;\tilde{X}_2|U_1)}{\left(1+h_b\left(\frac{\Delta_n}{nR_2}\right)\right)}\cdot\Delta_n. \tag{52}$$

Define the set

$$\mathcal{A}_n \triangleq \{(\mathsf{m}_1,\mathsf{m}_2,y^n)\colon g^{(n)}(\mathsf{m}_1,\mathsf{m}_2,y^n)=0\}, \tag{53}$$

and for each $(\mathsf{m}_1,\mathsf{m}_2)$:

$$\mathcal{A}_n(\mathsf{m}_1,\mathsf{m}_2)\triangleq\{y^n\colon(\mathsf{m}_1,\mathsf{m}_2,y^n)\in\mathcal{A}_n\}. \tag{54}$$

Define further the Hamming neighborhoods of these sets:

$$\begin{aligned} \hat{\mathcal{A}}_n^{\ell_n}(\mathsf{m}_1,\mathsf{m}_2) \triangleq \{\tilde{y}^n : \exists\, y^n\in\mathcal{A}_n(\mathsf{m}_1,\mathsf{m}_2) \\ \text{s.t. } d_{\mathrm{H}}(y^n,\tilde{y}^n)\le\ell_n\} \end{aligned} \tag{55}$$

for some real number $\ell_n$ satisfying $\lim_{n\to\infty}\ell_n/n=0$ and $\lim_{n\to\infty}\ell_n/\sqrt{n}=\infty$, and

$$\hat{\mathcal{A}}_n^{\ell_n}\triangleq\bigcup_{(\mathsf{m}_1,\mathsf{m}_2)}\{(\mathsf{m}_1,\mathsf{m}_2)\}\times\hat{\mathcal{A}}_n^{\ell_n}(\mathsf{m}_1,\mathsf{m}_2), \tag{56}$$

Since by definitions (22) and (24), for all $(x_1^n,x_2^n)\in\mathcal{D}_n$, $\mathsf{m}_1=\phi_1(x_1^n)$, and $\mathsf{m}_2=\phi_2(x_2^n,\phi_1(x_1^n))$ :

$$P_{\tilde{Y}^n|\tilde{X}_1^n\tilde{X}_2^n}\left(\mathcal{A}_n(\mathsf{m}_1,\mathsf{m}_2)\middle|x_1^n,x_2^n\right)\ge\eta, \tag{57}$$

by the blowing-up lemma [16]:

$$P_{\tilde{Y}^n|\tilde{X}_1^n\tilde{X}_2^n}\left(\hat{\mathcal{A}}_n^{\ell_n}(\mathsf{m}_1,\mathsf{m}_2)|x_1^n,x_2^n\right)\ge 1-\zeta_n \tag{58}$$

for a real number $\zeta_n>0$ such that $\lim_{n\to\infty}\zeta_n=0$. Moreover, taking expectation of (58) with respect to $(\tilde{X}_1^n,\tilde{X}_2^n)$ we obtain:

$$P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2\tilde{Y}^n}\left(\hat{\mathcal{A}}_n^{\ell_n}\right)\ge 1-\zeta_n. \tag{59}$$

In addition, using (30) and (31), we have the following:

$$\begin{aligned} &P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2}P_{\tilde{Y}^n}(\hat{\mathcal{A}}_n^{\ell_n}) \\ &\quad\le P_{\mathsf{M}_1\mathsf{M}_2}P_Y^n(\hat{\mathcal{A}}_n^{\ell_n})\cdot\Delta_n^{-2} && (60)\\ &\quad\le P_{\mathsf{M}_1\mathsf{M}_2}P_Y^n(\mathcal{A}_n)\cdot e^{nh_b(\ell_n/n)}\cdot p^{\ell_n}\cdot|\mathcal{Y}|^{\ell_n}\cdot\Delta_n^{-2} && (61)\\ &\quad= \beta_n\cdot F_n^{\ell_n}\cdot\Delta_n^{-2}, && (62) \end{aligned}$$

where $p\triangleq\min_{y,y'\colon P_Y(y')>0}\frac{P_Y(y)}{P_Y(y')}$ and $F_n^{\ell_n}\triangleq e^{nh_b(\ell_n/n)}\cdot p^{\ell_n}\cdot|\mathcal{Y}|^{\ell_n}$. Here, (61) holds by [12, Proof of Lemma 5.1].

By (62) and standard inequalities (see [9, Lemma 1]), we can upper bound the type-II error exponent as follows:

$$\begin{aligned} &-\log\beta_n \\ &\le -\log P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2}P_{\tilde{Y}^n}(\hat{\mathcal{A}}_n^{\ell_n})+\ell_n\log F_n-2\log\Delta_n \end{aligned} \tag{63}$$

$$\leq \frac{1}{1-\zeta_n}\left(D\left(P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2\tilde{Y}^n}||P_{\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2}P_{\tilde{Y}^n}\right)+1\right) + \ell_n \log F_n - 2\log\Delta_n \quad (64)$$

$$= \frac{1}{1-\zeta_n}\Big(I(\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2;\tilde{Y}^n)+1\Big) + \ell_n \log F_n - 2\log\Delta_n. \quad (65)$$

We further upper-bound the term $I(\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2;\tilde{Y}^n)$ as follows:

$$I(\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2;\tilde{Y}^n) \leq \sum_{t=1}^{n} I(\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2\tilde{X}_1^{t-1}\tilde{X}_2^{t-1}\tilde{Y}^{t-1};\tilde{Y}_t) \quad (66)$$

$$= \sum_{t=1}^{n} I(\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2\tilde{X}_1^{t-1}\tilde{X}_2^{t-1};\tilde{Y}_t) \quad (67)$$

$$\leq nI(U_1U_2;\tilde{Y}), \quad (68)$$

where (67) holds by the Markov chain $\tilde{Y}^{t-1} \leftrightarrow (\tilde{\mathsf{M}}_1\tilde{\mathsf{M}}_2,\tilde{X}_1^{t-1}\tilde{X}_2^{t-1}) \leftrightarrow \tilde{Y}_t$, (68) follows by the definitions of $\tilde{U}_{1,t}$ and $\tilde{U}_{2,t}$ and defining $\tilde{Y}=\tilde{Y}_T$.

We observe the Markov chain $\tilde{U}_{2,t} \leftrightarrow (\tilde{U}_{1,t},\tilde{X}_{2,t}) \leftrightarrow \tilde{Y}_t$ for any $t$, and thus $U_2 \leftrightarrow (U_1,\tilde{X}_2) \leftrightarrow \tilde{Y}$. The second desired Markov chain $U_1 \leftrightarrow \tilde{X}_1 \leftrightarrow (\tilde{X}_2,\tilde{Y})$ only holds in the limit as $n\to\infty$. To see this, notice that $\tilde{\mathsf{M}}_1 \leftrightarrow \tilde{X}_1^n \leftrightarrow (\tilde{X}_2^n,\tilde{Y}^n)$ forms a Markov chain and thus:

$$0 = I(\tilde{\mathsf{M}}_1;\tilde{X}_2^n\tilde{Y}^n|\tilde{X}_1^n) \quad (69)$$

$$\geq H(\tilde{X}_2^n\tilde{Y}^n|\tilde{X}_1^n) + D(P_{\tilde{X}_1^n\tilde{X}_2^n\tilde{Y}^n}||P_{X_1X_2Y}^n) + \log\Delta_n - H(\tilde{X}_2^n\tilde{Y}^n|\tilde{X}_1^n\tilde{\mathsf{M}}_1) \quad (70)$$

$$\geq n[H(\tilde{X}_{2,T}\tilde{Y}_T|\tilde{X}_{1,T}) + D(P_{\tilde{X}_{1,T}\tilde{X}_{2,T}\tilde{Y}_T}||P_{X_1X_2Y})] + \log\Delta_n - \sum_{t=1}^{n} H(\tilde{X}_{2,t}\tilde{Y}_t|\tilde{X}_1^n\tilde{X}_2^{t-1}\tilde{Y}^{t-1}\tilde{\mathsf{M}}_1) \quad (71)$$

$$\geq n[H(\tilde{X}_{2,T}\tilde{Y}_T|\tilde{X}_{1,T}) + D(P_{\tilde{X}_{1,T}\tilde{X}_{2,T}\tilde{Y}_T}||P_{X_1X_2Y})] + \log\Delta_n - \sum_{t=1}^{n} H(\tilde{X}_{2,t}\tilde{Y}_t|\tilde{X}_{1,t}\tilde{U}_{1,t}) \quad (72)$$

$$= n[I(\tilde{X}_{2,T}\tilde{Y}_T;\tilde{U}_{1,T}T|\tilde{X}_{1,T}) + D(P_{\tilde{X}_{1,T}\tilde{X}_{2,T}\tilde{Y}_T}||P_{X_1X_2Y})] + \log\Delta_n \quad (73)$$

$$\geq nI(\tilde{X}_2\tilde{Y};U_1|\tilde{X}_1) + \log\Delta_n, \quad (74)$$

where (70) holds by (32) and $P_{\tilde{Y}^n|\tilde{X}_1^n\tilde{X}_2^n} = P_{Y|X_1X_2}^n$; and (71) holds by the super-additivity property in [15, Proposition 1] and the chain rule. Since $\frac{1}{n}\log\Delta_n \to 0$ as $n\to\infty$, then $I(\tilde{X}_2\tilde{Y};U_1|\tilde{X}_1)\to 0$ as $n\to\infty$.

To sum up, we have proved so far in (51), (52), (65), (68), and (74) that for all $n\geq 1$ there exists a joint pmf $P^{(n)}_{\tilde{X}_1\tilde{X}_2\tilde{Y}U_1U_2}$ (abbreviated as $P^{(n)}$) and functions $g_1(n)$, $g_4(n)$, and $g_5(n)$ tending to 0 and $g_3(n)$ tending to 1 as $n\to\infty$, and $g_2(n,\eta)$ tending to $(1-\epsilon)$ as $n\to\infty$ and $\eta\to 0$, so that

$$P^{(n)}_{\tilde{X}_1\tilde{X}_2\tilde{Y}U_1U_2} = P^{(n)}_{\tilde{X}_1\tilde{X}_2\tilde{Y}} \cdot P^{(n)}_{U_1|\tilde{X}_1\tilde{X}_2} \cdot P^{(n)}_{U_2|U_1\tilde{X}_2}, \quad (75a)$$

$$R_1 \geq (I_{P^{(n)}}(U_1;\tilde{X}_1) + g_1(n))\cdot g_2(n,\eta), \quad (75b)$$

$$R_2 \geq I_{P^{(n)}}(U_2;\tilde{X}_2|U_1)\cdot g_2(n,\eta), \quad (75c)$$

$$\theta \leq g_3(n) I_{P^{(n)}}(U_1U_2;\tilde{Y}) + g_4(n), \quad (75d)$$

$$I_{P^{(n)}}(\tilde{X}_2\tilde{Y};U_1|\tilde{X}_1) \leq g_5(n), \quad (75e)$$

where $I_{P^{(n)}}$ indicates that the mutual information should be calculated according to the pmf $P^{(n)}$. The pmf $P^{(n)}_{\tilde{X}_1\tilde{X}_2\tilde{Y}U_1U_2}$ has almost the same structure as the pmf $P_{X_1X_2YU_1U_2}$ in the theorem, except that $P^{(n)}_{U_1|\tilde{X}_1\tilde{X}_2}$ can still depend on the realization of $\tilde{X}_2$. By (75e) and because $g_5(n)\to 0$ as $n\to\infty$, this dependence however vanishes as the blocklength grows.

Applying Carathéodory's theorem [11, Appendix C], one can restrict the auxiliary random variables $U_1$ and $U_2$ to alphabets of sizes

$$|\mathcal{U}_1| \leq |\mathcal{X}_1|\cdot|\mathcal{X}_2| + 3, \quad (76)$$

$$|\mathcal{U}_2| \leq |\mathcal{U}_1|\cdot|\mathcal{X}_2| + 1. \quad (77)$$

The proof is then concluded by invoking the Bolzano-Weierstrass theorem, and by considering a subsequence $P^{(n_k)}_{\tilde{X}_1\tilde{X}_2\tilde{Y}U_1U_2}$ that converges to a limiting pmf $P^*_{X_1X_2YU_1U_2}$. In fact, by (75) this limiting pmf factorizes as $P^*_{X_1X_2YU_1U_2} = P^*_{X_1X_2Y}\cdot P^*_{U_1|X_1}\cdot P^*_{U_2|U_1X_2}$ and satisfies the desired rate-constraints, and moreover $P^*_{X_1X_2Y} = P_{X_1X_2}\cdot P_{Y|X_1X_2}$ because for any $n\geq 1$, $P^{(n)}_{\tilde{Y}|\tilde{X}_1\tilde{X}_2} = P_{Y|X_1X_2}$ and $|P_{\tilde{X}_1\tilde{X}_2} - P_{X_1X_2}| \leq \mu_n$ (since $(\tilde{X}_1^n,\tilde{X}_2^n)\in\mathcal{T}^{(n)}_{\mu_n}(P_{X_1X_2})$) with $\mu_n\to 0$ as $n\to\infty$. ■

## ACKNOWLEDGMENT

M. Wigger and M. Hamad acknowledge funding support from the ERC under grant agreement 715111.

## REFERENCES


[1] R. Ahlswede and I. Csiszár, "Hypothesis testing with communication constraints," *IEEE Trans. Inf. Theory*, vol. 32, pp. 533–542, Jul. 1986.

[2] T. S. Han, "Hypothesis testing with multiterminal data compression," *IEEE Trans. Inf. Theory*, vol. 33, pp. 759–772, Nov. 1987.

[3] H. Shimokawa, T. Han, and S. I. Amari, "Error bound for hypothesis testing with data compression," in *Proc. ISIT*, p. 114, Jul. 1994.

[4] M. S. Rahman and A. B. Wagner, "On the optimality of binning for distributed hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 58, pp. 6282–6303, Oct. 2012.

[5] Y. Xiang and Y. H. Kim, "Interactive hypothesis testing against independence," in *Proc. ISIT*, pp. 2840–2844, Jun. 2013.

[6] P. Escamilla, M. Wigger, and A. Zaidi, "Distributed hypothesis testing with concurrent detection," in *Proc. ISIT*, Jun. 2018.

[7] S. Salehkalaibar and M. Wigger, "Distributed hypothesis testing based on unequal-error protection codes," *IEEE Trans. Inf. Theory*, vol. 66, pp. 4150–41820, Jul. 2020.

[8] S. Salehkalaibar, M. Wigger, and L. Wang, "Hypothesis testing over the two-hop relay network," *IEEE Trans. Inf. Theory*, vol. 65, pp. 4411–4433, Jul. 2019.

[9] S. Salehkalaibar and M. Wigger, "Distributed hypothesis testing with variable-length coding," *arXiv:2005.08610*, 2020.

[10] W. Zhao and L. Lai, "Distributed testing with cascaded encoders," *IEEE Trans. Inf. Theory*, vol. 64, no. 11, pp. 7339–7348, 2018.

[11] A. El Gamal and Y. H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[12] I. Csiszár and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[13] M. Hamad, M. Wigger, and M. Sarkiss, "Cooperative multi-sensor detection under variable-length coding," *arXiv:2010.09616*, 2020.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory, 2nd Ed.* Wiley, 2006.

[15] H. Tyagi and S. Watanabe, "Strong converse using change of measure arguments," *IEEE Trans. Inf. Theory*, vol. 66, no. 2, pp. 689–703, 2019.

[16] K. Marton, "A simple proof of the blowing-up lemma," *IEEE Trans. Inf. Theory*, vol. 32, pp. 445–446, May 1986.