How Many Queries Will Resolve Common Randomness?

Himanshu Tyagi and Prakash Narayan[†]

***Abstract*—A set of m terminals, observing correlated signals, communicate interactively to generate common randomness for a given subset of them. Knowing only the communication, how many direct queries of the value of the common randomness will resolve it? A general upper bound, valid for arbitrary signal alphabets, is developed for the number of such queries by using a query strategy that applies to all common randomness and associated communication. When the underlying signals are independent and identically distributed repetitions of m correlated random variables, the number of queries can be exponential in signal length. For this case, the mentioned upper bound is tight and leads to a single-letter formula for the largest query exponent, which coincides with the secret key capacity of a corresponding multiterminal source model. In fact, the upper bound constitutes a strong converse for the optimum query exponent, and implies also a new strong converse for secret key capacity. A key tool, estimating the size of a large probability set in terms of Rényi entropy, is interpreted separately, too, as a lossless block coding result for general sources. As a particularization, it yields the classic result for a discrete memoryless source.**

I. Introduction

A set of terminals observing correlated signals agree on common randomness (CR), i.e., shared bits, by communicating interactively among themselves. What is the maximum number of queries of the form "Is CR $= l$?" with yes-no answers, that an observer of (only) the communication must ask in order to resolve the value of the CR? As an illustration, suppose that two terminals observe, respectively, n independent and identically distributed (i.i.d.) repetitions of the finite-valued random variables (rvs) X_1 and X_2. The terminals agree on CR X_1^n with terminal 1 communicating to terminal 2 a Slepian-Wolf codeword of rate $H(X_1 \mid X_2)$ obtained by random binning. An observer of the bin index can ascertain the value of CR with large probability in approximately $\exp\left[nI(X_1 \wedge X_2)\right]$ queries (corresponding to bin size). Our results show that more queries cannot be incurred by any other form of CR and associated interactive communication.

In a general setting, terminals $1, ..., m$ observe, respectively, n i.i.d. repetitions of the rvs $X_1, ..., X_m$, and communicate interactively to create CR, say L, for the terminals in a given subset $\mathcal{A} \subseteq \{1, ..., m\}$. For appropriate CR L and communication $\mathbf{F}$, the number of queries of the form "Is $L = l$?" that an observer of $\mathbf{F}$ must ask to resolve L is exponential in n. We find a single-letter formula for the largest exponent E^*. Remarkably, this formula coincides with the secret key (SK) capacity for a multitermial source model with underlying rvs $X_1, ..., X_m$ [4]. The latter is the largest rate of nearly uniformly distributed CR for $\mathcal{A}$ that meets the security requirement of being nearly independent of the communication used to generate it. While it is to be expected that E^* is no smaller than SK capacity, the less-restricted E^* may seem *a priori* to be larger. But it is not so. The coincidence brings out, in effect, an equivalence between inflicting a maximum number of queries on an observer of $\mathbf{F}$ on the one hand, and imposing the explicit secrecy constraint above on the other hand. In fact, as in the achievability proof of SK capacity in [4], the exponent E^* is achieved by the terminals in $\mathcal{A}$ attaining "omniscience," i.e., by generating CR $L = (X_1^n, ..., X_m^n)$ for $\mathcal{A}$, using communication $\mathbf{F}$ of minimum rate.

Our main contribution is a new technique for proving converse results involving CR with interactive communication. It relies on query strategies for L given $\mathbf{F}$ that do not depend explicitly on the form of L or $\mathbf{F}$, and do not require the rvs $(X_{1t}, ..., X_{mt})_{t=1}^n$ to be finite-valued or i.i.d. In fact, our converse results hold even when the underlying alphabets are arbitrary, but under mild technical assumptions. Jointly Gaussian rvs are a special case. Furthermore, our converse is strong in that the characterization of E^* does not depend on the probability of recovery of the CR. This, in turn, leads to a new strong converse result for the SK capacity of the multiterminal source model [4]. A byproduct of our technique is a simple lossless block coding result for general finite sources, in terms of Rényi entropies. A particularization recovers the classic lossless block coding result for i.i.d. sources without recourse to the asymptotic equipartition property (AEP).

The number of queries above can be interpreted as a measure of the correlation among the random signals observed by the terminals: A stronger correlation necessitates more queries for resolving the CR that can be generated by them. Such a measure of correlation is in the spirit of the body of work on "guessing" the value of an rv based on a correlated observation [7], [2].

The problem formulation and our main result characterizing the optimum query exponent are given in the next section. A new technical tool for estimating the cardinality of a large probability set in terms of Rényi entropy, potentially of independent interest, is given in Section III. Section IV and V contain, respectively, the outlines of the achievability and converse proofs of the main result. The converse proof

[†] H. Tyagi and P. Narayan are with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. E-mail: {tyagi, prakash}@umd.edu.

This work was supported by the U.S. National Science Foundation under Grants CCF0830697 and CCF1117546.

is complicated and is sketched in steps, omitting the difficult details. The strong converse for SK capacity is given in Section VI. An application of the mentioned technical tool to lossless source coding as well as an extension of our converse approach to rvs with general alphabets are discussed in Section VII. This submission is an abridged version of a full-length manuscript [10].

II. Main Result

Let $X_1, \ldots, X_m$, $m \geq 2$, be rvs with finite alphabets $\mathcal{X}_1, \ldots, \mathcal{X}_m$, respectively, and with a known joint probability mass function (pmf) $\mathrm{P}_{X_1,\ldots,X_m}$. For any nonempty set $\mathcal{A} \subseteq \mathcal{M} = \{1, \ldots, m\}$, we denote $X_\mathcal{A} = (X_i,\ i \in \mathcal{A})$. We denote n i.i.d. repetitions of $X_\mathcal{M} = (X_1, \ldots, X_m)$ with values in $\mathcal{X}_\mathcal{M} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_m$ by $X_\mathcal{M}^n = (X_1^n, \ldots, X_m^n)$ with values in $\mathcal{X}_\mathcal{M}^n = \mathcal{X}_1^n \times \ldots \times \mathcal{X}_m^n$. Given $\epsilon > 0$, for rvs U, V, we say that U is *ϵ-recoverable* from V if $\mathrm{P}\left(U \neq f(V)\right) \leq \epsilon$ for some function $f(V)$ of V. The cardinality of the range of the rv U is denoted by $\|U\|$, and the complement of a set A by A^c. All logarithms and exponentials are with respect to the base 2.

We consider a multiterminal source model for generating CR using interactive communication. Terminals $1, \ldots, m$ observe, respectively, the sequences $X_1^n, \ldots, X_m^n$, of length n. The terminals in a given set $\mathcal{A} \subseteq \mathcal{M}$ wish to generate CR using communication over a noiseless channel, possibly interactively in several rounds.

Assume without any loss of generality that the communication of the terminals in $\mathcal{M}$ occurs in consecutive time slots in r rounds, where r can depend on n but is finite for every n. Specifically, a communication f_{ji} in time slot j by terminal i, $1 \leq j \leq r$, $1 \leq i \leq m$, is a function of X_i^n and of all previous communication. The corresponding rvs are termed collectively as *interactive communication*

$$\mathbf{F} = \{F_{11}, \ldots, F_{1m}, F_{21}, \ldots, F_{2m}, \ldots, F_{r1}, \ldots, F_{rm}\},$$

where $\mathbf{F} = \mathbf{F}^{(n)}(X_\mathcal{M}^n)$.

Definition 1. Given interactive communication $\mathbf{F}$ as above, an rv $L = L^{(n)}\left(X_\mathcal{M}^n\right)$ is *ϵ-common randomness* (ϵ-CR) for $\mathcal{A}$ from $\mathbf{F}$ if it is ϵ-recoverable from $(X_i^n, \mathbf{F})$, $i \in \mathcal{A}$, i.e., if there exist rvs $L_i = L_i^{(n)}\left(X_i^n, \mathbf{F}\right)$, $i \in \mathcal{A}$, satisfying

$$\mathrm{P}\left(L_i = L,\ i \in \mathcal{A}\right) \geq 1 - \epsilon. \tag{1}$$

The rv L_i will be called an estimate of L at terminal $i \in \mathcal{A}$.

A querier observing the communication $\mathbf{F}$ wants to resolve the value of this CR L by asking questions of the form "Is $L = l$?" with yes-no answers. While queries of this form have been termed "guessing" [7], [2], we use the terminology "query" since our approach covers a broader class of query strategies; see Section VII-B.

Definition 2. For rvs U, V with values in the sets $\mathcal{U}, \mathcal{V}$, a *query strategy* q for U given $V = v$ is a bijection $q(\cdot|v) : \mathcal{U} \to \{1, ..., |\mathcal{U}|\}$, where the querier, upon observing $V = v$, asks the question "Is $U = u$?" in the $q(u|v)^{\text{th}}$ query.

Thus, a query strategy q for resolving a CR L on the basis of an observed communication $\mathbf{F} = \mathbf{i}$ is an ordering of the possible values of L. The terminals seek to generate a CR L for $\mathcal{A}$ using communication $\mathbf{F}$ so as to make the task of the querier observing $\mathbf{F}$ as onerous as possible. For instance, if L were to be independent of $\mathbf{F}$, then the querier necessarily must search exhaustively over the set of possible values of L, which can be exponentially large (in n).

Definition 3. Given $0 < \epsilon < 1$, a *query exponent* $E > 0$ is ϵ-achievable if for every $0 < \epsilon' < 1$, there exists an ϵ-CR $L = L^{(n)}\left(X_\mathcal{M}^n\right)$ for $\mathcal{A} \subseteq \mathcal{M}$ from communication $\mathbf{F} = \mathbf{F}\left(X_\mathcal{M}^n\right)$ such that for every query strategy q for L given $\mathbf{F}$,

$$\mathrm{P}\big(q(L \mid \mathbf{F}) \geq \exp(nE)\big) > 1 - \epsilon', \tag{2}$$

for all $n \geq N(\epsilon, \epsilon')$. The ϵ-optimum query exponent, denoted $E^*(\epsilon)$, is the supremum of all ϵ-achievable query exponents; $E^*(\epsilon)$ is nondecreasing in ϵ. The *optimum query exponent* E^* is the infimum of $E^*(\epsilon)$ for $0 < \epsilon < 1$, i.e.,

$$E^* = \lim_{\epsilon \to 0} E^*(\epsilon).$$

Remark. Clearly, $0 \leq E^* \leq \log |\mathcal{X}_\mathcal{M}|$.

Condition (2) forces any query strategy adopted by the querier to have an exponential complexity (in n) with large probability; E^* is the largest value of the exponent that can be inflicted on the querier.

Our main result is a single-letter characterization of the optimum query exponent E^*.

Theorem 1. *The optimum query exponent E^* equals*

$$E^* = E^*(\epsilon) = H\left(X_\mathcal{M}\right) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right), \qquad 0 < \epsilon < 1, \tag{3}$$

where $\mathcal{B} = \{B \subsetneq \mathcal{M} : B \neq \emptyset, \mathcal{A} \nsubseteq B\}$ and $\Lambda(\mathcal{A})$ is the set of all collections $\lambda = \{\lambda_B : B \in \mathcal{B}\}$ of weights $0 \leq \lambda_B \leq 1$, satisfying $\sum_{B \in \mathcal{B}: B \ni i} \lambda_B = 1$, $i \in \mathcal{M}$.

Remarkably, the value of E^* coincides with the *secret key* (SK) capacity of a multiterminal source model [4]. The latter is the largest rate of a CR $K = K\left(X_\mathcal{M}^n\right)$ for $\mathcal{A}$ from communication $\mathbf{F}$, with K satisfying the "secrecy constraint" of [4]:

$$\lim_n s_{in}(K; \mathbf{F}) = 0, \tag{4}$$

where the security index s_{in} is given by

$$s_{in}(K; \mathbf{F}) = \log \|K\| - H(K \mid \mathbf{F}) = D\left(\mathrm{P}_{K,\mathbf{F}} \,\|\, \mathrm{P}_{unif} \times \mathrm{P}_\mathbf{F}\right), \tag{5}$$

with P_{unif} being the uniform pmf on $\{1, ..., \|K\|\}$. In fact, the achievability proof of Theorem 1 is straightforward and employs, in effect, an SK K in forming an appropriate CR $L \approx (K, \mathbf{F})$. We show that for such a CR L, any query strategy is tantamount to an exhaustive search over the set of values of the SK, a feature that is obvious for a "perfect" SK with $s_{in}(K; \mathbf{F}) = 0$. The difficult step in the proof of Theorem 1 is the converse part which involves finding an appropriate query strategy, for arbitrary L and $\mathbf{F}$, which limits the incurred query exponents. Our *strong* converse yields a uniform upper bound for $E^*(\epsilon)$, $0 < \epsilon < 1$.

III. Large probability sets and Rényi entropy

Lemma 2 below relates the cardinalities of large probability sets to Rényi entropy. The first part is used in the converse proof of Theorem 1. The lemma is of independent interest. For instance, in Section VII it is shown to yield an elementary alternative proof of the lossless source coding theorem for an i.i.d. (finite-valued) source.

For an i.i.d. probability measure μ on $\mathcal{U}^n$, the smallest cardinality of a large probability set in $\mathcal{U}^n$ is approximately $\exp[nH(\mu)]$. What is an analogous result for an arbitrary measure μ on a discrete set?

Definition 4. [9] Let μ be a nonnegative measure on $\mathcal{U}$. For $0 \leq \alpha \neq 1$, the *Rényi entropy of order* α of μ is

$$H_\alpha(\mu) = \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha.$$

Lemma 2. *(i) For every $0 < \delta < \mu(\mathcal{U})$, there exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ such that for every $0 \leq \alpha < 1$*

$$\mu\left(\mathcal{U}_\delta\right) \geq \mu(\mathcal{U}) - \delta, \tag{6}$$

and

$$|\mathcal{U}_\delta| \leq \delta^{-\alpha/(1-\alpha)} \exp\left(H_\alpha(\mu)\right). \tag{7}$$

(ii) Conversely, for $\delta, \delta' > 0$, $\delta + \delta' < \mu(\mathcal{U})$, any set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu\left(\mathcal{U}_\delta\right)$ as in (6) must satisfy for every $\alpha > 1$

$$|\mathcal{U}_\delta| \geq (\delta')^{1/(\alpha-1)} \left(\mu(\mathcal{U}) - \delta - \delta'\right) \exp\left(H_\alpha(\mu)\right). \tag{8}$$

IV. Sketch of achievability proof of Theorem 1

Achievability entails identifying a CR L for $\mathcal{A}$ from $\mathbf{F}$ such that any query strategy $q(L|\mathbf{F})$ necessitates at least approximately $\exp[nC]$ queries with large probability, where C denotes the right-side of (3). With U, V as proxies for $L, \mathbf{F}$, respectively, finding a lower bound for $q(U|V)$ involves finding a suitable upper bound for the conditional probabilities $\mathtt{P}_{U|V}\left(\cdot \mid \cdot\right)$. This idea is formalized by the following lemma.

Lemma 3. *Given $\gamma > 0$ and $0 < \delta < 1/2$, let the rvs U, V, satisfy*

$$\mathtt{P}\left(\left\{(u,v) : \mathtt{P}_{U|V}\left(u|v\right) \leq \frac{\delta}{\gamma}\right\}\right) \geq 1 - \delta. \tag{9}$$

Then for every query strategy q for U given V,

$$\mathtt{P}\left(q(U|V) \geq \gamma\right) \geq 1 - \epsilon', \tag{10}$$

for all $\epsilon' \geq 2\delta$.

Conversely, if (10) holds for every query strategy q for U given V, with $0 < \epsilon' \leq (1 - \sqrt{\delta})^2$, then

$$\mathtt{P}\left(\left\{(u,v) : \mathtt{P}_{U|V}\left(u|v\right) \leq \frac{1}{\gamma}\right\}\right) \geq \delta. \tag{11}$$

The achievability proof uses only the first part of Lemma 3. We claim, for $0 < \epsilon < 1$, $0 < \delta < 1/2$, $\beta > 0$, the existence of an ϵ-CR $L = X_{\mathcal{M}}^n$ for $\mathcal{A}$ from $\mathbf{F}$ with

$$\mathtt{P}\left(\left\{(x_{\mathcal{M}}^n, \mathbf{i}) : \mathtt{P}_{L|\mathbf{F}}\left(x_{\mathcal{M}}^n \mid \mathbf{i}\right) \leq \delta \exp\left[-n(C-\beta)\right]\right\}\right) \geq 1 - \delta, \tag{12}$$

for all n sufficiently large. Then the achievability assertion of Theorem 1 follows by applying Lemma 3 with $U = L$, $V = \mathbf{F}, \gamma = \exp[n(C - \beta)]$, to conclude from (10) that

$$E^*(\epsilon) \geq C,$$

since $\beta > 0$ was chosen arbitrarily.

The proof of the mentioned claim relies on the existence of communication $\mathbf{F}$ such that $L = X_{\mathcal{M}}^n$ is ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$ with

$$\frac{1}{n} \log \|\mathbf{F}\| \lesssim \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right),$$

for all n sufficiently large, which was shown earlier in [4, Proposition 1]. In fact, by [4], this choice of L equals $(K, \mathbf{F})$ where K is an optimum rate SK.

Remark. The achievability proof brings out a connection between a large probability uniform upper bound κ for $\mathtt{P}_L$, the size $\|\mathbf{F}\|$ of the communication $\mathbf{F}$, and the associated number of queries needed. Loosely speaking, the number of queries is approximately $\frac{1}{\|\mathbf{F}\|\kappa}$, which reduces to $\frac{\|L\|}{\|\mathbf{F}\|}$ if L is nearly uniformly distributed.

V. Sketch of converse proof of Theorem 1

We outline here the converse proof only for the case $\mathcal{A} = \mathcal{M}$ as it contains the essence of the general proof. For this case, a less-complicated proof is facilitated by the fact that the right-side of (3) can be written equivalently as [3] (see also [4, Example 4])

$$\min_\pi \frac{1}{|\pi| - 1} D\left(\mathtt{P}_{X_{\mathcal{M}}} \| \prod_{i=1}^{|\pi|} \mathtt{P}_{X_{\pi_i}}\right), \tag{13}$$

where the minimum is over all partitions $\pi = (\pi_1, ..., \pi_k)$ of $\mathcal{M}$ with $|\pi| = k$ parts, $2 \leq k \leq m$. Then, given such a partition π, we observe that for a consolidated source model with k sources and underlying rvs $Y_1, ..., Y_k$ where[1] $Y_i = X_{\pi_i}$, the ϵ-optimum query exponent $E_\pi^*(\epsilon)$ can be no smaller than $E^*(\epsilon)$ (since the terminals in each π_i coalesce, in effect). The following theorem provides an upper bound for $E_\pi^*(\epsilon)$, and a fortiori for $E^*(\epsilon)$.

Theorem 4. *For every partition π of $\mathcal{M}$ with $|\pi| = k$,*

$$E_\pi^*(\epsilon) \leq \frac{1}{k-1} D\left(\mathtt{P}_{Y_1, ..., Y_k} \| \prod_{i=1}^{k} \mathtt{P}_{Y_i}\right), \qquad 0 < \epsilon < 1,$$

and so

$$E^*(\epsilon) \leq \min_\pi E_\pi^*(\epsilon) \leq \min_\pi \frac{1}{|\pi| - 1} D\left(\mathtt{P}_{X_{\mathcal{M}}} \| \prod_{i=1}^{|\pi|} \mathtt{P}_{X_{\pi_i}}\right).$$

[1] For specificity, the elements in each π_i are arranged in increasing order.

Theorem 4 establishes, in view of (13), the converse part of Theorem 1 when $\mathcal{A} = \mathcal{M}$.

The proof of Theorem 4 relies on showing that for any ϵ-CR L for $\mathcal{M}$ from $\mathbf{F}$, a query strategy q exists such that with large probability $q(L|\mathbf{F}) \leq \exp[nC]$. The existence of such a strategy is given by the following general result which is the linchpin of our converse approach, and holds for queries of CR generated in a multiterminal source model with underlying rvs $Y_1, ..., Y_k$ for $n = 1$.

Theorem 5. *Let $L = L\left(Y_1, ..., Y_k\right)$ be ϵ-CR for $\{1, ..., k\}$ from interactive communication $\mathbf{F} = \mathbf{F}\left(Y_1, ..., Y_k\right)$, $0 < \epsilon < 1$. Given $\delta > 0$ such that $\delta + \sqrt{\delta + \epsilon} < 1$, let θ be such that*

$$\mathrm{P}\left(\left\{(y_1, ..., y_k) : \frac{\mathrm{P}_{Y_1,...,Y_k}\left(y_1, ..., y_k\right)}{\prod_{i=1}^{k} \mathrm{P}_{Y_i}\left(y_i\right)} \leq \theta\right\}\right) \geq 1 - \delta. \tag{14}$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}\right) \geq (1 - \delta - \sqrt{\delta + \epsilon})^2. \tag{15}$$

Proof of Theorem 4. We apply Theorem 5 to n i.i.d. repetitions of the rvs $Y_1, ..., Y_k$. Denoting by $\mathcal{T}_n'$ the set of $\mathrm{P}_{Y_1,...,Y_k}$-typical sequences with constant δ, we have

$$\mathrm{P}_{Y_1^n,...,Y_k^n}\left(\mathcal{T}_n'\right) \geq 1 - \delta,$$

and for $(y_1^n, ..., y_k^n) \in \mathcal{T}_n'$,

$$\begin{aligned}
&\frac{\mathrm{P}_{Y_1^n,...,Y_k^n}\left(y_1^n, ..., y_k^n\right)}{\prod_{i=1}^{k} \mathrm{P}_{Y_i^n}\left(y_i^n\right)} \\
&\leq \exp\left[n\left(\sum_{i=1}^{k} H\left(Y_i\right) - H\left(Y_1, ..., Y_k\right) + \delta\right)\right] \\
&= \exp\left[n\left(D\left(\mathrm{P}_{Y_1,...,Y_k} \| \prod_{i=1}^{k} \mathrm{P}_{Y_i}\right) + \delta\right)\right],
\end{aligned}$$

for all n large enough. Thus, the hypothesis of Theorem 5 holds with

$$\theta = \theta_n = \exp\left[n\left(D\left(\mathrm{P}_{Y_1,...,Y_k} \| \prod_{i=1}^{k} \mathrm{P}_{Y_i}\right) + \delta\right)\right]. \tag{16}$$

If E is an ϵ-achievable query exponent (see Definition 3), then there exists an ϵ-CR $L = L\left(Y_1^n, ..., Y_k^n\right)$ from communication $\mathbf{F} = \mathbf{F}\left(Y_1^n, ..., Y_k^n\right)$ such that (2) holds for the query strategy q_0 of Theorem 5 for this choice of L and $\mathbf{F}$. In particular for $\epsilon' < (1 - \delta - \sqrt{\delta + \epsilon})^2$, we get from (15) and (2) that

$$\begin{aligned}
\mathrm{P}\Bigg(&\exp(nE) \leq q_0(L \mid \mathbf{F}) \leq \frac{\theta}{\delta^2}^{\frac{1}{k-1}}\Bigg) \\
&\geq (1 - \delta - \sqrt{\delta + \epsilon})^2 - \epsilon' > 0,
\end{aligned}$$

for all n sufficiently large. It follows from (16) that

$$E \leq \frac{1}{k-1} D\left(\mathrm{P}_{Y_1,...,Y_k} \| \prod_{i=1}^{k} \mathrm{P}_{Y_i}\right) + \frac{2\delta}{k-1}.$$

Since E was any ϵ-achievable query exponent and $\delta > 0$ was chosen arbitrarily, the assertion of Theorem 4 is established. □

Outline of proof of Theorem 5. Denote by $\mathcal{L}$ the set of values of the CR L. Using the hypothesis (14) of the Theorem, the proof entails showing the existence of a set $\mathcal{I}_o$ of values of $\mathbf{F}$ and associated sets $\mathcal{L}(\mathbf{i}) \subseteq \mathcal{L}$, $\mathbf{i} \in \mathcal{I}_0$, such that for every $\mathbf{i} \in \mathcal{I}_0$,

$$\mathrm{P}_{L|\mathbf{F}}\left(\mathcal{L}(\mathbf{i}) \mid \mathbf{i}\right) \geq 1 - \delta - \sqrt{\epsilon + \delta}, \tag{17}$$

$$|\mathcal{L}(\mathbf{i})| \leq \delta^{-\alpha/(1-\alpha)} \exp\left(H_\alpha(\mu)\right) \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}} \tag{18}$$

$$\text{and} \quad \mathrm{P}_{\mathbf{F}}\left(\mathcal{I}_0\right) \geq 1 - \delta - \sqrt{\epsilon + \delta}, \tag{19}$$

where $\alpha = 1/k$. The large $\mathrm{P}_{L|\mathbf{F}}\left(\cdot \mid \mathbf{i}\right)$-probability sets $\mathcal{L}(\mathbf{i})$, $\mathbf{i} \in \mathcal{I}_0$, in (17) are obtained by Lemma 2(i) with $\mu = \mathrm{P}_{L|\mathbf{F}}\left(\cdot \mid \mathbf{i}\right)$, $\mathcal{U} = \mathcal{L}$. The first bound on $|\mathcal{L}(\mathbf{i})|$ in (18) is by (7). The second bound in (18) involves technical manipulations that use the interactive nature of $\mathbf{F}$ and Hölder's inequality.

Finally, consider the following query strategy: For each $\mathbf{i} \in \mathcal{I}_0$, order the elements of $\mathcal{L}$ arbitrarily but with the first $|\mathcal{L}(\mathbf{i})|$ elements being from $\mathcal{L}(\mathbf{i})$. This ordering defines a query strategy $q_0(\cdot|\mathbf{i})$, $\mathbf{i} \in \mathcal{I}_0$; for $\mathbf{i} \notin \mathcal{I}_0$, let $q_0(\cdot|\mathbf{i})$ be defined arbitrarily. Thus, for all $\mathbf{i} \in \mathcal{I}_0$, $l \in \mathcal{L}(\mathbf{i})$,

$$q_0(l \mid \mathbf{i}) \leq |\mathcal{L}(\mathbf{i})| \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}},$$

from which it follows that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}\right) \geq (1 - \delta - \sqrt{\delta + \epsilon})^2,$$

thereby establishing the assertion (15).

VI. Strong converse for secret key capacity

A byproduct of Theorem 1 is a new result that establishes a strong converse for the SK capacity of a multiterminal source model, for the terminals in $\mathcal{A} \subseteq \mathcal{M}$.

Definition 5. Given $0 < \epsilon < 1$, $R \geq 0$ is an ϵ-achievable SK rate for $\mathcal{A} \subseteq \mathcal{M}$ if for every $\rho > 0$, there is an $N = N(\epsilon, \rho)$ such that for every $n \geq N$, there exists an ϵ-CR $K = K\left(X_{\mathcal{M}}^n\right)$ for $\mathcal{A}$ from $\mathbf{F}$ satisfying

$$\frac{1}{n} \log \|K\| \geq R - \rho, \tag{20}$$

and

$$s_{var}(K; \mathbf{F}) = \sum_{\mathbf{i}} \mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right) \sum_{k=1}^{\|K\|} \left|\mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) - \frac{1}{\|K\|}\right| \leq \frac{\rho}{n}, \tag{21}$$

where (21) enforces a stronger secrecy requirement than (4) (see [4, Lemma 1]).

The supremum of ϵ-achievable SK rates is the ϵ-SK capacity, denoted $C(\epsilon)$. The SK capacity is the infimum of $C(\epsilon)$ for $0 < \epsilon < 1$. We recall the following.

Theorem 6. *[4] The secret key capacity for $\mathcal{A} \subseteq \mathcal{M}$ is*

$$C = E^* = H\left(X_{\mathcal{M}}\right) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right).$$

Our strong converse for SK capacity, valid under (21), is stated next without proof.

Theorem 7. *For every $0 < \epsilon < 1$, it holds that $C(\epsilon) = C$.*

VII. Discussion

A. General lossless source coding theorem

Lemma 2 can be interpreted as a source coding result for a general source with finite alphabet $\mathcal{U}$. Consider a sequence of probability measures μ_n on finite sets $\mathcal{U}_n$, $n \geq 1$. For $0 < \delta < 1$, R is a δ-achievable (block) source coding rate if there exists sets $\mathcal{V}_n \subseteq \mathcal{U}_n$ satisfying

$$\mu_n(\mathcal{V}_n) \geq 1 - \delta,$$

for all n sufficiently large, and

$$\limsup_n \frac{1}{n} \log |\mathcal{V}_n| \leq R.$$

The optimum source coding rate $R^*(\delta)$ is the infimum of all such δ-achievable rates.

Proposition 8. *For each $0 < \delta < 1$,*

$$\lim_{\alpha \downarrow 1} \limsup_n \frac{1}{n} H_\alpha(\mu_n) \leq R^*(\delta) \leq \lim_{\alpha \uparrow 1} \limsup_n \frac{1}{n} H_\alpha(\mu_n). \tag{22}$$

Corollary. *If μ_n is an i.i.d. probability measure on $\mathcal{U}_n = \mathcal{U} \times ... \times \mathcal{U}$, then*

$$R^*(\delta) = H(\mu_1), \qquad 0 < \delta < 1.$$

Proof. The Proposition is a direct consequence of Lemma 2 upon taking appropriate limits in (7) and (8) with $\mathcal{U}_n$ in the role of $\mathcal{U}$. The Corollary follows since for i.i.d. μ_n,

$$H_\alpha(\mu_n) = nH_\alpha(\mu_1) \text{ and } \lim_{\alpha \to 1} H_\alpha(\mu_1) = H(\mu_1).$$

□

We note that the Corollary above is proved without recourse to the AEP. Moreover, it contains a strong converse for the lossless coding theorem for an i.i.d. source. In general, Proposition 8 implies a strong converse whenever the lower and upper bounds for $R^*(\delta)$ in (22) coincide. This implication is a special case of a general source coding result in [6], where it was shown that a strong converse holds iff for rvs U_n with pmfs μ_n, the "lim-inf" and "lim-sup" of $Z_n = \frac{1}{n} \log \frac{1}{\mu_n(U_n)}$ in μ_n-probability coincide, i.e.,

$$\begin{aligned} &\sup\left\{\beta : \lim_n \mu_n(Z_n < \beta) = 0\right\} \\ &= \inf\left\{\beta : \lim_n \mu_n(Z_n > \beta) = 0\right\}. \end{aligned} \tag{23}$$

In fact, a straightforward calculation shows that the lower and upper bounds for $R^*(\delta)$ in (22) are admissible choices of β on the left- and right-sides of (23), respectively.

B. General alphabet converse for $\mathcal{A} = \mathcal{M}$

Theorem 5 can be generalized to rvs $Y^k = (Y_1, ..., Y_k)$ with a general alphabet $\mathcal{Y}^k = \mathcal{Y}_1 \times ... \times \mathcal{Y}_k$. Let $\mathsf{P} = \mathsf{P}_{Y_1 ... Y_k}$ be a probability measure on $(\mathcal{Y}^k, \sigma^k)$, with σ^k being a product σ-field on $\mathcal{Y}^k$, that satisfies the following absolute continuity assumption:

$$\mathsf{P}_{Y_1,...,Y_k|\mathbf{F}}\left(\cdot \mid \mathbf{i}\right) << \mathsf{P}_{Y_1,...,Y_k}, \qquad \mathsf{P}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}.$$

This assumption is satisfied, for instance, when the communication takes countably many values.

Theorem 9. *For $0 < \epsilon < 1$, let L be ϵ-CR from interactive communication $\mathbf{F}$. Let $\tilde{\mathsf{P}} = \tilde{\mathsf{P}}_{Y_1,...,Y_k}$ be a probability measure on $\left(\mathcal{Y}^k, \sigma^k\right)$ with*

$$\tilde{\mathsf{P}}\left(A_1 \times ... \times A_k\right) = \prod_{i=1}^{k} \mathsf{P}_{Y_i}\left(A_i\right) \qquad A_i \in \sigma_i,\ 1 \leq i \leq k.$$

Given $\delta > 0$ such that $\delta + \sqrt{\delta + \epsilon} < 1$, let θ be such that

$$\mathsf{P}\left(\left\{y^k : \frac{d\,\mathsf{P}}{d\,\tilde{\mathsf{P}}}(y^k) \leq \theta\right\}\right) \geq 1 - \delta.$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathsf{P}\left(q_0(L \mid \mathbf{F}) \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}\right) \geq (1 - \delta - \sqrt{\delta + \epsilon})^2.$$

As an application, Theorem 9 yields the following upper bound for $E^*(\epsilon)$ when the underlying rvs $X_{\mathcal{M}}^{(n)}$ are jointly Gaussian $\mathcal{N}(\mathbf{0}, \Sigma^n)$:

$$E^*(\epsilon) \leq \min_\pi \frac{1}{2(|\pi| - 1)} \limsup_n \frac{1}{n} \log \frac{\prod_{i=1}^{|\pi|} |\Sigma_{\pi_i}^n|}{|\Sigma^n|}, \qquad 0 < \epsilon < 1,$$

where $\Sigma_{\pi_i}^n$ is the covariance matrix of $X_{\pi_i}^{(n)}$, $i = 1, ..., |\pi|$, and $|\cdot|$ denotes determinant. In addition, when $X_{\mathcal{M}}^{(n)}$ is i.i.d. in n, it leads to an exact expression for E^*, resulting in a strong converse for Gaussian SK capacity [10] (see also [8]).

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part i: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[2] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 99–105, 1996.

[3] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," *in Proceedings of 44th Annual Conference on Information Sciences and Systems (CISS 2010).*

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[5] I. Csiszár and J. Körner, *Information theory: Coding theorems for discrete memoryless channels*. 2nd Ed. Cambridge, 2011.

[6] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 752–772, 1993.

[7] J. L. Massey, "Guessing and entropy," *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, 1994.

[8] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources." *IEEE Trans. Inform. Theory*, vol. 58, no. 6, pp. 3373–3391, June 2012.

[9] A. Rényi, "On measures of entropy and information," *Proc. Fourth Berkeley Symp. on Math. Statist. and Prob., Vol. 1 (Univ. of Calif. Press)*, pp. 547–561, 1961.

[10] H. Tyagi and P. Narayan, "How many queries will resolve common randomness?," *arXiv:1305.1397*, 2013.