

Article

Are Guessing, Source Coding and Tasks Partitioning Birds of A Feather? [†]

M. Ashok Kumar ^{1,*}, Albert Sunny ², Ashish Thakre ³, Ashisha Kumar ³ and G. Dinesh Manohar ⁴

¹ Department of Mathematics, Indian Institute of Technology Palakkad, Palakkad 678557, India

² Department of Computer Science and Engineering, Indian Institute of Technology Palakkad, Palakkad 678557, India

³ Department of Mathematics, Indian Institute of Technology Indore, Indore 453552, India

⁴ Institute for Communications Engineering, Technical University of Munich, 80333 Munich, Germany

* Correspondence: ashokm@iitpkd.ac.in

[†] This paper is an extended version of our paper published in 2022 IEEE International Symposium on Information Theory (ISIT), Espoo, Finland, 26 June–1 July 2022.

Abstract: This paper establishes a close relationship among the four information theoretic problems, namely Campbell source coding, Arıkan guessing, Huleihel et al. memoryless guessing and Bunte and Lapidoth tasks' partitioning problems in the IID-lossless case. We first show that the aforementioned problems are mathematically related via a general moment minimization problem whose optimum solution is given in terms of Renyi entropy. We then propose a general framework for the mismatched version of these problems and establish all the asymptotic results using this framework. The unified framework further enables us to study a variant of Bunte–Lapidoth's tasks partitioning problem which is practically more appealing. In addition, this variant turns out to be a generalization of Arıkan's guessing problem. Finally, with the help of this general framework, we establish an equivalence among all these problems, in the sense that, knowing an asymptotically optimal solution in one problem helps us find the same in all other problems.

Keywords: guessing; source coding; tasks partitioning; Shannon entropy; Rényi entropy; Kullback–Leibler divergence; relative α -entropy; Sundaresan's divergence

MSC: 94A15; 94A17; 94A50; 62B10



Citation: Ashok Kumar, M.; Sunny, A.; Thakre, A.; Kumar, A.; Dinesh Manohar, G. Are Guessing, Source Coding and Tasks Partitioning Birds of A Feather? *Entropy* **2022**, *24*, 1695. <https://doi.org/10.3390/e24111695>

Academic Editors: Nicusor Minculete and Shigeru Furuichi

Received: 15 August 2022

Accepted: 5 October 2022

Published: 19 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The concept of entropy is very central to information theory. In source coding, the expected number of bits required (per letter) to encode a source with (finite) alphabet set \mathcal{X} and probability distribution P is the Shannon entropy $H(P) := -\sum_{x \in \mathcal{X}} P(x) \log P(x)$. If the compressor does not know the true distribution P , but assumes a distribution Q (mismatch), then the number of bits required for compression is $H(P) + I(P, Q)$, where

$$I(P, Q) := -\sum_{x \in \mathcal{X}} P(x) \log Q(x) + \sum_{x \in \mathcal{X}} P(x) \log P(x), \quad (1)$$

is the entropy of P relative to Q (or the Kullback–Leibler divergence). In his seminal paper, Shannon [1] argued that $H(P)$ can also be regarded as a measure of uncertainty. Subsequently, Rényi [2] introduced an alternate measure of uncertainty, now known as Rényi entropy of order α , as

$$H_\alpha(P) := \frac{1}{1-\alpha} \log \sum_{x \in \mathcal{X}} P(x)^\alpha, \quad (2)$$

where $\alpha > 0$ and $\alpha \neq 1$. Rényi entropy can also be regarded as a generalization of the Shannon entropy as $\lim_{\alpha \rightarrow 1} H_\alpha(P) = H(P)$. Refer Aczel and Daroczy [3] and the references therein for an extensive study of various measures of uncertainty and their characterizations.

In 1965, Campbell [4] gave an operational meaning to Rényi entropy. He showed that, instead of expected code lengths, if one minimizes the cumulants of code lengths, then the optimal cumulant is Rényi entropy $H_\alpha(P)$, where $\alpha = 1/(1 + \rho)$ with ρ being the order of the cumulant. He also showed that the optimal cumulant can be achieved by encoding sufficiently long sequences of symbols. Sundaresan (Theorem 8 of [5]) (c.f. Blumer and McElice [6]) showed that, in the mismatched case, the optimal cumulant is $H_\alpha(P) + I_\alpha(P, Q)$, where

$$I_\alpha(P, Q) := \frac{\alpha}{1 - \alpha} \log \sum_x P(x) \left(\frac{Q(x)^\alpha}{\sum_y Q(y)^\alpha} \right)^{\frac{\alpha-1}{\alpha}} - H_\alpha(P) \quad (3)$$

is called α -entropy of P relative to Q or Sundaresan's divergence [7]. Hence, $I_\alpha(P, Q)$ can be interpreted as the penalty for not knowing the true distribution. The first term in (3) is sometimes called the Rényi cross-entropy and is analogous to the first term of (1). $I_\alpha(P, Q) \geq 0$ with equality if and only if $P = Q$. I_α -divergence can also be regarded as a generalization of the Kullback–Leibler divergence as $\lim_{\alpha \rightarrow 1} I_\alpha(P, Q) = I(P, Q)$. Refer to [5,8,9] for detailed discussions on the properties of I_α . Lutwak et al. also independently identified I_α in the context of maximum Rényi entropy and called it an α -Rényi relative entropy (Equation (4) of [10]). I_α , for $\alpha > 1$, also arises in robust inference problems (see [11] and the references therein).

In [12], Massey studied a guessing problem where one is interested in the expected number of guesses required to guess a random variable X that assumes values from an infinite set, and found a lower bound in terms of Shannon entropy. Arikan [13] studied it for a finite alphabet set and showed that Rényi entropy arises as the optimal solution in minimizing moments of the number of guesses. Subsequently, Sundaresan [5] showed that the penalty in guessing according to a distribution Q when the true distribution is P , is given by $I_\alpha(P, Q)$. It is interesting to note that guesswork has also been studied from a large deviations point of view [14–18]. Bunte and Lapidoth [8] studied a problem on partitioning of tasks and showed that Rényi entropy and Sundaresan's divergence play a similar role in the optimal number of tasks performed. We propose, in this paper, a variant of this problem where the tasks in each subset of the partition are performed according to the decreasing order of probabilities. We show that Rényi entropy and Sundaresan's divergences arise as optimal solutions in this problem too. Huleihel et al. [19,20] studied the memoryless guessing problem, a variant of Arikan's guessing problem, with i.i.d. (independent and identically distributed) guesses and showed that the minimum attainable factorial moments of number of guesses is the Rényi entropy. We show, in this paper, that the minimum factorial moment in the mismatched case is measured by the Sundaresan's divergence.

We observe that, in all these problems, the objective is to minimize usual moments or factorial moments of random variables, and Rényi entropy and Sundaresan's divergence arise in optimal solutions. The relationship between source coding and guessing is well-known in the literature. Arikan and Merhav established a close relationship between lossy source coding and guessing with distortion using large deviation techniques [14,21]. The same for the lossless case was done by Hanawal and Sundaresan [17]. In this paper, we establish a general framework for all the five problems in the IID-lossless case. We then use this to establish upper and lower bounds for the mismatched version of these problems. This helps us find an equivalence among all these problems, in the sense that knowing an asymptotically optimal solution in one problem helps us find the same in all other problems.

Our Contributions in the Paper:

- (a) a general framework for the problems on source coding, guessing and tasks partitioning;
- (b) lower and upper bounds for the general framework of these problems both in matched and mis-matched cases;
- (c) a unified approach to derive bounds for the mismatched version of these problems;
- (d) a generalized tasks partitioning problem; and
- (e) establishing operational commonality among the problems.

Organisation of the Paper:

In Section 2, we present our unified framework, and find conditions under which lower and upper bounds are attained. In Section 3, we present four well-known information-theoretic problems, namely, Campbell’s source coding, Arıkan’s guessing, Huleihel et al.’s memoryless guessing, and Bunte–Lapidoth’s tasks partitioning, and re-establish and refine major results pertaining to these problems. In Section 4, we propose and solve a generalized tasks partitioning problem. In Section 5, we establish a connection among the aforementioned problems. Finally, we summarize and conclude the paper in Section 6.

2. A General Minimization Problem

In this section, we present a general minimization problem whose optimum solution evaluates to Rényi entropy. We will later show that all problems stated in Section 3 are particular instances of this general problem.

Proposition 1. *Let $\psi : \mathcal{X} \rightarrow (0, \infty)$ be such that $\sum_{x \in \mathcal{X}} \psi(x)^{-1} \leq k$ for some $k > 0$. Then, for $\rho \in (-1, 0) \cup (0, \infty)$,*

$$\frac{1}{\rho} \log \mathbb{E}_P[\psi(X)^\rho] \geq H_\alpha(P) - \log k, \tag{4}$$

where $\mathbb{E}_P[\cdot]$ denotes the expectation with respect to probability distribution P on \mathcal{X} , $H_\alpha(P)$ is the Rényi entropy of order α , and $\alpha := \alpha(\rho) = 1/(1 + \rho)$. The lower bound is achieved if and only if

$$\psi(x)^{-1} = k \cdot P(x)^\alpha / Z_{P,\alpha} \quad \text{for } x \in \mathcal{X}, \tag{5}$$

where $Z_{P,\alpha} := \sum_{x \in \mathcal{X}} P(x)^\alpha$.

Proof. Observe that

$$\begin{aligned} \text{sgn}(\rho) \sum_{x \in \mathcal{X}} P(x) \psi(x)^\rho &= \text{sgn}(\rho) \sum_{x \in \mathcal{X}} P(x)^\alpha \left(\frac{\psi(x)^{-1}}{P(x)^\alpha} \right)^{-\rho} \\ &\stackrel{(a)}{\geq} \text{sgn}(\rho) \left(\sum_x P(x)^\alpha \right) \cdot \left(\frac{\sum_x \psi(x)^{-1}}{\sum_x P(x)^\alpha} \right)^{-\rho} \\ &= \text{sgn}(\rho) \left(\sum_x P(x)^\alpha \right)^{1+\rho} \cdot \left(\sum_x \psi(x)^{-1} \right)^{-\rho} \\ &\stackrel{(b)}{\geq} \text{sgn}(\rho) \left(\sum_x P(x)^\alpha \right)^{1+\rho} \cdot k^{-\rho}, \end{aligned}$$

where (a) is due to the generalised log-sum inequality (Equation (4.1) of [22]) applied to the function $f(x) = \text{sgn}(\rho) \cdot x^{-\rho}$; and (b) follows from the hypothesis that $\sum_x \psi(x)^{-1} \leq k$. By taking log and then dividing by ρ , we obtain (4). Equality holds in (a) if and only if $\psi(x)^{-1} = \nu P(x)^\alpha$ for some constant ν and in (b) if and only if $\sum_x \psi(x)^{-1} = k$. This completes the proof. \square

The left-side of (4) is called *normalised cumulant of $\psi(X)$ of order ρ* . The measure $P^{(\alpha)}(x) := P(x)^\alpha / Z_{P,\alpha}$ in (5) that attains the lower bound in (4) is called an α -scaled measure or *escort measure* of P . This measure also arises in robust inference (Equation (7) of [11]) and statistical physics [23]. The above proposition can also be proved using a variational

formula as follows. By a version of Donsker–Varadhan variational formula (Proposition 4.5.1 of [24]), for any real-valued f on \mathcal{X} , we have

$$\log \mathbb{E}_P[2^{f(X)}] = \max_Q \{ \mathbb{E}_Q[f(X)] - D(Q\|P) \}, \tag{6}$$

where the max is over all probability distributions Q on \mathcal{X} . Taking $\rho > 0$ and $f(x) = \rho \log \psi(x)$ in (6), we have

$$\begin{aligned} \log \mathbb{E}_P[\psi(X)^\rho] &= \max_Q \{ \rho \mathbb{E}_Q[\log \psi(X)] - D(Q\|P) \} \\ &= \max_Q \left\{ -\rho \sum_x Q(x) \log \frac{\psi(x)^{-1} Q(x)}{Q(x)} - D(Q\|P) \right\} \\ &= \max_Q \left\{ \rho H(Q) - \rho \sum_x Q(x) \log \frac{\psi(x)^{-1}}{Q(x)} - D(Q\|P) \right\} \\ &\stackrel{(a)}{\geq} \max_Q \left\{ \rho H(Q) - \rho \log \sum_x \psi(x)^{-1} - D(Q\|P) \right\} \\ &\stackrel{(b)}{\geq} \rho \max_Q \left\{ H(Q) - \frac{1}{\rho} D(Q\|P) \right\} - \rho \log k, \end{aligned}$$

where (a) is by the log-sum inequality (Equation (4.1) of [22]) and (b) is by applying the constraint $\sum_x \psi(x)^{-1} \leq k$. For $\rho \in (-1, 0)$, the inequalities in (a) and (b) are reversed, and the last max is replaced by min. Hence, (4) follows as the last max is equal to $H_\alpha(P)$ by (Theorem 1 of [25]). Equality in (a) and (b) holds if and only if $\psi(x)^{-1} = k \cdot Q(x)$. In addition, the last max is attained when $Q(x) = P(x)^\alpha / Z_{P,\alpha}$ for $x \in \mathcal{X}$. This completes the proof. The following is the analogous one for Shannon entropy.

Proposition 2. Let $\psi : \mathcal{X} \rightarrow (0, \infty)$ be such that $\sum_{x \in \mathcal{X}} \psi(x)^{-1} \leq k$. Then,

$$\mathbb{E}_P[\log \psi(X)] \geq H(P) - \log k. \tag{7}$$

Equality in (7) is achieved if and only if $\psi(x)^{-1} = k \cdot P(x) \forall x \in \mathcal{X}$.

Proof.

$$\begin{aligned} \mathbb{E}_P[\log \psi(X)] &= -\sum_x P(x) \log \frac{P(x) \cdot \psi(x)^{-1}}{P(x)} = H(P) - \sum_x P(x) \log \frac{\psi(x)^{-1}}{P(x)} \\ &\geq H(P) - \log \sum_x \psi(x)^{-1} \geq H(P) - \log k, \end{aligned}$$

where the penultimate inequality is due to the log-sum inequality. Equality holds in both inequalities if and only if $\psi(x)^{-1} = k \cdot P(x) \forall x \in \mathcal{X}$. \square

It is interesting to note that $\log \mathbb{E}_P[\psi(X)^\rho] / \rho \rightarrow \mathbb{E}_P[\log(\psi(X))]$ and $H_\alpha(P) \rightarrow H(P)$ as $\rho \rightarrow 0$ in (4). We now extend Propositions 1 and 2 to sequences of random variables. Let \mathcal{X}^n be the set of all n -length sequences of elements of \mathcal{X} , and P_n be the n -fold product distribution of P on \mathcal{X}^n , that is, for $x^n := x_1, \dots, x_n \in \mathcal{X}^n$, $P_n(x^n) = \prod_{i=1}^n P(x_i)$.

Corollary 1. Given any $n \geq 1$, if $\psi_n : \mathcal{X}^n \rightarrow [0, \infty)$ is such that $\sum_{x^n \in \mathcal{X}^n} \psi_n(x^n)^{-1} \leq k_n$ for some $k_n > 0$, then

(a) For $\rho \in (-1, 0) \cup (0, \infty)$,

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[\psi_n(X^n)^\rho] \geq H_\alpha(P) - \limsup_{n \rightarrow \infty} \frac{\log k_n}{n}.$$

(b)

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{P_n}[\log \psi_n(X^n)] \geq H(P) - \limsup_{n \rightarrow \infty} \frac{\log k_n}{n},$$

where $\mathbb{E}_{P_n}[\cdot]$ denotes the expectation with respect to probability distribution P_n on \mathcal{X}^n .

Proof. It is easy to see that $H_\alpha(P_n) = nH_\alpha(P)$ and $H(P_n) = nH(P)$. Applying Propositions 1 and 2, dividing throughout by n and taking $\liminf_{n \rightarrow \infty}$, the results follow. \square

A General Framework for Mismatched Cases

In this sub-section, we establish a unified approach for cases when there is mismatch between assumed and true distributions.

Proposition 3. Let $\rho > -1$, $\alpha = 1/(1 + \rho)$, and Q be a probability distribution on \mathcal{X} . For $n \geq 1$, let Q_n be the n -fold product distribution of Q on \mathcal{X}^n . If $\psi_n : \mathcal{X}^n \rightarrow (0, \infty)$ is such that

$$\psi_n(x^n) \leq \frac{c_n \cdot Z_{Q_n, \alpha}}{Q_n(x^n)^\alpha} \tag{8}$$

for some $c_n > 0$, then

(a) for $\rho \neq 0$, we have

$$\text{sgn}(\rho) \cdot \mathbb{E}_{P_n}[\psi_n(X^n)^\rho] \leq \text{sgn}(\rho) \cdot 2^{n\rho[H_\alpha(P) + I_\alpha(P, Q) + n^{-1} \log c_n]},$$

(b) for $\rho \neq 0$, we have

$$\limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[\psi_n(X^n)^\rho] \leq H_\alpha(P) + I_\alpha(P, Q) + \limsup_{n \rightarrow \infty} \frac{1}{n} \log c_n,$$

(c) for $\rho = 0$, we have

$$\mathbb{E}_{P_n}[\log \psi_n(X^n)] \leq n[H(P) + I(P, Q) + n^{-1} \log c_n],$$

(d) for $\rho = 0$, we have

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{P_n}[\log \psi_n(X^n)] \leq H(P) + I(P, Q) + \limsup_{n \rightarrow \infty} \frac{1}{n} \log c_n.$$

Proof. Part (a): From (8), we have

$$\begin{aligned} \text{sgn}(\rho) \cdot \mathbb{E}_{P_n}[\psi_n(X^n)^\rho] &= \text{sgn}(\rho) \cdot \sum_{x^n \in \mathcal{X}^n} P_n(x^n) \psi_n(x^n)^\rho \\ &\leq \text{sgn}(\rho) \cdot c_n^\rho Z_{Q_n, \alpha}^\rho \sum_{x^n \in \mathcal{X}^n} P_n(x^n) Q_n(x^n)^{-\alpha\rho} \\ &= \text{sgn}(\rho) \cdot 2^{\rho[H_\alpha(P_n) + I_\alpha(P_n, Q_n) + \log c_n]} \\ &= \text{sgn}(\rho) \cdot 2^{n\rho[H_\alpha(P) + I_\alpha(P, Q) + n^{-1} \log c_n]}, \end{aligned} \tag{9}$$

where the penultimate equality holds from the definition of I_α , and the last one holds because $H_\alpha(P_n) = nH_\alpha(P)$, $I_\alpha(P_n, Q_n) = nI_\alpha(P, Q)$.

Part (b): Taking log, dividing throughout by $n\rho$, and then applying \limsup successively on both sides of (9), the result follows.

Part (c): When $\rho = 0$, we have $\alpha = 1$ and (8) becomes $\psi_n(x^n) \leq \frac{c_n}{Q_n(x^n)}$. Hence,

$$\begin{aligned} \mathbb{E}_{P_n}[\log \psi_n(X^n)] &= \sum_{x^n \in \mathcal{X}^n} P_n(x^n) \log \psi_n(x^n) \\ &\leq \log c_n + \sum_{x^n \in \mathcal{X}^n} P_n(x^n) \log(1/Q_n(x^n)) \\ &= \log c_n + H(P_n) + I(P_n, Q_n) \\ &= n(H(P) + I(P, Q) + n^{-1} \log c_n), \end{aligned} \tag{10}$$

where the last equality holds because $H(P_n) = nH(P)$, and $I(P_n, Q_n) = nI(P, Q)$.

Part (d): Dividing (10) throughout by n , and taking limsup on both sides, the result follows. \square

Proposition 4. Let $\rho > -1$, $\alpha = 1/(1 + \rho)$, and Q be a probability distribution on \mathcal{X} . For $n \geq 1$, let Q_n be the n -fold product distribution of Q on \mathcal{X}^n . Suppose $\psi_n : \mathcal{X}^n \rightarrow (0, \infty)$ is such that

$$\psi_n(x^n) \geq \frac{a_n Z_{Q_n, \alpha}}{Q_n(x^n)^\alpha}$$

for some $a_n > 0$, then

(a) for $\rho \neq 0$, we have

$$\text{sgn}(\rho) \cdot \mathbb{E}_{P_n}[\psi_n(X^n)^\rho] \geq \text{sgn}(\rho) \cdot 2^{n\rho(H_\alpha(P) + I_\alpha(P, Q) + n^{-1} \log a_n)},$$

(b) for $\rho \neq 0$, we have

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[\psi_n(X^n)^\rho] \geq H_\alpha(P) + I_\alpha(P, Q) + \liminf_{n \rightarrow \infty} \frac{1}{n} \log a_n,$$

(c) for $\rho = 0$, we have

$$\mathbb{E}_{P_n}[\log \psi_n(X^n)] \geq n(H(P) + I(P, Q) + n^{-1} \log a_n),$$

(d) for $\rho = 0$, we have

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_{P_n}[\log \psi_n(X^n)] \geq H(P) + I(P, Q) + \liminf_{n \rightarrow \infty} \frac{1}{n} \log a_n.$$

Proof. Similar to proof of Proposition 3. \square

3. Problem Statements and Known Results

In this section, we discuss Campbell’s source coding problem, Arıkan’s guessing problem, Huleihel et al.’s memoryless guessing problem, and Bunte–Lapidoth’s tasks partitioning problem. Using the general framework presented in the previous section, we re-establish known results, and present a few new results relating to these problems.

3.1. Source Coding Problem

Let X be a random variable that assumes values from a finite alphabet set $\mathcal{X} = \{a_1, \dots, a_m\}$ according to a probability distribution P . The tuple (\mathcal{X}, P) is usually referred to as a source. A binary code C is a mapping from \mathcal{X} to the set of finite length binary strings. Let $L(C(X))$ be the length of code $C(X)$. The objective is to find a uniquely decodable code that minimizes the expected code-length, that is,

$$\text{Minimize } \mathbb{E}_P[L(C(X))]$$

over all uniquely decodable codes C . Kraft and McMillan independently proved the following relation between uniquely decodable codes and their code-lengths.

Kraft-McMillan Theorem [26]: If C a uniquely decodable code, then

$$\sum_{x \in \mathcal{X}} 2^{-L(C(x))} \leq 1. \tag{11}$$

Conversely, given a length sequence that satisfies the above inequality, there exists a uniquely decodable code C with the given length sequence.

Thus, one can confine the search space for C to codes satisfying the Kraft–McMillan inequality (11).

Theorem 5.3.1 of [26]: If C is a uniquely decodable code, then $\mathbb{E}_P[L(C(X))]$ $\geq H(P)$.

Proof. Choose $\psi(x) = 2^{L(C(x))}$, where $L(C(x))$ is the length of code $C(x)$ assigned to alphabet x . Since C is uniquely decodable, from (11), we have $\sum_{x \in \mathcal{X}} \psi(x)^{-1} \leq 1$. Now, an application of Proposition 2 with $k = 1$ yields the desired result. \square

Theorem 1. Let $X^n := X_1, \dots, X_n$ be an i.i.d. sequence from \mathcal{X}^n following the product distribution $P_n(X^n) = \prod_{i=1}^n P(X_i)$. Let $Q_n(X^n) = \prod_{i=1}^n Q(X_i)$, where Q is another probability distribution. Let C_n be a code such that $L(C_n(X^n)) = \lceil -\log Q_n(X^n) \rceil$. Then, C_n satisfies Kraft–McMillan inequality and

$$\lim_{n \rightarrow \infty} \frac{\mathbb{E}_{P_n}[L(C_n(X^n))]}{n} = H(P) + I(P, Q).$$

Proof. Choose $\psi_n(x^n) = 2^{L(C_n(x^n))}$, where $L(C_n(x^n))$ is the length of code $C_n(x^n)$ assigned to sequence x^n . Then, we have

$$\psi_n(x^n) = 2^{L(C_n(x^n))} = 2^{\lceil -\log Q_n(x^n) \rceil} \leq 2 \cdot 2^{-\log Q_n(x^n)} = 2/Q_n(x^n).$$

An application of Proposition 3 with $c_n = 2$ yields $\limsup_{n \rightarrow \infty} \mathbb{E}_{P_n}[L(C_n(X^n))]/n \leq H(P) + I(P, Q)$. Furthermore, we also have

$$\psi_n(x^n) = 2^{L(C_n(x^n))} = 2^{\lceil -\log Q_n(x^n) \rceil} \geq 2^{-\log Q_n(x^n)} = 1/Q_n(x^n).$$

An application of Proposition 4 with $a_n = 1$ gives $\liminf_{n \rightarrow \infty} \mathbb{E}_{P_n}[L(C_n(X^n))]/n \geq H(P) + I(P, Q)$. \square

3.2. Campbell Coding Problem

Campbell’s coding problem is similar to Shannon’s source coding problem except that, instead of minimizing the expected code-length, one is interested in minimizing the normalized cumulant of code lengths, that is,

$$\text{Minimize } \frac{1}{\rho} \log \mathbb{E}_P[2^{\rho L(C(X))}],$$

over all uniquely decodable codes C , and $\rho > 0$. This problem was shown to be equivalent to minimizing buffer overflow probability by Humblet in [27]. A lower bound for the normalized cumulants in terms of Rényi entropy was provided by Campbell [4].

Lemma 1 of [4]: Let C be a uniquely decodable code. Then,

$$\frac{1}{\rho} \log \mathbb{E}_{P_n}[2^{\rho L(C(X))}] \geq H_\alpha(P), \tag{12}$$

where $\alpha = 1/(1 + \rho)$.

Proof. Apply Proposition 1 with $\psi(x) = 2^{L(C(x))}$ and $k = 1$. \square

Notice that, if we ignore the integer constraint of the length function, then

$$L(C(x)) = \log \frac{Z_{P,\alpha}}{P(x)^\alpha}, \tag{13}$$

with $Z_{P,\alpha}$ as in Proposition 1, satisfies (11) and achieves the lower bound in (12). Campbell also showed that the lower bound in (12) can be achieved by encoding long sequences of symbols with code-lengths close to (13).

Theorem 1 of [4]: If C_n is a uniquely decodable code such that

$$L(C_n(x^n)) = \left\lceil \log \frac{Z_{P_n,\alpha}}{P_n(x^n)^\alpha} \right\rceil, \tag{14}$$

then

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [2^{\rho L(C_n(X^n))}] = H_\alpha(P).$$

Proof. Choose $\psi_n(x^n) = 2^{L(C_n(x^n))}$. Then, from (14), we have

$$\frac{Z_{P_n,\alpha}}{P_n(x^n)^\alpha} \leq \psi_n(x^n) < 2 \cdot \frac{Z_{P_n,\alpha}}{P_n(x^n)^\alpha}.$$

The result follows by applying Propositions 3 and 4 with $c_n = 2, a_n = 1$ and $Q = P$. \square

Mismatch Case:

Redundancy in the mismatched case of the Campbell’s problem was studied in [5,6]. Sundaresan showed that the difference in the normalized cumulant from the minimum when encoding according to an arbitrary uniquely decodable code is measured by I_α -divergence up-to a factor of 1 [5]. We provide a more general version of this result in the following.

Proposition 5. Let X be a random variable that assumes values from set \mathcal{X} according to a probability distribution P . Let $\rho \in (-1, 0) \cup (0, \infty)$ and $L : \mathcal{X} \rightarrow \mathbb{Z}_+$ be an arbitrary length function that satisfies (11). Define

$$R_c(P, L, \rho) := \frac{1}{\rho} \log \mathbb{E}_P [2^{\rho L(X)}] - \min_K \frac{1}{\rho} \log \mathbb{E}_P [2^{\rho K(X)}], \tag{15}$$

where the minimum is over all length functions K satisfying (11). Then, there exists a probability distribution Q_L such that

$$I_\alpha(P, Q_L) - \log \eta - 1 \leq R_c(P, L, \rho) \leq I_\alpha(P, Q_L) - \log \eta, \tag{16}$$

where $\eta = \sum_x 2^{-L(x)}$.

Proof. Since K satisfies (11), an application of Proposition 1 with $\psi(x) = 2^{K(x)}$ gives us $\frac{1}{\rho} \log \mathbb{E}_P [2^{\rho K(X)}] \geq H_\alpha(P)$. Since $K(x) = \lceil \log(Z_{P,\alpha}/P(x)^\alpha) \rceil$ satisfies (11) and $\psi(x) = 2^{K(x)} < 2 \cdot Z_{P,\alpha}/P(x)^\alpha$, applying Proposition 3 with $n = 1, c_1 = 2$, and $Q = P$, we have

$$\frac{1}{\rho} \log \mathbb{E}_P [2^{\rho K(X)}] \leq H_\alpha(P) + 1,$$

that is, the minimum in (15) is between $H_\alpha(P)$ and $H_\alpha(P) + 1$. Hence,

$$\frac{1}{\rho} \log \mathbb{E}_P [2^{\rho L(X)}] - H_\alpha(P) - 1 \leq R_c(P, L, \rho) \leq \frac{1}{\rho} \log \mathbb{E}_P [2^{\rho L(X)}] - H_\alpha(P). \tag{17}$$

Let us now define a probability distribution Q_L as

$$Q_L(x) = \frac{2^{-L(x)/\alpha}}{\sum_{x'} 2^{-L(x')/\alpha}}.$$

Then,

$$2^{L(x)} = Q_L(x)^{-\alpha} Z_{Q_L, \alpha} \cdot \frac{1}{\sum_{x'} 2^{-L(x')}} = Q_L(x)^{-\alpha} Z_{Q_L, \alpha} \cdot \frac{1}{\eta},$$

where $\eta = \sum_{x'} 2^{-L(x')}$. Applying Propositions 3 and 4 with $n = 1$, $\psi_1(x) = 2^{L(x)}$, $a_1 = c_1 = 1/\eta$, we obtain

$$\frac{1}{\rho} \log \mathbb{E}_P[2^{\rho L(X)}] = H_\alpha(P) + I_\alpha(P, Q_L) - \log \eta. \tag{18}$$

Combining (17) and (18), we obtain the desired result. \square

We remark that the bound in (16) can be loose when η is small. For example, for a source with two symbols, say x and y , with code lengths $L(x) = L(y) = 100$, we have $R_c(P, L, \rho) \geq I_\alpha(P, Q_L) + 98$. However, if one imposes the constraint $1/2 \leq \eta \leq 1$, then (16) simplifies to

$$|R_c(P, L, \rho) - I_\alpha(P, Q_L)| \leq 1,$$

which is (Theorem 8 of [5]). $I_\alpha(P, Q_L)$ is, in a sense, the penalty when Q_L does not match the true distribution P . In view of this, a result analogous to Proposition 5 also holds for the Shannon source coding problem.

3.3. Arikan’s Guessing Problem

Let \mathcal{X} be a set of objects with $|\mathcal{X}| = m$. Bob thinks of an object X (a random variable) from \mathcal{X} according to a probability distribution P . Alice guesses it by asking questions of the form “Is $X = x$?”. The objective is to minimize average number of guesses required for Alice to guess X correctly. By a guessing strategy (or guessing function), we mean a one-one map $G : \mathcal{X} \rightarrow \{1, \dots, m\}$, where $G(x)$ is to be interpreted as the number of questions required to guess x correctly. Arikan studied the ρ^{th} moment of number of guesses and found upper and lower bounds in terms of Rényi entropy.

Theorem 1 of [13]: Let G be any guessing function. Then, for $\rho \in (-1, 0) \cup (0, \infty)$,

$$\frac{1}{\rho} \log \mathbb{E}_P[G(X)^\rho] \geq H_\alpha(P) - \log(1 + \ln m).$$

Proof. Let G be any guessing function. Let $\psi(x) = G(x)$. Then, we have $\sum_{x \in \mathcal{X}} \psi(x)^{-1} = \sum_{x \in \mathcal{X}} 1/G(x) = \sum_{i=1}^m 1/i \leq 1 + \ln m$. An application of Proposition 1 with $k = 1 + \ln m$ yields the desired result. \square

Arikan showed that an optimal guessing function guesses according to the decreasing order of P -probabilities with ties broken using an arbitrary but fixed rule [13]. He also showed that normalized cumulant of an optimal guessing function is bounded above by the Rényi entropy. Next, we present a proof of this using our general framework.

Proposition 4 of [13]: If G^* is an optimal guessing function, then, for $\rho \in (-1, 0) \cup (0, \infty)$,

$$\frac{1}{\rho} \log \mathbb{E}_P[G^*(X)^\rho] \leq H_\alpha(P).$$

Proof. Let us rearrange the probabilities $\{P(x), x \in \mathcal{X}\}$ in non-increasing order, say

$$p_1 \geq p_2 \geq \dots \geq p_m.$$

Then, the optimal guessing function G^* is given by $G^*(x) = i$ if $P(x) = p_i$. Let us index the elements in set \mathcal{X} as $\{x_1, x_2, \dots, x_m\}$, according to the decreasing order of their probabilities. Then, for $i \in \{1, \dots, m\}$, we have

$$\frac{Z_{P,\alpha}}{P(x_i)^\alpha} = \frac{\sum_{j=1}^m p_j^\alpha}{p_i^\alpha} \geq i = G^*(x_i). \tag{19}$$

That is, $G^*(x) \leq \frac{Z_{P,\alpha}}{P(x)^\alpha}$ for $x \in \mathcal{X}$. Now, an application of Proposition 3 with $n = 1$, $Q = P$, $\psi_1(x) = G^*(x)$ and $c_1 = 1$, gives us

$$\frac{1}{\rho} \log \mathbb{E}_P[G^*(X)^\rho] = \frac{1}{\rho} \log \mathbb{E}_P[\psi(X)^\rho] \leq H_\alpha(P) + I_\alpha(P, P) + \log 1 = H_\alpha(P).$$

□

Arikan also proved that the upper bound of Rényi entropy can be achieved by guessing long sequences of letters in an i.i.d. fashion.

Proposition 5 of [13] Let X_1, X_2, \dots, X_n be a sequence of i.i.d. guesses. Let $G_n^*(X_1, \dots, X_n)$ be an optimal guessing function. Then, for $\rho \in (-1, 0) \cup (0, \infty)$,

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[G_n^*(X_1, X_2, \dots, X_n)^\rho] = H_\alpha(P).$$

Proof. Let G_n^* be the optimal guessing function from \mathcal{X}^n to $\{1, 2, \dots, m^n\}$. An application of Corollary 1 with $\psi_n(x^n) = G_n^*(x^n)$ and $k_n = 1 + n \ln m$ yields

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[G_n^*(X^n)^\rho] \geq H_\alpha(P) - \limsup_{n \rightarrow \infty} \frac{\log(1 + n \ln m)}{n} = H_\alpha(P). \tag{20}$$

As in the proof of the previous result, we know that $G^*(x^n) \leq \frac{Z_{P_n,\alpha}}{P_n(x^n)^\alpha}$ for $x^n \in \mathcal{X}^n$. Hence, an application of Proposition 3 with $Q_n = P_n$, $\psi_n(x^n) = G_n^*(x^n)$, and $c_n = 1$ yields

$$\limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[G_n^*(X^n)^\rho] \leq H_\alpha(P). \tag{21}$$

Combining (20) and (21), we obtain the desired result. □

Henceforth, we shall denote the optimal guessing function corresponding to a probability distribution P by G_P .

Mismatch Case:

Suppose Alice does not know the true underlying probability distribution P , and guesses according to some guessing function G . The following proposition tells us that the penalty for deviating from the optimal guessing function can be measured by I_α -divergence.

Proposition 6. Let G be an arbitrary guessing function. Then, for $\rho \in (-1, 0) \cup (0, \infty)$, there exists a probability distribution Q_G on \mathcal{X} such that

$$\frac{1}{\rho} \log \mathbb{E}_P[G(X)^\rho] \geq H_\alpha(P) + I_\alpha(P, Q_G) - \log(1 + \ln m).$$

Proof. Let G be a guessing function. Define a probability distribution Q_G on \mathcal{X} as

$$Q_G(x) = \frac{G(x)^{-1/\alpha}}{\sum_{x' \in \mathcal{X}} G(x')^{-1/\alpha}}. \tag{22}$$

Then, we have

$$\frac{Z_{Q_G, \alpha}}{Q_G(x)^\alpha} = G(x) \sum_{x' \in \mathcal{X}} \frac{1}{G(x')} \leq G(x) \cdot (1 + \ln m).$$

Now, an application of Proposition 4 with $n = 1$, $\psi_1(x) = G(x)$, and $a_1 = 1/(1 + \ln m)$ yields the desired result. \square

A converse result is the following.

Proposition 1 of [5]: Let G_Q be an optimal guessing function associated with Q . Then, for $\rho \in (-1, 0) \cup (0, \infty)$,

$$\frac{1}{\rho} \log \mathbb{E}_P [G_Q(X)^\rho] \leq H_\alpha(P) + I_\alpha(P, Q),$$

where the expectation is with respect to P .

Proof. Let us rearrange the probabilities $(Q(x), x \in \mathcal{X})$ in non-increasing order, say

$$q_1 \geq q_2 \geq \dots \geq q_m.$$

By definition, $G_Q(x) = i$ if $Q(x) = q_i$. Then, as in (19), we have $G_Q(x) \leq Z_{Q, \alpha} / Q(x)^\alpha$ for $x \in \mathcal{X}$. Hence, an application of Proposition 3 with $n = 1$, $\psi_1(x) = G_Q(x)$, and $c_1 = 1$ proves the result. \square

Observe that, given a guessing function G , if we apply the above proposition for $Q = Q_G$, where Q_G is as in (22), then we obtain

$$\frac{1}{\rho} \log \mathbb{E}_{P_n} [G_{Q_G}(X)^\rho] \leq H_\alpha(P) + I_\alpha(P, Q_G).$$

Thus, the above two propositions can be combined to state the following, which is analogous to Proposition 5 (refer Section 3.2).

Theorem 6 of [5]: Let G be an arbitrary guessing function and G_P be the optimal guessing function for P . For $\rho \in (-1, 0) \cup (0, \infty)$, let

$$R_g(P, G, \rho) := \frac{1}{\rho} \log \mathbb{E}_P [G(X)^\rho] - \frac{1}{\rho} \log \mathbb{E}_P [G_P(X)^\rho].$$

Then, there exists a probability distribution Q_G such that

$$|R_g(P, G, \rho) - I_\alpha(P, Q_G)| \leq \log(1 + \ln m).$$

3.4. Memoryless Guessing

In memoryless guessing, the setup is similar to that of Arıkan’s guessing problem except that this time the guesser Alice comes up with guesses independent of her previous guesses. Let $\hat{X}_1, \hat{X}_2, \dots$ be Alice’s sequence of independent guesses according to a distribution \hat{P} . The guessing function in this problem is defined as

$$G_{\hat{P}}(X) := \inf\{i \geq 1 : \hat{X}_i = X\},$$

that is, the number of guesses until a successful guess. Sundaresan [28], inspired by Arıkan’s result, showed that the minimum expected number of guesses required is $\exp\{H_{\frac{1}{2}}(P)\}$, and the distribution that achieves this is surprisingly not the underlying distribution P , but the “tilted distribution” $\hat{P}^*(x) := \sqrt{P(x)} / \sum_y \sqrt{P(y)}$.

Unlike in Arıkan’s guessing problem, Huleihel et al. [19] minimized what are called factorial moments, defined for $\rho \in \mathbb{Z}_+$ as

$$V_{\hat{P},\rho}(X) = \frac{1}{\rho!} \prod_{l=0}^{\rho-1} (G_{\hat{P}}(X) + l).$$

Huleihel et al. [19] (c.f. [20]) studied the following problem.

$$\text{Minimize } \mathbb{E}_P [V_{\hat{P},\rho}(X)],$$

over all $\hat{P} \in \mathcal{P}$, where \mathcal{P} is the probability simplex that is, $\mathcal{P} = \{(P(x))_{x \in \mathcal{X}} : P(x) \geq 0, \sum_x P(x) = 1\}$. Let \hat{P}^* be the optimal solution of the above problem.

Theorem 1 of [19]: For any integer $\rho > 0$, we have

$$\frac{1}{\rho} \log \mathbb{E}_P [V_{\hat{P}^*,\rho}(X)] = H_\alpha(P)$$

and $\hat{P}^*(x) = P(x)^\alpha / Z_{P,\alpha}$.

Proof. From [19], we know that

$$\mathbb{E}_P [V_{\hat{P},\rho}(X)] = \mathbb{E}_P [\hat{P}(X)^{-\rho}]. \tag{23}$$

Now, the result follows from Proposition 1 with $\psi(x) = \hat{P}(x)^{-1}$ and $k = 1$. Indeed, since \hat{P} is a probability distribution, we have $\sum_{x \in \mathcal{X}} \psi(x)^{-1} = \sum_{x \in \mathcal{X}} \hat{P}(x) = 1$. Hence, $\frac{1}{\rho} \log \mathbb{E}_P [V_{\hat{P},\rho}(X)] \geq H_\alpha(P)$, and the lower bound is attained by $\hat{P}^*(x) = P(x)^\alpha / Z_{P,\alpha}$. \square

For a sequence of guesses, the above theorem can be stated in the following way. Let $\hat{X}^n = (\hat{X}_1, \dots, \hat{X}_n)$, where \hat{X}_i ’s are i.i.d. guesses, drawn from \mathcal{X}^n with distribution \hat{P}_n —the n -fold product distribution of \hat{P} on \mathcal{X}^n . If the true underlying distribution is P_n , then

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [V_{\hat{P}_n^*,\rho}(X^n)] = H_\alpha(P),$$

where $\hat{P}_n^*(x) = P_n(x)^\alpha / Z_{P_n,\alpha}$. For the mismatched case, we have the following result.

Proposition 7. If the true underlying probability distribution is P , but Alice assumes it as Q and guesses according to its optimal one, namely $\hat{Q}^*(x) = Q(x)^\alpha / Z_{Q,\alpha}$, then

$$\frac{1}{\rho} \log \mathbb{E}_P [V_{\hat{Q}^*,\rho}(X)] = H_\alpha(P) + I_\alpha(P, Q).$$

Proof. Due to (23), the result follows easily by taking $n = 1$, $\psi_1(x) = \hat{Q}^*(x)^{-1}$, $c_1 = 1$, $a_1 = 1$ in Propositions 3 and 4. \square

3.5. Tasks Partitioning Problem

Encoding of Tasks problem studied by Bunte and Lapidoth [8] can be phrased in the following way. Let \mathcal{X} be a finite set of tasks. A task X is randomly drawn from \mathcal{X} according to a probability distribution P , which may correspond to the frequency of occurrences of tasks. Suppose these tasks are associated with M keys. Typically, $M < |\mathcal{X}|$. Due to a limited availability of keys, more than one task may be associated with a single key. When a task needs to be performed, the key associated with it is pressed. Consequently, all tasks associated with this key will be performed. The objective in this problem is to minimize the number of redundant tasks performed. Usual coding techniques suggest assigning tasks with high probability to individual keys and leaving the low probability tasks unassigned.

It may just be the case that some tasks may have a higher frequency of occurrence than others. However, for an individual, all tasks can be equally important. If $M \geq |\mathcal{X}|$, then one can perform tasks without any redundancy. However, Bunte and Lapidoth [8] showed that, even when $M < |\mathcal{X}|$, one can accomplish the tasks with much less redundancy on average, provided the underlying probability distribution is different from the uniform distribution.

Let $\mathcal{A} = \{A_1, A_2, \dots, A_M\}$ be a partition of \mathcal{X} that corresponds to the assignment of tasks to M keys. Let $A(x)$ be the cardinality of the subset containing x in the partition. We shall call A the *partition function* associated with partition \mathcal{A} . We shall assume that $\rho > 0$ throughout this section, though some of the results hold even when $\rho \in (-1, 0)$.

Theorem I.1 of [8]: *The following results hold.*

(a) *For any partition of \mathcal{X} of size M with partition function A , we have*

$$\frac{1}{\rho} \log \mathbb{E}_P[A(X)^\rho] \geq H_\alpha(P) - \log M.$$

(b) *If $M > \log |\mathcal{X}| + 2$, then there exists a partition of \mathcal{X} of size at most M with partition function A such that*

$$1 \leq \mathbb{E}_P[\widehat{A}(X)^\rho] \leq 1 + 2^{\rho(H_\alpha(P) - \log \tilde{M})},$$

where

$$\tilde{M} := (M - \log |\mathcal{X}| - 2) / 4. \tag{24}$$

Proof. *Part (a):* Let $\psi(x) = A(x)$. Then, we have $\sum_{x \in \mathcal{X}} \psi(x)^{-1} = \sum_{x \in \mathcal{X}} A(x)^{-1} = M$ (Prop. III-1 of [8]). Now, an application of Proposition 1 with $k = M$ gives us the desired result.

Part (b): For the proof of this part, we refer to [8]. \square

Bunte and Lapidoth also proved the following limit results.

Theorem I.2 of [8]: *Then, for every $n \geq 1$, there exists a partition \mathcal{A}_n of \mathcal{X}^n of size at most M^n with an associated partition function A_n such that*

$$\lim_{n \rightarrow \infty} \mathbb{E}_{P_n}[A_n(X^n)^\rho] = \begin{cases} 1 & \text{if } \log M > H_\alpha(P) \\ \infty & \text{if } \log M < H_\alpha(P), \end{cases}$$

where $X^n := (X_1, \dots, X_n)$.

It should be noted that, in a general set-up of the tasks partitioning problem, it is not necessary that the partition size is of the form M^n ; it can be some M_n (a function of n). Consequently, we have the following result.

Proposition 8. *Let $\{M_n\}$ be a sequence of positive integers such that $M_n \geq n \log |\mathcal{X}| + 3$, and*

$$\gamma := \lim_{n \rightarrow \infty} \frac{\log M_n}{n}$$

exists. Then, there exists a sequence of partitions of \mathcal{X}^n of size at most M_n with partition functions A_n such that

(a)
$$\lim_{n \rightarrow \infty} \mathbb{E}_{P_n}[A_n(X^n)^\rho] = 1 \quad \text{if } \gamma > H_\alpha(P),$$

(b)
$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[A_n(X^n)^\rho] = H_\alpha(P) - \gamma \quad \text{if } \gamma < H_\alpha(P).$$

Proof. Let

$$\tilde{M}_n := (M_n - n \log |\mathcal{X}| - 2)/4. \tag{25}$$

We first claim that $\lim_{n \rightarrow \infty} \frac{\log \tilde{M}_n}{n} = \gamma$. Indeed, since $\frac{\log(1/4)}{n} \leq \frac{\log \tilde{M}_n}{n} < \frac{\log M_n}{n}$, when $\gamma = 0$, we have $\lim_{n \rightarrow \infty} \frac{\log \tilde{M}_n}{n} = 0$. On the other hand, when $\gamma > 0$, we can find an n_γ such that $M_n \geq 2^{\gamma n/2} \forall n \geq n_\gamma$. Thus, we have $\lim_{n \rightarrow \infty} \frac{n}{M_n} = 0$. Consequently,

$$\lim_{n \rightarrow \infty} \frac{\log \tilde{M}_n}{n} = \lim_{n \rightarrow \infty} \frac{\log M_n}{n} + \lim_{n \rightarrow \infty} \frac{1}{n} \log \left(1 - \frac{(n \log |\mathcal{X}| + 2)}{M_n} \right) - \lim_{n \rightarrow \infty} \frac{2}{n} = \gamma.$$

This proves the claim. From Theorem I.1 of [11], for any $n \geq 1$ and $M_n > n \log |\mathcal{X}| + 2$, there exists a partition \mathcal{A}_n of \mathcal{X}^n of size at most M_n such that the associated partition function A_n satisfies

$$\mathbb{E}_{P_n}[A_n(X^n)^\rho] \leq 1 + 2^{\rho(H_\alpha(P_n) - \log \tilde{M}_n)} = 1 + 2^{n\rho(H_\alpha(P) - \frac{\log \tilde{M}_n}{n})}.$$

Part (a): When $\gamma > H_\alpha(P)$, let us choose $\epsilon = (\gamma - H_\alpha(P))/2 > 0$. Then, there exists an n_ϵ such that $\frac{\log \tilde{M}_n}{n} \geq \gamma - \epsilon \forall n \geq n_\epsilon$. Thus, we have

$$\mathbb{E}_{P_n}[A_n(X^n)^\rho] \leq 1 + 2^{n\rho(H_\alpha(P) - \gamma + \epsilon)} = 1 + 2^{-n\rho(\gamma - H_\alpha(P))/2} \quad \forall n \geq n_\epsilon$$

Consequently, $\limsup_{n \rightarrow \infty} \mathbb{E}_{P_n}[A_n(X^n)^\rho] \leq 1$. We also note that $A_n(x^n) \geq 1$ for all $x^n \in \mathcal{X}^n$.

Thus, $\liminf_{n \rightarrow \infty} \mathbb{E}_{P_n}[A_n(X^n)^\rho] \geq 1$.

Part (b): For any $\epsilon > 0$, there exists an n_ϵ such that $\frac{\log \tilde{M}_n}{n} \geq \gamma - \epsilon \forall n \geq n_\epsilon$. Thus, we have

$$\mathbb{E}_{P_n}[A_n(X^n)^\rho] \leq 1 + 2^{n\rho(H_\alpha(P) - \gamma + \epsilon)} \leq 2^{1+n\rho(H_\alpha(P) - \gamma + \epsilon)} \quad \forall n \geq n_\epsilon$$

Hence, we have

$$\limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[A_n(X^n)^\rho] \leq H_\alpha(P) - \gamma + \epsilon \quad \forall \epsilon > 0$$

Furthermore, an invocation of Corollary 1 with $\psi_n(x^n) = A_n(x^n)$ and $k_n = \sum_{x^n \in \mathcal{X}^n} 1/A_n(x^n) = M_n$ gives us

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[A_n(X^n)^\rho] \geq H_\alpha(P) - \limsup_{n \rightarrow \infty} \frac{\log M_n}{n} = H_\alpha(P) - \gamma.$$

□

Remark 1. It is interesting to note that, when $\gamma < H_\alpha(P)$, in addition to the fact that $\lim_{n \rightarrow \infty} \mathbb{E}_{P_n}[A_n(X^n)^\rho] = \infty$, we also have $\mathbb{E}_{P_n}[A_n(X^n)^\rho] \approx 2^{n\rho(H_\alpha(P) - \gamma)}$ for large values of n .

Mismatch Case:

Let us now suppose that one does not know the true underlying probability distribution P , but arbitrarily partitions \mathcal{X} . Then, the penalty due to such a partition can be measured by the I_α -divergence as stated in the following theorem.

Proposition 9. Let \mathcal{A} be a partition of \mathcal{X} of size M with partition function A . Then, there exists a probability distribution Q_A on \mathcal{X} such that

$$\frac{1}{\rho} \log \mathbb{E}_P[A(X)^\rho] = H_\alpha(P) + I_\alpha(P, Q_A) - \log M.$$

Proof. Define a probability distribution $Q_A = \{Q_A(x), x \in \mathcal{X}\}$ as

$$Q_A(x) := \frac{A(x)^{-1/\alpha}}{\sum_{x' \in \mathcal{X}} A(x')^{-1/\alpha}}.$$

Then,

$$\frac{Z_{Q_A, \alpha}}{Q_A(x)^\alpha} = A(x) \sum_{x' \in \mathcal{X}} \frac{1}{A(x')} = A(x) \cdot M,$$

where the last equality follows due to Proposition III.1 of [8]. Rearranging terms, we have $A(x) = \frac{Z_{Q_A, \alpha}}{M \cdot Q_A(x)^\alpha}$. Hence, an application of Propositions 3 and 4 with $n = 1$, $\psi_1(x) = A(x)$, $c_1 = 1/M$, $a_1 = 1/M$, and $Q = Q_A$ yields the desired result. \square

A converse result is the following.

Proposition 10. *Let X be a random task from \mathcal{X} following distribution P and $\rho \in (0, \infty)$. Let Q be another distribution on \mathcal{X} . If $M > \log |\mathcal{X}| + 2$, then there exists a partition \mathcal{A}_Q (with an associated partition function A_Q) of \mathcal{X} of size at most M such that*

$$\mathbb{E}_P[A_Q(X)^\rho] \leq 1 + 2^{\rho(H_a(P) + I_a(P, Q) - \log \tilde{M})},$$

where \tilde{M} is as in (24).

Proof. Similar to proof of Theorem I.1 of [8]. \square

4. Ordered Tasks Partitioning Problem

In Bunte–Lapidot’s tasks partitioning problem [8], one is interested in the average number of tasks associated with a key. However, in some scenarios, it might be more important to minimize the average number of redundant tasks performed, before the intended task. To achieve this, tasks associated with a key should be performed in a decreasing order of their probabilities. With such a strategy in place, this problem draws parallel with Arıkan’s guessing problem [13].

Let $\mathcal{A} = \{A_1, A_2, \dots, A_M\}$ be a partition of \mathcal{X} that corresponds to the assignment of tasks to M keys. Let $N(x)$ be the number of redundant tasks performed until and including the intended task x . We refer to $N(\cdot)$ as the *count function* associated with partition \mathcal{A} . We suppress the dependence of N on \mathcal{A} for the sake of notational convenience. If X denotes the intended task, then we are interested in the ρ^{th} moment of number of tasks performed, that is, $\mathbb{E}_P[N(X)^\rho]$, where $\rho > 0$.

Lemma 1. *For any count function associated with a partition of size M , we have*

$$\sum_{x \in \mathcal{X}} \frac{1}{N(x)} \leq M \left[1 + \ln \left(\frac{|\mathcal{X}|}{M} \right) \right]. \tag{26}$$

Proof. For a partition $\mathcal{A} = \{A_1, A_2, \dots, A_M\}$ of \mathcal{X} , observe that

$$\sum_{x \in \mathcal{X}} \frac{1}{N(x)} = \left(1 + \frac{1}{2} + \dots + \frac{1}{|A_1|} \right) + \dots + \left(1 + \frac{1}{2} + \dots + \frac{1}{|A_M|} \right). \tag{27}$$

Since $1 + \frac{1}{2} + \dots + \frac{1}{|A_k|} \leq 1 + \ln |A_k|$, for any $k \in \{1, \dots, M\}$, we have

$$\begin{aligned} \sum_{x \in \mathcal{X}} \frac{1}{N(x)} &\leq M + \ln(|A_1| \dots |A_M|) = M[1 + \ln(|A_1| \dots |A_M|)^{1/M}] \\ &\stackrel{(a)}{\leq} M \left[1 + \ln \left(\frac{|A_1| + \dots + |A_M|}{M} \right) \right] = M \left[1 + \ln \left(\frac{|\mathcal{X}|}{M} \right) \right], \end{aligned} \tag{28}$$

where (a) follows due to the AM–GM inequality. \square

Proposition 11. *Let X be a random task from \mathcal{X} following distribution P . Then, the following hold:*

(a) *For any partition of \mathcal{X} of size M , we have*

$$\frac{1}{\rho} \log \mathbb{E}_P[N(X)^\rho] \geq H_\alpha(P) - \log\{M[1 + \ln(|\mathcal{X}|/M)]\} \tag{29}$$

(b) *Let $M > \log |\mathcal{X}| + 2$. Then, there exists a partition of \mathcal{X} of size at most M with count function N such that*

$$1 \leq \mathbb{E}_P[N(X)^\rho] \leq 1 + 2^{\rho(H_\alpha(P) - \log \tilde{M})},$$

where \tilde{M} is as in (24).

Proof. *Part (a):* Applying Proposition 1 with $k = M[1 + \ln(|\mathcal{X}|/M)]$ and $\psi(x) = N(x)$, we obtain the desired result.

Part (b): If A and N are, respectively, the partition and count functions of a partition \mathcal{A} , then we have $1 \leq N(x) \leq A(x)$ for $x \in \mathcal{X}$. Once we observe this, the proof is same as Theorem I.1 (b) of [8]. \square

Proposition 12. *Let $\{M_n\}$ be a sequence of positive integers such that $M_n \geq n \log |\mathcal{X}| + 3$, and $\gamma := \lim_{n \rightarrow \infty} \log M_n/n$ exists. Then, there exists a sequence of partitions of \mathcal{X}^n of size at most M_n with count functions N_n such that*

(a)

$$\lim_{n \rightarrow \infty} \mathbb{E}_{P_n}[N_n(X^n)^\rho] = 1 \quad \text{if } \gamma > H_\alpha(P),$$

(b)

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[N_n(X^n)^\rho] = H_\alpha(P) - \gamma \quad \text{if } \gamma < H_\alpha(P).$$

Proof. Similar to proof of Proposition 8. \square

Remark 2. (a) *If we choose the trivial partition, namely $\mathcal{A}_n = \{\mathcal{X}^n\}$, then the ordered tasks partitioning problem simplifies to Arikan’s guessing problem, that is, we have $M_n = 1$, $N_n(x^n) = G_n(x^n)$ and (26) simplifies to*

$$\sum_{x^n \in \mathcal{X}^n} \frac{1}{G_n(x^n)} \leq 1 + n \ln |\mathcal{X}|.$$

Hence, all results pertaining to the Arikan’s guessing problem can be derived from the ordered tasks partitioning problem.

(b) *Structurally, ordered tasks partitioning problem differs from the Bunte–Lapidoth’s problem only due the factor $1 + \ln(|\mathcal{X}|/M)$ in (28). While this factor matters for one-shot results, for a sequence of i.i.d. tasks, this factor vanishes asymptotically.*

Mismatch Case:

Let us now suppose that one does not know the true underlying probability distribution P , but arbitrarily partitions \mathcal{X} and executes tasks within each subset of this partition in an arbitrary order. Then, the penalty due to such a partition and ordering can be measured by the I_α -divergence as stated in the following propositions.

Proposition 13. Let \mathcal{A} be a partition of \mathcal{X} of size M with count function N . Then, there exists a probability distribution Q_N on \mathcal{X} such that

$$\frac{1}{\rho} \log \mathbb{E}_P[N(X)^\rho] \geq H_\alpha(P) + I_\alpha(P, Q_N) - \log\{M[1 + \ln(|\mathcal{X}|/M)]\}.$$

Proof. Define a probability distribution $Q_N = \{Q_N(x), x \in \mathcal{X}\}$ as

$$Q_N(x) := \frac{N(x)^{-1/\alpha}}{\sum_{x' \in \mathcal{X}} N(x')^{-1/\alpha}}.$$

Then, by Lemma 1, we have

$$\frac{Z_{Q_N, \alpha}}{Q_N(x)^\alpha} = N(x) \sum_{x' \in \mathcal{X}} \frac{1}{N(x')} \leq N(x) \cdot M[1 + \ln(|\mathcal{X}|/M)].$$

Now, an application of Proposition 4 with $n = 1$, $\psi_1(x) = N(x)$, $Q = Q_N$, and $a_1 = 1/M[1 + \ln(|\mathcal{X}|/M)]$ yields the desired result. \square

A converse result is the following.

Proposition 14. Let X be a random task from \mathcal{X} following distribution P . Let Q be another distribution on \mathcal{X} . If $M > \log |\mathcal{X}| + 2$, then there exists partition \mathcal{A}_Q (with an associated count function N_Q) of size at most M such that

$$\mathbb{E}_P[N_Q(X)^\rho] \leq 1 + 2^{\rho(H_\alpha(P) + I_\alpha(P, Q) - \log \tilde{M})} \quad \text{if } \rho \in (0, \infty),$$

where \tilde{M} is as in (24).

Proof. Identical to the proof of Proposition 11(b). \square

5. Operational Connection Among the Problems

In this section, we establish an operational relationship among the five problems (refer Figure 1) that we studied in the previous section. The relationship we are interested in is “Does knowing an optimal or asymptotically optimal solution in one problem helps us find the same in another?” In fact, we end up showing that, under suitable conditions, all the five problems form an equivalence class with respect to the above-mentioned relation.

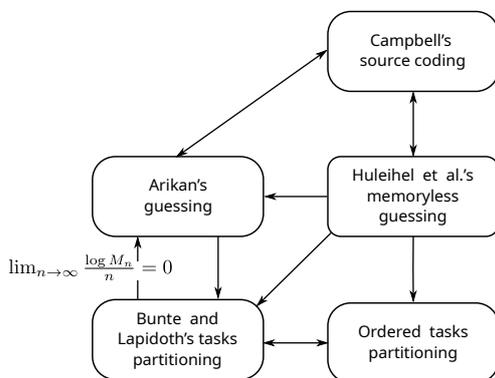


Figure 1. Relationships established among the five problems. A directed arrow from problem A to problem B means knowing optimal or asymptotically optimal solution of A helps us find the same in B .

In this section, we assume $\rho > 0$. First, we make the following observations:

- Among the five problems discussed in the previous section, only Arıkan’s guessing and Huleihel et al.’s memoryless guessing have a unique optimal solution; others only have asymptotically optimal solutions.
- Optimal solution of Huleihel et al.’s memoryless guessing problem is the α -scaled measure of the underlying probability distribution P . Hence, knowledge about the optimal solution of this problem implies knowledge about an optimal (or asymptotically optimal) solution of all other problems.
- Among the Bunte–Lapidot’s and ordered tasks problems, an asymptotically optimal solution of one yields that of the other. The partitioning lemma (Prop. III-2 of [8]) is the key result in these two problems, as it guarantees the existence of the asymptotically optimal partitions in both these problems.

5.1. Campbell’s Coding and Arıkan’s Guessing

An attempt to find a close relationship between these two problems was made, for example, by Hanawal and Sundaresan (Section II of [17]). Here, we show the equivalence between asymptotically optimal solutions of these two problems.

Proposition 15. *An asymptotically optimal solution exists for Campbell’s source coding problem if and only if an asymptotically optimal solution exists for Arıkan’s guessing problem.*

Proof. Let $\{G_n^*\}$ be an asymptotically optimal sequence of guessing functions, that is,

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[G_n^*(X^n)^\rho] = H_\alpha(P).$$

Define

$$Q_{G_n^*}(x^n) := c_n^{-1} \cdot G_n^*(x^n)^{-1}, \tag{30}$$

where c_n is the normalization constant. Notice that

$$c_n = \sum_{x^n} G_n^*(x^n)^{-1} \leq 1 + n \ln |\mathcal{X}|. \tag{31}$$

Let us now define

$$L_{G_n^*}(x^n) := \lceil -\log Q_{G_n^*}(x^n) \rceil.$$

Then, by (Proposition 1 of [17]),

$$L_{G_n^*}(x^n) \leq \log G_n^*(x^n) + 1 + \log c_n.$$

Hence,

$$2^{\rho L_{G_n^*}(x^n)} \leq 2^\rho \cdot c_n^\rho \cdot G_n^*(x^n)^\rho \leq 2^\rho \cdot (1 + n \ln |\mathcal{X}|)^\rho \cdot G_n^*(x^n)^\rho.$$

Thus, we have

$$\limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[2^{\rho L_{G_n^*}(X^n)}] \leq \limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[G_n^*(X^n)^\rho] = H_\alpha(P).$$

We observe that

$$\sum_{x^n \in \mathcal{X}^n} 2^{-L_{G_n^*}(x^n)} = \sum_{x^n \in \mathcal{X}^n} 2^{-\lceil -\log Q_{G_n^*}(x^n) \rceil} \leq \sum_{x^n \in \mathcal{X}^n} 2^{\log Q_{G_n^*}(x^n)} = 1.$$

Consequently, from (12), we have

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n}[2^{\rho L_{G_n^*}(X^n)}] \geq H_\alpha(P).$$

Thus, $\{L_{G_n^*}\}$ is an asymptotically optimal sequence of length functions for Campbell’s coding problem.

Conversely, given an asymptotically optimal sequence of length functions $\{L_n^*\}$ for Campbell’s coding problem, define

$$Q_{L_n^*}(x^n) := \frac{2^{-L_n^*(x^n)}}{\sum_{y^n} 2^{-L_n^*(y^n)}}.$$

Let $G_{L_n^*}$ be the guessing function on \mathcal{X}^n that guesses according to the decreasing order of $Q_{L_n^*}$ -probabilities. Then, by (Proposition 2 of [17]),

$$\log G_{L_n^*}(x^n) \leq L_n^*(x^n).$$

Thus,

$$\limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [G_{L_n^*}(X^n)^\rho] \leq \lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [2^{\rho L_n^*(X^n)}] = H_\alpha(P).$$

Furthermore, from Theorem 1 of [13], we have

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [G_{L_n^*}(X^n)^\rho] \geq H_\alpha(P) - \limsup_{n \rightarrow \infty} \frac{1}{n} \log(1 + n \ln |\mathcal{X}|) = H_\alpha(P).$$

This completes the proof. \square

5.2. Arikan’s Guessing and Bunte–Lapidoth’s Tasks Partitioning Problem

Bracher et al. found a close connection between Arikan’s guessing problem and Bunte–Lapidoth’s tasks partitioning problem in the context of distributed storage [29]. In this section, we establish a different relation between these problems.

Proposition 16. *An asymptotically optimal solution of Arikan’s guessing problem gives rise to an asymptotically optimal solution of tasks partitioning problem.*

Proof. Let $\{G_n^*\}$ be an asymptotically optimal sequence of guessing functions. Define

$$Q_{G_n^*}(x^n) = d_n^{-1} G_n^*(x^n)^{-1/\alpha},$$

where d_n is the normalization constant. Let $A_{G_n^*}$ be the partition function satisfying $A_{G_n^*}(x^n) \leq \lceil \beta_n \cdot Z_{Q_{G_n^*,\alpha}} / Q_{G_n^*}(x^n)^\alpha \rceil$ guaranteed by (Proposition III-2 of [8]), where

$$\beta_n = \frac{2}{M_n - n \log |\mathcal{X}| - 2}.$$

Thus, we have

$$\begin{aligned} A_{G_n^*}(x^n)^\rho &\leq \lceil \beta_n \cdot Z_{Q_{G_n^*,\alpha}} / Q_{G_n^*}(x^n)^\alpha \rceil^\rho && \stackrel{(a)}{\leq} \lceil \beta_n \cdot (1 + n \ln |\mathcal{X}|) \cdot G_n^*(x^n) \rceil^\rho \\ &&& \stackrel{(b)}{\leq} 1 + 2^\rho \beta_n^\rho \cdot (1 + n \ln |\mathcal{X}|)^\rho \cdot G_n^*(x^n)^\rho, \end{aligned}$$

where (a) holds because $Z_{Q_{G_n^*,\alpha}} = d_n^{-\alpha} \sum_{x^n \in \mathcal{X}^n} G_n^*(x^n)^{-1} \leq d_n^{-\alpha} (1 + n \ln |\mathcal{X}|)$; and (b) hold because $\lceil x \rceil^\rho \leq 1 + 2^\rho x^\rho$ for $x > 0$. Hence,

$$\begin{aligned} \mathbb{E}_{P_n} [A_{G_n^*}(X^n)^\rho] &\leq 1 + 2^\rho \beta_n^\rho \cdot (1 + n \ln |\mathcal{X}|)^\rho \cdot \mathbb{E}_{P_n} [G_n^*(X^n)^\rho] \\ &\stackrel{(c)}{\leq} 1 + 2^{2\rho} \left(\frac{1 + n \ln |\mathcal{X}|}{M_n - n \log |\mathcal{X}| - 2} \right)^\rho \cdot 2^{n\rho H_\alpha(P)} \\ &= 1 + 2^{n\rho} \left(H_\alpha(P) + \frac{\log(1 + n \ln |\mathcal{X}|)}{n} - \frac{\log M_n}{n} \right), \end{aligned}$$

where \tilde{M}_n is as in (25); and inequality (c) follows from Proposition 4 of [13] proved in Section 3. Thus, if M_n is such that $M_n \geq n \log |\mathcal{X}| + 3$ and if $\gamma := \lim_{n \rightarrow \infty} (\log M_n)/n$ exists and $\gamma > H_\alpha(P)$, then we have

$$\limsup_{n \rightarrow \infty} \mathbb{E}_{P_n} [A_{G_n^*}(X^n)^\rho] \leq 1.$$

Since $\mathbb{E}_{P_n} [A_{G_n^*}(X^n)^\rho] \geq 1$, we have $\liminf_{n \rightarrow \infty} \mathbb{E}_{P_n} [A_{G_n^*}(X^n)^\rho] \geq 1$. When $\gamma < H_\alpha(P)$, arguing along the lines of proof of Proposition 8(b), it can be shown that

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [A_{G_n^*}(X^n)^\rho] = H_\alpha(P) - \gamma.$$

□

Reverse implication of the above result does not hold always due to the additional parameter M_n in the tasks partitioning problem. For example, if $M_n = |\mathcal{X}|^n$ and $A_n(x^n) = 1$ for every x^n , the partition does not provide any information about the underlying distribution. As a consequence, we will not be able to conclude anything about the optimal (or asymptotically optimal) solutions of other problems. However, if M_n is such that $\log M_n$ increases sub-linearly, then it does help us find asymptotically optimal solutions of other problems.

Proposition 17. *An asymptotically optimal sequence of partition functions $\{A_n\}$ with partition sizes $\{M_n\}$ for the tasks partitioning problem gives rise to an asymptotically optimal solution for the guessing problem if $M_n \geq n \log |\mathcal{X}| + 3$ and $\lim_{n \rightarrow \infty} (\log M_n)/n = 0$.*

Proof. By hypothesis,

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [A_n(X^n)^\rho] = H_\alpha(P).$$

For every A_n , define the probability distribution

$$Q_{A_n}(x^n) := c_n^{-1} A_n(x^n)^{-1},$$

where $c_n := \sum_{x^n} A_n(x^n)^{-1} = M_n$. Let $G_{A_n}^*$ be the guessing function that guesses according to the decreasing order of Q_{A_n} -probabilities. Then, by (Proposition 2 of [17]), we have

$$G_{A_n}^*(x^n) \leq Q_{A_n}(x^n)^{-1} = c_n A_n(x^n) = M_n A_n(x^n).$$

Hence,

$$\limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [G_{A_n}^*(X^n)^\rho] \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \log M_n + \limsup_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [A_n(X^n)^\rho] = H_\alpha(P).$$

Furthermore, an application of Theorem 1 of [13] gives us

$$\liminf_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [G_{A_n}^*(X^n)^\rho] \geq H_\alpha(P) - \limsup_{n \rightarrow \infty} \frac{1}{n} \log(1 + n \ln |\mathcal{X}|) = H_\alpha(P).$$

This completes the proof. □

5.3. Huleihel et al.’s Memoryless Guessing and Campbell’s Coding

We already know that, if one knows the optimal solution of Huleihel et al.’s memoryless guessing problem, that is, the α -scaled measure of the underlying probability distribution P , one has knowledge about the optimal (or asymptotically optimal) solution of Campbell’s coding problem. In this section, we prove a converse statement. We first prove the following lemma.

Lemma 2. Let L_n^* denote the length function corresponding to an optimal solution for Campbell’s coding problem on the alphabet set \mathcal{X}^n endowed with the product distribution P_n . Then, $\sum_{x^n \in \mathcal{X}^n} 2^{-L_n^*(x^n)} \geq 1/2$.

Proof. Suppose $\sum_{x^n \in \mathcal{X}^n} 2^{-L_n^*(x^n)} < 1/2$. Then, we must have $L_n^*(x^n) \geq 2$ for every $x^n \in \mathcal{X}^n$. Define $\hat{L}_n(x^n) := L_n^*(x^n) - 1$. We observe that $\sum_{x^n \in \mathcal{X}^n} 2^{-\hat{L}_n(x^n)} < 1$, that is, the length function $\hat{L}_n(\cdot)$ satisfies (11). Hence, there exists a code C_n for \mathcal{X}^n such that $L(C_n(x^n)) = \hat{L}_n(x^n)$. Then, for $\rho > 0$, we have $\log \mathbb{E}_{P_n} [2^{\rho L_n^*(X^n)}] > \log \mathbb{E}_{P_n} [2^{\rho \hat{L}_n(X^n)}]$ —a contradiction. \square

Proposition 18. An asymptotically optimal solution for Huleihel et al.’s memoryless guessing problem exists if an asymptotically optimal solution exists for Campbell’s coding problem.

Proof. Let $\{L_n^*, n \geq 1\}$ denote a sequence of asymptotically optimal length functions of Campbell’s coding problem, that is,

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [2^{\rho L_n^*(X^n)}] = H_\alpha(P). \tag{32}$$

Let us define

$$Q_{L_n^*}(x^n) := \frac{2^{-L_n^*(x^n)/\alpha}}{\sum_{\hat{x}^n \in \mathcal{X}^n} 2^{-L_n^*(\hat{x}^n)/\alpha}}.$$

Then, we have

$$\begin{aligned} I_\alpha(P_n, Q_{L_n^*}) &= \frac{\alpha}{1-\alpha} \log \left(\sum_{x^n \in \mathcal{X}^n} P_n(x^n) \left[\sum_{\hat{x}^n \in \mathcal{X}^n} \left(\frac{Q_{L_n^*}(\hat{x}^n)}{Q_{L_n^*}(x^n)} \right)^\alpha \right]^{\frac{1-\alpha}{\alpha}} \right) - H_\alpha(P_n) \\ &= \frac{\alpha}{1-\alpha} \log \left(\sum_{x^n \in \mathcal{X}^n} P_n(x^n) \left[\sum_{\hat{x}^n \in \mathcal{X}^n} \frac{2^{-L_n^*(\hat{x}^n)}}{2^{-L_n^*(x^n)}} \right]^\rho \right) - nH_\alpha(P) \\ &= \frac{1}{\rho} \log \mathbb{E}_{P_n} [2^{\rho L_n^*(X^n)}] + \log \zeta_n - nH_\alpha(P), \end{aligned}$$

where $\zeta_n = \sum_{\hat{x}^n \in \mathcal{X}^n} 2^{-L_n^*(\hat{x}^n)}$. Hence,

$$\lim_{n \rightarrow \infty} \frac{1}{n} I_\alpha(P_n, Q_{L_n^*}) = \lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [2^{\rho L_n^*(X^n)}] + \lim_{n \rightarrow \infty} \frac{1}{n} \log \zeta_n - H_\alpha(P) \stackrel{(a)}{=} 0,$$

where (a) holds because $\zeta_n \in [1/2, 1]$ (refer Lemma 2). If we assume the underlying probability distribution to be $Q_{L_n^*}$ instead of P_n , and perform memoryless guessing according to the escort distribution of $Q_{L_n^*}$, namely $\hat{Q}_n^*(x^n) = Q_{L_n^*}(x^n)^\alpha / Z_{Q_{L_n^*}, \alpha}$, due to Proposition 7, we have

$$\lim_{n \rightarrow \infty} \frac{1}{n\rho} \log \mathbb{E}_{P_n} [V_{\hat{Q}_n^*, \rho}(X^n)] = H_\alpha(P) + \lim_{n \rightarrow \infty} \frac{1}{n} I_\alpha(P_n, Q_{L_n^*}) = H_\alpha(P).$$

\square

6. Summary and Conclusions

This paper was motivated by the need to find a unified framework for the problems on source coding, guessing and the tasks partitioning. To that end, we formulated a general moment minimization problem in the IID-lossless case and observed that the optimal value of its objective function is bounded below by Rényi entropy. We then re-established all achievable lower bounds in each of the above-mentioned problems using the generalized framework. It was interesting to note that the optimal solution did not depend on the moment function ψ , but only on the underlying probability distribution P and order of the moment ρ (refer Proposition 1). We also presented a unified framework for the mismatched version of the above-mentioned problems. This framework not only led to refinement of

the known theorems, but also helped us identify a few new results. We went on to extend the tasks partitioning problem by asking a more practical question and solved it using the unified theory. Finally, we established an equivalence among these problems, in the sense that an asymptotically optimal solution of one problem yields the asymptotically optimal solution of all other problems. Although the relationship between source coding and guessing is well-known in the literature [30–33], their connection to the tasks partitioning problem, and the connection in the mismatched version of the problems are new.

Our unified framework also has the potential to act as a general tool-set and provide insights for similar problems in information theory. For example, in Section 4, this framework enabled us to solve a more general tasks partitioning problem, namely, the ordered tasks partitioning problem using this framework. The presented that a unified approach can also be extended and explored further in several ways. This includes (a) *Extension to general alphabet set*: The guessing problem was originally studied for countably infinite alphabet set by Massey [12]. Courtade and Verdú have studied the source coding problem for a countably infinite alphabet set with a cumulant generating function of code word lengths as a design criterion [31]. It would be interesting to see if memory-less guessing and tasks partitioning problems can also be formulated for countably infinite alphabet sets and relationships among the problems can be extended. (b) *More general sources*: Relationship between source coding and guessing is very well-known in the literature. Relationship between guessing and source coding in the ‘with distortion’ case for finite alphabet was established by Merhav and Arikan [14] and for a countably infinite alphabet by Hanawal and Sundaresan [34]. Relationship between Guessing and Campbell’s coding in the universal case was established by Sundaresan [35]. It would be interesting to see if these can be extended to memoryless guessing and tasks partitioning also, possibly in a unified manner. (c) *Applications*: Arikan showed an application of the guessing problem in a sequential decoding problem [13]. Humblet showed that the cumulant of code-lengths arises in minimizing the probability of buffer overflow in source coding problems [27]. Rezaee et al. [36], Salamatian et al. [20], and Sundaresan [28] show the application of guessing in the security aspect of password protected systems. Our unified framework has the potential to help solve problems that arise in real life situations and fall in this framework.

Author Contributions: Conceptualization: M.A.K., A.S., A.T., A.K. and G.D.M.; Formal analysis: M.A.K. and A.S.; Investigation: M.A.K., A.S., A.T. and G.D.M.; Writing – original draft: M.A.K., A.S., A.T., A.K. and G.D.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shannon, C.E. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [[CrossRef](#)]
2. Rényi, A. On measures of entropy and information. In Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics, Berkeley, CA, USA, 20 June–30 July 1960; pp. 547–561.
3. Aczél, J.; Daróczy, Z. On Measures of Information and Their Characterizations. In *Mathematicas in Science and Engineering*; Academic Press: Cambridge, MA, USA, 1975; Volume 115.
4. Campbell, L.L. A coding theorem and Rényi’s entropy. *Inf. Control* **1965**, *8*, 423–429. [[CrossRef](#)]
5. Sundaresan, R. Guessing Under Source Uncertainty. *IEEE Trans. Inf. Theory* **2007**, *53*, 269–287. [[CrossRef](#)]
6. Blumer, A.C.; McEliece, R.J. The Rényi redundancy of generalized Huffman codes. *IEEE Trans. Inf. Theory* **1988**, *34*, 1242–1249. [[CrossRef](#)]
7. Sundaresan, R. A measure of discrimination and its geometric properties. In Proceedings of the IEEE International Symposium on Information Theory, Lausanne, Switzerland, 30 June–5 July 2002; p. 264.
8. Bunte, C.; Lapidoth, A. Encoding Tasks and Rényi Entropy. *IEEE Trans. Inf. Theory* **2014**, *60*, 5065–5076. [[CrossRef](#)]

9. Kumar, M.A.; Sundaresan, R. Minimization problems based on relative α -entropy I: Forward Projection. *IEEE Trans. Inf. Theory* **2015**, *61*, 5063–5080. [[CrossRef](#)]
10. Lutwak, E.; Yang, D.; Zhang, G. Cramér-Rao and moment-entropy inequalities for Rényi entropy and generalized Fisher information. *IEEE Trans. Inf. Theory* **2005**, *51*, 473–478. [[CrossRef](#)]
11. Ashok Kumar, M.; Sundaresan, R. Minimization Problems Based on Relative α -Entropy II: Reverse Projection. *IEEE Trans. Inf. Theory* **2015**, *61*, 5081–5095. [[CrossRef](#)]
12. Massey, J.L. Guessing and entropy. In Proceedings of the 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, 27 June–1 July 1994; p. 204.
13. Arikan, E. An inequality on guessing and its application to sequential decoding. *IEEE Trans. Inf. Theory* **1996**, *42*, 99–105. [[CrossRef](#)]
14. Arikan, E.; Merhav, N. Guessing subject to distortion. *IEEE Trans. Inf. Theory* **1998**, *44*, 1041–1056. [[CrossRef](#)]
15. Pfister, C.; Sullivan, W. Rényi entropy, guesswork moments, and large deviations. *IEEE Trans. Inf. Theory* **2004**, *50*, 2794–2800. [[CrossRef](#)]
16. Malone, D.; Sullivan, W. Guesswork and entropy. *IEEE Trans. Inf. Theory* **2004**, *50*, 525–526. [[CrossRef](#)]
17. Hanawal, M.K.; Sundaresan, R. Guessing Revisited: A Large Deviations Approach. *IEEE Trans. Inf. Theory* **2011**, *57*, 70–78. [[CrossRef](#)]
18. Christiansen, M.M.; Duffy, K.R. Guesswork, Large Deviations, and Shannon Entropy. *IEEE Trans. Inf. Theory* **2013**, *59*, 796–802. [[CrossRef](#)]
19. Huleihel, W.; Salamatian, S.; Médard, M. Guessing with limited memory. In Proceeding of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 2253–2257.
20. Salamatian, S.; Huleihel, W.; Beirami, A.; Cohen, A.; Médard, M. Why Botnets Work: Distributed Brute-Force Attacks Need No Synchronization. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2288–2299. [[CrossRef](#)]
21. Arikan, E.; Merhav, N. Joint source-channel coding and guessing with application to sequential decoding. *IEEE Trans. Inf. Theory* **1998**, *44*, 1756–1769. [[CrossRef](#)]
22. Csiszár, I.; Shields, P. *Information Theory and Statistics: A Tutorial, Foundations and Trends in Communications and Information Theory*; Now Publishers: Delft, The Netherlands, 2004.
23. Tsallis, C.; Mendes, R.S.; Plastino, A.R. The role of constraints within generalized non-extensive statistics. *Phys. A* **1998**, *261*, 534–554. [[CrossRef](#)]
24. Dupuis, P.; Ellis, R.S. *A Weak Convergence Approach to the Theory of Large Deviations*; John Wiley & Sons: Hoboken, NJ, USA, 1997.
25. Shayevitz, O. On Rényi measures and hypothesis testing. In Proceedings of the 2011 IEEE International Symposium on Information Theory Proceedings, St. Petersburg, Russia, 31 July–5 August 2011; pp. 894–898.
26. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2012.
27. Humblet, P. Generalization of Huffman coding to minimize the probability of buffer overflow. *IEEE Trans. Inf. Theory* **1981**, *27*, 230–232. [[CrossRef](#)]
28. Hanawal, M.K.; Sundaresan, R. Randomised Attacks on Passwords. *DRDO-IISc Programme on Advanced Research in Mathematical Engineering*. 2010. Available online: <https://ece.iisc.ac.in/rajeshs/reprints/TR-PME-2010-11.pdf> (accessed on 14 August 2022).
29. Bracher, A.; Hof, E.; Lapidoth, A. Guessing Attacks on Distributed-Storage Systems. *IEEE Trans. Inf. Theory* **2019**, *65*, 6975–6998. [[CrossRef](#)]
30. Salamatian, S.; Liu, L.; Beirami, A.; Médard, M. Mismatched guesswork and one-to-one codes. In Proceedings of the 2019 IEEE Information Theory Workshop (ITW), Gotland, Sweden, 25–28 August 2019; pp. 1–5.
31. Courtade, T.A.; Verdú, S. Cumulant generating function of codeword lengths in optimal lossless compression. In Proceedings of the 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 2494–2498. [[CrossRef](#)]
32. Kosut, O.; Sankar, L. Asymptotics and non-asymptotics for universal fixed-to-variable source coding. *IEEE Trans. Inf. Theory* **2017**, *63*, 3757–3772. [[CrossRef](#)]
33. Beirami, A.; Calderbank, R.; Christiansen, M.M.; Duffy, K.R.; Médard, M. A characterization of guesswork on swiftly tilting curves. *IEEE Trans. Inf. Theory* **2018**, *60*, 2850–2871.
34. Hanawal, M.K.; Sundaresan, R. *Guessing and Compression Subject to Distortion*; IndraStra Global: Sheridan, WY, USA, 2010.
35. Sundaresan, R. Guessing Based On Length Functions. In Proceedings of the 2007 IEEE International Symposium on Information Theory, Cambridge, MA, USA, 1–6 July 2007; pp. 716–719. [[CrossRef](#)]
36. Rezaee, A.; Beirami, A.; Makhdoumi, A.; Médard, M.; Duffy, K. Guesswork subject to a total entropy budget. In Proceedings of the 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 3–6 October 2017; pp. 1008–1015. [[CrossRef](#)]