

A Characterization of Guesswork on Swiftly Tilting Curves

Ahmad Beirami, Robert Calderbank, Mark Christiansen, Ken Duffy, and Muriel Médard

Abstract

Given a collection of strings, each with an associated probability of occurrence, the guesswork of each of them is their position in a list ordered from most likely to least likely, breaking ties arbitrarily. Guesswork is central to several applications in information theory: Average guesswork provides a lower bound on the expected computational cost of a sequential decoder to decode successfully the transmitted message; the complementary cumulative distribution function of guesswork gives the error probability in list decoding; the logarithm of guesswork is the number of bits needed in optimal lossless one-to-one source coding; and guesswork is the number of trials required of an adversary to breach a password protected system in a brute-force attack. In this paper, we consider memoryless string-sources that generate strings consisting of i.i.d. characters drawn from a finite alphabet, and characterize their corresponding guesswork. Our main tool is the tilt operation on a memoryless string-source. We show that the tilt operation on a memoryless string-source parametrizes an exponential family of memoryless string-sources, which we refer to as the tilted family of the string-source. We provide an operational meaning to the tilted families by proving that two memoryless string-sources result in the same guesswork on all strings of all lengths if and only if their respective categorical distributions belong to the same tilted family. Establishing some general properties of the tilt operation, we generalize the notions of weakly typical set and asymptotic equipartition property to tilted weakly typical sets of different orders. We use this new definition to characterize the large deviations for all atypical strings and characterize the volume of weakly typical sets of different orders. We subsequently build on this characterization to prove large deviation bounds on guesswork and provide an accurate approximation of its probability mass function.

Index Terms

Tilting; Ordering; Guesswork; One-to-One Codes; Rényi Entropy; Information Geometry; Weakly Typical Set.

I. INTRODUCTION

A. Motivation

An early motivation for the study of guesswork is to provide lower bounds on the computational complexity of sequential decoding [2] where the decoder sequentially examines several paths until it finds the correct coded sequence. Guesswork was first studied by Massey [3], who showed that average guesswork is lower bounded in terms of the Shannon entropy of the source. Arkan [4] considered guesswork on memoryless sources and proved that the moments of guesswork are related to the Rényi entropy rates of the source in the limit as the strings become long. This has been generalized to ergodic Markov chains [5] and a wide range of stationary sources [6]. Recently, tighter non-asymptotic bounds on the moments of guesswork were reported in [7]. Guesswork has also been studied subject to an allowable distortion [8], and subject to constrained Shannon entropy [9]. Hanawal and Sundaresan [10] rederived the moments of guesswork assuming that the logarithm of guesswork satisfies a large deviations principle (LDP). Christiansen and Duffy [11] established that guesswork satisfies a LDP and characterized the rate function. They also provided an approximation to the distribution of guesswork using the rate function associated with the LDP. That LDP for guesswork was subsequently leveraged to provide a new proof of the classical Channel Coding Theorem and to analyze the performance of a novel, universal maximum likelihood decoding algorithm [12].

In list decoding, rather than declaring one codeword message, the decoder returns a list of size L of possible codewords [13]–[15]. The error event in list decoding is the event where the message codeword is not returned in the list of the L returned codewords. For strings of fixed length, as the size of the list grows larger, the probability of error decreases. The list decoder can be used as an inner code for an outer code that eventually decides the intended message from the returned list of messages by the inner list decoder. The optimal list decoder returns the L most likely messages given the received codeword. Therefore, the probability of the error event in the optimal list decoder is characterized by the complementary cumulative distribution function of guesswork conditioned on the received codeword (see [16], [17]).

This work was presented in part in the 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton 2015) [1].

This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under awards FA 9550-14-1-043 and FA 9550-13-1-0076; the work of K. Duffy and M. Médard was also supported in part by Netapp through a Faculty Fellowship.

A. Beirami was with the Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA, and also with the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA. He is currently with EA Digital Platform – Data & AI, Electronic Arts, Redwood City, CA, USA (email: ahmad.beirami@gmail.com).

R. Calderbank is with the Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA (email: robert.calderbank@duke.edu).

M. Christiansen was with the Hamilton Institute, Maynooth University, Ireland. He is currently with Grand Thornton (email: markchristiansen4224@gmail.com).

K. Duffy is with the Hamilton Institute, Maynooth University, Ireland (email: ken.duffy@mu.ie).

M. Médard is with the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA (email: medard@mit.edu).

Guesswork can also be used to quantify computational security against brute-force attack [18]. Suppose that a secret string is drawn from a given process on a finite alphabet, and is used to secure a password-protected system. Further suppose that the system only grants access if the correct secret string is provided exactly, and does not reveal any information otherwise. If a brute-force attacker adversary decides to guess the secret string by query, the best strategy at an adversary's disposal is to query the possible secret strings from the most likely to the least likely (in terms of minimizing the average number of queries or maximizing the probability of success using a finite number of queries). In this case, guesswork gives the number of queries that it would take an attacker to find the secret string using the best strategy. Christiansen *et al.* [19] studied guesswork over the weakly typical set and proved that the exponent is strictly smaller than that of a uniform set with the same support size; they showed that the average guesswork of a password over an erasure channel does not relate to the average noise in general [20]; Christiansen *et al.* also considered the setting where an attacker wants to guess one or more out of many secret strings drawn independently from not necessarily identical string-sources [18]. Finally, the idea of guesswork has been extended to the setup where the probability distribution is unknown [9], [21], [22].

In the context of source coding, it is known that the length of the optimal one-to-one source code (that need not satisfy Kraft's inequality) is within one bit of the logarithm of guesswork. The average length of a one-to-one code is related to the normalized zeroth moment of guesswork or alternatively the expected logarithm of guesswork (see [22]). The source coding problem without prefix constraint dates back to Wyner [23], who showed that the average codeword length of one-to-one codes is upper bounded by the entropy. Alon and Orlistky derived a lower bound on the average codeword length in terms of the Shannon entropy [24], which was recently revisited for other moments of guesswork [25]. Szpankowski [26] derived the asymptotic average codeword length of one-to-one codes on binary memoryless sources, which was subsequently generalized to finite-alphabet independent and identically distributed (i.i.d.) processes [27], [28], and later studied under a universal setup [22], [29].

B. Problem setup, definitions, and notation

Let $\mathcal{X} := (a_1, \dots, a_{|\mathcal{X}|})$ be an ordered set that denotes a finite alphabet of size $|\mathcal{X}|$. We will subsequently use the ordering on \mathcal{X} to break ties for equally likely strings in guesswork (and reverse guesswork). Denote an n -string over \mathcal{X} by $x_k^{n+k-1} = x_k x_{k+1} \dots x_{n+k-1} \in \mathcal{X}^n$. Further, let $x^n = x_1^n$ and for $i > n$, $x_i^n = \emptyset$, where \emptyset denotes the null string. Let μ^n denote a multinomial probability distribution on the sample space \mathcal{X}^n , where μ^1 is the corresponding categorical distribution on \mathcal{X} , i.e., $\mu^n(x^n) = \prod_{i=1}^n \mu^1(x_i)$. We refer to $\mu := \{\mu^n : n \in \mathbb{N}\}$ as a (memoryless) string-source, also called source. Let $\theta = (\theta_1, \dots, \theta_{|\mathcal{X}|})$ be the parameter vector corresponding to the categorical distribution μ^1 . That is $\theta_i := \mu^1(a_i) = P[X = a_i]$ for all $i \in [|\mathcal{X}|]$. By definition, θ is an element of the $(|\mathcal{X}| - 1)$ dimensional simplex of all stochastic vectors of size $|\mathcal{X}|$. Denote $\Theta_{|\mathcal{X}|}$ as the $|\mathcal{X}|$ -ary probability simplex, i.e., $\Theta_{|\mathcal{X}|} := \left\{ \theta \in \mathbb{R}_{+*}^{|\mathcal{X}|} : \sum_{i \in [|\mathcal{X}|]} \theta_i = 1 \right\}$. We typically reserve upper case letters for random variables while lower case letters correspond to their realizations. For example, X^n denotes an n -string randomly drawn from μ while $x^n \in \mathcal{X}^n$ is a realization of the random n -string.

Note that as string lengths become large, the logarithm of the guesswork normalized by string length has been shown to satisfy a LDP for a more general set of sources [11]. While existing results on guesswork consider the ordering of strings from most likely to least likely, either unconditionally or conditionally (starting at [4]), or universal guessing orders [21], the more restrictive assumptions used here enable us to treat, for the first time, the reverse guesswork process. In reverse guessing, strings are ordered from least likely to most likely, breaking ties arbitrarily. At first glance, consideration of the worst possible strategy seems to be of limited value, but we will show that is not the case.

Forward guesswork provides good estimates of the likelihood of quickly discovered strings, but we shall demonstrate reverse guesswork provides better estimates on the likelihood that large numbers of guesses occur. We also establish an inherent geometrical correspondence between string-sources whose orders are reversed. Amongst other results, we prove that logarithm of reverse guesswork scaled by string length satisfies a LDP with a concave rate function. The concavity captures the fact that as one moves along the reverse order the rate of acquisition of probability increases initially. Due to that fact, the approach employed in [11], which leveraged earlier results on the scaling behavior of moments of guesswork, has no hope of success and we instead use distinct means.

Definition 1 (information): Let information $i_\mu^n : \mathcal{X}^n \rightarrow \mathbb{R}_{+*}$ be defined as:¹

$$i_\mu^n(x^n) := \log \frac{1}{\mu^n(x^n)}. \quad (1)$$

Note that throughout this paper we use $\log(\cdot)$ to denote the natural logarithm and hence information is measured in nats as defined above.

Definition 2 (Shannon entropy): Let $H^n(\mu)$ denote the entropy, which is defined as the expected information of a random n -string, and quantifies the average uncertainty that is revealed when a random n -string drawn from μ is observed:

$$H^n(\mu) := E_\mu \{i_\mu^n(X^n)\} = \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) i_\mu^n(x^n), \quad (2)$$

¹ $\mathbb{R}_{+*} := \{x \in \mathbb{R} | x > 0\}$.

where $E_{\mu}\{\cdot\}$ denotes the expectation operator with respect to the measure μ . The entropy rate, is denoted by $H(\mu)$ and is given by $H(\mu) := \lim_{n \rightarrow \infty} \frac{1}{n} H^n(\mu) = H^1(\mu)$.

Definition 3: For any $n \in \mathbb{N}$, we define $[n] := \{1, \dots, n\}$.

In what follows we put forth two assumptions on the string-source that enable us to prove that the logarithm of reverse guesswork satisfies a LDP. We will also later characterize the set of string-sources that satisfy the assumptions.

Assumption 1: We assume that $\mu^1(x) > 0$ for all $x \in \mathcal{X}$, i.e., $\theta_i > 0$ for all $i \in [|\mathcal{X}|]$.

Define

$$\underline{\varepsilon} := \min_{x \in \mathcal{X}} \mu^1(x), \quad (3)$$

$$\bar{\varepsilon} := \max_{x \in \mathcal{X}} \mu^1(x). \quad (4)$$

Assumption 1 excludes the boundaries of the probability simplex and ensures that the likelihood of the least likely n -string scales exponentially with n . In other words, for all $n \in \mathbb{N}$, and all $x^n \in \mathcal{X}^n$

$$\frac{1}{n} \log \frac{1}{\mu^n(x^n)} \leq \log \frac{1}{\underline{\varepsilon}} < \infty. \quad (5)$$

Assumption 2: We assume that $\arg \min_{x \in \mathcal{X}} \mu^1(x)$ and $\arg \max_{x \in \mathcal{X}} \mu^1(x)$ are unique.

Assumption 2 ensures that the most likely and the least likely words are unambiguously determined.

The probability simplex for a ternary alphabet, Θ_3 , is depicted in Fig. 1, where the green dashed and green solid lines represent the set of string-sources in Θ_3 that do not satisfy Assumption 2. Note that in this case, $(|\mathcal{X}| - 2) = 1$ and $\binom{|\mathcal{X}|}{2} = 3$ resulting in three 1-dimensional hyperplanes.

Definition 4 (set $\mathcal{M}_{\mathcal{X}}$ of string-sources): We denote by $\mathcal{M}_{\mathcal{X}}$, the set of all memoryless string-sources on alphabet \mathcal{X} that satisfy Assumptions 1 and 2.

In this paper, we focus our attention to string-sources in $\mathcal{M}_{\mathcal{X}}$.

Definition 5 (guesswork/optimal ordering for μ): A one-to-one function $G_{\mu}^n : \mathcal{X}^n \rightarrow [|\mathcal{X}|^n]$ is said to be the optimal ordering for μ (on n -strings) if

$$\mu^n(x^n) > \mu^n(y^n) \Rightarrow G_{\mu}^n(x^n) < G_{\mu}^n(y^n), \quad (6)$$

and further if $\mu^n(x^n) = \mu^n(y^n)$, then $G_{\mu}^n(x^n) < G_{\mu}^n(y^n)$ if and only if x^n appears prior to y^n in lexicographic ordering.

Definition 6 (reverse guesswork/reverse ordering for μ): We define $R_{\mu}^n(x^n)$ as the reverse guesswork, given by

$$R_{\mu}^n(x^n) := |\mathcal{X}|^n - G_{\mu}^n(x^n) \quad (7)$$

Note that as defined above, given μ , guesswork and reverse guesswork are unique functions. While guesswork corresponds to the best guessing strategy for recovering the string x^n , reverse guesswork corresponds to the worst guessing strategy for the string-source μ as it proceeds from the least likely string all the way to the most likely. Hence, the statistical performance of any other guessing strategy (ordering on n -strings) lies somewhere between that of guesswork and reverse guesswork. As will become clear later in the paper, our interest in reverse guesswork is mainly due to its usefulness in characterizing the PMF of guesswork.

Definition 7 (logarithm of forward/reverse guesswork): We define the logarithm of (forward) guesswork $g_{\mu}^n : \mathcal{X}^n \rightarrow [|\mathcal{X}|^n]$ and the logarithm of reverse guesswork $r_{\mu}^n : \mathcal{X}^n \rightarrow [|\mathcal{X}|^n]$ as

$$g_{\mu}^n(x^n) := \log G_{\mu}^n(x^n), \quad (8)$$

$$r_{\mu}^n(x^n) := \log R_{\mu}^n(x^n), \quad (9)$$

where G_{μ}^n and R_{μ}^n are guesswork and the reverse guesswork defined in (6) and (7), respectively.

Definition 8 (varentropy [30]): Let the varentropy, denoted by $V^n(\mu)$, be defined as

$$V^n(\mu) = \text{var}_{\mu} \{g_{\mu}^n(X^n)\} \quad (10)$$

where $\text{var}_{\mu}\{\cdot\}$ denotes the variance operator with respect to the measure μ . The varentropy rate is denoted by $V(\mu)$ and is given by

$$V(\mu) := \lim_{n \rightarrow \infty} \frac{1}{n} V^n(\mu) = V^1(\mu). \quad (11)$$

Definition 9 (relative entropy): Denote $D^n(\mu||\rho)$ as the relative entropy, also referred to as the Kullback-Leibler (KL) divergence, between the measures μ^n and ρ^n , given by

$$D^n(\mu||\rho) := \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) \log \left(\frac{\mu^n(x^n)}{\rho^n(x^n)} \right) = nD^1(\mu||\rho). \quad (12)$$

Definition 10 (cross entropy): Let the cross entropy, denoted by $H^n(\boldsymbol{\mu}||\boldsymbol{\rho})$, be defined as

$$H^n(\boldsymbol{\mu}||\boldsymbol{\rho}) := E_{\boldsymbol{\mu}} \left\{ \log \left(\frac{1}{\rho^n(X^n)} \right) \right\} \quad (13)$$

$$\begin{aligned} &= \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) \log \left(\frac{1}{\rho^n(x^n)} \right). \\ &= H^n(\boldsymbol{\mu}) + D^n(\boldsymbol{\mu}||\boldsymbol{\rho}) \\ &= nH^1(\boldsymbol{\mu}) + nD^1(\boldsymbol{\mu}||\boldsymbol{\rho}). \end{aligned} \quad (14)$$

Observe that $H^n(\boldsymbol{\mu}||\boldsymbol{\mu}) = H^n(\boldsymbol{\mu})$ recovers the Shannon entropy.

As a natural generalization of varentropy and cross entropy, we define cross varentropy in the following definition.

Definition 11 (cross varentropy): Let the cross varentropy, denoted by $V^n(\boldsymbol{\mu}||\boldsymbol{\rho})$, be defined as

$$\begin{aligned} V^n(\boldsymbol{\mu}||\boldsymbol{\rho}) &:= \text{var}_{\boldsymbol{\mu}} \left\{ \log \left(\frac{1}{\rho^n(X^n)} \right) \right\} \\ &= \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) \left[\log \left(\frac{1}{\rho^n(x^n)} \right) - H^n(\boldsymbol{\mu}||\boldsymbol{\rho}) \right]^2. \end{aligned} \quad (15)$$

Note that $V^n(\boldsymbol{\mu}||\boldsymbol{\mu}) = V^n(\boldsymbol{\mu})$ simplifies to the varentropy. Further note that $V^n(\boldsymbol{\mu}||\boldsymbol{\rho}) = nV^1(\boldsymbol{\mu}||\boldsymbol{\rho})$ because of our restriction to i.i.d. string-sources.

An operational interpretation of the cross entropy $H^n(\boldsymbol{\mu}||\boldsymbol{\rho})$ arises in prefix-free source coding, where it is known that, ignoring the integer constraints on the codeword length, the length of the codeword for the string x^n that minimizes the average codeword length equals $v_{\boldsymbol{\mu}}^n(x^n) = -\log \mu^n(x^n)$. In this case, the resulting average codeword length is given by

$$E_{\boldsymbol{\mu}} \{v_{\boldsymbol{\mu}}^n(X^n)\} = E_{\boldsymbol{\mu}} \left\{ \log \frac{1}{\mu^n(X^n)} \right\} = H^n(\boldsymbol{\mu}). \quad (16)$$

Therefore, if a source code is designed for the mismatched string-source $\boldsymbol{\rho}$, the length of the codeword for x^n would be chosen to be $v_{\boldsymbol{\rho}}^n(x^n)$. Hence, the average codeword length of the optimal prefix-free source code that is designed to minimize the average codeword length under the (mismatched) distribution $\boldsymbol{\rho}$ is equal to the cross entropy:

$$E_{\boldsymbol{\mu}} \{v_{\boldsymbol{\rho}}^n(X^n)\} = E_{\boldsymbol{\mu}} \left\{ \log \frac{1}{\rho^n(X^n)} \right\} = H^n(\boldsymbol{\mu}||\boldsymbol{\rho}). \quad (17)$$

Definition 12 (Rényi entropy): For any distribution μ^n , let the Rényi entropy of order α , denoted by $H_{\alpha}^n(\cdot)$, be defined as [31]

$$H_{\alpha}^n(\boldsymbol{\mu}) := \frac{1}{1-\alpha} \log \left(\sum_{x^n \in \mathcal{X}^n} [\mu^n(x^n)]^{\alpha} \right). \quad (18)$$

Further, define the Rényi entropy rate of order α (if it exists) as

$$H_{\alpha}(\boldsymbol{\mu}) := \lim_{n \rightarrow \infty} \frac{1}{n} H_{\alpha}^n(\boldsymbol{\mu}) = H_{\alpha}^1(\boldsymbol{\mu}). \quad (19)$$

Note that $\lim_{\alpha \rightarrow 1} H_{\alpha}(\boldsymbol{\mu}) = H(\boldsymbol{\mu})$, which recovers the Shannon entropy.

C. The tilt

The primary objective of this paper is to develop a tool, called the tilt, for the characterization of guesswork, its moments, and its large deviations behavior. The tilt operation T on any string-source $\boldsymbol{\mu}$ is formally defined below.

Definition 13 (tilted string-source of order α): Let the map T operate on a string-source $\boldsymbol{\mu}$ and a real-valued parameter $\alpha \in \mathbb{R}$ and output a string-source called “tilted $\boldsymbol{\mu}$ of order α ”, which is denoted by $T(\boldsymbol{\mu}, \alpha)$ and is defined as

$$T(\boldsymbol{\mu}, \alpha) := \{T(\mu^n, \alpha) : n \in \mathbb{N}\}, \quad (20)$$

where $T(\mu^n, \alpha)$ with overloading the notation for all $n \in \mathbb{N}$ and all $x^n \in \mathcal{X}^n$ is defined as

$$T(\mu^n, \alpha)(x^n) := \frac{[\mu^n(x^n)]^{\alpha}}{\sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^{\alpha}}. \quad (21)$$

Note that the tilt is a real analytic function of α in \mathbb{R} for all $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$ and all $n \in \mathbb{N}$, formally stated in Lemma 7. Tilted $\boldsymbol{\mu}$ of order 1 is the string-source $\boldsymbol{\mu}$ itself, i.e., $T(\boldsymbol{\mu}, 1) = \boldsymbol{\mu}$. Further, for any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, $T(\boldsymbol{\mu}, 0) = \mathbf{u}_{\mathcal{X}}$, where $\mathbf{u}_{\mathcal{X}}$ is defined as the uniform string-source on alphabet \mathcal{X} such that for all $x^n \in \mathcal{X}^n$

$$u_{\mathcal{X}}^n(x^n) := \frac{1}{|\mathcal{X}|^n}. \quad (22)$$

Notice that by definition $\mathbf{u}_{\mathcal{X}} \notin \mathcal{M}_{\mathcal{X}}$.

Observe that for all $n \in \mathbb{N}$, $T(\mu^n, \alpha)$ is a multinomial distribution with the corresponding categorical distribution given by $\tau(\theta, \alpha) = (\tau_1(\theta, \alpha), \dots, \tau_{|\mathcal{X}|}(\theta, \alpha))$, where $\tau_i : \Theta_{|\mathcal{X}|} \times \mathbb{R} \rightarrow \Theta_{|\mathcal{X}|}$ for all $i \in [|\mathcal{X}|]$ is given by

$$\tau_i(\theta, \alpha) := \frac{\theta_i^\alpha}{\sum_{i=1}^{|\mathcal{X}|} \theta_i^\alpha}. \quad (23)$$

Let $\Gamma_\theta^+ \in \Theta_{|\mathcal{X}|}$ denote the ‘‘tilted family of θ ’’ and be given by

$$\Gamma_\theta^+ := \{\tau(\theta, \alpha) : \alpha \in \mathbb{R}_{+*}\}. \quad (24)$$

Observe that $\Gamma_\theta^+ \in \Theta_{|\mathcal{X}|}$ is a set of stochastic vectors in the probability simplex. Thus, the tilted family of a memoryless string-source with parameter vector θ is comprised of a set of memoryless string-sources whose parameter vectors belong to the tilted family of the vector θ , i.e., Γ_θ^+ .

Definition 14 (reversed string-source): We define the reverse of the string-source μ (also called μ -reverse), denoted by $T(\mu, -1)$.

Note that the guesswork corresponding to μ -reverse is exactly the reverse guesswork. As an example, the reverse of a binary memoryless string-source with parameter vector $\theta = (p, 1-p)$ is a binary memoryless string-source with $\tau(\theta, -1) = (1-p, p)$. Observe that R_μ^n is the optimal ordering (guesswork) for the reverse string source $T(\mu, -1)$. Further, G_μ^n is the reverse ordering for $T(\mu, -1)$.

Definition 15 (tilted/reverse family of a string-source): Let the set \mathcal{T}_μ^+ denote the tilted family of the string-source μ , and be given by

$$\mathcal{T}_\mu^+ := \{T(\mu, \alpha) : \alpha \in \mathbb{R}_{+*}\}. \quad (25)$$

Further, define the reverse family of the string-source as

$$\mathcal{T}_\mu^- := \{T(\mu, \alpha) : \alpha \in \mathbb{R}_{-*}\}. \quad (26)$$

The first notable property of the tilted family of μ is that it parametrizes a standard exponential family of string-sources with α . In other words, for any $n \in \mathbb{N}$, the family of distributions $\{T(\mu^n, \alpha) : \alpha \in \mathbb{R}\}$ parametrized by α characterizes an exponential family of distributions on \mathcal{X}^n .

As a working example throughout the paper, we consider a memoryless string-source on a ternary alphabet ($|\mathcal{X}| = 3$) with the parameter vector $\theta = (0.2, 0.3, 0.5)$. The ternary alphabet is general enough to encompass the difficulties of the problem while simple enough for us to demonstrate the geometric techniques developed in this paper. The ternary probability simplex is depicted in Fig. 1, where the tilted family Γ_θ^+ is plotted for $\theta = (0.2, 0.3, 0.5)$. As can be seen, the tilted family of θ is a parametric curve that is contained within the 2-dimensional simplex of stochastic vectors. The curve starts arbitrarily close to the maximum entropy uniform parameter vector θ^0 (for $\alpha = 0^+$) and then moves towards one of the zero-entropy corner points of the simplex corresponding to the most likely symbol as $\alpha \rightarrow \infty$. We shall show that these properties hold generally for all string-sources in $\mathcal{M}_{\mathcal{X}}$.

As a final note, the tilt is intimately related to the concept of information geometry (see [32]), where several geometric properties of the Kullback-Leibler divergence (relative entropy) have been studied and their relevance to problems in information theory have been investigated. In particular, Borade and Zheng applied concepts from information geometry to the analysis of error exponents [33]; and Huang *et al.* performed a geometric study of hypothesis testing [34]. This work also builds upon the insights on the geometry of the probability simplex in the context of information theory and statistics pioneered by Barron, Clarke, and Cover [35], [36]. The preliminary version of this work relied on the method of types (see [1]) while in this paper we build on a generalized notion of the weakly typical set, called the tilted weakly typical sets. We believe that the current treatment may be generalized to a class of stationary ergodic string-sources as discussed in the concluding remarks.

D. Organization and contribution

In Section II, we provide the main properties of the tilt operation. In particular, we characterize the entropy $H^n(T(\mu, \alpha))$, the cross entropy $H^n(T(\mu, \alpha) || \mu)$, the relative entropy $D^n(T(\mu, \alpha) || \mu)$ of the tilted string-source as well as the Rényi entropy $H_\alpha^n(\mu)$. These quantities are used in Section V to implicitly characterize the large deviations rate function of the logarithm of reverse guesswork, the logarithm of (forward) guesswork, and information. We further show that the derivatives (with respect to the parameter α) of these quantities can be expressed in terms of the varentropy $V^n(T(\mu, \alpha))$ and the cross varentropy $V^n(T(\mu, \alpha) || \mu)$ of the tilted string-source.

In Section III, we define the equivalent order class of a string-source as the set of all string-sources that result in the same guesswork for all n , and denote this set of string-sources by \mathcal{C}_μ . In Theorem 1, we show that the equivalent order class of μ is equal to the tilted family, i.e., $\mathcal{C}_\mu = \mathcal{T}_\mu^+$, providing an operational meaning to the tilted family. Further, the set of all string-sources whose optimal orderings are inverse for μ is equal to \mathcal{T}_μ^- , i.e., $\mathcal{C}_{T(\mu, -1)} = \mathcal{T}_\mu^-$. This result draws an important

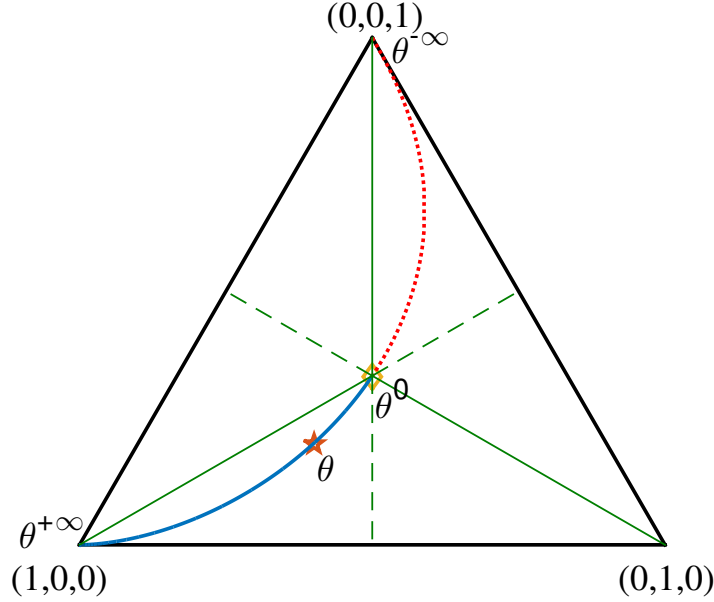


Fig. 1: The solid black lines depict the boundaries of the probability simplex Θ_3 of all ternary stochastic vectors, which are excluded from our analysis as they do not satisfy Assumption 1. The dashed green lines represent the string-sources that do not satisfy (28) in Assumption 2; and the solid green lines represent the string-sources that do not satisfy (29) in Assumption 2. The red pentagon marker is the ternary source parameter vector $\theta = (0.2, 0.3, 0.5)$; the blue solid curve depicts Γ_θ^+ , i.e., the tilted family of θ ; the red dotted curve depicts Γ_θ^- , i.e., the reverse family of θ ; the yellow diamond marker corresponds to the uniform parameter vector $\theta^0 = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$; and $\theta^\infty = (1, 0, 0)$ and $\theta^{-\infty} = (0, 0, 1)$. Note that θ^∞ and $\theta^{-\infty}$ are only achieved in the limit and do not belong to either Γ_θ^+ or Γ_θ^- .

distinction between information and guesswork. The string-source μ is uniquely determined if information $i_\mu^n(x^n)$ is provided for all $x^n \in \mathcal{X}^n$. On the other hand, it is not possible to recover uniquely the string-source μ if one is provided with the guesswork $G_\mu^n(x^n)$ for all strings $x^n \in \mathcal{X}^n$. Our result shows that one can only determine the string-source up to equivalence within the tilted family that the source belongs to given the guesswork for all $x^n \in \mathcal{X}^n$ leading to one less degree of freedom. This result has implications in terms of universal source coding [22], [29] and universal guesswork [9], [21], where the degree of freedom in the model class determines the penalty of universality, which is called redundancy in source coding.

In Section IV, we generalize the notion of the weakly typical set. The weakly typical set comprises of all strings $x^n \in \mathcal{X}^n$ such that $e^{-H^n(\mu) - n\epsilon} < \mu^n(x^n) < e^{-H^n(\mu) + n\epsilon}$. An important implication of the weakly typical set (known as the asymptotic equipartition property) is that the typical set roughly contains $\approx e^{H^n(\mu)}$ strings each of probability $\approx e^{-H^n(\mu)}$. For sufficiently large n , the probability of the typical set is close to one, i.e., if a string is randomly drawn from the source it is in the weakly typical set with high probability. The weakly typical set is used to prove key results in information theory that are dominated by the typical events, such as the source coding theorem, and the channel coding theorem. Despite the great intuition that typicality provides on such quantities, the arguments based on typicality fall short in providing intuition on other key quantities that are dominated by atypical events, such as the error exponents in decoding, and the cut-off rate in sequential decoding. In Section IV, we consider all strings $x^n \in \mathcal{X}^n$ such that $e^{-H^n(T(\mu, \alpha) || \mu) - n\epsilon} < \mu^n(x^n) < e^{-H^n(T(\mu, \alpha) || \mu) + n\epsilon}$ for $\alpha \in \mathbb{R}$, which we define as the tilted weakly typical set of order α and denote by $\mathcal{A}_{\mu, \alpha, \epsilon}^n$ (see Definition 18). We show that for a fixed ϵ , for any string $x^n \in \mathcal{X}^n$, there exists an α such that x^n is contained in the tilted weakly typical set of order α . Hence, this notion could be used to cluster/partition all of the strings $x^n \in \mathcal{X}^n$ based on their likelihoods. In Theorem 2, we derive tight bounds on the probability, size, guesswork, and reverse guesswork for all elements of the tilted weakly typical set of any order α . Roughly speaking, for any $\alpha \in \mathbb{R}_{+,*}$, we show that $\mathcal{A}_{\mu, \alpha, \epsilon}^n$ contains $\approx e^{H^n(T(\mu, \alpha) || \mu)}$ strings where the likelihood of each string is $\approx e^{-H^n(T(\mu, \alpha) || \mu)}$, and the probability of the entire set is $\approx e^{-D^n(T(\mu, \alpha) || \mu)}$, and the guesswork for each element in the set is $\approx e^{H^n(T(\mu, \alpha) || \mu)}$. For any $\alpha \in \mathbb{R}_{-,*}$, we show that $\mathcal{A}_{\mu, \alpha, \epsilon}^n$ contains $\approx e^{H^n(T(\mu, \alpha) || \mu)}$ strings where the likelihood of each string is $\approx e^{-H^n(T(\mu, \alpha) || \mu)}$, and the probability of the entire set is $\approx e^{-D^n(T(\mu, \alpha) || \mu)}$, and the “reverse” guesswork for each element in the set is $\approx e^{H^n(T(\mu, \alpha) || \mu)}$. Note that $\alpha = 1$ recovers the weakly typical set as $H^n(T(\mu, 1) || \mu) = H^n(T(\mu, 1)) = H^n(\mu)$, and for $\alpha \neq 1$, this provides a generalization of the well-known weakly typical set. This generalization could be used to provide new insights on understanding and proving results on information theoretic quantities that are dominated by atypical events.

In Section V, we prove that the logarithm of reverse guesswork $r_\mu^n(x^n)$, the logarithm of (forward) guesswork $g_\mu^n(x^n)$, and information $i_\mu^n(x^n)$ satisfy a LDP and provide an implicit formula for the rate function in each case based on entropy, cross entropy, and relative entropy. Although some of the results in this section have been previously proved in more generality,

we believe that the machinery built upon the tilt operation in this paper as well as the information theoretic characterization of the rate functions provide useful intuition in characterizing the large deviations behavior of these quantities. In particular, the LDP for the logarithm of reverse guesswork could not have been established using the previous methods by Christiansen and Duffy [11], as the resulting rate function here is concave. The most common way to prove a LDP is the Gärtner-Ellis Theorem [37, Theorem 2.3.6]. There, one first determines the scaled cumulant generating function of the process of interest, which identifies how moments scale, and then leverages properties of it to establish the LDP. This approach can only work if the resulting rate function is convex. Here, that is not the case.

In Section VI, we provide an approximation on the distribution of guesswork that captures the behavior even for small string lengths. The approximation is built based on the tilt operation, guesswork, and reverse guesswork. We empirically show that the approximation can be applied to a variety of string-sources to characterize the PMF of guesswork.

Finally, the conclusion is provided in Section VII, where we also present ideas on how to generalize these results beyond the setting considered in this paper.

II. PROPERTIES OF THE TILTED STRING-SOURCES

In this section, we provide the main properties of the tilt operation that shall be used in proving our results on the characterization of guesswork. This section may be skipped by the reader and only referred to whenever a particular lemma is needed.

Lemma 1: For any $\alpha, \beta \in \mathbb{R}$,

$$T(T(\boldsymbol{\mu}, \alpha), \beta) = T(T(\boldsymbol{\mu}, \beta), \alpha) = T(\boldsymbol{\mu}, \alpha\beta). \quad (27)$$

Proof: This is obtained from the definition using algebraic manipulation. ■

Lemma 2: The optimal ordering for $\boldsymbol{\mu}$ is the reverse ordering for $T(\boldsymbol{\mu}, -1)$ and the reverse ordering for $\boldsymbol{\mu}$ is the optimal ordering for $T(\boldsymbol{\mu}, -1)$.

Proof: The statement is a consequence of the definition. ■

Lemma 3: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$,

$$\lim_{\alpha \rightarrow \infty} H(T(\boldsymbol{\mu}, \alpha)) = 0, \quad (28)$$

$$\lim_{\alpha \rightarrow -\infty} H(T(\boldsymbol{\mu}, \alpha)) = 0. \quad (29)$$

Proof: The Lemma is a direct consequence of Assumption 2. ■

Next, we provide a lemma that relates Rényi entropy, Shannon entropy, relative entropy, and cross entropy.

Lemma 4: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, and any $\alpha \in \mathbb{R}$, the following relations hold:

$$H^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) - H_\alpha^n(\boldsymbol{\mu}) = \frac{1}{1-\alpha} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (30)$$

$$H^n(T(\boldsymbol{\mu}, \alpha)) - H_\alpha^n(\boldsymbol{\mu}) = \frac{\alpha}{1-\alpha} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (31)$$

where $\frac{1}{1-\alpha} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \Big|_{\alpha=1} := 0$.

Proof: To establish (30),

$$\begin{aligned} & H^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) - H_\alpha^n(\boldsymbol{\mu}) - \frac{1}{1-\alpha} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \\ &= \sum_{x^n \in \mathcal{X}^n} T(\boldsymbol{\mu}^n, \alpha)(x^n) \log \frac{1}{\mu^n(x^n)} \end{aligned} \quad (32)$$

$$- \frac{1}{1-\alpha} \sum_{x^n \in \mathcal{X}^n} [\mu^n(x^n)]^\alpha \quad (33)$$

$$- \frac{1}{1-\alpha} \sum_{x^n \in \mathcal{X}^n} T(\boldsymbol{\mu}^n, \alpha)(x^n) \log \left(\frac{[\mu^n(x^n)]^\alpha / \sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha}{\mu^n(x^n)} \right) \quad (34)$$

$$= 0, \quad (35)$$

where (34) follows from the definition, and (35) holds because the term $\sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha$ in (34) is a constant, and hence (34) could be decomposed into two terms one of which cancels the right hand side of (32), and the other cancels (33). Finally, (31) is established by putting together (14) and (30). ■

Lemma 5: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, and any $\alpha \in \mathbb{R}$, the following holds:

$$\begin{aligned} & \log \frac{1}{T(\mu^n, \alpha)(x^n)} - H^n(T(\mu, \alpha)) \\ &= \alpha \left(\log \frac{1}{\mu^n(x^n)} - H^n(T(\mu, \alpha) \parallel \mu) \right). \end{aligned} \quad (36)$$

Proof: The lemma is proved by considering the following chain of equations:

$$\begin{aligned} & \log \frac{1}{T(\mu^n, \alpha)(x^n)} - H^n(T(\mu, \alpha)) \\ &= \alpha \log \frac{1}{\mu^n(x^n)} + \log \left(\sum_{x^n \in \mathcal{X}^n} [\mu^n(x^n)]^\alpha \right) \\ & \quad - \sum_{x^n \in \mathcal{X}^n} T(\mu^n, \alpha)(x^n) \left(\alpha \log \frac{1}{\mu^n(x^n)} + \log \left(\sum_{x^n \in \mathcal{X}^n} [\mu^n(x^n)]^\alpha \right) \right) \\ &= \alpha \left(\log \frac{1}{\mu^n(x^n)} - H^n(T(\mu, \alpha) \parallel \mu) \right). \end{aligned}$$

Lemma 6: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, and any $\alpha \in \mathbb{R}$, the following holds:

$$\alpha^2 V^n(T(\mu, \alpha) \parallel \mu) = V^n(T(\mu, \alpha)). \quad (37)$$

Proof: We have

$$\begin{aligned} & \alpha^2 V^n(T(\mu, \alpha) \parallel \mu) \\ &= \sum_{x^n \in \mathcal{X}^n} T(\mu^n, \alpha)(x^n) \left[\alpha \left(\log \left(\frac{1}{\mu^n(x^n)} \right) - H^n(T(\mu, \alpha) \parallel \mu) \right) \right]^2 \\ &= \sum_{x^n \in \mathcal{X}^n} T(\mu^n, \alpha)(x^n) \left[\log \frac{1}{T(\mu^n, \alpha)(x^n)} - H^n(T(\mu, \alpha)) \right]^2 \\ &= V^n(T(\mu, \alpha)), \end{aligned} \quad (38)$$

where (38) follows from Lemma 5. ■

Lemma 7: For any string-source $\mu \in \mathcal{M}_{\mathcal{X}}$, for any $n \in \mathbb{N}$, $T(\mu^n, \alpha)$ is a real analytic function of $\alpha \in \mathbb{R}$. In particular, $\frac{d}{d\alpha} T(\mu^n, \alpha)$ exists; and $\lim_{\alpha \rightarrow 0} T(\mu^n, \alpha) = u_{\mathcal{X}^n}^n$, where $u_{\mathcal{X}^n}^n$ is the uniform distribution on \mathcal{X}^n .

Proof: The statement follows from the facts that the exponential function is real analytic in its argument and that the denominator in (21) in the definition of the tilt is non-zero for all $\alpha \in \mathbb{R}$. The limit as $\alpha \rightarrow 0$ holds since $\mu^n(x^n) > 0$ for all $x^n \in \mathcal{X}^n$ by Assumption 1. ■

Lemma 8: For any string-source $\mu \in \mathcal{M}_{\mathcal{X}}$, for any $n \in \mathbb{N}$, $H^n(T(\mu, \alpha))$, $D^n(T(\mu, \alpha) \parallel \mu)$, $H^n(T(\mu, \alpha) \parallel \mu)$, $V^n(T(\mu, \alpha))$, and $V^n(T(\mu, \alpha) \parallel \mu)$ are continuous and differentiable functions of $\alpha \in \mathbb{R}$.

Proof: Note that $H^n(\rho)$, $D^n(\rho \parallel \mu)$, $H^n(\rho \parallel \mu)$, $V^n(\rho)$, and $V^n(\rho \parallel \mu)$ are continuously differentiable with respect to $\rho \in \mathcal{M}_{\mathcal{X}}$, and by Lemma 7, $T(\mu, \alpha)$ is also continuous and differentiable with respect to $\alpha \in \mathbb{R}$, and hence the overall composition by considering $\rho = T(\mu, \alpha)$ is continuous and differentiable with respect to $\alpha \in \mathbb{R}$. ■

Lemma 9: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, and any $n \in \mathbb{N}$, and any $\alpha \in \mathbb{R}$:

$$\begin{aligned} & \frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \\ &= T(\mu^n, \alpha)(x^n) \left(H^n(T(\mu, \alpha) \parallel \mu) - \log \frac{1}{\mu^n(x^n)} \right). \end{aligned} \quad (39)$$

Proof: Let

$$T'(\mu^n, \alpha_0)(x^n) := \left. \frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \right|_{\alpha=\alpha_0}.$$

Note that by Lemma 1, we know that for any $\beta > 0$:

$$T(\mu^n, \alpha)(x^n) = T \left(T(\mu^n, \beta), \frac{\alpha}{\beta} \right) (x^n).$$

Differentiating both sides with respect to α , for all $\alpha_0, \beta > 0$ we have

$$\begin{aligned}
\left. \frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \right|_{\alpha=\alpha_0} &= T'(\mu^n, \alpha_0)(x^n) \\
&= \left. \frac{d}{d\alpha} T\left(T(\mu^n, \beta), \frac{\alpha}{\beta}\right)(x^n) \right|_{\alpha=\alpha_0} \\
&= \frac{1}{\beta} T' \left(T(\mu^n, \beta), \frac{\alpha_0}{\beta} \right) (x^n) \\
&= \frac{1}{\alpha_0} T' (T(\mu^n, \alpha_0), 1) (x^n),
\end{aligned} \tag{40}$$

where (40) follows by setting $\beta = \alpha_0$. In other words, (40) implies that the derivative of a tilt with respect to α can be derived by taking the derivative at $\alpha = 1$ and rescaling the derivative evaluated at the tilted distribution. Consequently, to prove the lemma it suffices to prove that

$$\left. \frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \right|_{\alpha=1} = \mu^n(x^n) \left(H^n(\boldsymbol{\mu}) - \log \frac{1}{\mu^n(x^n)} \right), \tag{41}$$

and then it follows from (40) that for any $\alpha \neq 0$, we will arrive at the following:

$$\begin{aligned}
\frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \\
= \frac{1}{\alpha} T(\mu^n, \alpha)(x^n) \left(H^n(T(\boldsymbol{\mu}, \alpha)) - \log \frac{1}{T(\mu^n, \alpha)(x^n)} \right).
\end{aligned}$$

On the other hand, the desired result is obtained by considering Lemma 5, and noting the continuity and differentiability of $T(\mu^n, \alpha)$ at 0 from Lemma 7 and that of $H(T(\mu^n, \alpha))$ at 0 from Lemma 8.

To establish (41), note the definition of the tilt in (21) and the fact that the derivative of the numerator with respect to α is $[\mu^n(x^n)]^\alpha \log \mu^n(x^n)$ and the derivative of the denominator with respect to α is $-H^n(\boldsymbol{\mu})$. ■

Lemma 10: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, we have

$$\lim_{\alpha \rightarrow 0} \frac{1}{\alpha^2} V^n(T(\boldsymbol{\mu}, \alpha)) = V^n(\mathbf{u}_{\mathcal{X}} || \boldsymbol{\mu}). \tag{42}$$

Proof: Observe that

$$\begin{aligned}
\lim_{\alpha \rightarrow 0} \frac{1}{\alpha^2} V^n(T(\boldsymbol{\mu}, \alpha)) &= \lim_{\alpha \rightarrow 0} V^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \\
&= V^n(\mathbf{u}_{\mathcal{X}} || \boldsymbol{\mu}),
\end{aligned} \tag{43}$$

where (43) follows from Lemma 6, completing the proof. ■

Lemma 11: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, and any $\alpha \in \mathbb{R}$,

$$\frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha)) = -\alpha V^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}). \tag{44}$$

Proof: First, owing to Lemma 8, the derivative of $H^n(T(\mu^n, \alpha))$ with respect to α exists.

To prove the result for all $\alpha \neq 0$, it suffices to show that

$$\left. \frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha)) \right|_{\alpha=1} = -V^n(\boldsymbol{\mu}) \tag{45}$$

for any given $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$. Then, by Lemma 1, $T(\cdot, \alpha + d\alpha) = T(T(\cdot, 1 + d\alpha/\alpha), \alpha)$ which for $\alpha \neq 0$ leads to (see (40) in the proof of Lemma 9 for a more formal statement of this part of the claim):

$$\frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha)) = -\frac{1}{\alpha} V^n(T(\boldsymbol{\mu}, \alpha)).$$

This, in conjunction with Lemma 6 and continuity and differentiability of $H^n(T(\boldsymbol{\mu}, \alpha))$ with respect to all $\alpha \in \mathbb{R}$ from Lemma 8 leads to the desired result.

To show that (45) holds, we have

$$\begin{aligned}
& \left. \frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha)) \right|_{\alpha=1} \\
&= \sum_{x^n \in \mathcal{X}^n} \left. \frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \right|_{\alpha=1} \log \frac{1}{\mu^n(x^n)} \\
&\quad + \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) \left. \frac{d}{d\alpha} \log \frac{1}{T(\mu^n, \alpha)(x^n)} \right|_{\alpha=1} \\
&= \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) \left(H^n(\boldsymbol{\mu}) - \log \frac{1}{\mu^n(x^n)} \right) \log \frac{1}{\mu^n(x^n)} \\
&\quad + \sum_{x^n \in \mathcal{X}^n} \mu^n(x^n) \left(\log \frac{1}{\mu^n(x^n)} - H^n(\boldsymbol{\mu}) \right) \tag{46}
\end{aligned}$$

$$\begin{aligned}
&= E_{\boldsymbol{\mu}} \left\{ \left(H^n(\boldsymbol{\mu}) - \log \frac{1}{\mu^n(X^n)} \right) \log \frac{1}{\mu^n(X^n)} \right\} \\
&= -\text{var}_{\boldsymbol{\mu}} \{ \log \frac{1}{\mu^n(X^n)} \} = -V^n(\boldsymbol{\mu}), \tag{47}
\end{aligned}$$

where (46) follows from Lemma 9, and (47) follows from the definition of the varentropy in (10). The limit as $\alpha \rightarrow 0$ also follow from Lemma 10. \blacksquare

Lemma 12: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$ and any $\alpha \in \mathbb{R}$,

$$\frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) = -V^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}). \tag{48}$$

Proof: We have

$$\begin{aligned}
& \frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) \\
&= \sum_{x^n \in \mathcal{X}^n} \frac{d}{d\alpha} T(\mu^n, \alpha)(x^n) \log \frac{1}{\mu^n(x^n)} \\
&= \sum_{x^n \in \mathcal{X}^n} T(\mu^n, \alpha)(x^n) \left(H^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) - \log \frac{1}{\mu^n(x^n)} \right) \log \frac{1}{\mu^n(x^n)} \tag{49} \\
&= E_{T(\boldsymbol{\mu}, \alpha)} \left\{ \left(H^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) - \log \frac{1}{\mu^n(X^n)} \right) \log \frac{1}{\mu^n(X^n)} \right\} \\
&= -\text{var}_{T(\boldsymbol{\mu}, \alpha)} \{ \log \frac{1}{\mu^n(X^n)} \} \\
&= -V^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}), \tag{50}
\end{aligned}$$

where (49) follows from Lemma 9, and (50) follows from the definition of information in (1) and cross entropy in (13) leading to the fact that

$$E_{T(\boldsymbol{\mu}, \alpha)} \left\{ \log \frac{1}{\mu^n(X^n)} \right\} = H^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}). \tag{51}$$

Lemma 13: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$ and any $\alpha \in \mathbb{R}$,

$$\frac{d}{d\alpha} D^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) = (\alpha - 1) V^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}). \tag{52}$$

Proof: Note that from (14),

$$D^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) = H^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}) - H^n(T(\boldsymbol{\mu}, \alpha)).$$

The lemma then follows by differentiating both sides with respect to α and applying Lemmas 11 and 12 on the right hand side. \blacksquare

Lemma 14: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$ and any $\alpha \neq 1$,

$$\frac{d}{d\alpha} H_{\alpha}^n(\boldsymbol{\mu}) = -\frac{1}{(1-\alpha)^2} D^n(T(\boldsymbol{\mu}, \alpha) \| \boldsymbol{\mu}), \tag{53}$$

and

$$\left. \frac{d}{d\alpha} H_{\alpha}^n(\boldsymbol{\mu}) \right|_{\alpha=1} = -\frac{1}{2} V^n(\boldsymbol{\mu}). \tag{54}$$

Proof: To establish (53), consider:

$$\frac{d}{d\alpha} H_\alpha^n(\boldsymbol{\mu}) = \frac{d}{d\alpha} H^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) - \frac{d}{d\alpha} \left(\frac{1}{1-\alpha} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \right) \quad (55)$$

$$\begin{aligned} &= -\frac{1}{\alpha^2} V^n(T(\boldsymbol{\mu}, \alpha)) + \frac{1}{\alpha^2} V^n(T(\boldsymbol{\mu}, \alpha)) \\ &\quad - \frac{1}{(1-\alpha)^2} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \\ &= -\frac{1}{(1-\alpha)^2} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \end{aligned} \quad (56)$$

where (55) follows by invoking (30) in Lemma 4, and (56) follows from the chain rule of derivatives.

To establish (54), we have

$$\left. \frac{d}{d\alpha} H_\alpha^n(\boldsymbol{\mu}) \right|_{\alpha=1} = \lim_{\alpha \rightarrow 1} \frac{d}{d\alpha} H_\alpha^n(\boldsymbol{\mu}) \quad (57)$$

$$= \lim_{\alpha \rightarrow 1} \frac{-D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu})}{(1-\alpha)^2} \quad (58)$$

$$= \lim_{\alpha \rightarrow 1} -\frac{\frac{\alpha-1}{\alpha^2} V^n(T(\boldsymbol{\mu}, \alpha))}{2(\alpha-1)} \quad (59)$$

$$= -\frac{1}{2} V^n(\boldsymbol{\mu}),$$

where (57) follows from the continuity of the derivative of $H_\alpha^n(\boldsymbol{\mu})$ with respect to α , (58) follows from (53), and (59) follows from L'Hôpital's rule and Lemma 13. \blacksquare

This result recovers the fact that Rényi entropies are monotonically decreasing with respect to the order, and further characterizes their rate of change with respect to the parameterization.

Lemma 15: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$,

$$\lim_{n \rightarrow \infty} \frac{1}{n} V^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) = V(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}). \quad (60)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} H^n(T(\boldsymbol{\mu}, \alpha)) = H(T(\boldsymbol{\mu}, \alpha)), \quad (61)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} H^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) = H(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (62)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} D^n(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) = D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (63)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} H_\alpha^n(\boldsymbol{\mu}) = H_\alpha(\boldsymbol{\mu}), \quad (64)$$

Further, for all $\alpha \in \mathbb{R}$,

$$\frac{d}{d\alpha} H(T(\boldsymbol{\mu}, \alpha)) = -\alpha V(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (65)$$

$$\frac{d}{d\alpha} H(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) = -V(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (66)$$

$$\frac{d}{d\alpha} D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) = (\alpha - 1) V(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}). \quad (67)$$

$$\frac{d}{d\alpha} H_\alpha(\boldsymbol{\mu}) = -\frac{1}{(1-\alpha)^2} D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}), \quad (68)$$

where $D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu})$ is differentiable with respect to α , and $\left. \frac{1}{(1-\alpha)^2} D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \right|_{\alpha=1} := \frac{1}{2} V(\boldsymbol{\mu})$.

Proof: The first part of the claim is straightforward as the equalities hold for all n and hence also hold in the limit as $n \rightarrow \infty$. The claim in (65) hence follows by invoking Lemma 11. Equations (66) and (67) and (68) are established similarly considering Lemmas 12, 13, and 14, respectively. \blacksquare

Lemma 16: If $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, then, for all $\alpha \neq 0$, we have $T(\boldsymbol{\mu}, \alpha) \in \mathcal{M}_{\mathcal{X}}$. In other words, $\mathcal{M}_{\mathcal{X}}$ is closed under all non-zero tilts, and hence $\mathcal{T}_{\boldsymbol{\mu}}^+, \mathcal{T}_{\boldsymbol{\mu}}^- \subseteq \mathcal{M}_{\mathcal{X}}$.

Proof: We need to show that $T(\boldsymbol{\mu}, \alpha)$ satisfies Assumptions 1 and 2.

To check Assumption 1, for $\alpha \in \mathbb{R}_{+*}$, we have:

$$\begin{aligned} \frac{1}{n} \log \frac{1}{T(\mu^n, \alpha)(x^n)} &= \frac{1}{n} \log \frac{\sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha}{[\mu^n(x^n)]^\alpha} \\ &= \frac{1}{n} \left[\log \sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha + \log \frac{1}{[\mu^n(x^n)]^\alpha} \right]. \end{aligned} \quad (69)$$

Further, considering $\alpha \geq 1$,

$$-\alpha \log |\mathcal{X}| \leq (1 - \alpha) \log |\mathcal{X}| \leq \frac{1}{n} \log \sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha \leq 0, \quad (70)$$

and for all $0 < \alpha \leq 1$,

$$0 \leq \frac{1}{n} \log \sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha \leq (1 - \alpha) \log |\mathcal{X}| \leq \log |\mathcal{X}|. \quad (71)$$

Thus, for all $\alpha \in \mathbb{R}_{+*}$, by taking the maximum of the upper bounds and the minimum of the lower bounds in (70) and (71), and applying them to (69), we have

$$-\alpha \log |\mathcal{X}| + \alpha \log \frac{1}{\underline{\varepsilon}} \leq \frac{1}{n} \log \frac{1}{T(\mu^n, \alpha)(x^n)} \leq \log |\mathcal{X}| + \alpha \log \frac{1}{\underline{\varepsilon}},$$

where $\underline{\varepsilon}$ and $\bar{\varepsilon}$ are defined in (3) and (4), respectively. On the other hand, for all $\alpha \in \mathbb{R}_{-*}$, we have

$$\begin{aligned} \frac{1}{n} \log \frac{1}{T(\mu^n, \alpha)(x^n)} &= \frac{1}{n} \left[\log \sum_{y^n \in \mathcal{X}^n} [\mu^n(y^n)]^\alpha + \log \frac{1}{[\mu^n(x^n)]^\alpha} \right] \\ &\leq \frac{1}{n} \log \sum_{y^n \in \mathcal{X}^n} \underline{\varepsilon}^{n\alpha} \\ &= \log |\mathcal{X}| - \alpha \log \frac{1}{\underline{\varepsilon}}. \end{aligned}$$

Thus, for all $\alpha \in \mathbb{R}$, we have

$$\frac{1}{n} \log \frac{1}{T(\mu^n, \alpha)(x^n)} \leq \log |\mathcal{X}| + |\alpha| \log \frac{1}{\underline{\varepsilon}} < \infty. \quad (72)$$

Next, we need to show that for all $\alpha \neq 0$,

$$H(T(\mu, \alpha)) > 0.$$

Due to Lemma 15, $H(T(\mu, \alpha))$ is differentiable with respect to α and its derivative is given by $\alpha V(T(\mu, \alpha) \| \mu)$. On the other hand, for $\alpha > 0$, the derivative is strictly positive implying that $H(T(\mu, \alpha))$ is strictly decreasing with respect to α , and hence it is non-zero for all $\alpha > 0$. This together with (72) demonstrate that for all $\alpha \in \mathbb{R}$, $T(\mu, \alpha)$ satisfies Assumption 1.

To show that Assumption 2 holds for the tilted source, we note that for any $\alpha > 0$, we have

$$\begin{aligned} \arg \min_{x \in \mathcal{X}} T(\mu^1, \alpha)(x) &= \arg \min_{x \in \mathcal{X}} \left\{ \frac{(\mu^1(x))^\alpha}{\sum_{y \in \mathcal{X}} (\mu^1(y))^\alpha} \right\} \\ &= \arg \min_{x \in \mathcal{X}} (\mu^1(x))^\alpha \\ &= \arg \min_{x \in \mathcal{X}} \mu^1(x), \end{aligned}$$

which is unique by the fact that μ satisfies Assumption 2. Similarly, we can argue that $\arg \max_{x \in \mathcal{X}} T(\mu^1, \alpha)(x)$ is also unique. On the other hand, for $\alpha < 0$, we have

$$\begin{aligned} \arg \min_{x \in \mathcal{X}} T(\mu^1, \alpha)(x) &= \arg \min_{x \in \mathcal{X}} \left\{ \frac{(\mu^1(x))^\alpha}{\sum_{y \in \mathcal{X}} (\mu^1(y))^\alpha} \right\} \\ &= \arg \min_{x \in \mathcal{X}} (\mu^1(x))^\alpha \\ &= \arg \max_{x \in \mathcal{X}} \mu^1(x), \end{aligned}$$

which is again unique by the fact that μ satisfies Assumption 2. Finally, $\arg \max_{x \in \mathcal{X}} T(\mu^1, \alpha)(x)$ is unique by the fact that $\arg \min_{x \in \mathcal{X}} \mu^1(x)$ is unique completing the proof. \blacksquare

III. EQUIVALENT ORDER CLASS

In this section, we characterize the set of all string-sources that induce the same optimal ordering of the strings (from the most likely to the least likely) on all strings of all lengths.

Definition 16 (order equivalent string-sources): We say two string-sources $\mu, \rho \in \mathcal{M}_{\mathcal{X}}$ are order equivalent and denote by $\mu \equiv \rho$, if for all $n \in \mathbb{N}$, $G_{\mu}^n = G_{\rho}^n$, i.e., the optimal ordering for μ is also the optimal ordering for ρ .

Note that two string-sources may be order equivalent while they are not necessarily indistinguishable sources. By contrast, if for all $n \in \mathbb{N}$, $\mu^n = \rho^n$, then the two are indistinguishable, and we write $\mu = \rho$.

Definition 17 (equivalent order class): The equivalent order class of a string-source $\mu \in \mathcal{M}_{\mathcal{X}}$ is denoted by \mathcal{C}_{μ} and is given by $\mathcal{C}_{\mu} = \{\rho \in \mathcal{M}_{\mathcal{X}} : \rho \equiv \mu\}$.

We also need another definition that generalizes the weakly typical set.

Definition 18 (tilted weakly typical set of order α): For any $\alpha \in \mathbb{R}$, denote by $\mathcal{A}_{\mu, \alpha, \epsilon}^n$ the tilted weakly typical set of order α with respect to μ , which is the set of all x^n such that for an $\epsilon \in \mathbb{R}_{+*}$:

$$e^{-H^n(T(\mu, \alpha) \| \mu) - n\epsilon} < \mu^n(x^n) < e^{-H^n(T(\mu, \alpha) \| \mu) + n\epsilon}, \quad (73)$$

where $H(\cdot \| \cdot)$ is the cross entropy defined in (13).

Note that in the case of $\alpha = 1$, $\mathcal{A}_{\mu, 1, \epsilon}^n$ is the familiar weakly typical set (see (3.6) in [38]); and Definition 18 generalizes the weakly typical set for $\alpha \neq 1$. We shall establish some useful properties of the tilted weakly typical sets in the next section.

Our interest in finding the equivalent order class of a string-source μ lies in the fact that such string-sources are subject to the same optimal guessing procedure, which renders them equivalent in terms of many problems, such as brute-force password guessing, list decoding, sequential decoding, and one-to-one source coding.

Theorem 1: For any string-source $\mu \in \mathcal{M}_{\mathcal{X}}$, if $\rho \in \mathcal{C}_{\mu}$, then there exists a unique $\alpha \in \mathbb{R}_{+*}$ such that $\rho = T(\mu, \alpha)$. Consequently, the equivalent order class of μ is equal to the tilted family, i.e., $\mathcal{C}_{\mu} = \mathcal{T}_{\mu}^+$. Further, the set of all string-sources whose optimal orderings are inverse for μ is equal to \mathcal{T}_{μ}^- , i.e., $\mathcal{C}_{T(\mu, -1)} = \mathcal{T}_{\mu}^-$.

Theorem 1 characterizes the set of all string-sources that would result in the same ordering of strings for any length. As discussed above, these string-sources are called order equivalent as their optimal guesswork procedure is exactly the same. Theorem 1 establishes that any such order equivalent string-source is necessarily the result of a tilt providing an operational meaning to the tilted family.

To prove the theorem, we state two intermediate lemmas and a definition.

Lemma 17: For any string-source μ , the equivalent order class of μ contains \mathcal{T}_{μ}^+ , i.e., $\mathcal{T}_{\mu}^+ \subseteq \mathcal{C}_{\mu}$.

Proof: To prove the lemma, we need to show that for any $\alpha \in \mathbb{R}_{+*}$, we have $T(\mu, \alpha) \equiv \mu$, i.e., $T(\mu, \alpha) \in \mathcal{C}_{\mu}$. To this end, we show that $G_{\mu}^n = G_{T(\mu, \alpha)}^n$, i.e., G_{μ}^n is also the optimal ordering on n -strings for $T(\mu, \alpha)$. Thus, we need to show that

$$T(\mu^n, \alpha)(x^n) < T(\mu^n, \alpha)(y^n) \Rightarrow G_{\mu}^n(x^n) > G_{\mu}^n(y^n). \quad (74)$$

Considering (6), this establishes that G_{μ}^n is the optimal ordering for $T(\mu^n, \alpha)$, and hence $G_{\mu}^n = G_{T(\mu, \alpha)}^n$. It suffices to show that for any $\alpha \in \mathbb{R}_{+*}$, we have

$$\mu^n(x^n) > \mu^n(y^n) \Leftrightarrow T(\mu^n, \alpha)(x^n) > T(\mu^n, \alpha)(y^n). \quad (75)$$

We show here that

$$\begin{aligned} & \mu^n(x^n) > \mu^n(y^n) \\ & \Leftrightarrow [\mu^n(x^n)]^{\alpha} > [\mu^n(y^n)]^{\alpha} \end{aligned} \quad (76)$$

$$\begin{aligned} & \Leftrightarrow \frac{[\mu^n(x^n)]^{\alpha}}{\sum_{z^n \in \mathcal{X}^n} [\mu^n(z^n)]^{\alpha}} > \frac{[\mu^n(y^n)]^{\alpha}}{\sum_{z^n \in \mathcal{X}^n} [\mu^n(z^n)]^{\alpha}} \\ & \Leftrightarrow T(\mu^n, \alpha)(x^n) > T(\mu^n, \alpha)(y^n), \end{aligned} \quad (77)$$

where (76) holds because $\alpha > 0$, and (77) follows from the definition of the tilt in (21). ■

Next, we state a simple lemma about the weakly typical set (which is a special case of the tilted weakly typical sets).

Lemma 18: For any $\mu \in \mathcal{M}_{\mathcal{X}}$,

$$\mathbb{P}_{\mu} \{X^n \in \mathcal{A}_{\mu, 1, \epsilon}^n\} \geq 1 - \frac{V^n(\mu)}{n^2 \epsilon^2}, \quad (78)$$

$$|\mathcal{A}_{\mu, 1, \epsilon}^n| > e^{H^n(\mu) - n\epsilon} \left(1 - \frac{V^n(\mu)}{n^2 \epsilon^2}\right), \quad (79)$$

$$|\mathcal{A}_{\mu, 1, \epsilon}^n| < e^{H^n(\mu) + n\epsilon}. \quad (80)$$

Proof:

$$\begin{aligned}\mathbb{P}_\mu \{X^n \in \mathcal{A}_{\mu,1,\epsilon}^n\} &= \mathbb{P}_\mu \{|\nu_\mu(X^n) - H^n(\mu)| \leq n\epsilon\} \\ &\geq 1 - \frac{V^n(\mu)}{n^2\epsilon^2},\end{aligned}\tag{81}$$

where (81) follows from Chebyshev's inequality. Note that Chernoff bounds could be used to establish an exponential decay in (81) but the weaker bound above is sufficient for our purposes. To derive the lower bound in (79) on the size of the set $\mathcal{A}_{\mu,1,\epsilon}$, observe that

$$\begin{aligned}|\mathcal{A}_{\mu,1,\epsilon}| &\geq \frac{\mathbb{P}_\mu \{X^n \in \mathcal{A}_{\mu,1,\epsilon}\}}{\max_{x^n \in \mathcal{A}_{\mu,1,\epsilon}} \{\mu^n(x^n)\}} \\ &> \frac{1 - \frac{V^n(\mu)}{n^2\epsilon^2}}{e^{-H^n(\mu) + n\epsilon}} \\ &= \left(1 - \frac{V^n(\mu)}{n^2\epsilon^2}\right) e^{H^n(\mu) - n\epsilon}.\end{aligned}$$

The bound in (80) is established similarly. \blacksquare

Definition 19 (Shannon entropy contour): Let $\mathcal{S}_h \subset \mathcal{M}_\mathcal{X}$ denote the Shannon entropy contour h , which is the set of all string-sources in $\mathcal{M}_\mathcal{X}$ whose entropy rate equals $h \in (0, \log |\mathcal{X}|)$, i.e.,

$$\mathcal{S}_h := \{\mu \in \mathcal{M}_\mathcal{X} : H(\mu) = h\}.\tag{82}$$

Next, we provide the proof of the main result of this section on the equivalent order class of a string-source.

Proof of Theorem 1: To prove the theorem, we take two steps. We first show that one element of the tilted family \mathcal{T}_μ^+ is also contained in the intersection of the Shannon entropy contour and the equivalent order class, i.e., $\mathcal{T}_\mu^+ \cap \mathcal{C}_\mu \cap \mathcal{S}_h \in \mathcal{M}_\mathcal{X}$ is not empty. We also show that for any string-source $\mu \in \mathcal{M}_\mathcal{X}$ and any $h \in (0, \log |\mathcal{X}|)$, if $\rho_1, \rho_2 \in \mathcal{M}_\mathcal{X}$ are in the intersection of \mathcal{S}_h (see Definition 19) and \mathcal{C}_μ denoted by $\mathcal{C}_\mu \cap \mathcal{S}_h$, then ρ_1 and ρ_2 are indistinguishable sources, i.e., $\rho_1 = \rho_2$. Putting these two steps together ensures that the intersection $\mathcal{C}_\mu \cap \mathcal{S}_h$ contains one and only one element, which is a member of the tilted family by Lemma 17, and completes the proof. The second part of the theorem is proved by invoking Lemma 2 and the first part of the theorem.

We first show that $\mathcal{C}_\mu \cap \mathcal{S}_h$ is not empty and contains one element from \mathcal{T}_μ^+ . This is carried out by noting the continuity and monotonicity of $H(T(\mu, \alpha))$ in the parameter α proved in Lemma 7 and noting that $H(\mathbf{u}_\mathcal{X}) = \log |\mathcal{X}|$ and $\lim_{\alpha \rightarrow \infty} H^n(T(\mu, \alpha)) = 0$.

Next, we proceed the proof of uniqueness by contradiction. Let $\rho_1, \rho_2 \in \mathcal{C}_\mu \cap \mathcal{S}_h$ be two string-sources that are contained in the intersection of \mathcal{S}_h and \mathcal{C}_μ . Note that by Definition 17, $\rho_1, \rho_2 \in \mathcal{M}_\mathcal{X}$. Therefore, by definition as $\rho_1, \rho_2 \in \mathcal{S}_h$, we have

$$H(\rho_1) = H(\rho_2) = h,$$

where $h \in (0, \log |\mathcal{X}|)$ by Definition 19. The claim is negated to assume that ρ_1 and ρ_2 are not equal, i.e., there exists $\delta \in \mathbb{R}_{+*}$ such that for all $n \in \mathbb{N}$:

$$D^n(\rho_2 || \rho_1) = E_{\rho_2} \left\{ \log \left(\frac{\rho_2^n(X^n)}{\rho_1^n(X^n)} \right) \right\} > 2n\delta.$$

Then, we can decompose the expectation over the weakly typical set and the rest of the strings as follows:

$$\begin{aligned}E_{\rho_2} \left\{ \log \left(\frac{\rho_2^n(X^n)}{\rho_1^n(X^n)} \right) \right\} &= \sum_{x^n \in \mathcal{A}_{\rho_2,1,\epsilon}^n} \rho_2^n(x^n) \log \left(\frac{\rho_2^n(x^n)}{\rho_1^n(x^n)} \right) \\ &\quad + \sum_{x^n \notin \mathcal{A}_{\rho_2,1,\epsilon}^n} \rho_2^n(x^n) \log \left(\frac{\rho_2^n(x^n)}{\rho_1^n(x^n)} \right).\end{aligned}\tag{83}$$

By Assumption 1 for the string-source $\rho_1 \in \mathcal{M}_\mathcal{X}$, there exists $\underline{\epsilon}$ such that

$$\max_{x^n \in \mathcal{X}^n} \log \frac{1}{\rho_1^n(x^n)} < n \log \frac{1}{\underline{\epsilon}}.\tag{84}$$

On the other hand, by (78) in Lemma 18,

$$\sum_{x^n \notin \mathcal{A}_{\rho_2,1,\epsilon}^n} \rho_2^n(x^n) \leq \frac{V^n(\rho_2)}{n^2\epsilon^2},\tag{85}$$

Putting together (84) and (85), we have

$$\begin{aligned}
& \sum_{x^n \notin \mathcal{A}_{\rho_2, 1, \epsilon}^n} \rho_2^n(x^n) \log \left(\frac{\rho_2^n(x^n)}{\rho_1^n(x^n)} \right) \\
& \leq \sum_{x^n \notin \mathcal{A}_{\rho_2, 1, \epsilon}^n} \rho_2^n(x^n) \log \left(\frac{1}{\rho_1^n(x^n)} \right) \\
& \leq \frac{V^n(\rho_2)}{n\epsilon^2} \log \frac{1}{\underline{\epsilon}} = \frac{V^1(\rho_2)}{\epsilon^2} \log \frac{1}{\underline{\epsilon}},
\end{aligned} \tag{86}$$

leading to the fact that the term in (83) is $O_n(1)$. Using the above in conjunction with the fact that $P_\mu \left\{ X^n \in \mathcal{A}_{\rho_2, 1, \epsilon}^n \right\} \geq 1 - \frac{V^n(\mu)}{n^2\epsilon^2}$, we conclude that for sufficiently large n :

$$E_{\rho_2} \left\{ \log \left(\frac{\rho_2^n(X^n)}{\rho_1^n(X^n)} \right) \middle| X^n \in \mathcal{A}_{\rho_2, 1, \epsilon}^n \right\} > n\delta.$$

Consequently, there exists $y^n \in \mathcal{A}_{\rho_2, 1, \epsilon}^n$ such that

$$\log \frac{1}{\rho_1^n(y^n)} > \log \frac{1}{\rho_2^n(y^n)} + n\delta. \tag{87}$$

Since $y^n \in \mathcal{A}_{\rho_2, 1, \epsilon}^n$, by definition, we have

$$nh - n\epsilon \leq \log \frac{1}{\rho_2^n(y^n)} \leq nh + n\epsilon,$$

which in conjunction with (87) leads to

$$\log \frac{1}{\rho_1^n(y^n)} > \log \frac{1}{\rho_2^n(y^n)} + n\delta \geq nh - n\epsilon + n\delta.$$

By swapping ρ_1 and ρ_2 and noting that

$$D(\rho_2 || \rho_1) = 0 \Leftrightarrow D(\rho_1 || \rho_2) = 0,$$

and repeating similar arguments, we could pick a different sequence $\hat{y}^n \in \mathcal{X}^n$ such that

$$\log \frac{1}{\rho_2^n(\hat{y}^n)} > nh - n\epsilon + n\delta.$$

and

$$\log \frac{1}{\rho_1^n(\hat{y}^n)} \leq nh + n\epsilon.$$

Note that the above holds for any $\epsilon \in \mathbb{R}_{+*}$. By choosing ϵ to be small enough (smaller than $\delta/2$) we then ensure that for n sufficiently large, $\rho_2^n(y^n) > \rho_2^n(\hat{y}^n)$ and hence $G_{\rho_2}^n(y^n) < G_{\rho_2}^n(\hat{y}^n)$. Similarly, we can show that for sufficiently large n , we have $\rho_1^n(y^n) < \rho_1^n(\hat{y}^n)$, which leads to $G_{\rho_1}^n(y^n) > G_{\rho_1}^n(\hat{y}^n)$. Therefore, ρ_1 and ρ_2 cannot be order equivalent, which is a contradiction. Hence, it must be true that for any $\delta \in \mathbb{R}_{+*}$, for sufficiently large n :

$$E_{\rho_2} \left\{ \log \left(\frac{\rho_2^n(X^n)}{\rho_1^n(X^n)} \right) \right\} < n\delta,$$

which directly implies that $D(\rho_1 || \rho_2) = D(\rho_2 || \rho_1) = 0$, and $\rho_1 = \rho_2$, i.e., any two string-sources in the intersection of \mathcal{C}_μ and \mathcal{S}_h must be equal, which completes the proof of the uniqueness. \blacksquare

IV. TILTED WEAKLY TYPICAL SET

The main result in this section is a generalization of the asymptotic equipartition property on the weakly typical set concerning information and guesswork. We call this generalized notion the tilted weakly typical set and define it in Definition 18 in the previous section. Although these results resemble the asymptotic equipartition property on the weakly typical set, they are concerned with the large deviations, i.e., atypical behavior, rather than the typical behavior. We will consequently use these results in establishing the large deviation properties of guesswork and information in the next section.

We need two more definitions before we can provide the statement of the main result in this section.

Definition 20: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, let $\mathcal{B}_{\mu, \alpha, \epsilon}^n \subset \mathcal{A}_{\mu, \alpha, \epsilon}^n$ be a subset such that $|\mathcal{B}_{\mu, \alpha, \epsilon}^n| = \lfloor \frac{1}{2} |\mathcal{A}_{\mu, \alpha, \epsilon}^n| \rfloor$ and for any $x^n \in \mathcal{B}_{\mu, \alpha, \epsilon}^n$ and $y^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n \cap \overline{\mathcal{B}_{\mu, \alpha, \epsilon}^n}$ we have $T(\mu^n, \alpha)(x^n) < T(\mu^n, \alpha)(y^n)$.

Definition 21: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, let $\mathcal{D}_{\mu,\alpha,\epsilon}^n \supseteq \mathcal{A}_{\mu,\alpha,\epsilon}^n$ be defined as follows:

$$\mathcal{D}_{\mu,\alpha,\epsilon}^n := \left\{ x^n \in \mathcal{X}^n : T(\mu^n, \alpha)(x^n) > e^{-H^n(T(\mu,\alpha)) - n|\alpha|\epsilon} \right\}. \quad (88)$$

Definition 22: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, let $\mathcal{E}_{\mu,\alpha,\epsilon}^n \supseteq \mathcal{A}_{\mu,\alpha,\epsilon}^n$ be defined as follows:

$$\mathcal{E}_{\mu,\alpha,\epsilon}^n := \left\{ x^n \in \mathcal{X}^n : T(\mu^n, \alpha)(x^n) < e^{-H^n(T(\mu,\alpha)) + n|\alpha|\epsilon} \right\}. \quad (89)$$

Theorem 2: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, any $\epsilon \in \mathbb{R}_{+*}$, and any $\alpha \neq 0$,

(a) For any $x^n \in \mathcal{A}_{\mu,\alpha,\epsilon}^n$,

$$\mu^n(x^n) > e^{-H^n(T(\mu,\alpha)\|\mu) - n\epsilon}, \quad (90)$$

$$\mu^n(x^n) < e^{-H^n(T(\mu,\alpha)\|\mu) + n\epsilon}; \quad (91)$$

(b) For any $n \in \mathbb{N}$,

$$|\mathcal{A}_{\mu,\alpha,\epsilon}^n| > \left(1 - \frac{V^n(T(\mu,\alpha)\|\mu)}{n^2\epsilon^2} \right) e^{H^n(T(\mu,\alpha)) - |\alpha|n\epsilon}, \quad (92)$$

$$|\mathcal{A}_{\mu,\alpha,\epsilon}^n| < e^{H^n(T(\mu,\alpha)) + |\alpha|n\epsilon}; \quad (93)$$

(c) For any $n \in \mathbb{N}$, and $\alpha \in (-\infty, 0) \cup [1, \infty)$,

$$\begin{aligned} \mathbb{P}_{\mu} \{ X^n \in \mathcal{D}_{\mu,\alpha,\epsilon}^n \} &\geq \mathbb{P}_{\mu} \{ X^n \in \mathcal{A}_{\mu,\alpha,\epsilon}^n \} \\ &> \left(1 - \frac{V^n(T(\mu,\alpha)\|\mu)}{n^2\epsilon^2} \right) e^{-D^n(T(\mu,\alpha)\|\mu) - |1-\alpha|n\epsilon}, \end{aligned} \quad (94)$$

$$\begin{aligned} \mathbb{P}_{\mu} \{ X^n \in \mathcal{A}_{\mu,\alpha,\epsilon}^n \} &\leq \mathbb{P}_{\mu} \{ X^n \in \mathcal{D}_{\mu,\alpha,\epsilon}^n \} \\ &\leq e^{-D^n(T(\mu,\alpha)\|\mu) + |1-\alpha|n\epsilon}, \end{aligned} \quad (95)$$

$$\mathbb{P}_{\mu} \{ X^n \in \mathcal{E}_{\mu,\alpha,\epsilon}^n \} \geq 1 - e^{-D^n(T(\mu,\alpha)\|\mu) + |1-\alpha|n\epsilon}; \quad (96)$$

(d) For any $n \in \mathbb{N}$, and $\alpha \in (0, 1]$,

$$\begin{aligned} \mathbb{P}_{\mu} \{ X^n \in \mathcal{E}_{\mu,\alpha,\epsilon}^n \} &\geq \mathbb{P}_{\mu} \{ X^n \in \mathcal{A}_{\mu,\alpha,\epsilon}^n \} \\ &> \left(1 - \frac{V^n(T(\mu,\alpha)\|\mu)}{n^2\epsilon^2} \right) e^{-D^n(T(\mu,\alpha)\|\mu) - |1-\alpha|n\epsilon}, \end{aligned} \quad (97)$$

$$\begin{aligned} \mathbb{P}_{\mu} \{ X^n \in \mathcal{A}_{\mu,\alpha,\epsilon}^n \} &\leq \mathbb{P}_{\mu} \{ X^n \in \mathcal{E}_{\mu,\alpha,\epsilon}^n \} \\ &\leq e^{-D^n(T(\mu,\alpha)\|\mu) + |1-\alpha|n\epsilon}, \end{aligned} \quad (98)$$

$$\mathbb{P}_{\mu} \{ X^n \in \mathcal{D}_{\mu,\alpha,\epsilon}^n \} \geq 1 - e^{-D^n(T(\mu,\alpha)\|\mu) + |1-\alpha|n\epsilon}; \quad (99)$$

(e) For any $n \in \mathbb{N}$ and any $\alpha > 0$:

$$\begin{aligned} x^n \in \mathcal{B}_{\mu,\alpha,\epsilon}^n &\Rightarrow \\ G_{\mu}^n(x^n) &> \frac{1}{2} \left(1 - \frac{V^n(T(\mu,\alpha)\|\mu)}{n^2\epsilon^2} \right) e^{H^n(T(\mu,\alpha)) - \alpha n\epsilon}, \end{aligned} \quad (100)$$

$$x^n \in \mathcal{D}_{\mu,\alpha,\epsilon}^n \Rightarrow G_{\mu}^n(x^n) \leq e^{H^n(T(\mu,\alpha)) + \alpha n\epsilon}, \quad (101)$$

$$\begin{aligned} x^n \in \mathcal{D}_{\mu,\alpha,\epsilon}^n &\Leftarrow \\ G_{\mu}^n(x^n) &\leq \left(1 - \frac{V^n(T(\mu,\alpha)\|\mu)}{n^2\epsilon^2} \right) e^{H^n(T(\mu,\alpha)) - \alpha n\epsilon}, \end{aligned} \quad (102)$$

$$x^n \in \mathcal{E}_{\mu,\alpha,\epsilon}^n \Leftarrow G_{\mu}^n(x^n) > e^{H^n(T(\mu,\alpha)) + \alpha n\epsilon}. \quad (103)$$

(f) For any $n \in \mathbb{N}$ and any $\alpha < 0$:

$$\begin{aligned} x^n \in \mathcal{B}_{\mu, \alpha, \epsilon}^n &\Rightarrow \\ R_{\mu}^n(x^n) &> \frac{1}{2} \left(1 - \frac{V^n(T(\mu, \alpha) \|\mu)}{n^2 \epsilon^2} \right) e^{H^n(T(\mu, \alpha)) - |\alpha|n\epsilon}, \end{aligned} \quad (104)$$

$$x^n \in \mathcal{D}_{\mu, \alpha, \epsilon}^n \Rightarrow R_{\mu}^n(x^n) \leq e^{H^n(T(\mu, \alpha)) + |\alpha|n\epsilon}, \quad (105)$$

$$\begin{aligned} x^n \in \mathcal{D}_{\mu, \alpha, \epsilon}^n &\Leftarrow \\ R_{\mu}^n(x^n) &\leq \left(1 - \frac{V^n(T(\mu, \alpha) \|\mu)}{n^2 \epsilon^2} \right) e^{H^n(T(\mu, \alpha)) - |\alpha|n\epsilon}, \end{aligned} \quad (106)$$

$$x^n \in \mathcal{E}_{\mu, \alpha, \epsilon}^n \Leftarrow R_{\mu}^n(x^n) > e^{H^n(T(\mu, \alpha)) + |\alpha|n\epsilon}. \quad (107)$$

Recall that Shannon entropy, cross entropy, and relative entropy are measured in nats throughout this paper. We first provide a few lemmas that specialize to the typical set, which we use to prove the theorem.

Lemma 19: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, let $x^n \in \mathcal{B}_{\mu, 1, \epsilon}^n$ (see Definition 20). Then,

$$G_{\mu}^n(x^n) > \frac{1}{2} \left(1 - \frac{V^n(\mu)}{n^2 \epsilon^2} \right) e^{H^n(\mu) - n\epsilon}. \quad (108)$$

Proof: Note that by definition for all $x^n \in \mathcal{B}_{\mu, 1, \epsilon}^n$, we have $G_{\mu}^n(x^n) > |\overline{\mathcal{B}_{\mu, 1, \epsilon}^n}| \geq \frac{1}{2} |\mathcal{A}_{\mu, 1, \epsilon}^n|$. The proof is completed noticing the bound in (79). ■

Lemma 20: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, let $x^n \in \mathcal{D}_{\mu, 1, \epsilon}^n$ (see Definition 22). Then,

$$G_{\mu}^n(x^n) \leq e^{H^n(\mu) + n\epsilon}. \quad (109)$$

Proof: We have

$$G_{\mu}^n(x^n) \leq |\mathcal{D}_{\mu, 1, \epsilon}^n| \quad (110)$$

$$\leq \frac{1}{\min_{x^n \in \mathcal{D}_{\mu, 1, \epsilon}^n} \{\mu^n(x^n)\}} \quad (111)$$

$$= e^{H^n(\mu) + n\epsilon}, \quad (112)$$

where (110) follows from the definition in (88), (111) follows from the fact that the probability of the set $\mathcal{D}_{\mu, 1, \epsilon}^n$ is upper bounded by 1, and (112) again follows from the definition in (88). ■

Lemma 21: Suppose the following holds:

$$G_{\mu}^n(x^n) \leq \left(1 - \frac{V^n(\mu)}{n^2 \epsilon^2} \right) e^{H^n(\mu) - n\epsilon}. \quad (113)$$

Then, $x^n \in \mathcal{D}_{\mu, 1, \epsilon}^n$.

Proof: We proceed the proof with contradiction. Suppose that $x^n \notin \mathcal{D}_{\mu, 1, \epsilon}^n$. Hence, $\mu^n(x^n) \leq e^{-nH(\mu) - n\epsilon}$. Thus, $\mu^n(x^n) < \mu^n(y^n)$ for all $y^n \in \mathcal{A}_{\mu, 1, \epsilon}^n$. Consequently,

$$G_{\mu}^n(x^n) > |\mathcal{A}_{\mu, 1, \epsilon}^n| > \left(1 - \frac{V^n(\mu)}{n^2 \epsilon^2} \right) e^{H^n(\mu) - n\epsilon},$$

which contradicts the supposition of the lemma in (113). ■

Lemma 22: Suppose the following holds:

$$G_{\mu}^n(x^n) > e^{H^n(\mu) + n\epsilon}. \quad (114)$$

Then, $x^n \in \mathcal{E}_{\mu, 1, \epsilon}^n$.

Proof: We proceed the proof with contradiction. Suppose that $x^n \notin \mathcal{E}_{\mu, 1, \epsilon}^n$. Hence, $\mu^n(x^n) \geq e^{-nH(\mu) + n\epsilon}$. Thus, $\mu^n(x^n) > \mu^n(y^n)$ for all $y^n \in \mathcal{A}_{\mu, 1, \epsilon}^n$. Consequently,

$$G_{\mu}^n(x^n) < G_{\mu}^n(y^n) \leq e^{H^n(\mu) + n\epsilon},$$

which contradicts the supposition of the lemma in (114). ■

Next, we provide a lemma of equivalence between tilted weakly typical sets and weakly typical sets of a tilted source, which we will rely on in proving the main theorem of this section.

Lemma 23: Let $\mu \in \mathcal{M}_{\mathcal{X}}$. Then, for all $\alpha \neq 0$, the following equivalences hold:

$$\mathcal{A}_{\mu, \alpha, \epsilon}^n = \mathcal{A}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n, \quad (115)$$

$$\mathcal{B}_{\mu, \alpha, \epsilon}^n = \mathcal{B}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n, \quad (116)$$

$$\mathcal{D}_{\mu, \alpha, \epsilon}^n = \mathcal{D}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n, \quad (117)$$

$$\mathcal{E}_{\mu, \alpha, \epsilon}^n = \mathcal{E}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n. \quad (118)$$

Proof: We have

$$\mathcal{A}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n = \left\{ x^n \in \mathcal{X}^n : \left| \log \frac{1}{T(\mu^n, \alpha)(x^n)} - H^n(T(T(\mu, \alpha), 1) \| T(\mu, \alpha)) \right| < |\alpha| n \epsilon \right\} \quad (119)$$

$$= \left\{ x^n \in \mathcal{X}^n : \left| \frac{1}{\alpha} \log \frac{1}{T(\mu^n, \alpha)(x^n)} - \frac{1}{\alpha} H^n(T(\mu, \alpha)) \right| < n \epsilon \right\} \quad (120)$$

$$= \left\{ x^n \in \mathcal{X}^n : \left| \log \frac{1}{\mu^n(x^n)} - H^n(T(\mu, \alpha) \| \mu) \right| < n \epsilon \right\} \quad (121)$$

$$= \mathcal{A}_{\mu, \alpha, \epsilon}^n,$$

where (119) follows from Definition 18, (120) follows by noting that $T(\mu, 1) = \mu$ and $H^n(\mu \| \mu) = H^n(\mu)$ and the fact that $\alpha \neq 0$, and (121) follows from Lemma 5.

Next, note that (116) follows directly from (115) and Definition 20.

To establish (117) note that:

$$\mathcal{D}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n = \left\{ x^n \in \mathcal{X}^n : \log \frac{1}{T(\mu^n, \alpha)(x^n)} - H^n(T(T(\mu, \alpha), 1) \| T(\mu, \alpha)) < |\alpha| n \epsilon \right\} \quad (122)$$

$$= \left\{ x^n \in \mathcal{X}^n : \log \frac{1}{T(\mu^n, \alpha)(x^n)} - H^n(T(\mu, \alpha)) < |\alpha| n \epsilon \right\} \quad (123)$$

$$= \mathcal{D}_{\mu, \alpha, \epsilon}^n,$$

where (122) follows from Definition 18, (123) follows by noting that $T(\mu, 1) = \mu$ and $H^n(\mu \| \mu) = H^n(\mu)$ and the fact that $\alpha \neq 0$. Finally, the proof for (118) is very similar to that of (117) with all the inequalities reversed, and is omitted for brevity. \blacksquare

Next, we proceed to the proof of Theorem 2.

Proof of Theorem 2: Part (a) is simply a reiteration of Definition 18, which is presented here for the completeness of the characterization.

To establish Part (b), notice that by Lemma 23, for all $\alpha \neq 0$, we have $\mathcal{A}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n = \mathcal{A}_{\mu, \alpha, \epsilon}^n$. Part (b) is established by applying the bounds in (79) and (80) in Lemma 18 to $\mathcal{A}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n$, and noting that $\alpha^2 V(T(\mu, \alpha) \| \mu) = V(T(\mu, \alpha))$ from Lemma 6.

In Parts (c) and (d), first notice that by definition $\mathcal{A}_{\mu, \alpha, \epsilon}^n \subseteq \mathcal{D}_{\mu, \alpha, \epsilon}^n$ and $\mathcal{A}_{\mu, \alpha, \epsilon}^n \subseteq \mathcal{E}_{\mu, \alpha, \epsilon}^n$ and hence $\mathbb{P}_{\mu} \{X^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n\} \leq \mathbb{P}_{\mu} \{X^n \in \mathcal{D}_{\mu, \alpha, \epsilon}^n\}$ and $\mathbb{P}_{\mu} \{X^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n\} \leq \mathbb{P}_{\mu} \{X^n \in \mathcal{E}_{\mu, \alpha, \epsilon}^n\}$. Hence, we only need to prove the right hand side inequalities in the claims.

To prove (94) in Part (c), consider (78) in Lemma 18 applied to $\mathcal{A}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n$, in conjunction with (115) in Lemma 23:

$$\begin{aligned} \mathbb{P}_{T(\mu, \alpha)} \{X^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n\} &= \mathbb{P}_{T(\mu, \alpha)} \left\{ \mathcal{A}_{T(\mu, \alpha), 1, |\alpha| \epsilon}^n \right\} \\ &\geq 1 - \frac{V^n(T(\mu, \alpha) \| \mu)}{n^2 \epsilon^2}. \end{aligned} \quad (124)$$

On the other hand, we have

$$\begin{aligned} \mathbb{P}_{T(\mu, \alpha)} \{X^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n\} &= \sum_{x^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n} T(\mu^n, \alpha)(x^n) \\ &= \frac{\sum_{x^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n} [\mu^n(x^n)]^\alpha}{\sum_{x^n \in \mathcal{X}^n} [\mu^n(x^n)]^\alpha} \end{aligned} \quad (125)$$

$$= \frac{\sum_{x^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n} \mu^n(x^n) [\mu^n(x^n)]^{\alpha-1}}{e^{(1-\alpha)H_\alpha^n(\mu)}} \quad (126)$$

$$< e^{(1-\alpha)(H^n(T(\mu, \alpha) \| \mu) - H_\alpha^n(\mu)) + |\alpha-1|n\epsilon} \sum_{x^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n} \mu^n(x^n) \quad (127)$$

$$= e^{D^n(T(\mu, \alpha) \| \mu) + |\alpha-1|n\epsilon} \mathbb{P}_{\mu} \{X^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n\}, \quad (128)$$

where (125) follow from the definition of the tilt in (21), (126) follows from the definition of the Rényi entropy in (18), (127) follows from (90) or (91) applied to $[\mu^n(x^n)]^{\alpha-1}$ depending on the sign of $(\alpha-1)$, and (128) follows from (30) in Lemma 4. Putting (124) and (128) together we arrive at the right hand side inequality in (94). Note that all the steps are applicable for $\alpha \neq 0$, and hence are also applicable to the case where $\alpha \in (0, 1]$. This also establishes the right hand side inequality in (98) for Part (d).

In Part (c), the upper bound in (95) would be established as follows. We first note:

$$\mathbb{P}_{T(\boldsymbol{\mu}, \alpha)} \{X^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n\} = \mathbb{P}_{T(\boldsymbol{\mu}, \alpha)} \left\{ \mathcal{D}_{T(\boldsymbol{\mu}, \alpha), 1, |\alpha|\epsilon}^n \right\} \leq 1. \quad (129)$$

We also note that (88) in conjunction with Lemma 5 imply that for $\alpha > 0$:

$$\mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n = \left\{ x^n \in \mathcal{X}^n : \mu^n(x^n) > e^{-H^n(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu}) - n\epsilon} \right\}. \quad (130)$$

and for $\alpha < 0$:

$$\mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n = \left\{ x^n \in \mathcal{X}^n : \mu^n(x^n) < e^{-H^n(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu}) + n\epsilon} \right\}. \quad (131)$$

Thus,

$$\mathbb{P}_{T(\boldsymbol{\mu}, \alpha)} \{X^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n\} = \frac{\sum_{x^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n} \mu^n(x^n) [\mu^n(x^n)]^{\alpha-1}}{e^{(1-\alpha)H_\alpha^n(\boldsymbol{\mu})}} \quad (132)$$

$$> e^{(1-\alpha)(H^n(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu}) - H_\alpha^n(\boldsymbol{\mu})) - |\alpha-1|n\epsilon} \sum_{x^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n} \mu^n(x^n) \quad (133)$$

$$= e^{D^n(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu}) - |\alpha-1|n\epsilon} \mathbb{P}_{\boldsymbol{\mu}} \{X^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n\}, \quad (134)$$

where (133) follows from (130) (for $\alpha > 1$) and (131) (for $\alpha < 0$) applied to $[\mu^n(x^n)]^{\alpha-1}$, and (134) follows from (30) in Lemma 4. Putting (129) and (134) together we arrive at the desired upper bound in (95). The upper bound in (98) is achieved by repeating (132)–(134) for $\mathcal{E}_{\boldsymbol{\mu}, \alpha, \epsilon}^n$ in the case of $\alpha \in (0, 1]$ and applying (89).

To establish Parts (e) and (f), we first apply Lemmas 19–22, to the sets $\mathcal{B}_{T(\boldsymbol{\mu}, \alpha), 1, |\alpha|\epsilon}^n$, $\mathcal{D}_{T(\boldsymbol{\mu}, \alpha), 1, |\alpha|\epsilon}^n$, and $\mathcal{E}_{T(\boldsymbol{\mu}, \alpha), 1, |\alpha|\epsilon}^n$ and notice the equivalences in Lemma 23 to get:

$$\begin{aligned} x^n \in \mathcal{B}_{\boldsymbol{\mu}, \alpha, \epsilon}^n &\Rightarrow G_{T(\boldsymbol{\mu}, \alpha)}^n(x^n) \geq \frac{1}{2} \left(1 - \frac{V^n(T(\boldsymbol{\mu}, \alpha))}{n^2 \alpha^2 \epsilon^2} \right) e^{H^n(T(\boldsymbol{\mu}, \alpha)) - |\alpha|n\epsilon}, \\ x^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n &\Rightarrow G_{T(\boldsymbol{\mu}, \alpha)}^n(x^n) < e^{H^n(T(\boldsymbol{\mu}, \alpha)) + |\alpha|n\epsilon}, \\ x^n \in \mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n &\Leftarrow G_{T(\boldsymbol{\mu}, \alpha)}^n(x^n) < \left(1 - \frac{V^n(T(\boldsymbol{\mu}, \alpha))}{n^2 \alpha^2 \epsilon^2} \right) e^{H^n(T(\boldsymbol{\mu}, \alpha)) + |\alpha|n\epsilon}, \\ x^n \in \mathcal{E}_{\boldsymbol{\mu}, \alpha, \epsilon}^n &\Leftarrow G_{T(\boldsymbol{\mu}, \alpha)}^n(x^n) > e^{H^n(T(\boldsymbol{\mu}, \alpha)) + |\alpha|n\epsilon}. \end{aligned}$$

Parts (e) and (f) then follow by invoking Theorem 1 to notice that for all $x^n \in \mathcal{X}^n$, $G_{T(\boldsymbol{\mu}, \alpha)}^n(x^n) = G_{\boldsymbol{\mu}}^n(x^n)$ for $\alpha > 0$ and $G_{T(\boldsymbol{\mu}, \alpha)}^n(x^n) = R_{\boldsymbol{\mu}}^n(x^n)$ for $\alpha < 0$, and noting that $\alpha^2 V(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu}) = V(T(\boldsymbol{\mu}, \alpha))$ from Lemma 6. \blacksquare

Theorem 2 (a)–(d), for $\alpha = 1$, reduces to the properties of the weakly typical set for finite-alphabet memoryless sources (see [38, Theorem 3.1.2]). Part (e) for $\alpha = 1$ provides a characterization of guesswork for weakly typical strings. For values of $\alpha \neq 1$, the theorem further provides an asymptotic equipartition property for atypical strings generated by memoryless sources. It is well known that several information theoretic quantities, such as the average length of the optimal source coding, and the channel capacity, could be analyzed through the typical or jointly typical sequences, and the entropy rate of the process appears as the fundamental performance limit. On the other hand, several other important notions, such as the error exponents are governed by the rare events comprising of atypical behavior. For different values of α , Theorem 2 describes the large deviation performance of information and the logarithm of (forward) guesswork, which generalizes the notion of the typical set. In particular, it also recovers the large deviations performance of the optimal length function for prefix-free source coding as well. We remark that Theorem 2 could also be used to recover known results that are concerned with rare events in a more intuitive way. Finally, we expect Theorem 2 to be generalizable to a wider class of stationary ergodic sources in light of the generalized version of the asymptotic equipartition property proved by Bobkov and Madiman [39], [40].

Note that the tighter non-asymptotic bounds on the moments of guesswork derived in [7] could not be used to fully characterize the distribution of guesswork as in Theorem 2. In particular, for the unlikely half of the sequences, the characterization involves reverse guesswork which is first studied in this paper.

V. LARGE DEVIATIONS

Thus far, we provided an operational meaning of the tilted family of the string-source in Theorem 1, and generalized the notion of the weakly typical set to the tilted weakly typical sets that characterize all strings in Theorem 2. Before we use these tools to provide results on large deviations, we need one more definition.

Definition 23 (Large Deviation Principle): A sequence of random variables $\{Y_n : n \in \mathbb{N}\}$ taking values in \mathbb{R} satisfies the Large Deviation Principle with rate function $J : \mathbb{R} \rightarrow [0, \infty]$ if J is lower semi-continuous and has compact level-sets, and for all Borel sets B

$$-\inf_{t \in B^\circ} J(t) \leq \liminf_{n \rightarrow \infty} \frac{1}{n} \log \mathbb{P}\{Y_n \in B\} \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \log \mathbb{P}\{Y_n \in B\} \leq -\inf_{t \in \bar{B}} J(t),$$

where B° is the interior of B and \bar{B} is its closure.

If the Y_n take values in a compact subset K of \mathbb{R} , then to establish that $\{Y_n : n \in \mathbb{N}\}$ satisfies the LDP it is sufficient [37, Theorem 4.1.11 and Lemma 1.2.18] to prove that the following exists for all $t \in K$

$$\lim_{\epsilon \downarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \log \mathbb{P}\{Y_n \in (t - \epsilon, t + \epsilon)\} = \lim_{\epsilon \downarrow 0} \limsup_{n \rightarrow \infty} \frac{1}{n} \log \mathbb{P}\{Y_n \in (t - \epsilon, t + \epsilon)\} = -J(t),$$

where \downarrow and \uparrow denote approaching from above and from below, respectively. Note that all of the processes of interest to us take values in compact sets, since for all $x^n \in \mathcal{X}^n$,

$$\frac{1}{n} g_\mu^n(x^n) \in [0, \log |\mathcal{X}|], \quad \frac{1}{n} r_\mu^n(x^n) \in [0, \log |\mathcal{X}|], \quad \frac{1}{n} i_\mu^n(x^n) \in \left[\log \frac{1}{\bar{\epsilon}}, \log \frac{1}{\underline{\epsilon}} \right].$$

Thus, for our purposes it is sufficient to prove that

$$\lim_{\epsilon \downarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \log \left(\frac{1}{\mathbb{P}\{|Y_n - t| < \epsilon\}} \right) = J(t). \quad (135)$$

Christiansen and Duffy proved that the logarithm of (forward) guesswork, $\{\frac{1}{n} g_\mu^n(X^n) : n \in \mathbb{N}\}$, defined in Definition 7 satisfies a LDP and characterized the rate function as the solution to an optimization problem [11], which is the Legendre-Fenchel transform of the scaled cumulant generating function. In the rest of this section, we characterize the large deviations behavior of reverse guesswork, guesswork, and information, respectively, and provide their rate functions in terms of information theoretic quantities.

A. Reverse guesswork

First, we use the generalization of the typical set and its properties, established in the previous section, to prove that the logarithm of reverse guesswork satisfies a LDP. We emphasize that the method used by Christiansen and Duffy [11] would not lead to proving a LDP for the logarithm of reverse guesswork because the resulting rate function is non-convex as will be proved later in this section.

Theorem 3: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, the sequence $\{\frac{1}{n} r_\mu^n(x^n) : n \in \mathbb{N}\}$ satisfies a LDP, and the corresponding rate function is implicitly given by

$$J_\mu^r(t) = D(T(\mu, \alpha_\mu^r(t)) || \mu), \quad (136)$$

where

$$\alpha_\mu^r(t) = \arg_{\alpha \in \mathbb{R}_{-*}} \{H(T(\mu, \alpha)) = t\}. \quad (137)$$

Proof: Consider $\alpha_\mu^r(t)$ defined in (137) implying that $H(T(\mu, \alpha_\mu^r(t))) = t$. Hence, for sufficiently large n ,

$$\begin{aligned} \mathbb{P}_\mu \left\{ \left| \frac{1}{n} \log R_\mu^n(X^n) - t \right| < \epsilon \right\} &= \mathbb{P}_\mu \left\{ \left| \frac{1}{n} \log R_\mu^n(X^n) - H(T(\mu, \alpha_\mu^r(t))) \right| < \epsilon \right\} \\ &= \mathbb{P}_\mu \left\{ \left| \log R_\mu^n(X^n) - H^n(T(\mu, \alpha_\mu^r(t))) \right| < n\epsilon \right\} \\ &\leq \mathbb{P}_\mu \left\{ X^n \in \mathcal{D}_{\mu, \alpha_\mu^r(t), (2\epsilon)/\alpha_\mu^r(t)}^n \right\} \end{aligned} \quad (138)$$

$$\leq e^{-D^n(T(\mu, \alpha_\mu^r(t)) || \mu) + 2 \frac{1 - \alpha_\mu^r(t)}{\alpha_\mu^r(t)} n\epsilon}, \quad (139)$$

where (138) holds because (106) ensures that for sufficiently large n we have

$$\{x^n : |\log R_\mu^n(x^n) - H^n(T(\mu, \alpha_\mu^r(t)))| < n\epsilon\} \subseteq \mathcal{D}_{\mu, \alpha_\mu^r(t), (2\epsilon)/\alpha_\mu^r(t)}^n,$$

and hence

$$P_\mu \{x^n : |\log R_\mu^n(x^n) - H^n(T(\mu, \alpha_\mu^r(t)))| < n\epsilon\} \leq P_\mu \left\{ X^n \in \mathcal{D}_{\mu, \alpha_\mu^r(t), (2\epsilon)/\alpha_\mu^r(t)}^n \right\},$$

and (139) is a direct application of the upper bound in (98) to $\mathcal{D}_{\mu, \alpha_\mu^r(t), 2\epsilon/\alpha_\mu^r(t)}^n$. Consequently,

$$\frac{1}{n} \log \left(\frac{1}{\mathbb{P}_\mu \left\{ \left| \frac{1}{n} \log R_\mu^n(X^n) - t \right| < \epsilon \right\}} \right) \geq \frac{1}{n} D^n(T(\mu, \alpha_\mu^r(t)) || \mu) - 2 \frac{1 - \alpha_\mu^r(t)}{\alpha_\mu^r(t)} \epsilon.$$

Taking limits as $n \rightarrow \infty$ and letting $\epsilon \downarrow 0$ would lead to

$$\lim_{\epsilon \downarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \log \left(\frac{1}{\mathbb{P}_{\boldsymbol{\mu}} \left\{ \left| \frac{1}{n} \log R_{\boldsymbol{\mu}}^n(X^n) - t \right| < \epsilon \right\}} \right) \geq D(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)) || \boldsymbol{\mu}). \quad (140)$$

Next, we will show that the left hand side of (140) is also upper bounded by $D(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)) || \boldsymbol{\mu})$. We have

$$\begin{aligned} \mathbb{P}_{\boldsymbol{\mu}} \left\{ \left| \frac{1}{n} \log R_{\boldsymbol{\mu}}^n(X^n) - t \right| < \epsilon \right\} &= \mathbb{P}_{\boldsymbol{\mu}} \left\{ \left| \log R_{\boldsymbol{\mu}}^n(X^n) - nH(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t))) \right| < n\epsilon \right\} \\ &\geq \mathbb{P}_{\boldsymbol{\mu}} \left\{ X^n \in \mathcal{B}_{\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t), \epsilon/(2\alpha_{\boldsymbol{\mu}}^r(t))}^n \right\} \end{aligned} \quad (141)$$

$$\geq e^{-D^n(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)) || \boldsymbol{\mu}) - \frac{|1 - \alpha_{\boldsymbol{\mu}}^r(t)|}{2\alpha_{\boldsymbol{\mu}}^r(t)} n\epsilon}, \quad (142)$$

where (141) holds because (104) and (105) ensure that

$$\mathcal{B}_{\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t), \epsilon/(2\alpha_{\boldsymbol{\mu}}^r(t))}^n \subseteq \{x^n : |\log R_{\boldsymbol{\mu}}^n(x^n) - H^n(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)))| < n\epsilon\},$$

and (142) is due to the lower bound in (94). Hence, following steps similar to the previous case, we have

$$\lim_{\epsilon \downarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \log \left(\frac{1}{\mathbb{P}_{\boldsymbol{\mu}} \left\{ \left| \frac{1}{n} \log R_{\boldsymbol{\mu}}^n(X^n) - t \right| < \epsilon \right\}} \right) \leq D(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)) || \boldsymbol{\mu}),$$

which in conjunction with (140) completes the proof. \blacksquare

The parametric representation of the rate function allows us to readily deduce some of the properties of the rate function.

Theorem 4: The LDP rate function $J_{\boldsymbol{\mu}}^r(t)$ associated with the logarithm of the reverse guesswork is a concave function of t , with its first and second derivatives given by

$$\frac{d}{dt} J_{\boldsymbol{\mu}}^r(t) = \frac{1 - \alpha_{\boldsymbol{\mu}}^r(t)}{\alpha_{\boldsymbol{\mu}}^r(t)}, \quad (143)$$

$$\frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^r(t) = \frac{1}{\alpha_{\boldsymbol{\mu}}^r(t) V(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)))}. \quad (144)$$

It also satisfies the following properties:

$$\lim_{t \downarrow 0} \frac{d}{dt} J_{\boldsymbol{\mu}}^r(t) = -1, \quad (145)$$

$$\lim_{t \uparrow \log |\mathcal{X}|} \frac{d}{dt} J_{\boldsymbol{\mu}}^r(t) = -\infty, \quad (146)$$

$$\lim_{t \downarrow 0} \frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^r(t) = 0, \quad (147)$$

$$\lim_{t \uparrow \log |\mathcal{X}|} \frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^r(t) = -\infty. \quad (148)$$

Proof: To establish (143), note that since $J_{\boldsymbol{\mu}}^r(\cdot)$ could be implicitly defined as given in Theorem 3, and hence its derivative is given by the chain rule

$$\frac{d}{dt} J_{\boldsymbol{\mu}}^r(t) = \frac{d\alpha_{\boldsymbol{\mu}}^r(t)}{dt} \frac{d}{d\alpha} D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu}) \Big|_{\alpha=\alpha_{\boldsymbol{\mu}}^r(t)} \quad (149)$$

$$\begin{aligned} &= \frac{\frac{d}{d\alpha} D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu})}{\frac{d}{d\alpha} H(T(\boldsymbol{\mu}, \alpha))} \Big|_{\alpha=\alpha_{\boldsymbol{\mu}}^r(t)} \\ &= \frac{\alpha_{\boldsymbol{\mu}}^r(t) - 1}{\alpha_{\boldsymbol{\mu}}^r(t)}, \end{aligned} \quad (150)$$

where (149) follows from the chain rule, and (150) follows from the implicit function theorem implying that

$$\frac{d\alpha_{\boldsymbol{\mu}}^r(t)}{dt} = \frac{1}{\frac{d}{d\alpha} H(T(\boldsymbol{\mu}, \alpha))} \Big|_{\alpha=\alpha_{\boldsymbol{\mu}}^r(t)}. \quad (151)$$

Invoking Lemmas 11 and 13 to calculate the numerator and denominator in (150) would lead to the desired result in (143).

To establish (144), note that

$$\begin{aligned} \frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^r(t) &= \frac{d}{dt} \left\{ \frac{d}{dt} J_{\boldsymbol{\mu}}^r(t) \right\} \\ &= \frac{d}{dt} \left\{ \frac{\alpha_{\boldsymbol{\mu}}^r(t) - 1}{\alpha_{\boldsymbol{\mu}}^r(t)} \right\} \end{aligned} \quad (152)$$

$$= \frac{d\alpha_{\boldsymbol{\mu}}^r(t)}{dt} \frac{d}{d\alpha} \left\{ \frac{\alpha - 1}{\alpha} \right\} \Big|_{\alpha=\alpha_{\boldsymbol{\mu}}^r(t)} \quad (153)$$

$$\begin{aligned} &= \frac{\frac{d}{d\alpha} \frac{\alpha-1}{\alpha}}{\frac{d}{d\alpha} H(T(\boldsymbol{\mu}, \alpha))} \Big|_{\alpha=\alpha_{\boldsymbol{\mu}}^r(t)} \\ &= \frac{1}{\alpha_{\boldsymbol{\mu}}^r(t) V(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^r(t)))}, \end{aligned} \quad (154)$$

where (152) follows from (143), (153) follows from the application of the implicit function theorem in (151), and (154) follows from Lemma 11, leading to the desired result in (144).

Equations (145) and (147) are derived by noting that the limit as $t \downarrow 0$, would be equivalent to the limit as $\alpha \rightarrow -\infty$ in the parametric form. Similarly, equations (146) and (148) are derived by noting that the limit as $t \uparrow \log |\mathcal{X}|$, would be equivalent to the limit as $\alpha \uparrow 0$ in the parametric form. Finally note that the concavity of $J_{\boldsymbol{\mu}}^r(t)$ is evident as $\frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^r(t) > 0$ from (144) for all $\alpha < 0$. ■

B. Guesswork

The same proof methodology used for the logarithm of reverse guesswork leads us to establish a LDP for the logarithm of (forward) guesswork. Although this result is already proved by Christiansen and Duffy [11], we further provide the implicit characterization of the rate function of the logarithm of guesswork for all string-sources in $\mathcal{M}_{\mathcal{X}}$ using information theoretic quantities.

Theorem 5: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, the sequence $\{\frac{1}{n} g_{\boldsymbol{\mu}}^n(X^n) : n \in \mathbb{N}\}$ satisfies the large deviations principle with rate function $J_{\boldsymbol{\mu}}^g$. The rate function is implicitly given by

$$J_{\boldsymbol{\mu}}^g(t) = D(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^g(t)) || \boldsymbol{\mu}), \quad (155)$$

where

$$\alpha_{\boldsymbol{\mu}}^g(t) := \arg_{\alpha \in \mathbb{R}_{+*}} \{H(T(\boldsymbol{\mu}, \alpha)) = t\}. \quad (156)$$

Further, $J_{\boldsymbol{\mu}}^g(0) = \lim_{\alpha \rightarrow \infty} D(T(\boldsymbol{\mu}, \alpha) || \boldsymbol{\mu})$ and $J_{\boldsymbol{\mu}}^g(\log |\mathcal{X}|) = D(\mathbf{u}_{\mathcal{X}} || \boldsymbol{\mu})$, where $\mathbf{u}_{\mathcal{X}}$ is the uniform string-source on the alphabet \mathcal{X} (see (22)).

Proof: The steps of the proof are very similar to the steps of the proof of Theorem 3 except that in this case $\alpha > 0$, and we will be invoking the bounds on $G_{\boldsymbol{\mu}}^n$ in (100)–(102). We will also need to separate the $\alpha \in (0, 1)$ case and use the bounds on $\mathcal{E}_{\boldsymbol{\mu}, \alpha, \epsilon}^n$ instead of $\mathcal{D}_{\boldsymbol{\mu}, \alpha, \epsilon}^n$. ■

Next, we use Theorem 5 to establish some properties of the rate function for the logarithm of guesswork.

Theorem 6: The rate function $J_{\boldsymbol{\mu}}^g(\cdot)$ associated with the logarithm of guesswork is a convex function of its argument, and particularly its first and second derivatives are given by

$$\frac{d}{dt} J_{\boldsymbol{\mu}}^g(t) = \frac{1 - \alpha_{\boldsymbol{\mu}}^g(t)}{\alpha_{\boldsymbol{\mu}}^g(t)}, \quad (157)$$

$$\frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^g(t) = \frac{1}{\alpha_{\boldsymbol{\mu}}^g(t) V(T(\boldsymbol{\mu}, \alpha_{\boldsymbol{\mu}}^g(t)))}. \quad (158)$$

Further, the following properties are satisfied:

$$\lim_{t \downarrow 0} \frac{d}{dt} J_{\boldsymbol{\mu}}^g(t) = -1, \quad (159)$$

$$\lim_{t \uparrow \log |\mathcal{X}|} \frac{d}{dt} J_{\boldsymbol{\mu}}^g(t) = +\infty, \quad (160)$$

$$\lim_{t \downarrow 0} \frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^g(t) = 0, \quad (161)$$

$$\lim_{t \uparrow \log |\mathcal{X}|} \frac{d^2}{dt^2} J_{\boldsymbol{\mu}}^g(t) = +\infty. \quad (162)$$

Proof: The proof steps are similar to that of the proof of Theorem 4. We only point out the differences here. The limit as $t \uparrow \log |\mathcal{X}|$, would be equivalent to the limit as $\alpha \downarrow 0$ in the parametric form. The convexity of $J_{\mu}^g(t)$ is proved by noting that $\frac{d^2}{dt^2} J_{\mu}^g(t) > 0$ from (158) for all $\alpha > 0$. \blacksquare

C. Information

Next, we state a result on the large deviations of information. This result could be viewed as a generalization of the Shannon-McMillan-Breiman Theorem [41], [42] and the characterization of the exponential rate of decay for the probability of atypical strings (see [40] for a survey on the recent results on that front).

Theorem 7: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, the sequence $\{\frac{1}{n} \iota_{\mu}^n(X^n) : n \in \mathbb{N}\}$ satisfies a LDP, and the rate function is implicitly given by

$$J_{\mu}^n(t) = D(T(\mu, \alpha_{\mu}^n(t)) || \mu), \quad (163)$$

where

$$\alpha_{\mu}^n(t) = \arg_{\alpha \in \mathbb{R}} \{H(T(\mu, \alpha) || \mu) = t\}. \quad (164)$$

Proof: First notice that for any $\alpha \neq 0$ we have:

$$\begin{aligned} \left\{ x^n : \left| \frac{1}{n} \iota_{\mu}^n(x^n) - H(T(\mu, \alpha) || \mu) \right| < \epsilon \right\} &= \left\{ x^n : e^{-H^n(T(\mu, \alpha) || \mu) - n\epsilon} < \mu^n(x^n) < e^{-H^n(T(\mu, \alpha) || \mu) + n\epsilon} \right\} \\ &= \left\{ x^n : x^n \in \mathcal{A}_{\mu, \alpha, \epsilon}^n \right\}. \end{aligned} \quad (165)$$

Now, consider $\alpha_{\mu}^n(t)$ defined in (164) implying that $H(T(\mu, \alpha_{\mu}^n(t)) || \mu) = t$.

$$\begin{aligned} \mathbb{P}_{\mu} \left\{ \left| \frac{1}{n} \iota_{\mu}^n(X^n) - t \right| < \epsilon \right\} &= \mathbb{P}_{\mu} \left\{ \left| \frac{1}{n} \iota_{\mu}^n(X^n) - H(T(\mu, \alpha_{\mu}^n(t)) || \mu) \right| < \epsilon \right\} \\ &= \mathbb{P}_{\mu} \left\{ X^n \in \mathcal{A}_{\mu, \alpha_{\mu}^n(t), \epsilon}^n \right\} \end{aligned} \quad (166)$$

$$< e^{-D^n(T(\mu, \alpha_{\mu}^n(t)) || \mu) + |1 - \alpha_{\mu}^n(t)| n \epsilon}, \quad (167)$$

where (166) follows from (165), and (167) is a direct application of the upper bound in (95). Consequently,

$$\frac{1}{n} \log \left(\frac{1}{\mathbb{P}_{\mu} \left\{ \left| \frac{1}{n} \iota_{\mu}^n(X^n) - t \right| < \epsilon \right\}} \right) \geq \frac{1}{n} D^n(T(\mu, \alpha_{\mu}^n(t)) || \mu) - |1 - \alpha_{\mu}^n(t)| \epsilon.$$

Taking limits as $n \rightarrow \infty$ and letting $\epsilon \downarrow 0$ would lead to

$$\lim_{\epsilon \downarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \log \left(\frac{1}{\mathbb{P}_{\mu} \left\{ \left| \frac{1}{n} \iota_{\mu}^n(X^n) - t \right| < \epsilon \right\}} \right) \geq D(T(\mu, \alpha_{\mu}^n(t)) || \mu). \quad (168)$$

The rest of the proof entails showing that the above limit is upper bounded by $D(T(\mu, \alpha_{\mu}^n(t)) || \mu)$. We have

$$\begin{aligned} \mathbb{P}_{\mu} \left\{ \left| \frac{1}{n} \iota_{\mu}^n(X^n) - t \right| < \epsilon \right\} &= \mathbb{P}_{\mu} \left\{ X^n \in \mathcal{A}_{\mu, \alpha_{\mu}^n(t), \epsilon}^n \right\} \\ &> \left(1 - \frac{V^n(T(\mu, \alpha) || \mu)}{n^2 \epsilon^2} \right) e^{-D^n(T(\mu, \alpha_{\mu}^n(t)) || \mu) - |1 - \alpha_{\mu}^n(t)| n \epsilon}, \end{aligned} \quad (169)$$

where (169) is a direct application of the upper bound in (94). Hence, following steps similar to the previous case, we have

$$\lim_{\epsilon \downarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \log \left(\frac{1}{\mathbb{P}_{\mu} \left\{ \left| \frac{1}{n} \iota_{\mu}^n(X^n) - t \right| < \epsilon \right\}} \right) \leq D(T(\mu, \alpha_{\mu}^n(t)) || \mu).$$

which in conjunction with (168) completes the proof. \blacksquare

The above theorem on large deviations of information also lets us establish some properties of information.

Definition 24 (min(max)-cross entropy): For any $\mu \in \mathcal{M}_{\mathcal{X}}$, the min-cross entropy is defined as

$$t_{\mu}^{-} := \lim_{\alpha \rightarrow +\infty} H(T(\mu, \alpha) || \mu), \quad (170)$$

and the max-cross entropy is defined as

$$t_{\mu}^{+} := \lim_{\alpha \rightarrow -\infty} H(T(\mu, \alpha) || \mu). \quad (171)$$

Roughly speaking, the likelihood of the most likely string scales like $e^{-t_{\mu}^{-}n}$. In words, the likelihood of the most likely string scales exponentially with n and the exponent of the scaling is the negative min-cross entropy. Similarly, the likelihood of the least likely string scales as $e^{-t_{\mu}^{+}n}$. By definition, for any $x^n \in \mathcal{X}^n$, up to a multiplicative $(1 + o_n(1))$ term, we have

$$t_{\mu}^{-} \leq \frac{1}{n} \log \frac{1}{\mu^n(x^n)} \leq t_{\mu}^{+}. \quad (172)$$

Thus, the normalized negative log-likelihood is bounded between the min-cross entropy and the max-cross entropy. Equipped with this definition, we will characterize the properties of the rate function for information in the next theorem.

Theorem 8: The information rate function J_{μ}^{ν} is a convex function, and its first two derivatives are given by

$$\frac{d}{dt} J_{\mu}^{\nu}(t) = 1 - \alpha_{\mu}^{\nu}(t), \quad (173)$$

$$\frac{d^2}{dt^2} J_{\mu}^{\nu}(t) = \frac{\alpha_{\mu}^{\nu}(t)^2}{V(T(\mu, \alpha_{\mu}^{\nu}(t)))}. \quad (174)$$

Further, it satisfies the following properties:

$$\lim_{t \downarrow t_{\mu}^{-}} \frac{d}{dt} J_{\mu}^{\nu}(t) = -\infty, \quad (175)$$

$$\lim_{t \rightarrow \log |\mathcal{X}|} \frac{d}{dt} J_{\mu}^{\nu}(t) = 1, \quad (176)$$

$$\lim_{t \uparrow t_{\mu}^{+}} \frac{d}{dt} J_{\mu}^{\nu}(t) = +\infty, \quad (177)$$

$$\lim_{t \downarrow t_{\mu}^{-}} \frac{d^2}{dt^2} J_{\mu}^{\nu}(t) = +\infty, \quad (178)$$

$$\lim_{t \rightarrow \log |\mathcal{X}|} \frac{d^2}{dt^2} J_{\mu}^{\nu}(t) = \frac{1}{V(\mathbf{u}_{\mathcal{X}} \parallel \mu)}, \quad (179)$$

$$\lim_{t \uparrow t_{\mu}^{+}} \frac{d^2}{dt^2} J_{\mu}^{\nu}(t) = +\infty, \quad (180)$$

where t_{μ}^{-} and t_{μ}^{+} are the min-cross entropy and the max-cross entropy, respectively, as in Definition 24.

Proof: To establish (173), note that J_{μ}^{ν} could be implicitly defined as given in Theorem 5, and thus its derivative would be given by

$$\frac{d}{dt} J_{\mu}^{\nu}(t) = \frac{\frac{d}{d\alpha} D(T(\mu, \alpha) \parallel \mu)}{\frac{d}{d\alpha} H(T(\mu, \alpha) \parallel \mu)} \Bigg|_{\alpha=\alpha_{\mu}^{\nu}(t)}, \quad (181)$$

invoking the implicit function theorem similar to the proof of Theorem 4. Invoking Lemmas 12 and 13 to calculate the numerator and denominator in (181) would lead to (173).

To establish (174), note that applying the implicit function theorem we get

$$\frac{d^2}{dt^2} J_{\mu}^{\nu}(t) = \frac{d}{dt} \frac{d}{dt} J_{\mu}^{\nu}(t) = \frac{\frac{d}{d\alpha} (1 - \alpha)}{\frac{d}{d\alpha} H(T(\mu, \alpha) \parallel \mu)} \Bigg|_{\alpha=\alpha_{\mu}^{\nu}(t)}. \quad (182)$$

The desired result is obtained by applying Lemma 12 to the denominator of (182).

The rest of the properties are established by noting the definition of t_{μ}^{-} and t_{μ}^{+} in Definition 24 and considering the limits as $\alpha \rightarrow +\infty$ and $\alpha \rightarrow -\infty$, respectively. ■

VI. APPROXIMATION OF THE PROBABILITY MASS FUNCTION OF GUESSWORK

Thus far, we provided some results on the asymptotic scaling of guesswork. In this section, we would like to provide more practical results that would be applicable for small sequences in practice. Inspired from the characterization of guesswork using the tilt, we provide an approximation formula that is accurate even when the length n is small. Our justification mostly relies on Theorem 2 where we employ additional insights to compensate the impact of the finite sequence length. The main contribution of this section is the following set of approximation formulas.

Approximation 1: For any $\mu \in \mathcal{M}_{\mathcal{X}}$, the size of the tilted weakly typical set of order $\alpha \neq 0$ can be approximated by:

$$|\mathcal{A}_{\mu, \alpha, \epsilon}^n| \approx \frac{1 - e^{-2\alpha n \epsilon}}{\sqrt{2\pi V^n(T(\mu, \alpha))}} e^{H^n(T(\mu, \alpha)) + \alpha n \epsilon} \quad (183)$$

Approximation 2: For any $\boldsymbol{\mu} \in \mathcal{M}_{\mathcal{X}}$, and for any x^n such that $\mu^n(x^n) = e^{-H^n(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu})}$ for some $\alpha \in \mathbb{R}_{+*}$, we can approximately express its guesswork as

$$G_{\boldsymbol{\mu}}^n(x^n) \approx \frac{e^{H^n(T(\boldsymbol{\mu}, \alpha))}}{\sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha))} + \sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha)) + 4}}. \quad (184)$$

Furthermore, for any x^n such that $\mu^n(x^n) = e^{-H^n(T(\boldsymbol{\mu}, \alpha) \|\boldsymbol{\mu})}$ for some $\alpha \in \mathbb{R}_{-*}$, the reverse guesswork is approximately given by

$$R_{\boldsymbol{\mu}}^n(x^n) \approx \frac{e^{H^n(T(\boldsymbol{\mu}, \alpha))}}{\sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha))} + \sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha)) + 4}}. \quad (185)$$

Alternatively, guesswork can be approximated by

$$\begin{aligned} G_{\boldsymbol{\mu}}^n(x^n) &= |\mathcal{X}|^n - R_{\boldsymbol{\mu}}^n(x^n) \\ &\approx |\mathcal{X}|^n - \frac{e^{H^n(T(\boldsymbol{\mu}, \alpha))}}{\sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha))} + \sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha)) + 4}}. \end{aligned} \quad (186)$$

Finally, for any x^n such that $\mu^n(x^n) = e^{-H^n(u_{\mathcal{X}} \|\boldsymbol{\mu})}$, the guesswork would be approximated as

$$G_{\boldsymbol{\mu}}^n(x^n) \approx \frac{1}{2} |\mathcal{X}|^n. \quad (187)$$

Justification: We have

$$G_{\boldsymbol{\mu}}^n(x^n) \approx \int_0^{\infty} \frac{1}{\sqrt{2\pi V^n(T(\boldsymbol{\mu}, \alpha))}} e^{H^n(T(\boldsymbol{\mu}, \alpha)) - t - \frac{1}{2V^n(T(\boldsymbol{\mu}, \alpha))} t^2} dt \quad (188)$$

$$= \frac{1}{2} \exp\left(\frac{1}{2}V^n(T(\boldsymbol{\mu}, \alpha))\right) \operatorname{erfc}\left(\sqrt{\frac{1}{2}V^n(T(\boldsymbol{\mu}, \alpha))}\right) \exp(H^n(T(\boldsymbol{\mu}, \alpha))) \quad (189)$$

$$\approx \frac{e^{H^n(T(\boldsymbol{\mu}, \alpha))}}{\sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha))} + \sqrt{\frac{\pi}{2}V^n(T(\boldsymbol{\mu}, \alpha)) + 4}}, \quad (190)$$

where (188) follows because of the Laplace's method, (189) follows the definition of $\operatorname{erfc}(\cdot)$, and (190) follows by applying the lower bound in [43]. \blacksquare

In the rest of this section, we provide numerical examples to show the effectiveness of the approximation formulas in Approximation 2. We will also plot their asymptotic properties, such as the large deviations performance of the logarithm of guesswork using the formulas derived in the previous sections. To this end, we formally define the four string-sources that will be used in the numerical experiments. The subscript in the following definitions denotes the alphabet size.

The first example is a binary string-source.

Definition 25 (string-source S_8): Let S_2 refer to a Bernoulli source on alphabet on a binary alphabet with parameter vector (categorical distribution) $\theta = (0.2, 0.8)$. We will use the notation $S_{2,n}$ to denote a source with output of length n .

The next string-source is the ternary memoryless source used as the working example throughout the paper.

Definition 26 (string-source S_3): Let S_3 refer to a memoryless string-source alphabet $\mathcal{X} = \{a, b, c\}$ of size $|\mathcal{X}| = 3$ with parameter vector (categorical distribution) $\theta = (0.2, 0.3, 0.5)$.

Our last working example is a 77-ary source that is inspired from the true distribution of characters in password databases.

Definition 27 (string-source S_{77}): Let S_{77} refer to a memoryless string-source alphabet size $|\mathcal{X}| = 77$ where the parameter vector (categorical distribution) is inspired from the empirical distribution of characters in passwords from [44].

We let X^n be a random string of length n that will be drawn from the string-source S_i where i will be clear from the context. The approximations of the probability are plotted in Fig. 2, where we have chosen the sequence length to be $n = 8$. As can be seen the approximations in (184) and (186) collectively approximate well the distribution of guesswork for different string-sources with very good accuracy even for small sequence lengths. Note that it is straightforward to calculate the formulas provided in Approximation 2 for any memoryless process by sweeping α over the real line.

In Fig. 3, we further plot the rate functions $J_{\boldsymbol{\mu}}^g$, $J_{\boldsymbol{\mu}}^r$, and $J_{\boldsymbol{\mu}}^l$ for string-sources S_2 , S_3 , and S_{77} . As can be seen, $J_{\boldsymbol{\mu}}^g(t)$ and $J_{\boldsymbol{\mu}}^l(t)$ are convex functions of t whereas $J_{\boldsymbol{\mu}}^r(t)$ is a concave function of t (as has already been proved). The rest of the properties of the rate functions could also be verified numerically and are observable from the plots.

VII. CONCLUDING REMARKS AND FUTURE WORK

Guesswork is an important element of information theory that is intimately related to famous problems in information theory, such as the distribution of the length of one-shot source coding, the computational complexity of sequential decoding, the probability of error in list decoding, and the quantification of computational security against brute-force attacks. In this paper, we defined the tilt operation, leading to derivation of tight bounds and accurate approximations to the distribution, and

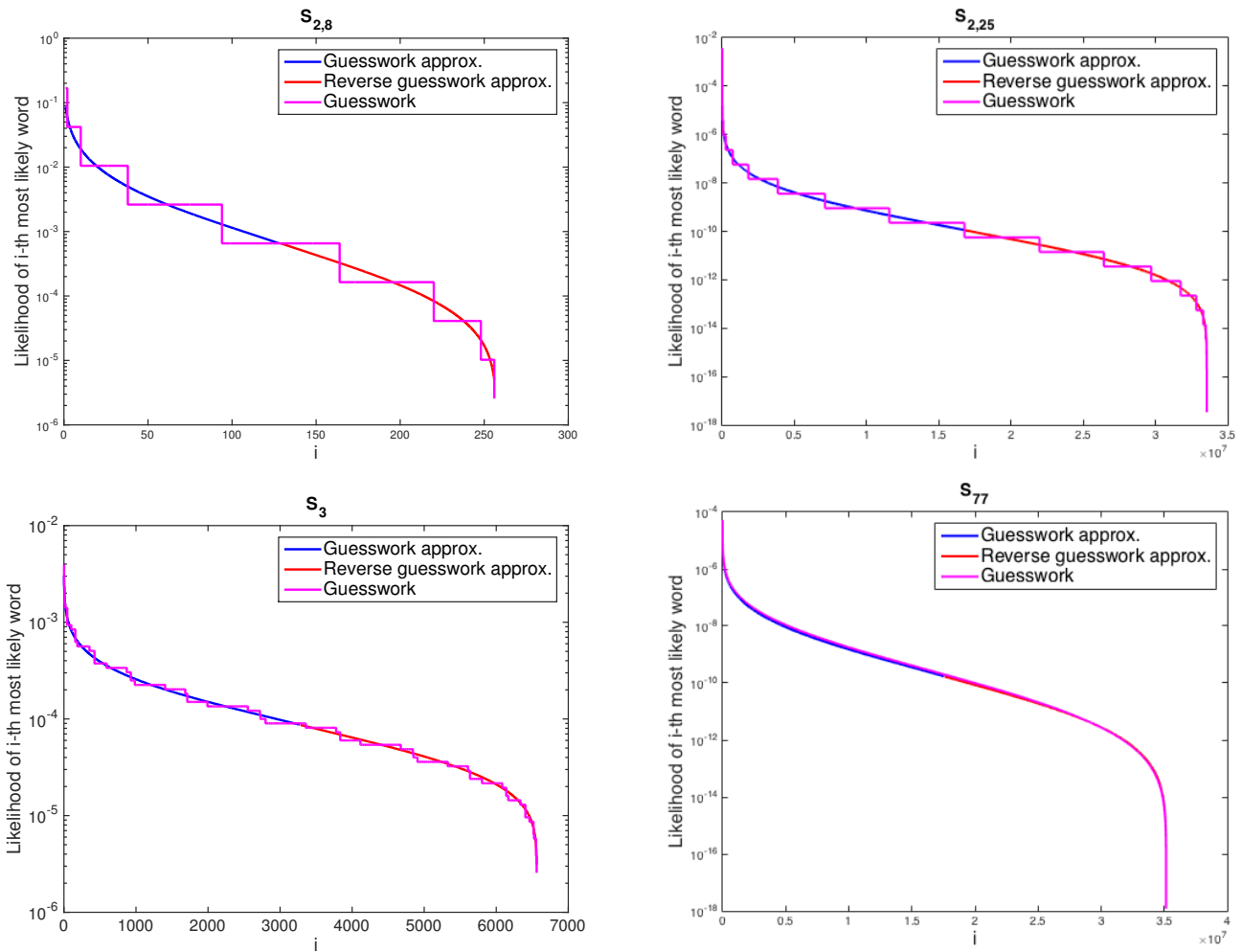


Fig. 2: The approximation on the distribution of the guesswork for string-sources S_2 , S_3 , and S_{77} . Note that $S_{2,8}$ denotes strings of length $n = 8$ and $S_{2,25}$ denotes strings of length $n = 25$. The string length for S_3 and S_{77} are chosen to be $n = 8$ and $n = 4$ respectively. The pink curve represents the probability mass function of guesswork on the $|\mathcal{X}|^n$ strings; the blue curve is the approximation derived from the forward path in (184); and the red curve is the approximation derived from the reverse path in (186).

the large deviations behavior of guesswork. Using the tilt operation, we characterized the tilted family of a string-source and established several main properties of the tilted family. In particular, we showed that the set of all string-sources that result in the same ordering of all strings from the most likely to the least likely coincides with the tilted family of the string-source. We also used the tilted family of the string-source to characterize the large deviations behavior of the logarithm of forward/reverse guesswork and information. Finally, we provided an approximation formula for the PMF of guesswork and established its effectiveness using several numerical examples.

While this paper was focused on memoryless string-sources, future work would naturally consider a richer set of stationary ergodic string-sources, such as Markov or hidden Markov processes, or other mixing processes. This research direction appears promising, as empirically comparing actual distributions and the approximations that are obtained by applying our approximation formulas to Markov or hidden Markov string-sources yield excellent concordance. To illustrate this point, let us define two string-sources as follows.

Definition 28 (string-source S_3^M): Let S_3^M refer to a first order Markov source on alphabet $\mathcal{X} = \{a, b, c\}$ of size $|\mathcal{X}| = 3$ with transition matrix T_3^M given by

$$T_3^M = \begin{pmatrix} 0.7 & 0.1 & 0.2 \\ 0.2 & 0.3 & 0.5 \\ 0.3 & 0.6 & 0.1 \end{pmatrix},$$

and where the initial distribution is chosen to be the stationary distribution of the chain.

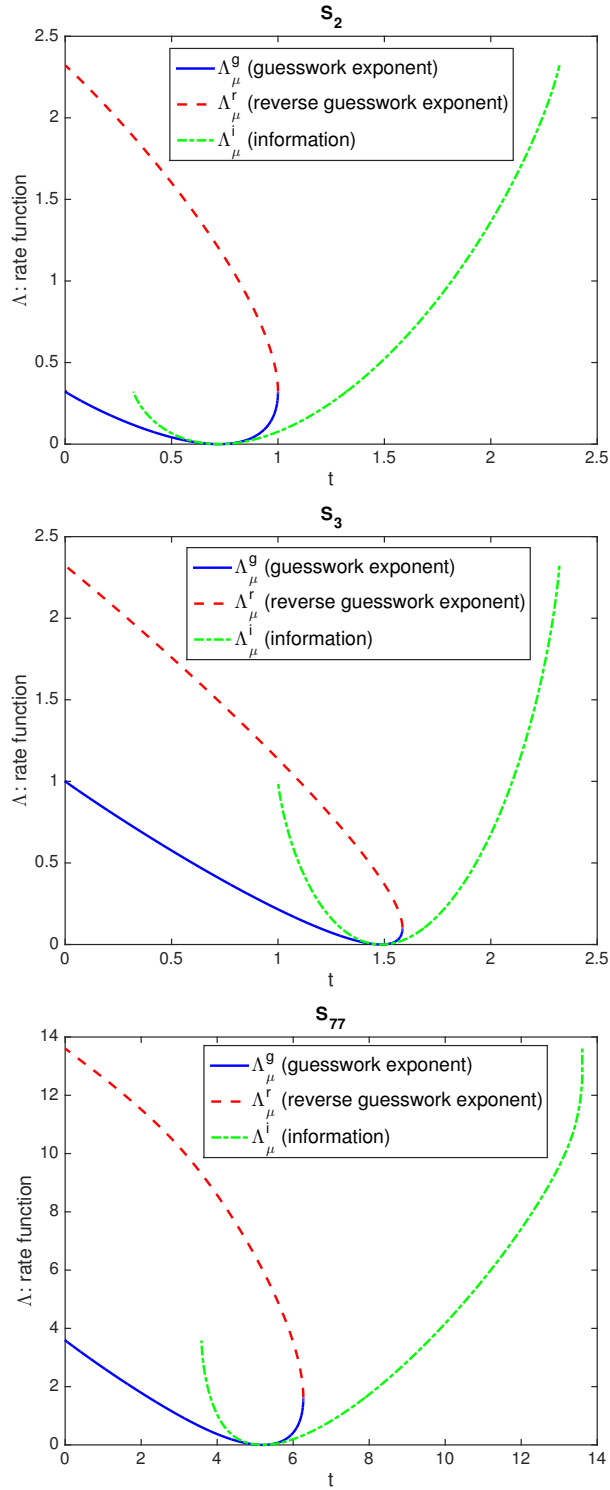


Fig. 3: The LDP rate function for S_2 , S_3 , and S_{77} . The solid blue curve represents J_μ^g ; the dashed red curve represents J_μ^r ; and the dotted green curve represents J_μ^i .

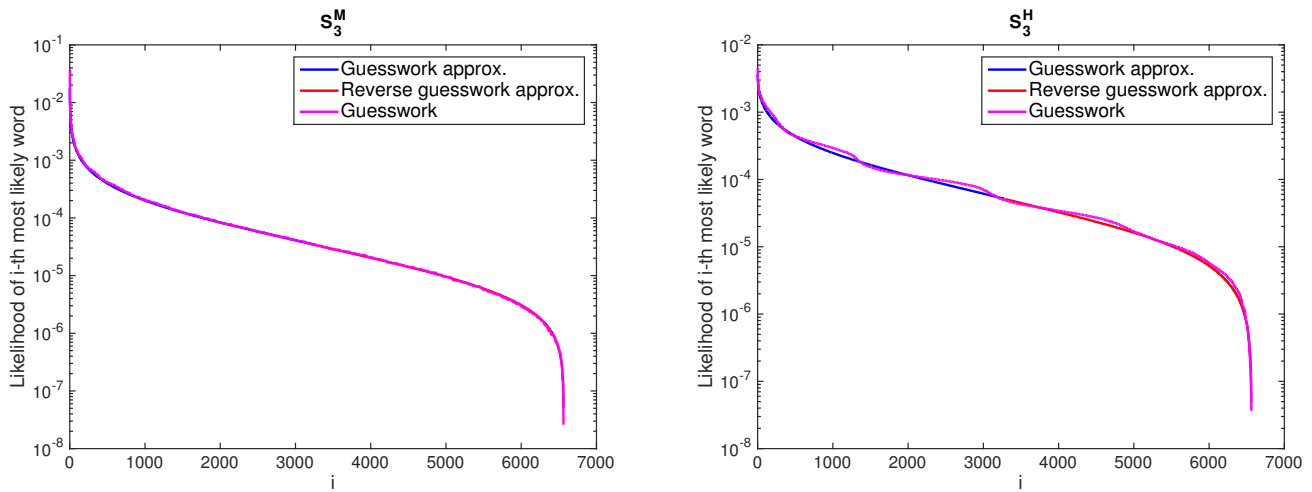


Fig. 4: The approximation on the distribution of the guesswork for string-sources S_3^M and S_3^H . The string length is $n = 8$. The pink staircase represents the probability mass function of guesswork on the 3^8 strings; the blue curve is the approximation derived from the forward path in (184); and the red curve is the approximation derived from the reverse path in (186).

Definition 29 (string-source S_3^H): Let S_3^H refer to a hidden Markov string-source on alphabet $\mathcal{X} = \{a, b, c\}$ of size $|\mathcal{X}| = 3$ with hidden states d and e , with 2×2 transition matrix T_3^H given by

$$T_3^H = \begin{pmatrix} 0.8 & 0.2 \\ 0.4 & 0.6 \end{pmatrix}$$

and the emission probabilities are grouped in the matrix E_3^H below.

$$E_3^H = \begin{pmatrix} 0.1 & 0.3 & 0.6 \\ 0.2 & 0.6 & 0.2 \end{pmatrix}.$$

In Fig. 4, we use the formulas (184) and (186) to provide an approximation on the distribution of guesswork. Note that in this case we have used the entropy and varentropy of the words rather than the rates in order to obtain the approximation. We observe that the formulas provide accurate approximations on the distribution of guesswork even for a hidden Markov source with infinite memory, and we conclude that the generalizing techniques developed in this paper is a direction for further work that is solidly motivated by empirical evidence. Moreover, from a heuristic perspective, our guesswork approximation techniques may provide some indicative information regarding guesswork for more sources beyond memoryless string-sources, even though the analysis currently does not provide guarantees.

ACKNOWLEDGEMENT

The authors are thankful to Erdal Arkan (Bilkent University) for informative discussions about guesswork and sequential decoding, Andrew Barron (Yale University) for discussions that led to the improvement of the approximations in the small sequence length regime, Mokshay Madiman (University of Delaware) for discussions on the connections with the Shannon-McMillan-Breiman Theorem, Ali Makhdoumi (Duke University) for several discussions about the properties of exponential families and careful reading of an earlier version of this paper, and Jossy Sayir (University of Cambridge) for suggesting the symmetric plotting of the probability simplex on an equilateral triangle.

REFERENCES

- [1] A. Beirami, R. Calderbank, M. Christiansen, K. Duffy, A. Makhdoumi, and M. Médard, "A geometric perspective on guesswork," in *53rd Annual Allerton Conference (Allerton)*, Oct. 2015.
- [2] I. Jacobs and E. Berlekamp, "A lower bound to the distribution of computation for sequential decoding," *IEEE Trans. Inf. Theory*, vol. 13, no. 2, pp. 167–174, April 1967.
- [3] J. L. Massey, "Guessing and entropy," in *1994 IEEE International Symposium on Information Theory Proceedings*, 1994, p. 204.
- [4] E. Arkan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 99–105, Jan. 1996.
- [5] D. Malone and W. G. Sullivan, "Guesswork and entropy," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 525–526, Mar. 2004.
- [6] C. E. Pfister and W. G. Sullivan, "Renyi entropy, guesswork moments, and large deviations," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2794–2800, Nov. 2004.
- [7] I. Sason and S. Verdú, "Improved bounds on lossless source coding and guessing moments via rényi measures," *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4323–4346, 2018.
- [8] E. Arkan and N. Merhav, "Guessing subject to distortion," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1041–1056, May 1998.
- [9] A. Beirami, R. Calderbank, K. Duffy, and M. Médard, "Quantifying computational security subject to source constraints, guesswork and inscrutability," in *2015 IEEE International Symposium on Information Theory Proceedings (ISIT)*, Jun. 2015.

- [10] M. K. Hanawal and R. Sundaresan, "Guessing revisited: A large deviations approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 70–78, Jan. 2011.
- [11] M. M. Christiansen and K. R. Duffy, "Guesswork, large deviations, and Shannon entropy," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 796–802, Feb. 2013.
- [12] K. R. Duffy, J. Li, and M. Médard, "Guessing noise, not code-words," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 671–675.
- [13] P. Elias, *List decoding for noisy channels*, 1957.
- [14] —, "Error-correcting codes for list decoding," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 5–12, 1991.
- [15] M. Sudan, "List decoding: Algorithms and applications," in *Theoretical Computer Science: Exploring New Frontiers of Theoretical Informatics*. Springer, 2000, pp. 25–41.
- [16] R. G. Gallager, *Information theory and reliable communication*. Springer, 1968, vol. 2.
- [17] N. Merhav, "List decoding—Random coding exponents and expurgated exponents," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6749–6759, 2014.
- [18] M. Christiansen, K. Duffy, F. du Pin Calmon, and M. Médard, "Multi-user guesswork and brute force security," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6876–6886, Dec 2015.
- [19] M. M. Christiansen, K. R. Duffy, F. du Pin Calmon, and M. Médard, "Brute force searching, the typical set and guesswork," in *2013 IEEE International Symposium on Information Theory Proceedings (ISIT)*, July 2013, pp. 1257–1261.
- [20] —, "Guessing a password over a wireless channel (on the effect of noise non-uniformity)," in *2013 Asilomar Conference on Signals, Systems and Computers*, 2013, pp. 51–55.
- [21] R. Sundaresan, "Guessing under source uncertainty," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 269–287, Jan. 2007.
- [22] O. Kosut and L. Sankar, "Asymptotics and non-asymptotics for universal fixed-to-variable source coding," *arXiv preprint arXiv:1412.4444*, 2014.
- [23] A. D. Wyner, "An upper bound on the entropy series," *Information and Control*, vol. 20, no. 2, pp. 176–181, 1972.
- [24] N. Alon and A. Orlitsky, "A lower bound on the expected length of one-to-one codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1670–1672, Sept. 1994.
- [25] T. Courtade and S. Verdú, "Cumulant generating function of codeword lengths in optimal lossless compression," in *2014 IEEE International Symposium on Information Theory (ISIT)*, July 2014, pp. 2494–2498.
- [26] W. Szpankowski, "A one-to-one code and its anti-redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4762–4766, Oct. 2008.
- [27] W. Szpankowski and S. Verdú, "Minimum expected length of fixed-to-variable lossless compression without prefix constraints," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4017–4025, Jul. 2011.
- [28] I. Kontoyiannis and S. Verdú, "Optimal lossless data compression: Non-asymptotics and asymptotics," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 777–795, Feb. 2014.
- [29] A. Beirami and F. Fekri, "Fundamental limits of universal lossless one-to-one compression of parametric sources," in *2014 IEEE Information Theory Workshop (ITW '14)*, Nov. 2014, pp. 212–216.
- [30] V. Strassen, "Asymptotische abschätzungen in shannons informations theorie," in *Trans. Third Prague Conf. Inf. Theory*, 1962, pp. 689–723.
- [31] A. Rényi, "On measures of entropy and information," in *Fourth Berkeley Symposium in Mathematical Statistics*, 1961.
- [32] I. Csiszár and P. C. Shields, *Information theory and statistics: A tutorial*. Now Publishers Inc, 2004.
- [33] S. Borade and L. Zheng, "I-projection and the geometry of error exponents," in *Proceedings of the Forty-Fourth Annual Allerton Conference on Communication, Control, and Computing*, Sept 27-29, 2006.
- [34] J. Huang, C. Pandit, S. Meyn, M. Médard, and V. Veeravalli, "Entropy, inference, and channel coding," in *Wireless Communications*. Springer, 2007, pp. 99–124.
- [35] A. R. Barron and T. M. Cover, "Minimum complexity density estimation," *IEEE Trans. Inf. Theory*, vol. 37, no. 4, pp. 1034–1054, Jul. 1991.
- [36] B. Clarke and A. Barron, "Information-theoretic asymptotics of Bayes methods," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 453–471, May 1990.
- [37] A. Dembo and O. Zeitouni, *Large deviations techniques and applications*. Springer Science & Business Media, 2009, vol. 38.
- [38] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley and Sons, 2006.
- [39] S. Bobkov and M. Madiman, "Concentration of the information in data with log-concave distributions," *The Annals of Probability*, vol. 39, no. 4, pp. 1528–1543, 2011.
- [40] S. Bobkov and M. M. Madiman, "An equipartition property for high-dimensional log-concave distributions," in *Allerton Conference*, 2012, pp. 482–488.
- [41] D. Ornstein and B. Weiss, "Entropy and data compression schemes," *IEEE Trans. Inf. Theory*, vol. 39, no. 1, pp. 78–83, Jan. 1993.
- [42] A. R. Barron, "The strong ergodic theorem for densities: generalized Shannon-McMillan-Breiman theorem," *The Annals of Probability*, pp. 1292–1303, 1985.
- [43] F. R. Kschischang, "The complementary error function," [Online, April 2017] <https://www.comm.utoronto.ca/frank/notes/erfc.pdf>.
- [44] "Character occurrence in passwords," [Online, June 2011] <https://csgillespie.wordpress.com/2011/06/16/character-occurrence-in-passwords>.

Ahmad Bierami is a research scientist at Electronic Arts Digital Platform – Data & AI, leading fundamental research and development on training AI agents in multi-agent systems. His research interests broadly include AI, machine learning, statistics, information theory, and networks. Prior to joining EA in 2018, he held postdoctoral fellow positions at Duke, MIT, and Harvard. He received the BS degree in 2007 from Sharif University of Technology, Iran, and the PhD degree in 2014 from the Georgia Institute of Technology, in electrical and computer engineering. He is the recipient of the 2015 Sigma Xi Best PhD Thesis Award from Georgia Tech.

Robert Calderbank (M'89–SM'97–F'98) received the BSc degree in 1975 from Warwick University, England, the MSc degree in 1976 from Oxford University, England, and the PhD degree in 1980 from the California Institute of Technology, all in mathematics.

Dr. Calderbank is Professor of Electrical and Computer Engineering at Duke University where he directs the Information Initiative at Duke (iiD). Prior to joining Duke in 2010, Dr. Calderbank was Professor of Electrical Engineering and Mathematics at Princeton University where he directed the Program in Applied and Computational Mathematics. Prior to joining Princeton in 2004, he was Vice President for Research at AT&T, responsible for directing the first industrial research lab in the world where the primary focus is data at scale. At the start of his career at Bell Labs, innovations by Dr. Calderbank were incorporated in a progression of voiceband modem standards that moved communications practice close to the Shannon limit. Together with Peter Shor and colleagues at AT&T Labs he developed the mathematical framework for quantum error correction. He is a co-inventor of space-time codes for wireless communication, where correlation of signals across different transmit antennas is the key to reliable transmission.

Dr. Calderbank served as Editor in Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY from 1995 to 1998, and as Associate Editor for Coding Techniques from 1986 to 1989. He was a member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and from 2006 to 2008. Dr. Calderbank was honored by the IEEE Information Theory Prize Paper Award in 1995 for his work on the Z4 linearity of Kerdock and Preparata Codes (joint with A.R. Hammons Jr., P.V. Kumar, N.J.A. Sloane, and P. Sole), and again in 1999 for the invention of space-time codes (joint with V. Tarokh and N. Seshadri). He has received the 2006 IEEE Donald G. Fink Prize Paper Award, the IEEE Millennium Medal, the 2013 IEEE Richard W. Hamming Medal, and the 2015 Shannon Award. He was elected to the US National Academy of Engineering in 2005.

Mark M. Christiansen is an assistant manager in the quantitative risk team in Grant Thornton. He received his B.A. (mod) in mathematics from Trinity College Dublin and his PhD in mathematics at Hamilton Institute in Maynooth. His interests include Probability Theory, Information Theory and their use in finance and security.

Ken R. Duffy is a Professor at Maynooth University where he is currently the Director of the Hamilton Institute. He received the B.A.(mod) and Ph.D. degrees in mathematics from the Trinity College Dublin. His primary research interests are in probability and statistics, and their applications in science and engineering.

Muriel Médard is the Cecil H. Green Professor in the Electrical Engineering and Computer Science (EECS) Department at MIT and leads the Network Coding and Reliable Communications Group at the Research Laboratory for Electronics at MIT. She has co-founded three companies to commercialize network coding, CodeOn, Steinwurf and Chocolate Cloud. She has served as editor for many publications of the Institute of Electrical and Electronics Engineers (IEEE), of which she was elected Fellow, and she has served as Editor in Chief of the IEEE Journal on Selected Areas in Communications. She was President of the IEEE Information Theory Society in 2012, and served on its board of governors for eleven years. She has served as technical program committee co-chair of many of the major conferences in information theory, communications and networking. She received the 2009 IEEE Communication Society and Information Theory Society Joint Paper Award, the 2009 William R. Bennett Prize in the Field of Communications Networking, the 2002 IEEE Leon K. Kirchmayer Prize Paper Award, the 2018 ACM SIGCOMM Test of Time Paper Award and several conference paper awards. She was co-winner of the MIT 2004 Harold E. Edgerton Faculty Achievement Award, received the 2013 EECS Graduate Student Association Mentor Award and served as Housemaster for seven years. In 2007 she was named a Gilbreth Lecturer by the U.S. National Academy of Engineering. She received the 2016 IEEE Vehicular Technology James Evans Avant Garde Award, the 2017 Aaron Wyner Distinguished Service Award from the IEEE Information Theory Society and the 2017 IEEE Communications Society Edwin Howard Armstrong Achievement Award.