Non-Asymptotic and Asymptotic Fundamental Limits of Guessing Subject to Distortion

Shota Saito and Toshiyasu Matsushima
Department of Applied Mathematics, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo, 169-8555 JAPAN
E-mail: shota@aoni.waseda.jp and toshimat@waseda.jp

Abstract—This paper considers the problem of guessing random variables subject to distortion. We investigate both non-asymptotic and asymptotic fundamental limits of the minimum \( t \)-th moment of the number of guesses. These fundamental limits are characterized by the quantity related to the Rényi entropy.

To derive the non-asymptotic bounds, we use our techniques developed in lossy compression. Moreover, using the results obtained in the non-asymptotic setting, we derive the asymptotic result and show that it coincides with the previous result by Arikan and Merhav.

I. INTRODUCTION

The problem of guessing random variables is one of the research topics in information theory. This problem has been investigated in various contexts (e.g., [1] – [8], [12], [13] – [15]). Among them, we investigate the problem of guessing subject to distortion, which was studied by Arikan and Merhav [2].

Although we describe the formal setup in Section II, in this section, we explain this problem as the following two player game. First, Bob draws a sample \( x \in \mathcal{X} \) from a random variable \( X \sim P_X \), where \( \mathcal{X} \) is a finite set called a source alphabet. Next, Alice, who does not see \( x \) but want to guess it at least approximately, shows Bob a fixed sequence of guesses \( \hat{x}(1), \hat{x}(2), \cdots \), where \( \hat{x}(i) \in \hat{\mathcal{X}} \) and \( \hat{\mathcal{X}} \) is a finite set called a reproduction alphabet. Then, Bob checks the guessed successively until he finds a guess \( \hat{x}(i) \) such that \( d(\hat{x}, \hat{x}(i)) \leq D \) for some distortion measure \( d : \mathcal{X} \times \hat{\mathcal{X}} \to [0, \infty) \) and distortion level \( D \). After that, Bob tells Alice \( \hat{x}(i) \) and Alice pays Bob an amount \( G(x) = i \), which is equal to the number of guesses checked by Bob. In this game, a natural question is

What is the best strategy for Alice in designing a guessing \( \hat{x}(1), \hat{x}(2), \cdots \) in order to minimize the expected number of guesses \( \mathbb{E}[G(X)] \), or more generally, the \( t \)-th moment of the number of guesses \( \mathbb{E}[G(X)^t] \), where \( t > 0 \).

For this question, Arikan and Merhav [2] gave an answer in the asymptotic sense when a source distribution \( P_X \) is stationary and memoryless. That is, for a source sequence \( x^n = x_1x_2 \cdots x_n \), they characterized the asymptotic fundamental limit of the minimum \( t \)-th moment of the number of guesses under a stationary memoryless source.

This paper considers the same problem discussed in [2], but the main differences are

1) we analyze both non-asymptotic and asymptotic cases, while primary concern in [2] is the asymptotic analysis;
2) we characterize the fundamental limit of the minimum \( t \)-th moment of the number of guesses by using the quantity related to the Rényi entropy; whereas previous study [2] has characterized it by using the quantity related to the relative entropy.

To derive the non-asymptotic bounds on the minimum \( t \)-th moment of the number of guesses, we use our techniques in lossy compression [11]; to prove the achievability result, we show the explicit construction of guesses based on the distortion \( D \)-ball around \( \hat{x} \), which is similar technique to prove the achievability result in [11]; to prove the converse result, we also utilize the result obtained in [11]. Furthermore, using the results obtained in the non-asymptotic setting, we derive the asymptotic results on the minimum \( t \)-th moment of the number of guesses. It is shown that this result coincides with the result in [2].

The organization of this paper is as follows. Section II formulates the problem setup. Section III describes the related work by Arikan and Merhav [2]. Sections IV shows the main results of this paper. In Section IV, we first define a quantity based on the Rényi entropy. Then, using this quantity, we show non-asymptotic upper and lower bounds of the fundamental limit of the minimum \( t \)-th moment of the number of guesses. Moreover, we establish an asymptotic result from the non-asymptotic results. Proofs of the main results are in Section V.

II. PROBLEM FORMULATION

Let \( \mathcal{X} \) be a source alphabet and \( \hat{\mathcal{X}} \) be a reproduction alphabet, where both are finite sets. Let \( X \) be a random variable taking a value in \( \mathcal{X} \) and \( x \) be a realization of \( X \). The probability distribution of \( X \) is denoted as \( P_X \). A distortion measure \( d \) is defined as \( d : \mathcal{X} \times \hat{\mathcal{X}} \rightarrow [0, +\infty) \). As in the previous study [2], we assume that for ever \( x \in \mathcal{X} \), there exists \( \hat{x} \in \hat{\mathcal{X}} \) such that \( d(\hat{x}, \hat{x}) = 0 \).

A \( D \)-admissible guessing strategy is defined as follows.

Definition 1: For \( D \geq 0 \), a \( D \)-admissible guessing strategy with respect to \( P_X \) is an ordered list

\[
\mathcal{G} = \{ \hat{x}(1), \hat{x}(2), \cdots \}
\]
of elements in \( \hat{X} \) such that
\[
P[\hat{d}(X, \hat{x}(j)) \leq D \text{ for some } j] = 1. \tag{2}
\]
By a D-admissible guessing strategy, a guessing function is induced. Its definition is as follows.

**Definition 2:** The guessing function \( G : X \to \mathbb{N} \) induced by a D-admissible guessing strategy \( G \) is the function that maps each \( x \in X \) into a natural number, which is the index \( j \) of the first element \( \hat{x}(j) \in G \) such that \( d(x, \hat{x}(j)) \leq D \).

The quantity that we investigate is the \( t \)-th moment of the number of guesses for a given parameter \( t > 0 \):
\[
\frac{1}{t} \log \mathbb{E}[G(X)^t],
\tag{3}
\]
where all logarithms are of base 2 throughout this paper.

When we consider the setup of blocklength \( n \), we formulate the problem as follows. Let \( X^n \) and \( X^n \) be the \( n \)-th Cartesian product of \( X \) and \( \hat{X} \), respectively. Let \( X^n \) be a random variable taking a value in \( X^n \) and \( x^n \) be a realization of \( X^n \). The probability distribution of \( X^n \) is denoted as \( P_{X^n} \). A distortion measure \( d_n : X^n \times X^n \to [0, +\infty) \) is separable, i.e.,
\[
d_n(x^n, \hat{x}^n) = \sum_{i=1}^{n} d(x_i, \hat{x}_i). \tag{4}
\]
For blocklength \( n \), a D-admissible guessing strategy with respect to \( P_{X^n} \) is denoted as \( \mathcal{G}_n \) and a guessing function is denoted as \( G_n(\cdot) \).

### III. Previous Study

Let \( R(D, P_X) \) be the rate-distortion function, i.e.,
\[
R(D, P_X) := \inf_{P_{X|\hat{X}^n} : \mathbb{E}[d(X, \hat{X})] \leq D} I(X; \hat{X}), \tag{5}
\]
where \( I(X; \hat{X}) \) denotes the mutual information between \( X \) and \( \hat{X} \). Also, let \( D(Q_X, P_X) \) be the relative entropy between two probability distributions \( P_X \) and \( Q_X \) on \( X \). Using these quantities, Arikan and Merhav [2] characterized the asymptotic fundamental limit of the \( t \)-th moment of the number of guesses as shown in the next theorem.

**Theorem 1 ([2]):** Suppose that the distortion measure satisfy \( \mathcal{G} \) and a source is stationary and memoryless. Then, for any \( D \geq 0 \) and \( t > 0 \), it holds that
\[
\lim_{n \to \infty} \frac{1}{n t} \min_{G_n} \mathbb{E}[G_n(X^n)^t] = \max_{Q_X} \left( R(D, Q_X) - \frac{1}{n} D(Q_X||P_X) \right), \tag{6}
\]
where the maximum is taken over all probability distribution \( Q_X \) on \( X \). Further, when we consider the special case \( \lim_{t \to 0} \), we have
\[
\lim_{n \to \infty} \frac{1}{n t} \min_{G_n} \mathbb{E}[G_n(X^n)^t] = R(D, P_X). \tag{7}
\]

### IV. Main Results

Before showing our main results, we first review the definition of the Rényi entropy and introduce the quantity based on the Rényi entropy. For \( \alpha \in (0, 1) \cup (1, \infty) \), the Rényi entropy is defined as
\[
H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_{x \in X} [P_X(x)]^\alpha. \tag{8}
\]
Next, we introduce a new quantity based on the Rényi entropy. This quantity plays an important role in producing our main results.

**Definition 3:** For \( D \geq 0 \) and \( \alpha \in (0, 1) \cup (1, \infty) \), \( H^D_\alpha(X) \) is defined as
\[
H^D_\alpha(X) = \inf_{P_{X|\hat{X}^n}} H_\alpha(\hat{X}) \tag{9}
\]
where \( \hat{G}^*(\cdot) \) is the guessing function induced by \( \mathcal{G}^* \).

**Proof:** See Section V-A.

The next theorem shows the converse bound.

**Theorem 2:** Let \( \mathcal{G} \) be an arbitrary D-admissible guessing strategy. Then, for any \( D \geq 0 \) and \( t > 0 \), we have
\[
\frac{1}{t} \log \mathbb{E}[G^*(X)^t] \leq H^D_\alpha(\hat{X}) + 1, \tag{10}
\]
where \( G^*(\cdot) \) is the guessing function induced by \( \mathcal{G}^* \).

**Proof:** See Section V-B.

We can immediately obtain the next corollaries by using the same discussion which is used to prove Theorems 2 and 3.

**Corollary 1:** For any \( D \geq 0, t > 0 \), and blocklength \( n \in \mathbb{N} \), there exists a D-admissible guessing strategy \( \mathcal{G}^*_n \) such that
\[
\frac{1}{n t} \log \mathbb{E}[G^*_n(X^n)^t] \leq \frac{1}{n} H^D_\alpha(\hat{X}) + \frac{1}{n}, \tag{12}
\]
where \( G^*_n(\cdot) \) is the guessing function induced by \( \mathcal{G}^*_n \).

**Corollary 2:** Let \( \mathcal{G}^*_n \) be an arbitrary D-admissible guessing strategy. Then, for any \( D \geq 0, t > 0 \), and blocklength \( n \in \mathbb{N} \), we have
\[
\frac{1}{n t} \log \mathbb{E}[G_n(X^n)^t] \geq \frac{1}{n} H^D_\alpha(\hat{X}) - \frac{1}{n} \log \log(1 + \min\{|X^n|, |\hat{X}^n|\}). \tag{13}
\]

**Proof:** See Section V-B.

The next theorem yields the next theorem, which coincides the previous result.

**Theorem 4:** Suppose that the distortion measure satisfy \( \mathcal{G} \) and a source is stationary and memoryless. Then, for any \( D \geq 0 \) and \( t > 0 \), it holds that
\[
\lim_{n \to \infty} \frac{1}{n t} \min_{G_n} \mathbb{E}[G_n(X^n)^t] = R(D, P_X). \tag{14}
\]
V. PROOF OF MAIN RESULTS

A. Proof of Theorem 2

First, some notations are defined.

- For any \( \hat{x} \in \hat{X} \) and \( D \geq 0 \), a distortion \( D \)-ball around \( \hat{x} \) is defined as
  \[
  B_D(\hat{x}) := \{ x \in X : d(x, \hat{x}) \leq D \}.
  \]
  \[\text{(15)}\]

- We define \( \hat{x}^*(i) (i = 1, 2, \ldots) \) by the following procedure. Let \( \hat{x}^*(1) \) be defined as
  \[
  \hat{x}^*(1) = \arg \max_{\hat{x} \in \hat{X}} P[X \in B_D(\hat{x})].
  \]
  \[\text{(16)}\]

For \( i = 2, 3, \ldots, s \), let \( \hat{x}^*(i) \) be defined as
  \[
  \hat{x}^*(i) = \arg \max_{\hat{x} \in \hat{X}} \left[ P[X \in B_D(\hat{x}) \setminus \bigcup_{j=1}^{i-1} B_D(\hat{x}^*(j))] \right].
  \]
  \[\text{(17)}\]

- For \( i = 1, 2, \ldots, s \), we define \( A_D(y_i) \) by
  \[
  A_D(\hat{x}^*(1)) = B_D(\hat{x}^*(1)),
  \]
  \[\text{(18)}\]
  \[
  A_D(\hat{x}^*(i)) = B_D(\hat{x}^*(i)) \setminus \bigcup_{j=1}^{i-1} B_D(\hat{x}^*(j)) \quad (\forall i \geq 2).
  \]
  \[\text{(19)}\]

From the definition, we have
  \[
  \bigcup_{i=1}^{s} A_D(y_i) = \bigcup_{i=1}^{s} B_D(y_i) \quad (\forall i \geq 1),
  \]
  \[\text{(20)}\]
  \[
  A_D(y_i) \cap A_D(y_j) = \emptyset \quad (\forall i \neq j),
  \]
  \[\text{(21)}\]
  \[
  X = \bigcup_{i=1}^{s} A_D(\hat{x}^*(i)),
  \]
  \[\text{(22)}\]
  \[
  P[X \in A_D(\hat{x}^*(1))] \geq P[X \in A_D(\hat{x}^*(2))]
  \]
  \[\geq \cdots
  \]
  \[\geq P[X \in A_D(\hat{x}^*(s))].
  \]
  \[\text{(23)-(25)}\]

Let \( G^* \) be
  \[
  G^* = \{ \hat{x}^*(1), \hat{x}^*(2), \ldots, \hat{x}^*(s) \}.
  \]
  \[\text{(26)}\]

In other words, \( G^* \) is the guessing strategy with elements \( \hat{x}^*(1), \hat{x}^*(2), \ldots, \hat{x}^*(s) \) that we have constructed above. From the construction, we can see that \( G^* \) is a \( D \)-admissible guessing strategy with respect to \( P_X \). Further, let \( G^*(\cdot) \) be the guessing function induced by \( G^* \).

Now, we evaluate the \( t \)-th moment of the number of guesses with the guessing strategy \( G^* \). From the definition of \( A_D(\hat{x}^*(i)) \), we have
  \[
  \frac{1}{t} \log \mathbb{E}[G^*(X)^t] = \frac{1}{t} \log \sum_{x \in X} P_X(x) G^*(x)^t
  \]
  \[= \frac{1}{t} \log \sum_{i=1}^{s} P[X \in A_D(\hat{x}^*(i))]^t.
  \]
  \[\text{(27)-(28)}\]

To evaluate the right-hand side of \( (28) \), we use the results of variable-length lossy compression in [11]: from the construction of variable-length lossy source code \( (f, g) \) in [11] (see Appendix A), it holds that
  \[
  \ell(g^{-1}(\hat{x}^*(i))) = \lfloor \log i \rfloor,
  \]
  \[\text{(29)}\]
  where \( \ell(\cdot) \) denotes the length of a binary sequence. Thus, we have
  \[
  \log i - 1 < \ell(g^{-1}(\hat{x}^*(i)))
  \]
  \[\text{(30)}\]
  which indicates that
  \[
  i^t < 2^{t \ell(g^{-1}(\hat{x}^*(i)))}.
  \]
  \[\text{(31)}\]

Combining \( (28) \) and \( (31) \), we have
  \[
  \frac{1}{t} \log \mathbb{E}[G^*(X)^t] < 1 + \frac{1}{t} \log \sum_{i=1}^{s} P[X \in A_D(\hat{x}^*(i))] 2^{t \ell(g^{-1}(\hat{x}^*(i)))}
  \]
  \[\leq 1 + \frac{1}{t} \log \mathbb{E}[2^{t \ell(f(X))}]
  \]
  \[\leq 1 + \mathbb{H}_D^D(\hat{X}),
  \]
  \[\text{(32)-(35)}\]

where \( (a) \) is due to the construction of the code \( (f, g) \) shown in Appendix A and \( (b) \) follows from Lemma 1 in [11].

B. Proof of Theorem 3

Let \( G \) be a \( D \)-admissible guessing strategy with guessing function \( G(\cdot) \) and let \( \alpha_i \) be
  \[
  \alpha_i = \sum_{x \in X : G(x) = i} P_X(x).
  \]
  \[\text{(36)}\]

Without loss of generality, we assume that \( \alpha_1 \geq \alpha_2 \geq \cdots \). This is because we consider a lower bound of the following equation \( \text{(38)} \).

Then, the \( t \)-th moment of the number of guesses of this guessing strategy is calculated as
  \[
  \frac{1}{t} \log \mathbb{E}[G(X)^t] = \frac{1}{t} \log \sum_{x \in X} P_X(x) G(x)^t
  \]
  \[= \frac{1}{t} \log \sum_{i=1}^{r} \alpha_i i^t.
  \]
  \[\text{(37)-(38)}\]

for some \( r \in \mathbb{N} \).

Hence, we have
  \[
  \frac{1}{t} \log \mathbb{E}[G(X)^t] = \frac{1}{t} \log \sum_{i=1}^{r} \alpha_i i^t
  \]
  \[\geq (a) \frac{1}{t} \log \sum_{i=1}^{s} P[X \in A_D(\hat{x}^*(i))] i^t
  \]
  \[\geq (b) \frac{1}{t} \log \mathbb{H}_D^D(\hat{X}) - \log \log(1 + \min\{|X|, |\hat{X}|\}),
  \]
  \[\text{(39)-(41)}\]

where we can verify the inequality \( (a) \) by using the notion of majorization (see Appendix B), and \( (b) \) follows from Lemma 2 in [11].
APPENDIX A

CONSTRUCTION OF VARIABLE-LENGTH LOSSY SOURCE CODE

In [11], we have considered the problem of variable-length lossy source coding. In this appendix, we review the construction of the encoder and decoder shown in [11].

Let $\{0, 1\}^*$ denote the set of all finite-length binary strings and the empty string $\lambda$, i.e.,

$$\{0, 1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, \ldots\}. \quad (42)$$

Also, let $w_i$ be the $i$-th binary string in $\{0, 1\}^*$ in the increasing order of the length and ties are arbitrarily broken. For example, $w_1 = \lambda$, $w_2 = 0$, $w_3 = 1$, $w_4 = 00$, $w_5 = 01$, etc.

Then, the encoder $f$ and decoder $g$ are constructed as follows:

**[Encoder]** For $x \in A_D(\hat{x}^*(i))$ ($i = 1, \ldots, s$), set

$$f(x) = w_i. \quad (43)$$

**[Decoder]** For $i = 1, \ldots, s$, set

$$g(w_i) = \hat{x}^*(i). \quad (44)$$

APPENDIX B

PROOF OF (40)

To prove (40), we first review the notion of majorization and Schur concave functions.

**Definition 4:** Let $\mathbb{R}_+$ be the set of non-negative real numbers and $\mathbb{R}_+^m$ be the $m$-th Cartesian product of $\mathbb{R}_+$, where $m$ is a positive integer. Suppose that $x = (x_1, \ldots, x_m) \in \mathbb{R}_+^m$ and $y = (y_1, \ldots, y_m) \in \mathbb{R}_+^m$ satisfy

$$x_i \geq x_{i+1}, \quad y_i \geq y_{i+1} \quad (i = 1, 2, \ldots, m - 1). \quad (45)$$

If $x \in \mathbb{R}_+^m$ and $y \in \mathbb{R}_+^m$ satisfy, for $k = 1, \ldots, m - 1,$

$$\sum_{i=1}^k x_i \leq \sum_{i=1}^k y_i \quad \text{and} \quad \sum_{i=1}^m x_i = \sum_{i=1}^m y_i, \quad (46)$$

then we say that $y$ majorizes $x$ (it is denoted as $x \prec y$ in this paper).

**Definition 5:** We say that a function $h(\cdot) : \mathbb{R}_+^m \rightarrow \mathbb{R}$ is a Schur concave function if $h(y) \leq h(x)$ for any $x, y \in \mathbb{R}_+^m$ satisfying $x \prec y$.

Now, we shall show

$$\sum_{i=1}^r \alpha_i \hat{x}^i \geq \sum_{i=1}^s \hat{p}[X \in A_D(\hat{x}^*(i))] \hat{x}^i, \quad (47)$$

from which (40) holds. To this end, let

$$x = (x_1, \ldots, x_m) = (\alpha_1, \ldots, \alpha_m) \quad (48)$$

and

$$y = (y_1, \ldots, y_m) \quad (49)$$

$$= (\hat{p}[X \in A_D(\hat{x}^*(1))], \ldots, \hat{p}[X \in A_D(\hat{x}^*(m))]), \quad (50)$$

where $m := \max(r, s)$ and $y_{s+1} = y_{s+2} = \cdots = y_m = 0$ when $r > s$ and $x_{r+1} = x_{r+2} = \cdots = x_m = 0$ when $r < s$.

Then, from the definition of $\hat{p}[X \in A_D(\hat{x}^*(i))]$, we see that $x \prec y$. Next, let

$$h(z) := \sum_{i=1}^m z_i x_i, \quad (51)$$

where $z = (z_1, \ldots, z_m) \in \mathbb{R}_+^m$. Then, from [9, page 133], we see that $h(\cdot) : \mathbb{R}_+^m \rightarrow \mathbb{R}$ is a Schur concave function and $h(x) \geq h(y)$ holds. Therefore, we have (47).

ACKNOWLEDGMENT

This work was supported in part by JSPS KAKENHI Grant Numbers JP16K00195, JP16K00417, JP17K00316, and JP17K06446.

REFERENCES

[1] E. Arikan, “An inequality on guessing and its application to sequential decoding,” IEEE Trans. Inf. Theory, vol. 42, no. 1, pp. 99–105, Jan. 1996.
[2] E. Arikan and N. Merhav, “Guessing subject to distortion,” IEEE Trans. Inf. Theory, vol. 44, no. 3, pp. 1041–1056, May 1998.
[3] E. Arikan and N. Merhav, “Joint source-channel coding and guessing with application to sequential decoding,” IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 1756–1769, Sep. 1998.
[4] A. Burin and O. Shayevitz, “Reducing guesswork via an unreliable oracle.” [Online]. Available: https://arxiv.org/abs/1703.01672.
[5] M. M. Christiansen and K. R. Dufy, “Guesswork, large deviations, and Shannon entropy,” IEEE Trans. Inf. Theory, vol. 59, no. 2, pp. 796–802, Feb. 2013.
[6] 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.
[7] W. Huleihel, S. Salamatian, and M. Médard, “Guessing with limited memory,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Aachen, Germany, pp. 2258–2262, Jun. 2017.
[8] D. Malone and W. G. Sullivan, “Guesswork and entropy,” IEEE Trans. Inf. Theory, vol. 50, no. 3, pp. 525–526, Mar. 2004.
[9] A. W. Marshall, I. Olkin, and B. C. Arnold, Inequalities: Theory of Majorization and its Applications (2nd ed.), Springer, 2010.
[10] A. Rönni, “On measures of entropy and information,” 4th Berkeley Symposium on Mathematics, Statistics and Probability, pp. 547–561, 1960.
[11] S. Saito and T. Matsuhashima, “Cumulant generating function of codeword lengths in variable-length lossy compression allowing positive excess distortion probability,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Vail, Colorado, USA, pp. 881–885, June 2018.
[12] S. Salamatian, A. Beirami, A. Cohen, and M. Médard, “Centralized versus decentralized multi-agent guesswork,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Aachen, Germany, pp. 2263–2267, Jun. 2017.
[13] R. Sundaresan, “Guessing under source uncertainty,” IEEE Trans. Inf. Theory, vol. 53, no. 1, pp. 269–287, Jan. 2007.
[14] R. Sundaresan, “Guessing based on length functions,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Nice, France, pp. 716–719, Jun. 2007.
[15] Y. Yona and S. Diggavi, “The effect of bias on the guesswork of hash functions,” Proc. IEEE Int. Symp. Inf. Theory (ISIT), Aachen, Germany, pp. 2253–2257, Jun. 2017.