Upper and Lower Bounds on the Reliability of Content Identification

Gautam Dasarathy
Electrical and Computer Engineering
University of Wisconsin - Madison
dasarathy@wisc.edu

Stark C. Draper
Electrical and Computer Engineering
University of Toronto
stark.draper@utoronto.ca

Abstract—In this paper we quantify upper and lower bounds on the reliability function for the problem of content identification from a large database based on noisy queries.

I. INTRODUCTION

We consider the problem of content identification from a database. The database houses quantized representations of $2^{nR_I}$ length-$n$ “enrollment” vectors, where $R_I > 0$ is what we call the identification rate (we will not worry about integer effects in this paper). When presented with a noisy observation of one of the (non-quantized) enrollment vectors, the goal is to identify (using only this observation and the stored data) which enrollment vector generated the noisy observation (or the “query”).

The information-theoretic limits of this problem were found in [1] (see also [2] for related problem formulations) under the following model. The enrollment vectors, $X_m$ for $m = 1, \ldots, 2^{nR_I}$ are chosen in an i.i.d. manner according to $p_X$. An index of a codeword in a pre-defined rate-$R_C$ codebook $C$ is used to represent each of these vectors in a database, where $R_C > 0$ is what we call the compression rate. As it takes $nR_C$ bits to store the index of the representation of each enrollment, and $2^{nR_I}$ representations are stored, the entire database is of size $nR_C 2^{nR_I}$ bits. The query $Y$ presented during the identification phase is a length-$n$ observation of one of the $2^{nR_I}$ (unquantized) enrollment vectors observed via the discrete memoryless channel (DMC) $P_{Y|X}(\cdot|\cdot)$. The decoder’s objective is to identify reliably the codeword corresponding to the enrollment vector from which the query was generated.

In [1], the capacity region of this problem was shown to be parameterized by a (rate-distortion) test channel $p_{U|X}$. Given the joint distribution $p_{U|X}(u(x)p_X(x)P_{Y|X}(y|x)$, the “compression/identification” rate pair $(R_C, R_I)$ is achievable if

$$R_C > I(U; X) \quad R_I < I(U; Y).$$

The achievable rate region is the convex hull of the union of achievable rate pairs over all test channels. The achievability is closely related to the the Wyner-Ziv problem. The codebook $C$ needs to have good covering properties ($R_C > I(U; X)$) to ensure reliable encoding. The union of codewords stored in the database (which is a subset of $C$) needs to form a code that has good packing properties ($R_I < I(U; Z)$) for reliable decoding.

In a previous paper [3], we quantified an achievable error exponent tradeoff for a particular encoding and decoding strategy, in other words, we derived a lower bound on the reliability function for the content identification problem. Our results used a novel lemma [3, Lemma 2] that characterized the end-to-end statistical relationship between the codeword and the channel output. In this paper, we will first quantify an upper bound on the error exponent over all encoding/decoding strategies. This upper bound can be shown to be strictly tighter than the naive sphere packing upper bound. We also derive a modification of the lower bound from [3] whose form parallels the upper bound expression obtained here.

II. PROBLEM FORMULATION

In this section we formally state the problem setting and define the notation that we will use throughout the paper.

Environment: We suppose that there are $M = 2^{nR_I}$ items to be represented in the database. To each item is associated a length-$n$ “feature vector” or “enrollment vector” $X(m) \in \mathcal{X}^n$, $m = 1, 2, \ldots, M$ which are drawn independently from $p_X$ in an i.i.d manner where $\mathcal{X}$ is a finite alphabet.

Enrollment Phase: In the enrollment phase, each feature vector is mapped to a codeword selected from a pre-defined rate-$R_C$ codebook $C \triangleq \{u(1), u(2), \ldots, u(2^{nR_C})\}$ ignoring integer effects. The codewords are made up of symbols from the finite alphabet $\mathcal{U}$. We represent the operation of assigning a codeword $u$ to the feature vector $x$ by the function $f : \mathcal{X}^n \rightarrow \{1, 2, \ldots, L\}$, where we define $L = 2^{nR_C}$. The notation $J(m)$ will be used to denote the (random) quantity $f(X(m))$. Observe that the codeword that gets assigned to object $m$ is $u(J(m))$. The set of all (possibly non-distinct) codewords corresponding to the enrolled items $\{u(J(1)), u(J(2)), \ldots, u(J(M))\}$ will henceforth be called the database and will be denoted as $D$. The database $D \subset C$ can be thought of as an analogue to the random bin of codewords in the Wyner-Ziv problem.

Identification Phase: An index $W$ is selected uniformly at random from $\{1, 2, \ldots, M\}$. This corresponds to the item that the user wishes to query for. A noisy version of $X^n(W)$, $Y^n \in \mathcal{Y}^n$ is then observed at the database where the conditional distribution of $Y^n$ is given by $p_{Y|X} = y|x = x = \prod_{i=1}^n p_{Y|X}(y_i|X_i)$, i.e., we model the noise as a DMC $p_{Y|X} : \mathcal{X} \rightarrow \mathcal{Y}$, where $\mathcal{Y}$ is also assumed to be a finite
alphabet. The objective at the identification phase is to produce an estimate $\hat{W}$ from the observed random vector $Y$ and the stored sequences $D$. This estimation operation, which we will call decoding, is denoted by the function $g : \mathcal{Y}^n \times \mathcal{U}^M \to \{1, 2, \ldots, M\}$. Our aim is to design an encoding function $f(\cdot)$ and a decoding function $g(\cdot)$ such that, with high probability, $g(\cdot)$ returns the correct value of $W$.

Given a finite alphabet $\mathcal{S}$, we write $\Pi(\mathcal{S})$ to denote the set of all distributions on $\mathcal{S}$. For other notation, we mainly follow [4].

III. MAIN RESULTS

We will now state the main results of our paper. Given some joint distribution $p_{XY} \in \Pi(\mathcal{X} \times \mathcal{Y})$, let $P_e(f, g, p_{XY})$ denote the probability that a particular choice $(f, g)$ of encoding and decoding function does not estimate $W$ correctly. Then, we can define the content identification reliability function as follows

$$
\rho(p_{XY}, R_I, R_C) = \lim_{n \to \infty} \sup_{f, g} \frac{1}{n} \log \left( \min_{q_{xy}} \frac{P_e(f, g, p_{XY})}{\log \left( \frac{n}{p_{XY}(x, y)} \right)} \right).
$$

where the minimization is over all encoding and decoding function pairs $(f, g)$ such that $\log M \leq n(R_I - \epsilon)$ and $\log L \leq n(R_C + \epsilon)$.

The following theorem provides an upper bound for the reliability function $\rho$. That is, it gives us a lower bound on the probability of error over all choices of valid encoding and decoding functions for the problem.

Theorem 1. Given $p_{XY} \in \Pi(\mathcal{X} \times \mathcal{Y})$ and $R_I, R_C > 0$, the reliability function $\rho(p_{XY}, R_I, R_C)$ is upper bounded by

$$
\rho_U(p_{XY}, R_I, R_C) \triangleq \inf_{q_Y} \sup_{q_{xy}} \inf_{1/(X,Y) \leq R_C} \inf_{1/(X,Y) \leq R_I} D(q_{XY} \| p_{XY}) - I(Y; X). \tag{1}
$$

Here $Y, X, S$ have the joint distribution $q_{Y \mid q_{S}} q_{S \mid X}$ and the cardinality of $S$ satisfies

$$|S| \leq |\mathcal{X}| \cdot |\mathcal{Y}| + |\mathcal{X}| + 2
$$

Next, we will state a theorem that provides a lower bound to the reliability function $\rho$ and therefore upper bounds the probability of error over all choices of encoders and decoders.

Theorem 2. Given $p_{XY} \in \Pi(\mathcal{X} \times \mathcal{Y})$ and $R_I, R_C > 0$, the reliability function $\rho(p_{XY}, R_I, R_C)$ is lower bounded by the quantity

$$
\rho_L \triangleq \inf_{q_X} \sup_{q_{XY} \mid q_{X}} \inf_{D(q_{XY} \| p_{XY} q_{U \mid X})} |I(U, Y) - R_I|^+ - D(q_{XY} \| p_{XY} q_{U \mid X}) \tag{2}
$$

where the joint distribution of $X, Y, U$ is $q_X q_{U \mid X} q_{Y \mid X, U}$.

The rest of the paper will be devoted to proving these two results.

IV. PROOFS

A. Proof of Theorem 1

In order to prove Theorem 1, we begin by picking an arbitrary encoder-decoder pair $f, g$ that satisfies the rate constraints. That is, $f$ and $g$ are such that

$$
\log M \leq nR_I \quad \log L \leq nR_C. \tag{2}
$$

Let us define the “error set”

$$
\mathcal{E} = \{ (x(1), \ldots, x(M), w, y) : g(y, x(1), \ldots, x(M)) \neq w \}.
$$

Our proof will follow these steps:

(A) We will first fix a bad joint distribution $q_{XY}$ such that $I(Y, f(X)) \leq n(R_I - \epsilon)$. We will then show that $q_{XY}^n(\mathcal{E})$ is bounded away from zero.

(B) We will then use this fact to bound the probability of error from below over all valid encoder/decoder pairs. Notice that probability of error is the quantity $p_{XY}^n(\mathcal{E})$.

(C) We will next work to “single letterize” the expressions in the above bound. This will involve introducing the right auxiliary random variable and then ensuring that the corresponding alphabet size does not grow with $n$.

Since this step is somewhat standard, we will only sketch the argument here.

(D) Finally, we use continuity arguments to show that we can take $\epsilon \to 0$, the details of which we will omit in this short manuscript.

Step (A): Let $q_{XY} \in \Pi(\mathcal{X} \times \mathcal{Y})$ be a distribution such that $I(Y, f(X)) \leq n(R_I - \epsilon)$. Recall that $g$ is an estimator for the random variable $W$ and it has access to the random variables $\{J(i)\}_{i \in [M]}$ and $Y$. Therefore, Fano’s inequality (see e.g., [5]) tells us that

$$
q_{XY}^n(\mathcal{E}) \geq \frac{H(W | J(1), \ldots, J(M), Y) - 1}{\log M}. \tag{4}
$$

Notice here that the conditional entropy is computed with respect to the joint distribution $q_{XY}^n$.

To get a lower bound on $q_{XY}^n(\mathcal{E})$, we will lower bound the conditional entropy term above.

$$
H(W | J(1), \ldots, J(M), Y)
$$

$$
= H(W) - I(W; J(1), \ldots, J(M), Y)
$$

$$
\geq H(W) - I(W; Y | J(1), \ldots, J(M)) \tag{a}
$$

$$
\geq I(W) - H(Y | J(1), \ldots, J(M)) \tag{b}
$$

$$
\geq I(W) - H(Y | J(1), \ldots, J(M), W) \tag{c}
$$

$$
\geq nR_I - I(f(X); Y) \tag{d}
$$

In (a), we have used the definition of conditional mutual information and that fact that $I(W; J(1), \ldots, J(M)) = 0$ since these quantities are independent. In (b) we expand out the conditional mutual information term and in (c) we use
the fact that conditioning cannot increase entropy (i.e., \(H(Y | J(i), c_{M,i}) \leq H(Y)\)) and that \(Y\) only depends on \(J(W)\) and therefore \(H(Y | J(i), c_{M,i}) = H(Y | J(W))\). Finally, in (d) we use the fact that \(W\) is a uniform random variable over a set of size \(M = 2^{nR_t}\) and the fact that, by definition, \(J(W) = f(X)\). The final step follows from our assumption on \(q_{XY}\). Let us assume that \(n \geq 2e^{-1}\). Substituting this lower bound back in (4), we have

\[
q_{XY}(E) \geq \frac{ne - 1}{nR_t} \geq \frac{\varepsilon}{2R_t}.
\]

**Step (B):** In order to lower bound the probability of error, \(P_{XY}(E)\), we will use the so-called “change of measure” argument typically used in establishing large deviation rate functions (see e.g., [6] and [4, Page 268, Problem 13]) for a version that is more applicable to an information theoretic setting. The idea is to lower bound the mass of a set (in this case \(E\)) under one measure (in this case \(p_{XY}\)) using the mass of the same set under a different measure (in this case \(q_{XY}\)). For \(\delta > 0\), let us define the set of all \((q_{XY}, p_{XY}) - divergence\) typical sequences as follows

\[
\mathcal{D} = \left\{ (x, y) : \left| \frac{1}{n} \log q_{XY}(x, y) - D(q_{XY} \| p_{XY}) \right| \leq \delta \right\}.
\]

Notice that by Chebyshev’s inequality, we have that \(q_{XY}(\mathcal{D}^c)\) is no greater than \(\frac{\log^2 q_{XY}}{nR_t} \cdot p_{XY}(\mathcal{D}^c)\). Assuming that \(p_{XY} > 0\), this quantity can be uniformly upper bounded by some \(\Delta > 0\) over all \(q_{XY}\) when \(X\) and \(Y\) are finite. Of course, one could obtain a tighter bound for \(q_{XY}(\mathcal{D}^c)\) using, for instance, Chernoff bounds. However, this weaker bound suffices for our current purpose. We can now proceed to bound the probability of error as follows for \(n \geq \frac{4R_t}{\Delta}\).

\[
P[error] = p_{XY}(E) \geq p_{XY}(E \cap \mathcal{D}) = \sum_{x, y : (x, y) \in E \cap \mathcal{D}} q_{XY}(x, y) p_{XY}(x, y) q_{XY}(x, y) \]

\[
\geq q_{XY}(E \cap \mathcal{D}) e^{-n[D(q_{XY} \| p_{XY}) + \delta]}
\]

In (a) we use the definition of the divergence typical set \(\mathcal{D}\) and in (b) we use the fact that \(P(A \cap B) \geq |P(A) - P(B)|\). Finally in (c) we use our assumption that \(n \geq \frac{4R_t}{\Delta}\). This bound holds for any \(q_{XY}\) such that \(I(f(X), Y) \leq n(R_t - \epsilon)\), it has to hold even if we take the supremum over all such \(q_{XY}\)’s. Also, since we want our lower bound to hold irrespective of the quality of the encoder/decoder pair picked, we can take the infimum of right side with respect to all valid coding functions. Therefore, the probability of error can be lower bounded by the following quantity

\[
\inf_{\hat{q}_{XY}} \sup_{f : I(X; \hat{q}_{XY}, W) \leq n(R_t + \epsilon)} \inf_{I(Y; \hat{q}_{XY}, W) \leq n(R_t - \epsilon)} \epsilon \exp \left( -n \left| D(q_{XY} \| p_{XY}) + \delta \right| \right).
\]

**Step (C):** Before we proceed, let us restrict our attention to the exponent. Notice that our objective will now be to upper bound the subsequent quantities.

\[
\sup_{f} \inf_{\hat{q}_{XY}} \inf_{I(Y; \hat{q}_{XY}, W) \leq n(R_t - \epsilon)} D(q_{XY} \| p_{XY})
\]

\[
\leq \inf_{\hat{q}_{XY}} \sup_{f : I(f(X); W) \leq n(R_t + \epsilon)} D(q_{XY} \| p_{XY})
\]

\[
\leq \inf_{\hat{q}_{XY}} \sup_{f} \inf_{I(U; X) \leq n(R_t + \epsilon)} D(q_{XY} \| p_{XY})
\]

In (a) we changed the order of minimization and maximization, and we used the fact that \(\log L = H(f(X)) \geq I(f(X); X)\). In (b), we are replacing the deterministic mapping \(f(X)\) by a random variable \(U\) (whose alphabet has cardinality no less than the range of \(f(X)\)). Since deterministic functions are a special case of such random mappings, we are increasing the domain of maximization, and hence the inequality (this does not affect the inner minimization since the domain of that infimum is over \(q_{XY}\)). Towards “single-letterizing” the arguments of the optimizations above, we do the following two calculations. First, we observe that

\[
I(Y; U) = \sum_{i=1}^{n} H(Y_i | Y_{1:i-1}, U_{1:i-1})
\]

\[
\leq \sum_{i=1}^{n} H(Y_i) - H(Y_i | U, X_{1:i-1}) = \sum_{i=1}^{n} I(Y_i; U, X_{1:i-1})
\]

\[
\leq \sum_{i=1}^{n} I(Y_i; V_i) \leq I(Y_T; V_T, T),
\]

where (a) follows from observing that \(H(Y_i | X_{1:i-1}) \leq H(Y_i)\) and that \(H(Y_i | U, X_{1:i-1}) = H(Y_i | U, X_{1:i-1}, Y_{1:i-1}) \leq H(Y_i | U, X_{1:i-1}, Y_{1:i-1} - X_{1:i-1})\) because of the Markov chain \(Y_{i-1} - U, X_{1:i-1} - Y_{1:i-1}\). In (b), we set \(V_i = (U, X_{1:i-1})\) and in (c) we merely introduce a random variable \(T\) that is uniformly distributed in \([1, \ldots, n]\) (this is the so called “time sharing” random variable.) Second, using a similar calculation, we have

\[
I(X; U) = \sum_{i=1}^{n} I(X_i; U | X_{i-1}) = \sum_{i=1}^{n} I(X_i; X_{i-1}, U)
\]

\[
= \sum_{i=1}^{n} I(X_i; V_i) = I(X_T; V_T, T)
\]

Using these two calculations and defining \(W \triangleq (V_T, T)\), we can upper bound (7) as

\[
\inf_{\hat{q}_{XY}} \sup_{f : I(X; \hat{q}_{XY}, W) \leq n(R_t + \epsilon)} \inf_{I(Y; \hat{q}_{XY}, W) \leq n(R_t - \epsilon)} D(q_{XY} \| p_{XY})
\]
Finally, using continuity arguments, we can show that 

\[
\lim_{\epsilon \to 0} \tilde{\rho}_U(p_{XY}, R_C + \epsilon, R_I + \epsilon) = \inf_{q_X} \sup_{q_{S|X}} \inf_{q_{Y|X}} D(q_{XY} \| p_{XY}).
\]  

(8)

In order to conclude, we must next show that the auxiliary random variable that we introduced has an alphabet size that does not grow with \( n \).

We will only sketch the rest of the argument since the techniques are somewhat standard. Let \( \tilde{\rho}_U \) be the same expression as (8) but with an extra cardinality constraint \( |S| \leq |X| + |Y| + 2 \). Our goal will be to show that \( \tilde{\rho}_U = \tilde{\rho}_U \).

It is of course easy to see that \( \tilde{\rho}_U \leq \tilde{\rho}_U \). In order to show the other direction, notice that it suffices to show that for each \( q_X \) and \( q_{S|X} \) such that \( I(X; S) \leq R_C + \epsilon \), there exists a \( q_{S|X} \) such that (a) it satisfies the same mutual information constraints, (b) it has \(|S| \leq |X| \cdot |Y| \cdot |X| + 2 \) and (c) if one defines the function

\[
f(q_{X}, q_{S|X}) \triangleq \inf_{q_{Y|X}} D(q_{XY} \| p_{XY}),
\]

(9)

then \( f(q_{X}, q_{S|X}) \leq f(q_{X}, q_{S|X}) \).

Since \( p_{XY} \geq 0 \) and the optimization problem above has a convex bounded objective over a compact set, a minimizer \( \tilde{q}_{Y|X} \) exists such that

\[
f(q_{X}, q_{S|X}) = D(q_{X}q_{Y|X} \| p_{XY}).
\]  

(10)

Also, since the optimization problem is convex, we know that \( \tilde{q}_{Y|X} \) satisfies the KKT conditions [7]. To conclude this step, we use the fact that the KKT conditions are essentially \([|X| \cdot |Y|] \) linear equalities involving \( \tilde{q}_{Y|X} \) (which correspond to the gradient condition) and a set of \([|X| \cdot |Y|] \) linear equalities corresponding to the mutual information constraint. Therefore, by Caratheodory’s theorem, we have that the cardinality \(|S| \leq |X| \cdot |Y| \cdot |X| + 2 \) and that \( q_{S|Y} \) satisfies the necessary constraints.

**Step (D):** Finally, using continuity arguments, we can show that

\[
\lim_{\epsilon \to 0} \tilde{\rho}_U(p_{XY}, R_I + \epsilon, R_C + \epsilon) \rightarrow \rho_U(p_{XY}, R_I, R_C).
\]

This concludes the proof.

**B. Proof of Theorem 2**

In [3], we show, using an important lemma about the end-to-end behavior across a Markov chain, that the reliability function \( \rho \) of the problem is lower bounded by

\[
\tilde{\rho}_L = \inf_{q_X} \sup_{q_{S|X}} \inf_{q_{Y|X}} D(q_{XY} \| p_{XY}) + D \left( \tilde{J}_{q_{Y|S}, q_{S|X}} \mid J \mid q_{S} \right) \\
+ |I(S; Y) - R_I|^+.
\]  

(11)

where \( q_{S}(\cdot) = \sum_{x \in X} q_X(x)q_{S|X}(\cdot | x) \) is the distribution induced on \( S \) by \( q_X \) and \( q_{S|X} \), \( J : S \rightarrow X \times Y \) is a stochastic matrix defined as \( J(x, y | s) = q_X(x | s)q_{S|X}(y | x) \), for all \((s, x, y) \in S \times X \times Y \), and \( \tilde{J}_{q_{Y|S}, q_{S|X}}^{*} : S \rightarrow X \times Y \) is a stochastic matrix defined as

\[
\tilde{J}_{q_{Y|S}, q_{S|X}}^{*} = \arg \min_{J \in \mathbb{E}(q_{Y|S})} D(J \| J \mid q_S).
\]  

(12)

It can be shown that this error exponent is positive in the capacity region indicated in [1]. We will now show that \( \tilde{\rho}_L \) equals \( \rho_L \) so that the expression matches \( \rho_U \) more closely.

Towards this end, consider the first two terms in the expression for \( \tilde{\rho}_L \) and observe that

\[
D(q_{X} \| p_{X}) + D \left( \tilde{J} \mid J \mid q_{S} \right)
\]

\[
= D(q_{X} \| p_{X}) + D \left( q_{X}q_{S|X}\tilde{q}_{Y|X,S} \mid q_{X}q_{S|X}\tilde{q}_{Y|X,S} \right)
\]

\[
= D(q_{X}q_{S|X}\tilde{q}_{Y|X,S} \| p_{X}q_{S|X}\tilde{q}_{Y|X,S}) + D \left( q_{X}q_{S|X}\tilde{q}_{Y|X,S} \mid q_{X}q_{S|X}\tilde{q}_{Y|X,S} \right)
\]

\[
= D(q_{X}q_{S|X}\tilde{q}_{Y|X,S} \| p_{X}q_{S|X}\tilde{q}_{Y|X,S})
\]

(12)

where (a) follows from the definition of the conditional KL divergence, (b) follows from multiplying and dividing the appropriate term in the first KL divergence term, and the last line is a simple algebraic simplification of (b). Finally we note that every choice of \( q_X, q_{Y|X}, \) and \( q_{Y|X,S} \) fixes the \( q_{S|Y} \) distribution and therefore, one can equivalently optimize over \( q_{S|X} \) in the inner most infimum of (11). This concludes the proof.

**References**


