$$w(j) \geq \frac{1}{n} + \frac{1}{n-1} > \frac{1}{n+1} + \frac{1}{n+1} = \frac{1}{(n+1)/2}, \quad (5)$$

which is the largest weight of a node at the highest level. Thus, at that level the nodes can be ordered to satisfy the sibling property.

Suppose now that all levels higher than level $n+i$ have been ordered. The $(n+i)$th level can be ordered if no node at any lower level has a lower weight than any node at level $n+i$. Let us find a lower bound on the weight at level $n+i-1$.

Using the induction assumption, any weight $w(i)$ at level $n+i$ is at least as large as any weight at level $n+i+1$, including the largest leaf at that level. Then, by property 3),

$$w(i) \geq \frac{1}{2^i}. \quad (6)$$

A node at level $n+i-1$ is either a leaf, or has extensions into nodes at level $n+i$. If it is a leaf, by property 3), its weight $w(i-1)$ satisfies

$$w(i-1) \geq \frac{1}{2^{i-1}-1}.$$

If it is an internal node, by (6),

$$w(i-1) \geq \frac{1}{2^i} + \frac{1}{2^i} = \frac{1}{2^{i-1}}.$$

Thus, for any node at level $n+i-1$,

$$w(i-1) \geq \frac{1}{2^{i-1}}. \quad (7)$$

By property 4) and (7) it follows that any weight at level $n+i-1$ is at least as large as any weight at level $n+i$.

It is left to prove the same holds for levels lower than $n+i-1$. It follows by similar arguments; each weight at lower level is a sum of weights of leaves and nodes. Those include at least one leaf at a level lower than $n+i-1$, or a node at level $n+i-1$. In each case the claim holds.

IV. Conclusion

This note proves that the fixed-prefix logarithmic representation of the integers up to some fixed number $|X| = 2^{2^n}-1$ is optimum, since it is equivalent to a Huffman code for a logarithmic probability distribution.

Although the problem was presented in the context of recency rank encoding and interval encoding of fixed messages, it has applications in variable-length encoding of variable-vocabulary schemes, such as the Ziv–Lempel source coding algorithms [7], [8].

References

[1] J. L. Bentley, D. D. Sleator, and R. E. Tarjan, "A locally adaptive data compression scheme,"*Commun. ACM*, vol. 29, pp. 320–330, Apr. 1986.

[2] P. Elias, "Interval and recency rank source coding: Two on-line adaptive variable-length schemes," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 3–10, Jan. 1987.

[3] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[4] P. Elias, "Universal codeword sets and representation of the integers," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 194–203, Mar. 1975.

[5] J. L. Bentley and A. C. Yao, "An almost optimal algorithm for unbounded searching," *Inform. Process. lett. 5, 3*, pp. 82–87, August 1976.

[6] R. G. Gallager, "Variations on a theme by Huffman," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 668–674, Nov. 1978.

[7] J. Ziv and S. Lempel, "A universal algorithm for sequential data compression," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 337–343, May 1977.

[8] M. Rodeh, V. R. Pratt, S. Even, "Linear algorithm for data compression via string matching," *J. ACM*, vol. 28, pp. 16–24, Jan. 1981.

A Large Deviations Approach to Error Exponents in Source Coding and Hypothesis Testing

V. ANANTHARAM

Abstract—**The usual approach to finding the error exponents in binary hypothesis testing and in source coding for finite Markov chains involves combinatorial "type-counting" arguments. The purpose of this correspondence is to point out that the basic results can be proved fairly easily if one uses a Sanov theorem for the distribution of types. Such a theorem comes easily from large deviations theory. A caveat is that this technique only identifies the error exponent up to terms of order $o(n)$ in the exponent, whereas the combinatorial arguments give an estimate up to terms of order $O(\log n)$ in the exponent.**

I. Introduction

In this correspondence we discuss two basic communication-theoretic problems—the *binary hypothesis testing problem* and the *source coding problem* for finite Markov chains. These problems are defined precisely in Section III. We are interested in studying the asymptotics of the achievable performance as the size of the sample becomes large. The performance measure in both problems is an error probability, and it turns out that this error probability decays exponentially in sample size. We are interested in determining the error exponent.

Such problems have been thoroughly studied for finite state independent and identically distributed (i.i.d.) processes and Markov chains, and the error exponents have been determined. For the binary hypothesis testing problem, one can find the results for i.i.d. sources in [1], [3], and for Markov sources in [10]. For the source coding problem for i.i.d. sources, one can find the results in [3], and for Markov sources in [4], [9], [10], and [14].

In all of these papers, the approach to finding the error exponents involves combinatorial "type-counting" arguments. The purpose of this note is to point out that the basic results can be proved fairly easily if one uses a Sanov theorem for the distribution of types. With this approach, which appears to be somewhat novel, one does not have to face the intricacies of the combinatorics, which is replaced by topological arguments. A caveat is that this technique only identifies the error exponent up to terms of order $o(n)$ in the exponent, whereas the combinatorial arguments give an estimate up to terms of order $O(\log n)$ in the exponent.

Sanov theorems come from the subject of large deviations theory. A Sanov theorem for Markov chains may be written down directly from a powerful large deviation result of Ellis, [7]. The structure of the note is the following: After introducing notation and the basic Sanov theorem in Section II, in Section III we state the problems to be considered in a precise manner and state the main results. The derivation of the error exponents for binary hypothesis testing and for source coding is carried out in Sections IV and V, respectively. Some concluding remarks are made in Section VI.

Manuscript received September 11, 1987; revised October 23, 1989. The author was supported by the National Science Foundation under NCR 8710840 and under a PYI award, and by IBM and BellCore, Inc.

The author is with the School of Electrical Engineering, Phillips Hall, Cornell University, Ithaca, NY 14853.

IEEE Log Number 9034939.

II. Notation, Basic Concepts, and Sanov Theorem for Markov Chains

A discussion of the problems to be addressed in this correspondence requires some notation and basic concepts connected with the sample path behavior of finite Markov chains. Let X be a finite set of cardinality d. Let $\{X_n, n \geq 0\}$, be an irreducible Markov chain on X, with initial distribution p and transition matrix P. Let $\boldsymbol{M}$ denote the space of probability measures on $X \times X$. We think of $\boldsymbol{M}$ as the unit simplex in $R^{d \times d}$.

A sequence $\tau_n \in \boldsymbol{M}$ is said to converge weakly to $\tau \in \boldsymbol{M}$, written $\tau_n \xrightarrow{w} \tau$, if $\tau_n(i,j) \to \tau(i,j)$ for all $(i,j) \in X \times X$. This is the same as the standard notion of convergence in the Euclidean topology when $\boldsymbol{M}$ is identified with the unit simplex in $R^{d \times d}$.

For $\tau \in \boldsymbol{M}$, let $\tau(i,\cdot)$ denote $\Sigma_j \tau(i,j)$ and $\tau(\cdot,j)$ denote $\Sigma_i \tau(i,j)$. The subset of probability distributions on $X \times X$ having identical marginals will be of special importance. We denote this subset by

$$\boldsymbol{M}_S \triangleq \{\tau \in \boldsymbol{M}: \tau(i,\cdot) = \tau(\cdot,i), \quad \forall i \in X\}. \tag{2.1}$$

For $\tau \in \boldsymbol{M}_S$, let $\tau(i) \triangleq \tau(i,\cdot) = \tau(\cdot,i)$.

An important information-theoretic measure of how different one stochastic matrix is from another follows.

Definition: For $\tau, \eta \in \boldsymbol{M}$, the *information discrimination* of τ with respect to η, $D(\tau,\eta)$ is

$$D(\tau,\eta) \triangleq \sum_{ij} \tau(i,j) \log \frac{\tau(i,j)}{\tau(i,\cdot)} \left(\frac{\eta(i,j)}{\eta(i,\cdot)} \right)^{-1}.$$

Here $\log 0/0 \triangleq 0$ and logarithms are base 2.

Remark: Normalize the rows of τ and η by their row sums to get stochastic matrices. $D(\tau,\eta)$ is just the information discrimination between the normalized rows of τ and η averaged over the distribution $\{\tau(i,\cdot), i \in X\}$.

For $\tau, \eta \in \boldsymbol{M}$, we write $\tau \ll \eta$ if and only if $\eta(i,j) = 0$ implies $\tau(i,j) = 0$. Let P and Q be irreducible stochastic matrices, with stationary distributions π and μ, respectively. Note that $\pi P, \mu Q, \epsilon \boldsymbol{M}_S$, where

$$(\pi P)(i,j) \triangleq \pi(i) P(i,j)$$

and μQ is defined similarly. We shall write $D(P,Q)$ for $D(\pi P, \mu Q)$. For $\tau \in \boldsymbol{M}$, we shall write $D(\tau,P)$ for $D(\tau,\pi P)$. We shall also write $\tau \ll P$ for $\tau \ll \pi P$.

Now suppose we observe the Markov chain $\{X_n, n \geq 0\}$ for $n+1$ time units, seeing the sequence of symbols $\boldsymbol{x} = (i_0, i_1, \cdots, i_n) \in X^{n+1}$. We may summarize the information contained in the sample by means of a matrix, defined next.

Definition: For a sample of size $n+1$, $\boldsymbol{x} = (i_0, i_1, \cdots, i_n) \in X^{n+1}$, its *empirical transition-count matrix* or *type* is the probability distribution on $X \times X$ giving mass $n^{-1} N(i,j|\boldsymbol{x})$ to $(i,j) \in X \times X$, where $N(i,j|\boldsymbol{x})$ denotes the number of transitions from i to j in $\boldsymbol{x}$. This defines a map $T^n: X^{n+1} \to \boldsymbol{M}$.

Remark: Note that the image of T^n is almost in $\boldsymbol{M}_S$. In fact, if $\tau \in$ image (T^n), then $|\tau(i,\cdot) - \tau(\cdot,i)| \leq n^{-1}$ for all $i \in X$.

We let $P_p^{(n)}$ denote the distribution of the $n+1$ sample empirical transition-count matrix. This is the distribution on $\boldsymbol{M}$ induced through T^n from the (p,P) Markov distribution P_p^n on X^{n+1}. Let π denote the stationary distribution of P. We note that, from the Ergodic theorem, $P_p^{(n)} \xrightarrow{w} \delta_{\pi P}$.

A theorem due to Ellis, [7] leads directly to a description of how fast the distribution $P_p^{(n)}$ of the $n+1$ sample empirical transition-count matrix of a Markov chain (p,P) approaches the distribution concentrated on πP. The probability of seeing sample sequences with atypical empirical transition-count matrices decreases to zero exponentially in the sample size. Such a result is called a Sanov theorem, after Sanov, [11], and will be the main ingredient of our proofs of Theorems 3.2 and 3.5.

Let $I: \boldsymbol{M} \to R_+$ be given by

$$I(\tau) = D(\tau,P), \qquad \text{for } \tau \in \boldsymbol{M}_S$$
$$= \infty, \qquad \text{for } \tau \in \boldsymbol{M} - \boldsymbol{M}_S. \tag{2.2}$$

Theorem 1: For any closed set $K \subseteq \boldsymbol{M}$,

$$\limsup_{n \to \infty} n^{-1} \log P_p^{(n)}(K) \leq - \inf_{\tau \in K} I(\tau) \tag{2.3a}$$

whereas, for any open set $G \subseteq \boldsymbol{M}$,

$$\liminf_{n \to \infty} n^{-1} \log P_p^{(n)}(G) \geq - \inf_{\tau \in G} I(\tau). \tag{2.3b}$$

Proof: A simple proof of this result may be found in Chapter IX of Ellis, [8]. The result was first proved in a much more general context by Donsker and Varadhan, [6], [13]. Proofs of this result are also available in [5] and [12]. □

III. Statement of Results

The *binary hypothesis testing* problem is the following: Let X be a finite set of cardinality d. We observe X valued samples $i_0, i_1, i_2, \cdots$, which may be produced by a Markov source with initial distribution p and irreducible transition probability matrix P, (Hypothesis $\boldsymbol{P}$), or by a Markov source with initial distribution q and irreducible transition probability matrix Q, (Hypothesis $\boldsymbol{Q}$). We are to decide on the basis of $n+1$ samples, which of the hypotheses holds, so as to minimize $Pr\{\text{decide } \boldsymbol{P}|\boldsymbol{Q}\}$, subject to a lower bound on $Pr\{\text{decide } \boldsymbol{P}|\boldsymbol{P}\}$. $1 - Pr\{\text{decide } \boldsymbol{P}|\boldsymbol{Q}\}$ is commonly called the power of the test and $Pr\{\text{decide } \boldsymbol{P}|\boldsymbol{P}\}$ is called its size. $\boldsymbol{P}$ is called the null hypothesis, and $\boldsymbol{Q}$ is called the alternate hypothesis.

In a signal processing context, $\boldsymbol{Q}$ may represent the situation where a signal is present, and $\boldsymbol{P}$ the situation where no signal is present. The aim is to minimize the probability of missed detection subject to an upper bound on the probability of false alarm.

For simplicity, we shall assume that $p(i) > 0$ and $q(i) > 0$ for each $i \in X$. Let the upper bound on the probability of false alarm be ϵ. Then the minimum achievable probability of missed detection is

$$e(n,\epsilon) = \min_{S \subseteq X^{n+1}; P_p^n(S) \geq 1-\epsilon} Q_q^n(S). \tag{3.1}$$

We are interested in the asymptotic behavior of $e(n,\epsilon)$ as $n \to \infty$. It turns out that $e(n,\epsilon)$ decreases to zero exponentially in n up to terms of order $o(n)$ in the exponent. This result is called Stein's lemma.

Theorem 2: If $P \ll Q$, then

$$\lim_{n \to \infty} n^{-1} \log e(n,\epsilon) = - D(P,Q).$$

Further, for any null hypothesis $\boldsymbol{P}$, there is a decision rule that achieves the optimum error exponent simultaneously for every alternate hypothesis $\boldsymbol{Q}$.

For more on hypothesis testing, see [1].

The source coding problem for Markov chains is the following: Let X be a finite set of cardinality d, a Markov source with

initial distribution p and transition matrix P produces a sequence of letters at times $t=0,1,2,\cdots$, namely X valued random variables $X_0, X_1, X_2, \cdots$ which form a Markov chain with initial distribution p and transition matrix P. We assume that P is irreducible. An n to m binary block code for the source consists of a pair of mappings

$$e: X^{n+1} \to \{0,1\}^m \quad \text{and} \quad d: \{0,1\}^m \to X^{n+1}$$

the encoding and decoding maps respectively. The error probability associated to the code (e,d) is given by

$$E(e,d) = P_p^n\{x: d \circ e(x) \neq x\}. \tag{3.2}$$

The rate of an n to m binary block code is m/n.

We are interested in the asymptotic behavior of the error probability as $n \to \infty$, for codes with bounded rate. This error probability decreases to zero exponentially in n up to terms of order $o(n)$ in the exponent. To make a precise statement, we need the following.

Definition: The entropy of $\tau \in \boldsymbol{M}$ is

$$H(\tau) \triangleq -\sum_{ij} \tau(i,j) \log \frac{\tau(i,j)}{\tau(i,\cdot)}.$$

For an irreducible stochastic matrix P with stationary distribution π, we write $H(P)$ for $H(\pi P)$, i.e.,

$$H(P) \triangleq -\sum_i \pi(i) \sum_j P(i,j) \log P(i,j).$$

If we think of the rows of P as probability distributions on X, $H(P)$ is just the usual entropy of these rows, averaged over π.

With this definition, a description of the behavior of the error probability in source coding is given by the following.

Theorem 3: For any R, $0 \le R \le \log d$, there exists a sequence of n to m_n binary block codes (e_n, d_n) such that

$$\lim_{n\to\infty} \frac{m_n}{n} = R \tag{3.3}$$

with

$$\limsup_{n\to\infty} n^{-1} \log E(e_n, d_n) \le -\inf_{\tau \in \boldsymbol{M}_S:\, H(\tau) \ge R} D(\tau, P) \tag{3.4}$$

and

$$\liminf_{n\to\infty} n^{-1} \log(1 - E(e_n, d_n)) \ge -\inf_{\tau \in \boldsymbol{M}_S:\, H(\tau) < R} D(\tau, P) \tag{3.5}$$

for every irreducible Markov source with source alphabet X and transition probability P.

Further, this result is optimal in the sense that, for any sequence of n to m_n binary block codes (e_n, d_n) such that

$$\limsup_{n\to\infty} \frac{m_n}{n} \le R, \tag{3.6}$$

we have

$$\liminf_{n\to\infty} n^{-1} \log E(e_n, d_n) \ge -\inf_{\tau \in \boldsymbol{M}_S:\, H(\tau) > R} D(\tau, P) \tag{3.7}$$

and

$$\limsup_{n\to\infty} n^{-1} \log(1 - E(e_n, d_n)) \le -\inf_{\tau \in \boldsymbol{M}_S:\, H(\tau) \le R} D(\tau, P) \tag{3.8}$$

for every irreducible Markov source with source alphabet X and transition probability P.

Remark: Equations (3.4) and (3.7) are interesting when $R > H(P)$, whereas (3.5) and (3.8) are interesting when $H(P) > R$. It is easy to verify from the continuity properties of $H(\tau)$ and $D(\tau,P)$ that when $0 < R < \log d$ the right sides of (3.4) and (3.7) are equal, as are the right sides of (3.5) and (3.8). For more on source coding, see [2].

Theorems 2 and 3 will be proved using ideas from the large deviations theory, in Sections IV and V.

IV. Error Exponent for Hypothesis Testing

In this section, we prove Theorem 2. Before proceeding with the proof, note that if there is $(i,j) \in X \times X$ such that $P(i,j) > 0$ but $Q(i,j) = 0$, then the rule.

Decide

$$\boldsymbol{P} \text{ iff } N(i,j|x) > 0$$

satisfies

$$\lim_{n\to\infty} P_p^n\{x: \text{decide } \boldsymbol{P}\} = 1$$

and

$$Q_q^n\{x: \text{decide } \boldsymbol{P}\} \equiv 0, \qquad \text{for all } n > 0,$$

so that, for any $\epsilon > 0$, for all sufficiently large n,

$$e(n,\epsilon) = 0.$$

This indicates why the theorem is only stated for $P \ll Q$.

Let $x \in X^{n+1}$ be a sample with empirical transition-count matrix τ. We take $D(\tau, P)$ as a measure of how likely it is that the sample came from the distribution P_p^n. This motivates us to consider rules of the following type: If we observe $x \in X^{n+1}$, and $T^n(x) = \tau$, we decide $\boldsymbol{P}$ if and only if

$$D(\tau, P) \le \eta_n \tag{4.1}$$

where η_n decrease to zero, and will be chosen appropriately next. Let D_n denote the set of $x \in X^{n+1}$ determined by (4.1). Let Δ_n denote $\{\tau: D(\tau,P) \le \eta_n\}$. Note that Δ_n is closed in $\boldsymbol{M}$. Also

$$\cdots \subseteq \Delta_{n+1} \subseteq \Delta_n \cdots \text{ and } \bigcap_n \Delta_n = \{\pi P\} \tag{4.2}$$

because η_n decrease to zero.

From (2.3a) with $Q_q^{(n)}$ as the underlying measure, we have, for any fixed k

$$\limsup_{n\to\infty} n^{-1} \log Q_q^n(D_k) \le -\inf_{\tau \in \Delta_k \cap \boldsymbol{M}_S} D(\tau, Q). \tag{4.3}$$

From (4.2) and (4.3), it follows that for any fixed k

$$\limsup_{n\to\infty} n^{-1} \log Q_q^n(D_n) \le -\inf_{\tau \in \Delta_k \cap \boldsymbol{M}_S} D(\tau, Q). \tag{4.4}$$

Letting $k \to \infty$ in (4.4) and appealing to the continuity of $D(\tau, Q)$ in τ gives

$$\begin{aligned}\limsup_{n\to\infty} n^{-1} \log Q_q^n(D_n) &\le -\sup_k \inf_{\tau \in \Delta_k \cap \boldsymbol{M}_S} D(\tau, Q) \\ &= -D(P, Q).\end{aligned} \tag{4.5}$$

Note that (4.5) is true for any sequence η_n decreasing to zero. We next show that it is possible to choose η_n decreasing to zero so that

$$\lim_{n\to\infty} P_p^n(D_n) = \lim_{n\to\infty} P_p^{(n)}(\Delta_n) = 1. \tag{4.6}$$

It is then clear that the decision rules corresponding to this choice of η_n have asymptotic size at least $1-\epsilon$ for any $\epsilon > 0$ and achieve the error exponent in Theorem 2.

To show (4.6), it is enough to show that we can choose η_n decreasing to zero so that

$$\lim_{n\to\infty} P_p^{(n)}\left(\overline{\boldsymbol{M} - \Delta_n}\right) = 0. \tag{4.7}$$

Given $\eta > 0$, let $\Delta(\eta)$ denote $\{\tau\colon D(\tau, P) \le \eta\}$. From (2.3a) we have

$$\limsup_{n\to\infty} n^{-1} \log P_p^{(n)}\left(\overline{\boldsymbol{M} - \Delta(\eta)}\right) \le - \inf_{\tau \in \overline{\boldsymbol{M} - \Delta(\eta)}} D(\tau, P) = -\eta. \tag{4.8}$$

Thus we can find $n_0(\eta)$ such that for all $n \ge n_0(\eta)$ we have

$$n^{-1} \log P_p^{(n)}\left(\overline{\boldsymbol{M} - \Delta(\eta)}\right) \le -\frac{\eta}{2}. \tag{4.9}$$

Now pick some sequence η_i decreasing to zero. We may assume without loss of generality that $n_0(\eta_i)$ increases to ∞. We define the function $i(n)$ by the following rule:

$$i(n) = \max\left\{i\colon \eta_i > \frac{\log n}{n} \text{ and } n_0(\eta_i) \le n\right\} \tag{4.10}$$

if the set on the right of (4.10) is not empty and

$$i(n) = 1$$

otherwise. Finally, we choose

$$\eta_n = \eta_{i(n)}.$$

From the definitions it follows that $i(n)$ increases to ∞ with n, and if n is sufficiently large so that the set on the right of (4.10) is not empty, we have

$$\begin{aligned} P_p^{(n)}\left(\overline{\boldsymbol{M} - \Delta(\eta_n)}\right) &= P_p^{(n)}\left(\overline{\boldsymbol{M} - \Delta(\eta_{i(n)})}\right) \\ &\le \exp\left(-\frac{n\eta_{i(n)}}{2}\right) \\ &\le \exp\left(-\frac{1}{2}\log n\right) = \frac{1}{n^{1/2}} \end{aligned} \tag{4.11}$$

where we first used the fact that $n_0(\eta_{i(n)}) \le n$, and next that $\eta_{i(n)} \ge (\log n)/n$. Letting $n \to \infty$ gives (4.7) as desired.

Conversely, let $S_n \subseteq X^{n+1}$ be the optimum set on which to decide $\boldsymbol{P}$, so that $P_p^{(n)}(S_n) \ge 1-\epsilon$ and $Q_q^n(S_n) = e(n,\epsilon)$. Consider

$$U_\delta = \left\{\tau\colon \sum_{ij} \tau(i,j) \log \frac{P(i,j)}{Q(i,j)} \le D(P,Q) + \delta\right\}.$$

Note that

$$\sum_{ij} \tau(i,j) \log \frac{P(i,j)}{Q(i,j)} = D(\tau, Q) - D(\tau, P).$$

Also, $D(\tau,Q) - D(\tau,P)$ is continuous on $\{\tau \in \boldsymbol{M}\colon \tau \ll P\}$. Since the value of this function at πP is $D(P,Q)$, it follows that there is an open set $G \subseteq U_\delta$ with $\pi P \in G$. Applying (2.3a) to the complement of U_δ with $P_p^{(n)}$ as the underlying measure proves that

$$P_p^{(n)}\{U_\delta\} \to 1.$$

Let

$$U_\delta^n = \left\{x \in X^{n+1}\colon T^n(x) \in U_\delta\right\}.$$

It follows that, for all sufficiently large n,

$$P_p^n(S_n \cap U_\delta^n) \ge \frac{1}{2}(1-\epsilon).$$

A short calculation shows that, for

$$x \in U_\delta^n,\ Q_q^n(x) \ge \alpha P_p^n(x) 2^{-n(D(P,Q)+\delta)}$$

where

$$\alpha \triangleq \inf_{i \in X} \frac{q(i)}{p(i)}.$$

Thus

$$e(n,\epsilon) = Q_q^n(S_n) \ge Q_q^n(S_n \cap U_\delta^n) \ge \frac{1}{2}(1-\epsilon)\alpha 2^{-n(D(P,Q)+\delta)}.$$

Hence

$$\liminf_{n\to\infty} n^{-1} \log e(n,\epsilon) \ge -D(P,Q) + \delta.$$

Letting $\delta \to 0$ concludes the proof of the theorem. □

Remark: Stein's lemma may also be proved by type counting arguments, such as those in Csiszár and Körner, [3] (for the i.i.d. case), and in [4], [9], and [10].

V. Error Exponent for Source Coding

In this section, we prove Theorem 3. To begin, let $I \in \boldsymbol{M}$ denote the uniform transition matrix assigning mass d^{-1} to each element of $X \times X$. First observe that, for any $\tau \in \boldsymbol{M}$:

$$D(\tau, I) = \log d - H(\tau). \tag{5.1}$$

Let $I^{(n)}$ denote the distribution on $\boldsymbol{M}$ induced through the map T^n by the Markov distribution on X^{n+1} with transition matrix I and uniform initial distribution. We first establish the existence of codes satisfying (3.3)–(3.5) for every Markov chain with initial distribution p and irreducible transition probability matrix P.

Let

$$A \triangleq \{\tau \in \boldsymbol{M}\colon H(\tau) < R\}.$$

Note that A is open. Let

$$D_n \triangleq \left\{x \in X^{n+1}\colon T^n(x) \in A\right\}.$$

Then,

$$\operatorname{card}(D_n) = d^{n+1} I^{(n)}(A).$$

Let $\bar{A}$ denote the closure of A. Applying (2.3a) to $\bar{A}$ with $I^{(n)}$ as the underlying measure, and using (5.1)

$$\begin{aligned} \limsup_{n\to\infty} n^{-1} \log I^{(n)}(A) &\le - \inf_{\tau \in \bar{A} \cap \boldsymbol{M}_S} D(\tau, I) \\ &= -\log d + \sup_{\tau \in \bar{A} \cap \boldsymbol{M}_S} H(\tau) = -\log d + R. \end{aligned}$$

Hence,

$$\limsup_{n\to\infty} n^{-1} \log \operatorname{card} D_n \le R. \tag{5.2}$$

Applying (2.3b) to A, with $I^{(n)}$ as the underlying measure, we similarly get

$$\liminf_{n\to\infty} n^{-1} \log \operatorname{card}(D_n + 1) \ge R. \tag{5.3}$$

Applying (2.3a) to $\boldsymbol{M} - A$ with $P_p^{(n)}$ as the underlying measure, gives

$$\limsup_{n\to\infty} n^{-1} \log P_p^{(n)}(\boldsymbol{M} - A) \le - \inf_{\tau \in (\boldsymbol{M} - A) \cap \boldsymbol{M}_S} D(\tau, P). \tag{5.4}$$

Applying (2.3b) to A with $P_p^{(n)}$ as the underlying measure, gives

$$\liminf_{n\to\infty} n^{-1}\log P_p^{(n)}(A) \geq -\inf_{\tau\in \bar{A}\cap \boldsymbol{M}_S} D(\tau,P). \quad (5.5)$$

Using binary strings of length $m_n \triangleq \lceil \log(\operatorname{card} D_n + 1)\rceil$, we can code each source n-string in D_n individually. We use an extra binary m_n-string to code all the source n-strings in $X^{n+1} - D_n$. This defines e_n. We decode the binary strings coding for D_n as the corresponding source n-string. We decode any other binary m_n-string arbitrarily. This defines d_n. Equations (5.2) and (5.3) tell us that the preceding prescription yields a sequence of n to m_n codes satisfying (3.6). Clearly $E(e_n,d_n)\leq P_p^n(X^{n+1}-D_n) = P_p^{(n)}(\boldsymbol{M}-A)$ for this sequence of codes. Hence, (5.4) tells us that (3.4) holds and (5.5) tells us that (3.5) holds for this sequence of codes.

Note that the definition of the code is independent of P.

To prove this sequence of codes is optimal, let (e_n,d_n) be any sequence of n to m_n codes satisfying (3.6). Let $S_n = \operatorname{image}(d_n)$. Then $\operatorname{card}(S_n)\leq 2^{m_n}$, hence, by (3.6):

$$\limsup_{n\to\infty} n^{-1}\log\operatorname{card} S_n \leq R. \quad (5.6)$$

Note that $\tau\to H(\tau)$ and $\tau\to D(\tau,P)$ are continuous functions on $\{\tau\in\boldsymbol{M}\colon \tau\ll P\}$. Hence, given $\tau_0\in\boldsymbol{M}_S$, $\tau_0\ll P$, for any $\epsilon>0$, we can find an open set, $\tilde{U}\subseteq\boldsymbol{M}$ such that $U=\tilde{U}\cap\{\tau\in\boldsymbol{M}\colon \tau\ll P\}$ is relatively open in $\{\tau\in\boldsymbol{M}\colon\tau\ll P\}$, $\tau_0\in U$, and

$$|H(\tau)-H(\tau_0)|<\epsilon, \qquad \forall \tau\in U, \quad (5.7)$$

and

$$|D(\tau,P)-D(\tau_0,P)|<\epsilon, \qquad \forall\tau\in U. \quad (5.8)$$

Applying (2.3b) to $\tilde{U}$, with $I^{(n)}$ as the underlying measure, we get

$$\begin{aligned}\liminf_{n\to\infty} n^{-1}\log\operatorname{card}\{x\in X^{n+1}\colon T^n(x)\in\tilde{U}\} &\geq \log d - \inf_{\tau\in\tilde{U}\cap\boldsymbol{M}_S} D(\tau,I)\\ &= \sup_{\tau\in\tilde{U}\cap\boldsymbol{M}_S} H(\tau)\\ &\geq H(\tau_0). \end{aligned} \quad (5.9)$$

Since

$$\operatorname{card}\{x\in X^{n+1}\colon T^n(x)\in\tilde{U}, x_0=i_0\} = d^{-1}\operatorname{card}\{x\in X^{n+1}\colon T^n(x)\in\tilde{U}\}$$

we also have

$$\liminf_{n\to\infty} n^{-1}\log\operatorname{card}\{x\in X^{n+1}\colon T^n(x)\in\tilde{U}, x_0=i_0\}\geq H(\tau_0). \quad (5.10)$$

If $H(\tau_0)>R$, it follows from (5.6) and (5.10) that, for each $i_0\in X$, for all sufficiently large n, at least half the sequences with empirical distribution in U and initial state i_0 are outside S_n. Now observe that, for any $\tau\in U$ and $x\in X^{n+1}$ such that $T^n(x)=\tau$ and $x_0=i_0$, we have

$$\begin{aligned}P_p^n(x) &= p(i_0)\prod_{(i,j)\in X\times X} P(i,j)^{n\tau(i,j)}\\ &= p(i_0)2^{n\sum_{ij}\tau(i,j)\log P(i,j)}\\ &= p(i_0)2^{-n[D(\tau,P)+H(\tau)]}\\ &\geq p(i_0)2^{-n\sup_{\tau\in U}[D(\tau,P)+H(\tau)]}\\ &\geq p(i_0)2^{-n[D(\tau_0,P)+H(\tau_0)+2\epsilon]} \end{aligned} \quad (5.11)$$

where we have used (5.7) and (5.8) to write the last line.

From the reasoning following (5.10) and (5.11) we have, for all sufficiently large n,

$$\begin{aligned}E(e_n,d_n) &\geq P_p^n\{x\in X^{n+1}-S_n\colon T^n(x)\in U\}\\ &= \sum_{i_0\in X} P_p^n\{x\in X^{n+1}-S_n\colon T^n(x)\in U, x_0=i_0\}\\ &\geq \sum_{i_0\in X}\frac{1}{2}\operatorname{card}\{x\in X^{n+1}\colon T^n(x)\in U, x_0=i_0\}\\ &\quad\cdot p(i_0)2^{-n[D(\tau_0,P)+H(\tau_0)+2\epsilon]}\\ &= (2d)^{-1}\operatorname{card}\{x\in X^{n+1}\colon T^n(x)\in U\}\\ &\quad\cdot 2^{-n[D(\tau_0,P)+H(\tau_0)+2\epsilon]}\end{aligned}$$

so that, from (5.9)

$$\liminf_{n\to\infty} n^{-1}\log E(e_n,d_n)\geq -D(\tau_0,P)-2\epsilon.$$

Letting $\epsilon\to 0$ and then letting τ_0 range over $\{\tau\in\boldsymbol{M}_S\colon H(\tau)>R\}$ yields (3.7).

Let $\tau\in\boldsymbol{M}$ and $x\in X^{n+1}$ be such that $T^n(x)=\tau$ and $x_0=i_0$. Then $P_p^n(x)=p(i_0)2^{-n[D(\tau,P)+H(\tau)]}$. Further, note that $|\tau(i,\cdot)-\tau(\cdot,i)|\leq n^{-1}$ for all $i\in X$. Writing

$$S_n\subseteq\{x\in X^{n+1}\colon H(T^n(x))\leq R\} \cup\big(S_n\cap\{x\in X^{n+1}\colon H(T^n(x))>R\}\big)$$

we have

$$1-E(e_n,d_n)\leq 2^{m_n}2^{-n\inf_{\tau\in\boldsymbol{M}_S\colon H(\tau)>R}[D(\tau,P)+H(\tau)]} + P_p^{(n)}\{\tau\in\boldsymbol{M}\colon H(\tau)\leq R\}. \quad (5.12)$$

From (5.6), (5.12), and (2.3a) applied to $\{\tau\in\boldsymbol{M}\colon H(\tau)\leq R\}$ with $P_p^{(n)}$ as the underlying measure, we have, for any $\epsilon>0$,

$$\begin{aligned}\limsup_{n\to\infty} n^{-1}\log(1-E(e_n,d_n)) \leq \max\Big(&R+\epsilon-\inf_{\tau\in\boldsymbol{M}_S\colon H(\tau)>R}[D(\tau,P)+H(\tau)],\\ &-\inf_{\tau\in\boldsymbol{M}_S\colon H(\tau)\leq R} D(\tau,P)\Big).\end{aligned}$$

We observe that

$$\inf_{\tau\in\boldsymbol{M}_S\colon H(\tau)>R} D(\tau,P)+H(\tau)-R\geq\inf_{\tau\in\boldsymbol{M}_S\colon H(\tau)\leq R} D(\tau,P).$$

Indeed,

$$\begin{aligned}D(\tau,P)+H(\tau)-R &= \sum_{ij}\tau(i,j)\log\frac{\tau(i,j)}{\tau(i,\cdot)P(i,j)}\\ &\quad-\sum_{ij}\tau(i,j)\log\frac{\tau(i,j)}{\tau(i,\cdot)}-R\\ &= -\sum_{ij}\tau(i,j)\log P(i,j)-R\end{aligned}$$

is a linear function on the convex set $\{\tau\in\boldsymbol{M}_S\colon H(\tau)>R\}$. Hence, it attains its minimum over this set on the boundary. It follows that

$$\limsup_{n\to\infty} n^{-1}\log[1-E(e_n,d_n)]\leq\epsilon-\inf_{\tau\in\boldsymbol{M}_S\colon H(\tau)\leq R} D(\tau,P)).$$

Letting $\epsilon\to 0$ establishes (3.11). □

Remarks: The first proof of Theorem 3 is due to by Davisson, Longo and Sgarro, [4], [9], who use ingenious combinatorial arguments to count the number of Markov sequences resulting in a specific transition-count matrix. Theorem 3 was also proved independently by Vasek, [14].

VI. Conclusion

We have considered the problems of binary hypothesis testing and source coding for finite Markov chains. The contribution has been to point out that the basic results on error exponents for these problems, which were already known using combinatorial arguments, can be fairly simply deduced from a Sanov theorem for the distribution of the empirical transition-count matrix. For Markov chains, such Sanov theorems follow from the large deviations theory. One can reasonably expect that a similar line of reasoning will carry over to yield expressions for the error exponents in the analogous problems for more general stationary sources, in situations where a Sanov theorem is known.

Acknowledgment

The author would like to thank the anonymous referees for their careful review of earlier versions of this correspondence.

References

[1] R. R. Bahadur, "Some Limit Theorems in Statistics," *CBMS Regional Conf. Series in Appl. Math.*, no. 4, 1971.
[2] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*. New York: Prentice Hall, 1971.
[3] Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Sources*. New York: Academic 1981.
[4] L. D. Davisson, G. Longo, and A. Sgarro, "The error exponent for the noiseless encoding of finite ergodic Markov sources," *IEEE Trans. Inform. Theory*, vol. IT-27, no. 4, pp. 431–438, 1981.
[5] J. Deuschel and D. Stroock, *Large Deviations*. New York: Academic, 1989.
[6] M. Donsker and S. R. S. Varadhan, "Asymptotic evaluation of certain Markov process expectations for large time, part I," *Commun. Pure and Appl. Math.*, vol. 28, pp. 1–47, 1975.
[7] R. S. Ellis, "Large deviations for a general class of random vectors," *Ann. Probability*, vol. 12, no. 1, pp. 1–12, 1984.
[8] R. S. Ellis, "Entropy, large deviations, and statistical mechanics," *Graduate Texts in Mathematics*, vol. 271. New York: Springer-Verlag, 1985.
[9] G. Longo and A. Sgarro, "The source coding theorem revisited: A combinatorial approach," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 5, pp. 544–548, 1979.
[10] S. Natarajan, "Large deviations, hypothesis testing, and source coding for finite Markov chains," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 3, pp. 360–365, 1985.
[11] I. N. Sanov, "On the probability of large deviations of random variables," *Selected Translations on Mathematical Statistics and Probability*, American Mathematical Society, no. 1, pp. 213–244, 1957.
[12] D. Stroock, *An Introduction to the Theory of Large Deviations*. New York: Springer-Verlag, Universitext, 1984.
[13] S. R. S. Varadhan, "Large Deviations and Applications," *CBMS-NSF, Regional Conf. Ser. Appl. Math.*, no. 46, 1989, pp. 31–55.
[14] K. Vasek, "On the error exponent for ergodic Markov source," *Kybernetika*, vol. 16, no. 4, pp. 318–329, 1980.

The Hardness of Solving Subset Sum with Preprocessing

ANTOINE LOBSTEIN

***Abstract*—The two problems *subset sum* and *linear decoding* (which have given birth to the knapsack and the McEliece public-key cryptosystems) are known to be NP-complete. For *linear decoding*, it has been proved that, even if one knows the linear code in advance and can preprocess it, the existence of a polynomial-time decoding algorithm would imply that the polynomial-time hierarchy collapses at an early stage. It is proven that the same holds for *subset sum*: Even if the knapsack is known in advance and can be preprocessed, there is no polynomial-time algorithm solving it, unless the polynomial hierarchy collapses. We also give the sketch of a new, straightforward proof of this result for *linear decoding*.**

Manuscript received July 13, 1989; revised October 31, 1989.
The author is with the Centre National de la Recherche Scientifique, URA 820, Télécom Paris, Département Informatique, 46 rue Barrault 75634, Paris Cedex 13, France.
IEEE Log Number 9034947.

I. Introduction

The following two decision problems are *NP*-complete.

Name: subset sum ([3], p. 247).
Input: $n+1$ nonnegative integers $a_1, a_2, \cdots, a_n, S$.
Question: Is there a binary vector $\boldsymbol{x}$ (with length n) such that $\sum_{1 \le i \le n} a_i \cdot x_i = S$?
The sequence $a_1, a_2, \cdots, a_n$ is usually called a *knapsack*.

Name: linear decoding [1].
Input: A binary matrix $\boldsymbol{H}$, a binary vector $\boldsymbol{y}$, and a nonnegative integer w.
Question: Is there a binary vector $\boldsymbol{x}$ such that $\boldsymbol{Hx} = \boldsymbol{y}$ and $wt(\boldsymbol{x}) \le w$?

Linear decoding corresponds to the decision problem for the closest codeword to an erroneous word, with syndrome $\boldsymbol{y}$, received at the end of a binary symmetric channel on which a linear error-correcting block code, with parity-check matrix $\boldsymbol{H}$, is used. Note that linear decoding can also be formulated, in an equivalent way, using a generator matrix $\boldsymbol{G}$ of the code, instead of a parity-check matrix (we refer to [1] for these basic notations, definitions and properties from coding theory).

Apart from its interest in coding theory, linear decoding has also been used to devise a public-key cryptosystem known as the McEliece cryptosystem, and subset sum is the basis of the so-called knapsack cryptosystem.

The scheme of these two public-key systems is as follows ([6] and [7]): consider an "easy" (polynomial-time solvable) class of inputs of these *NP*-complete problems (a generator matrix $\boldsymbol{G}$ of a Goppa code for linear decoding, or a "super-increasing" knapsack $a_1, a_2, \cdots, a_n$ for subset sum, for instance). Any user $\mathscr{B}$ wishing to receive a ciphertext chooses such an easy input, and transforms it into a new one, which looks like any difficult input of the problem (for linear decoding, $\mathscr{B}$ multiplies $\boldsymbol{G}$ by a nonsingular matrix $\boldsymbol{S}$ and a permutation matrix $\boldsymbol{P}$, to get $\boldsymbol{G'} = \boldsymbol{SGP}$; for subset sum, $\mathscr{B}$ chooses two integers m and w, with $gcd(m, w) = 1$, and computes $a'_i = w \cdot a_i (\mathrm{mod}\, m)$, for $i = 1, \cdots, n$). Only $\boldsymbol{G'}$ (and t, its error-correcting capacity), or $a'_1, a'_2, \cdots, a'_n$ are made public, whereas $\boldsymbol{G}$, $\boldsymbol{S}$ and $\boldsymbol{P}$, or $a_1, a_2, \cdots, a_n$, m and w, are not. Any user $\mathscr{A}$ wishing to send a ciphertext to $\mathscr{B}$ looks for $\mathscr{B}$'s public key $(\boldsymbol{G'}, t)$ or $(a'_1, a'_2, \cdots, a'_n)$.

Next, in the McEliece system, $\mathscr{A}$ enciphers a message $\boldsymbol{M}$ (which must be a binary vector of appropriate length) by computing $\boldsymbol{C} = \boldsymbol{MG'} + \boldsymbol{E}$, where $\boldsymbol{E}$ is a binary random vector (of appropriate length) with weight t. When receiving $\boldsymbol{C}$, user $\mathscr{B}$, who is the only one knowing $\boldsymbol{G}$, $\boldsymbol{S}$ and $\boldsymbol{P}$, computes $\boldsymbol{CP}^{-1} = (\boldsymbol{MS})\boldsymbol{G} + \boldsymbol{EP}^{-1}$; because $wt(\boldsymbol{EP}^{-1}) = wt(\boldsymbol{E}) = t$, which is the error-correcting capacity of the Goppa code, $\mathscr{B}$ can now quickly decode $\boldsymbol{CP}^{-1}$ and recover $\boldsymbol{MS}$, hence $\boldsymbol{M}$. But a cryptanalyst, intercepting $\boldsymbol{C}$, has seemingly some sort of a general input, of an *NP*-complete problem, to solve: to recover $\boldsymbol{M}$ directly from $\boldsymbol{C} = \boldsymbol{MG'} + \boldsymbol{E}$ is the decoding of the code defined by $\boldsymbol{G'}$.

In the knapsack system, $\mathscr{A}$ enciphers a message $\boldsymbol{M}$ (which is a binary vector of length n) by computing $C = \sum_{1 \le i \le n} M_i \cdot a'_i$.