Random Coding Bound for $E$-Capacity of DMC
with Stochastic Encoding

Farshin Hormozi nejad
Islamic Azad University Ahvaz branch, Iran
hormozi-nejad@iauahvaz.ac.ir

Nasrin Afshar
Hamadan Payame Noor University, Iran
afshar-math@yahoo.com

Abstract

This paper gives a lower bound for rate-reliability function of the discrete memoryless channel (DMC) with stochastic encoding. The result shows that, the stochastic encoding gets bigger random coding bound rather than that of the discrete memoryless channel where deterministic encoding is applied.

Mathematics Subject Classification: 68P30, 94A24

Keywords: E-capacity, error probability exponent, method of types, random coding bound, stochastic encoding

1 Introduction

We study the rate-reliability function ($E$-capacity) of the discrete memoryless channel (DMC). The rate-reliability function $R(E) = C(E)$ was first introduced by Haroutunian [3]. The function is inverse to Shannon’s reliability function [9], which characterizes fundamental properties of every communication channel. The reliability function was defined by Shannon as the optimal exponent of the exponential decrease $\exp\{-NE(R)\}$ of the decoding error probability for one-way channel [9]. Furthermore the concept of $E$-capacity is a generalization to the Shannon’s channel capacity. The notion $C(E)$ is in natural conformity with the notion of the channel capacity $C$. Random coding bound for $E$-capacity of DMC [4] and random coding bound for $E$-capacity of different broadcast channels have been studied [6]. So broadcast channel with
confidential messages [2], Random coding bound for E-capacity region of the broadcast channel [7] and Bounds for E-Capacity of DMC [5] are investigated which those problems involve security, the stochastic encoding is applied.

In this paper, we investigate the stochastic encoding to find a lower bound for E-capacity of the DMC.

2 Preliminary Notes

We begin with notations. Through out this work, capital letters represent random variables (RV’s), and specific realizations of them are denoted by the corresponding lower case letters. Random vectors of dimension $N$ will be denoted by bold-face letters. For any finite set $X$, the cardinality of $X$ is denoted by $|X|$. The notation $U → X → Y$ means that these RV’s form a Markov chain in this order. The functions log and exp are taken to the base 2.

**Definition 2.1** [1, 6, 8] A discrete memoryless channel (DMC) $W$ with input alphabet $X$ and output alphabet $Y$ is defined by a stochastic matrix of transition probabilities $W : X → Y$. An element $W(y|x)$ of the matrix is a conditional probability of receiving the symbol $y ∈ Y$ on the channel’s output if the symbol $x ∈ X$ is transmitted from the input.

Let $M$ be a finite message set and $U$ some finite set.

**Definition 2.2** [1, 6] A $N$-block code $(f, g)$ for the channel $W$ is a pair of mappings, where $f : M → X^N$ is encoding and $g : Y^N → M$ is decoding. $N$ is called the code length. $x = (x_1, ..., x_N) ∈ X^N$ is the input codeword and $y ∈ Y^N$ is the output vector of length $N$. The code rate is $R = \frac{1}{N} \log |M|$. The $N$-th extension of the DMC transition probability is denoted by $W^N(y|x)$, where

$$W^N(y|x) = \prod_{n=1}^{N} W(y_n|x_n).$$

**Definition 2.3** [1, 6] The probability of erroneous transmission of the message $m ∈ M$ by the channel using the code $(f, g)$ is defined as follows

$$e(f, g, W, m) = \sum_{x_m} f(x_m|m)W^N(Y^N - g^{-1}(m)|x_m),$$

Where $x_m$ is the encoded vector of the message $m$. 
Let $N(x|x)$ denote the number of occurrences of symbol $x$ in $x$. The type $P_x$ of $x$ is defined as the probability mass function [1],

$$ P_x(x) = \frac{N(x|x)}{N}, \quad x \in \mathcal{X}. $$

Let $\mathcal{P}_N(\mathcal{X}) = \{P_x : x \in \mathcal{X}^N\}$ denotes the set of all possible types of $N$-vectors in $\mathcal{X}^N$ and

$$ T_Q^N(\mathcal{X}) = \{x : P_x = Q\}. $$

Let us define the canonical conditional type $P_{y|x}$ of $y$ given $x$ as follows [1]

$$ P_{y|x}(y|x) = \begin{cases} 0, & N(x|x) = 0; \\ \frac{N(x,y|x,y)}{N(x|x)}, & \text{otherwise}, \end{cases} $$

where $N(x,y|x,y)$ is the number of occurrences of $(x,y)$ in pair $(x,y)$. If $V : \mathcal{X} \to \mathcal{Y}$ is the conditional type of $y$ given $x \in T_Q^N(\mathcal{X})$, then $y$ is said to lie in $T_{Q,V}^N(Y|x)$. We denote

$$ \mathcal{Y}_N(Q,Y) = \{P_{y|x} : x \in T_Q^N(\mathcal{X}), \ y \in \mathcal{Y}^N\}. $$

**Definition 2.4** [6] (E-achievable rate)

Let $E > 0$. Nonnegative real number $R$ is called $E$-achievable rate for DMC $W$, if for any $\delta > 0$ and sufficiently large $N$ there exists a code such that

$$ \frac{1}{N} \log |\mathcal{M}| \geq R - \delta, $$

and

$$ \overline{e}(f, g, W) \leq \exp\{-NE\}. $$

Rate reliability function $C(E)$, which by analogy with the capacity is called $E$-capacity, for average error probability is defined the set of all $E$-achievable rates $R$.

### 3 Random code construction with Stochastic Encoding

As a preliminary for the random code construction some finite set $\mathcal{U}$ is chosen. The $\text{DMC}\{W : \mathcal{X} \to \mathcal{Y}\}$ is extended, with an additional input symbol $W : \mathcal{U} \times \mathcal{X} \to \mathcal{Y}$, where

$$ W(y|u,x) = W(y|x), \text{ for all } (u,x) \in \mathcal{U} \times \mathcal{X}. $$
A type $Q_0 \in \mathcal{P}_N(U)$ is chosen for the constraint length $N$. Then each of the set $\Theta_0 = \{u_m\}_{m \in M}$ of $N$-vectors is uniformly, randomly and independently chosen from $\mathcal{T}_{Q_0}^N(U)$. Then the conditional type $Q_1 \in \mathcal{V}_N(Q_0, \mathcal{X})$ is chosen. For each $u_m$, consider its $Q_1$-shell $\mathcal{T}_{Q_0,Q_1}^N(X|u_m)$. Each of the set $\Theta_1(m) = \{x_{j,m}\}_{j \in J}$ of distinct $N$-vectors is chosen uniformly, independently from $\mathcal{T}_{Q_0,Q_1}^N(X|u_m)$.

Then the conditional type $Q_1 \in \mathcal{V}_N(Q_0, X)$ is chosen. For each $u_m$, consider its $Q_1$-shell $\mathcal{T}_{Q_0,Q_1}^N(X|u_m)$. Each of the set $\Theta_1(m) = \{x_{j,m}\}_{j \in J}$ of distinct $N$-vectors is chosen uniformly, independently from $\mathcal{T}_{Q_0,Q_1}^N(X|u_m)$.

Then the random code $\Theta$ is defined as the structure $\{x_{j,m}\}_{j \in J, m \in M}$. We specify the structure of stochastic encoder $f$ and its uniform randomization over junk data $J$. The junk data $J$ is a random variable chosen randomly from $\{1, \ldots, |J|\}$. Then the conditional probability $f$ is

$$f(x|m) = \begin{cases} \frac{1}{|J|}, & \text{if } x \in \{x_{j,m}\}_{j \in J}; \\ 0, & \text{otherwise}. \end{cases}$$

So the expected average error probability over the random code is the following

$$E(\tau_\theta(f, g, W)) = E\left(\sum_{m \in M} \sum_{x \in \Theta} W_N((g^{-1}(m))^c|x)f(x|m)\right) = \sum_{V \in \mathcal{V}_N(Q,Y)} \exp\{-ND(V||W|Q)\} \times$$

$$E\left(\sum_{x \in \Theta} \frac{1}{|M|} \sum_{m \in M} \frac{|(g^{-1}(m))^c \cap \mathcal{T}_{Q,V}^N(Y|x)|}{|\mathcal{T}_{Q,V}^N(Y|x)|} \times f(x|m)\right).$$

Using Lemma 4.1 [6], we obtain

$$E(\tau_\theta(f, g, W)) \leq (N + 1)^{|X|\times|Y|} \max_{V \in \mathcal{V}_N(Q,Y)} \left\{ \exp\{-ND(V||W|Q)\} \times \right.$$

$$\left. E\left(\frac{1}{|M| \times |J|} \sum_{m \in M, j \in J} \frac{|(g^{-1}(m))^c \cap \mathcal{T}_{Q,V}^N(Y|x)|}{|\mathcal{T}_{Q,V}^N(Y|x)|} \right)\right\}. \tag{1}$$

**Theorem 3.1** For DMC $W$, for all $E > 0$ the following bound of $E$-capacity holds,

$$C(E, W) \geq \max_Q \min_{V: D(V||W|Q) \leq E} \left| I_{Q,V}(X \land Y) - I_{Q_0,Q_1}(U \land X) + D(V||W|Q) - E \right|^+. $$

where $U \rightarrow X \rightarrow Y$ is a Markov chain.

**Proof:** We must show that for any $\delta > 0$ and $N$ large enough there exists a code of length $N$ with

$$|M| = \exp\{N|I_{Q,V}(X \land Y) - I_{Q_0,Q_1}(U \land X) + D(V||W|Q) - E - \delta|\}^+. \tag{2}$$
and average error probability tends to zero.

Let us choose \( \Theta = \{ x_{j,m} \} \) \( j \in J, m \in M \subset T_{Q_0Q_1}(X|u_m) \). We specify the structure of stochastic encoder \( f \) and its uniform randomization over junk data \( J \) as described in Section 2.

Let us apply decoding rule for decoder \( g \) using criterion of the minimum divergence. Each \( y \) can be decoded to such \( m' \) that for some \( V' \)

\[
y \in T_{Q,V'}^N(Y|x_{j',m'}) \text{ and } D(V'|W|Q) \text{ is minimal.}
\]

The decoder \( g \) can make an error, if the message \( m \) is transmitted, but there exists \( m' \neq m \), such that for some \( V' \)

\[
y \in T_{Q,V'}^N(Y|x_{j',m'}) \cap T_{Q,V}^N(Y|x_{j,m}) \text{ and } D(V'|W|Q) \leq D(V|W|Q). \tag{3}
\]

Denote for some \( V \)

\[
D(Q,V) = \{ V \in \mathcal{V}^N(Q,V) : D(V'|W|Q) \leq D(V|W|Q) \}
\]

Then from (3) we have

\[
|\{(g^{-1}(m))^c \cap T_{Q,V}^N(Y|x_{j,m})\}| \leq \sum_{V' \in D(Q,V)} \sum_{m' \neq m} \sum_{j' \in J} |T_{Q,V'}^N(Y|x_{j',m'}) \cap T_{Q,V}^N(Y|x_{j,m})|.
\tag{4}
\]

So in light of (4), to bound \( E(|\{(g^{-1}(m))^c \cap T_{Q,V}^N(Y|x_{j,m})\}) \) in (1), it suffices we bound:

\[
E(|T_{Q,V'}^N(Y|x_{j',m'}) \cap T_{Q,V}^N(Y|x_{j,m})|) =
\]

\[
\sum_{y \in T_{Q,V'}^N(Y) \cap T_{Q,V}^N(Y)} Pr\{ y \in T_{Q,V}^N(Y|x_{j,m}) \cap T_{Q,V}^N(Y|x_{j',m'}) \} \leq
\]

\[
|T_{Q,V}^N(Y)| \times \exp\{-N(I_{Q,V}(X \land Y) + \delta)\} \times \exp\{-N(I_{Q,V'}(X \land Y) + \delta)\}. \tag{5}
\]

From (5) and Lemma 1.2 in [6] we obtain

\[
E\left( \frac{|T_{Q,V}^N(Y|x_{j,m}) \cap T_{Q,V}^N(Y|x_{j,m})|}{|T_{Q,V}^N(Y|x_{j,m})|} \right) \leq (N+1)|\mathcal{Y}| \exp\{-N(I_{Q,V'}(X \land Y) + 2\delta)\}.
\]

From (2) for every \( V' \in \mathcal{V}(Q,Y) \) we have

\[
|M| = \exp\{N[I_{Q,V'}(X \land Y) - I_{Q_0Q_1}(U \land X) + D(V'|W|Q) - E - \delta^\dagger}\}.
\]
So it follows that
\[
\sum_{m' \neq m} E \left( \frac{|T_{Q,V}^N(Y|x_{j,m'}) \cap T_{Q,V}^N(Y|x_{j,m})|}{|T_{Q,V}^N(Y|x_{j,m})|} \right) \leq (N + 1)^{|\mathcal{Y}|} \exp \left\{ N \left( I_{Q,V'}(X \wedge Y) - I_{Q_0,Q_1}(U \wedge X) + D(V'\|W|Q) - E - \delta \right) \right\} \\
\times \exp \left\{ -N \left( I_{Q,V'}(X \wedge Y) + 2\delta \right) \right\} = (N + 1)^{|\mathcal{Y}|} \times \exp \left\{ -N \left( I_{Q_0,Q_1}(U \wedge X) + E - D(V'\|W|Q) + \delta \right) \right\}. \tag{6}
\]

From (1), (5) and (6) we conclude
\[
E(\tau_\Theta(f,g,W)) \leq (N + 1)^{2|\mathcal{Y}| + |\mathcal{X}|} \times |\mathcal{J}| \times \exp \left\{ -N \left( I_{Q_0,Q_1}(U \wedge X) + E - D(V'\|W|Q) + \delta' \right) \right\} \times \exp \left\{ -ND(V\|W|Q) \right\} \leq \exp \{ -NE \}.
\]

4 Main Results

We studied a lower bound for rate-reliability function of the discrete memoryless channel with stochastic encoding and derived a random coding bound for E-capacity region of it. We obtained that the stochastic encoding gets bigger random coding bound rather than that of the DMC where the deterministic encoding is applied.

ACKNOWLEDGMENTS.

This work was supported by Islamic Azad University Ahvaz branch grant 5106391126004.

References


Random coding bound for $E$-capacity of DMC with stochastic encoding


Received: July, 2011