Mathematical Problems of Computer Science 35, 53-62, 2011.

Random Coding Bound for E-capacity Region of Asymmetric Broadcast Channel With Stochastic Encoding

Nasrin Afshar

Institute for Informatics and Automation Problems of NAS of RA

Abstract

E-capacity (rate-reliability) region of the asymmetric broadcast channel with stochastic encoding is studied. The asymmetric broadcast channel involves two discrete memoryless channels with a common input. A common message is transmitted to both receivers and one private message to the intended receiver. We derive an inner bound for rate-reliability region.

Key words: Asymmetric broadcast channel, E-capacity, error exponent, random coding bound, rate-reliability region, stochastic encoding.

1. Introduction

The rate-reliability function for a discrete memoryless channel (DMC), which by analogy with the capacity is called E-capacity, was first introduced by E. Haroutunian in 1967 [4]. The survey studies the function $R(E) = C(E)$, which presents optimal dependence between rate R and reliability E. The function $R(E)$ is inverse to reliability function $E(R)$ introduced by Shannon [12] as the optimal exponent of the exponential decrease $\exp\{-NE(R)\}$ of the decoding error probability for oneway channel. Along with achievements in this part of Shannon theory a lot of problems have remained unsolved. It seems that the approach, rate-reliability function, is useful for this purpose [4], [5]. Furthermore the concept of the E-capacity is a generalization to the Shannon's capacity of a channel. The notion $C(E)$ is in natural conformity with Shannon's notions of the channel capacity C and the zero error capacity C_0. When E increases from zero to infinity the function $C(E)$ decreases from C to C_0.

In a broadcast channel (BC), as introduced by Cover [1], one source is communicating to two receivers. In later works, different broadcast channels has been considered. Asymmetric broadcast channel contains two receivers with one common and one private messages. Works on asymmetric broadcast channels include [9], [10], the capacity region was found in [10]. E-capacity region $C(E)$ for maximal error probability is the set of all E-achievable rates. Random coding bound for E-capacity region of the BC, where one common and two private messages are transmitted was found by M. E. Haroutunian [8].

In this paper, we consider the discrete memoryless asymmetric broadcast channel with stochastic encoding and we will find an inner bound for E-capacity region. We apply the method of types. Although for problems not involving secrecy, stochastic encoding seldom offers any advantage, this study can be useful through out future works which contains secrecy.

The reminder of the paper is organized as follows. In section 2, the formal setting and notation and problem formulation is given. Section 3 is dedicated to prove the theorem established in section 2. Finally, section 4 is devoted to the result and future direction.

2. Preliminaries and Problem Formulation

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 $\mathcal{X}$, the cardinality of $\mathcal{X}$ is denoted by $|\mathcal{X}|$. The set of N-vactors of elements of $\mathcal{X}$ is denoted by $\mathcal{X}^N$.

We investigate a discrete memoryless asymmetric broadcast channel with a finite input alphabet set $\mathcal{X}$, and finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$. The broadcast channel is defined by the pair (W_1, W_2) of conditional probability distributions, $W_1 : \mathcal{X} \to \mathcal{Y}$, $W_2 : \mathcal{X} \to \mathcal{Z}$, where

$$W_1^N(\mathbf{y}|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_1(y_n|x_n). \quad W_2^N(\mathbf{z}|\mathbf{x}) \triangleq \prod_{n=1}^{N} W_2(z_n|x_n),$$

where the product expression follows from the fact that channels are memoryless, and the vector $\mathbf{x} \in \mathcal{X}^N$ is the input codeword, $\mathbf{y} \in \mathcal{Y}^N$, $\mathbf{z} \in \mathcal{Z}^N$ are the output vectors of length N. $\mathcal{M}_N$ is the set of common messages which should be sent to the both receivers and $\mathcal{L}_N$ is the set of private messages which should be sent to receiver 1. Let $\mathcal{U}_1$, $\mathcal{U}_2$ be some auxiliary finite sets and U_1, U_2, X, Y and Z are random variables with values correspondingly in $\mathcal{U}_1, \mathcal{U}_2, \mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$. The notation $(U_1.U_2) \to X \to Y$ means that these RV's form a Markov chain in this order. Randomized encoding is defined as follows

Definition 1: *A stochastic encoder f with block length N for the asymmetric broadcast channel is specified by a matrix of conditional probabilities $f(\mathbf{x}|m, l)$, where $\mathbf{x} \in \mathcal{X}^N$, $m \in \mathcal{M}_N$, $l \in \mathcal{L}_N$ and $\sum_{\mathbf{x} \in \mathcal{X}^N} f(\mathbf{x}|m, l) = 1$.*

Definition 2: *A code is a triple of mappings $(f. g_1. g_2)$, where $f : \mathcal{M}_N \times \mathcal{L}_N \to \mathcal{X}^N$ is a stochastic encoder and $g_1 : \mathcal{Y}^N \to \mathcal{M}_N \times \mathcal{L}_N$ and $g_2 : \mathcal{Z}^N \to \mathcal{M}_N$ are deterministic decoders. $g_1^{-1}(m. l)$ is the set of all $\mathbf{y} \in \mathcal{Y}^N$, which are decoded to m, l, and $g_2^{-1}(m)$ is the set of all $\mathbf{z} \in \mathcal{Z}^N$, which are decoded to m.*

Definition 3: *The probabilities of erroneous transmission of the pair of messages $(m, l) \in \mathcal{M}_N \times \mathcal{L}_N$ by the channels W_1 and W_2 using a code $(f. g_1. g_2)$ are defined, respectively,*

$$e(f, g_1. W_1. m. l) \triangleq \sum_{\mathbf{x} \in \mathcal{X}^N} f(\mathbf{x}|m. l) W_1^N(\mathcal{Y}^N - g_1^{-1}(m, l)|\mathbf{x}).$$

$$e(f. g_2. W_2. m) \triangleq \sum_{\mathbf{x} \in \mathcal{X}^N} f(\mathbf{x}|m. l) W_2^N(\mathcal{Z}^N - g_2^{-1}(m)|\mathbf{x}).$$

Define maximal probabilities of error of the code $(f. g_1. g_2)$

$$e(f. g_1. W_1) \triangleq \max_{m \in \mathcal{M}_N. l \in \mathcal{L}_N} e(f. g_1. W_1. m, l).$$

$$e(f. g_2. W_2) \triangleq \max_{m \in \mathcal{M}_N} e(f. g_2. W_2. m).$$

and the average error probabilities for messages assuming that the pair of random messages M_N, L_N is uniformly distributed over $\mathcal{M}_N \times \mathcal{L}_N$ are defined :

$$\bar{e}(f, g_1, W_1) \triangleq \frac{1}{|\mathcal{M}_N| \times |\mathcal{L}_N|} \sum_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} e(f, g_1, W_1, m, l).$$

$$\bar{e}(f, g_2, W_2) \triangleq \frac{1}{|\mathcal{M}_N|} \sum_{m\in\mathcal{M}_N} e(f, g_2, W_2, m).$$

Definition 4: *A code (f, g_1, g_2) is characterized by rates R_1, R_2, where R_1 and R_2 are the transmission rates, respectively, for $m \in \mathcal{M}_N$ and $l \in \mathcal{L}_N$*

$$R_1 = \frac{1}{N}\log|\mathcal{M}_N|, \ R_2 = \frac{1}{N}\log|\mathcal{L}_N|.$$

The functions log and exp are taken to the base 2. For the definition of the rate-reliability function, we refer to [6], [7].

Definition 5: *(E-achievable rates) Let $E = (E_1, E_2)$, $E_i > 0$, $i = 1, 2$ be given. A rate pair R_1, R_2 is called E-achievable rates for the broadcast channel iff for any $\delta > 0$ and sufficiently large N there exists a code, such that*

$$\frac{1}{N}\log|\mathcal{M}_N||\mathcal{L}_N| \geq R_1 + R_2 - \delta, \ \frac{1}{N}\log|\mathcal{M}_N| \geq R_1 - \delta. \tag{1}$$

and maximal probabilities of error exponentially decrease with positive reliabilities E_1 and E_2, respectively,

$$e(f, g_1, W_1) \leq \exp\{-NE_1\}, \ \ e(f, g_2, W_2) \leq \exp\{-NE_2\}. \tag{2}$$

Definition 6: *E-capacity region $C(E)$ for maximal error probabilities is defined as the set of all E-achievable rates R_1, R_2. $\bar{C}(E)$ is denoted for E-capacity region when average error probabilities are applied.*

Let $Q_1 \triangleq \{Q_1(u_1) : u_1 \in \mathcal{U}_1\}$ be probability distribution (PD) of random variable U_1. $Q_2 \triangleq \{Q_2(u_2|u_1) : u_1 \in \mathcal{U}_1, \ u_2 \in \mathcal{U}_2\}$ conditional PD of random variable U_2 for given value u_1 and $P \triangleq \{P(x|u_1, u_2) : u_2 \in \mathcal{U}_2, \ x \in \mathcal{X}\}$ conditional PD of random variable X for given value u_2. Define $V_1 \triangleq \{V_1(y|x) : x \in \mathcal{X}, \ y \in \mathcal{Y}\}$ as the conditional PD of random variable Y for given values x, and $V_2 \triangleq \{V_2(z|x) : x \in \mathcal{X}, \ z \in \mathcal{Z}\}$ as the conditional PD of random variable Z for given value x. Let denote $Q(u_1, u_2) = Q_1(u_1)Q_2(u_2|u_1)$. We consider the following joint distributions

$$Q \circ P \circ V_1 = \{Q \circ P \circ V_1(u_1, u_2, x, y) = Q(u_1, u_2)P(x|u_1, u_2)V(y|x),$$
$$u_1 \in \mathcal{U}_1, \ u_2 \in \mathcal{U}_2, \ x \in \mathcal{X}, \ y \in \mathcal{Y}\}.$$
$$Q \circ P \circ V_2 = \{Q \circ P \circ V_2(u_1, u_2, x, z) = Q(u_1, u_2)P(x|u_1, u_2)V(z|x),$$
$$u_1 \in \mathcal{U}_1, \ u_2 \in \mathcal{U}_2, \ x \in \mathcal{X}, \ z \in \mathcal{Z}\}.$$

So we have Markov chain $(U_1, U_2) \to X \to (Y, Z)$.

For the notion of types and conditional types we refer to [3], [7]. The set of all probability distributions Q on $\mathcal{U}_1 \times \mathcal{U}_2$ is denoted by $\mathcal{Q}(\mathcal{U}_1 \times \mathcal{U}_2)$ and the subset of $\mathcal{Q}(\mathcal{U}_1 \times \mathcal{U}_2)$, consisting of all possible joint types Q of N-length vectors $\mathbf{u}_1$, $\mathbf{u}_2$, by $\mathcal{Q}_N(\mathcal{U}_1 \times \mathcal{U}_2)$.

We use the notations of entropies and mutual informations as defined in [7]. The notation $D(V\|W|Q,P)$ denotes the divergence between conditional distributions V, W given distribution Q and P.

If $V_1 : \mathcal{X} \to \mathcal{Y}$ and $V_2 : \mathcal{X} \to \mathcal{Z}$ are the conditional types of respectively $\mathbf{y}$ and $\mathbf{z}$ given $\mathbf{x} \in \mathcal{T}^N_{Q,P}(X)$, then according to lemma 1.2.6 in [3] we have

$$W_1^N(\mathbf{y}|\mathbf{x}) = \exp\{-N[D(V_1\|W_1|Q,P) + H_{Q,P,V_1}(Y|X)]\}, \text{ for all } \mathbf{y} \in \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{x}). \quad (3)$$

$$W_2^N(\mathbf{z}|\mathbf{x}) = \exp\{-N[D(V_2\|W_2|Q,P) + H_{Q,P,V_2}(Z|X)]\}, \text{ for all } \mathbf{z} \in \mathcal{T}^N_{Q,P,V_2}(Z|\mathbf{x}). \quad (4)$$

To formulate the inner bound of E-capacity region, we consider the following inequalities

$$0 \le R_1 \le \max_Q \min\left\{ \min_{V_1:D(V_1\|W_1|Q,P)\le E_1} \left| I_{Q,P,V_1}(Y \wedge U_1) + D(V_1\|W_1|Q,P) - E_1 \right|^+, \right.$$

$$\left. \min_{V_2:D(V_2\|W_2|Q,P)\le E_2} \left| I_{Q,P,V_2}(Z \wedge U_1) + D(V_2\|W_2|Q,P) - E_2 \right|^+ \right\}, \quad (5)$$

$$0 \le R_2 \le \max_Q \min_{V_1:D(V_1\|W_1|Q,P)\le E_1} \left| I_{Q,V_1}(Y \wedge U_2|U_1) + D(V_1\|W_1|Q,P) - E_1 \right|^+. \quad (6)$$

and the regions

$$R_r(Q,P,E) = \{(R_1,R_2) : (5) \text{ and } (6) \text{ take place for some } (U_1,U_2) \to X \to (Y,Z)\}.$$

$$R_r(E) = \bigcup_{QP \in QP(\mathcal{U}_1\times\mathcal{U}_2\times\mathcal{X})} R_r(Q,P,E).$$

Theorem: *For all $E_1 > 0, E_2 > 0$ the region $R_r(E)$ is an inner estimate for E-capacity region of the broadcast channel:*

$$R_r(E) \subseteq C(E) \subseteq \overline{C}(E).$$

Concerning methods for the bounds construction, E. Haroutunian proved that the Shannon's random coding method [11] to prove existence of codes with certain properties, can be applied to study the rate-reliability function as well [4], [5], see also [6], [7]. Proof of the theorem is presented in next section.

3. Proof of the Theorem

We shall show that the rate region specified in Theorem is E-achievable. To this end we must show that there exists a code with certain properties for achievement based on a random coding technique.

We assume given pair R_1, R_2 that satisfy (5), (6). We wish to find a code such that for any $\delta > 0$ and N large enough with

$$|\mathcal{M}_N| = \exp\left\{ N \max_Q \min\{ \min_{V_1:D(V_1\|W_1|Q,P)\le E_1} \left| I_{Q,P,V_1}(Y \wedge U_1) + D(V_1\|W_1|Q,P) - E_1 - \delta \right|^+, \right.$$

$$\left. \min_{V_2:D(V_2\|W_2|Q,P)\le E_2} \left| I_{Q,P,V_2}(Z \wedge U_1) + D(V_2\|W_2|Q,P) - E_2 - \delta \right|^+ \} \right\}. \quad (7)$$

$$|\mathcal{L}_N| = \exp\{N \max_{Q} \min_{V_1: D(V_1 \| W_1 | Q, P) \le E_1} |I_{Q,P,V_1}(Y \wedge U_2 | U_1) + D(V_1 \| W_1 | Q, P) - E_1 - \delta|^+\} \quad (8)$$

satisfy (1) and maximal error probabilities satisfy (2).

We explain codebook generation, then encoding scheme and decoding strategies separately

Codebook generation: Let $\mathcal{U}_1$, $\mathcal{U}_2$ be some finite sets and Q_1 some type. We generate the codebook by the following steps.

1. Generate $|\mathcal{M}_N|$ vectors $\mathbf{u}_1(m)$, which are drawn uniformly, independently from $\mathcal{T}^N_{Q_1}(U_1)$.

2. Let Q_2 be a conditional type. For each $\mathbf{u}_1(m)$ choose $|\mathcal{L}_N|$ vectors uniformly, independently from $\mathcal{T}^N_Q(U_2|\mathbf{u}_1(m))$. Denote the vectors with $\mathbf{u}_2(m,l)$, $l = 1, \dots, |\mathcal{L}_N|$.

3. Let P be a conditional type. For every $\mathbf{u}_2(m,l)$ choose uniformly, independently $|\mathcal{J}|$ codewords from P-shell $\mathcal{T}^N_{Q,P}(X|\mathbf{u}_1(m), \mathbf{u}_2(m,l))$, where $\mathcal{J}$ is a finite set. Let us denote codewords with $\mathbf{x}_{m,l,j}$, where $m \in \mathcal{M}_N$, $l \in \mathcal{L}_N$, $j \in \mathcal{J}$. Set

$$\Theta \triangleq \{\mathbf{x}_{m,l,j}\}_{m \in \mathcal{M}_N, l \in \mathcal{L}_N, j \in \mathcal{J}}. \quad (9)$$

Encoding scheme: $f : \mathcal{M}_N \times \mathcal{L}_N \to \mathcal{X}^N$ is a stochastic encoder. For message pair m, l one codeword $\mathbf{x}_{m,l,j}$ is chosen from Θ (9) with probability distribution $f(\mathbf{x}_{m,l,j}|m,l)$.

Decoding strategies: We apply the decoding rule for decoders g_1 and g_2 using the "divergence minimization" criterion. Suppose that the pair of messages m, l is transmitted, and m', l' is received at receiver 1 and m'' is received at receiver 2. Define the following decoding strategies at receivers 1 and 2

1. Every $\mathbf{y}$ is decoded to such m', l' that for some V_1'

$$\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'), \mathbf{u}_2(m', l'), \mathbf{x}_{m',l',j'}), \quad \text{and } D(V_1' \| W_1 | Q, P) \text{ is minimal.}$$

2. Every $\mathbf{z}$ is decoded to such m'' that for some V_2'

$$\mathbf{z} \in \mathcal{T}^N_{Q,P,V_2'}(Z|\mathbf{u}_1(m''), \mathbf{u}_2(m'', l''), \mathbf{x}_{m'',l'',j''}), \quad \text{and } D(V_2' \| W_2 | Q, P) \text{ is minimal.}$$

In the following we prove that for any $E = (E_1, E_2)$, $E_i > 0$, $i = 1, 2$, there exists a code as described in codebook generation such that (2) holds for sufficiently large N.

Decoder g_1 can make an error, if the pair of messages m, l is transmitted but there exists $(m', l') \neq (m, l)$, such that for some V_1'

$$\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l), \mathbf{x}_{m,l,j}) \cap \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'), \mathbf{u}_2(m', l'), \mathbf{x}_{m',l',j'}),$$

and

$$D(V_1' \| W_1 | Q, P) \le D(V_1 \| W_1 | Q, P). \quad (10)$$

To simplify the notations we define the following sets for decoding error at receivers 1 and 2. Suppose that the pair of messages m, l has been sent through the channels and m', l' is received at receiver 1 and m'' is received at receiver 2.

If m' is not equal to m, the following set is all possible received vectors at receiver 1 which can lead to error:
$B_1(V_1, V_1') \triangleq$

$$\triangleq \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l), \mathbf{x}_{m,l,j}) \bigcap \bigcup_{m' \neq m} \bigcup_{l' \in \mathcal{L}_N, j' \in \mathcal{J}} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'), \mathbf{u}_2(m', l'), \mathbf{x}_{m',l',j'}). \tag{11}$$

and if m' is equal to m but $l' \neq l$, the following set is all possible received vectors at receiver 1 which can lead to error:
$B_2(V_1, V_1') \triangleq$

$$\triangleq \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l), \mathbf{x}_{m,l,j}) \bigcap \bigcup_{l' \neq l} \bigcup_{j' \in \mathcal{J}} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m, l'), \mathbf{x}_{m,l',j'}). \tag{12}$$

If m'' is not equal to m, the following set is all possible received vectors at receiver 2 which can lead to error:
$B_3(V_2, V_2') \triangleq$

$$\mathcal{T}^N_{Q,P,V_2}(Z|\mathbf{u}_1(m), \mathbf{u}_2(m,l), \mathbf{x}_{m,l,j}) \bigcap \bigcup_{m'' \neq m} \bigcup_{l'' \in \mathcal{L}_N} \bigcup_{j'' \in \mathcal{J}} \mathcal{T}^N_{Q,P,V_2'}(Z|\mathbf{u}_1(m''), \mathbf{u}_2(m'', l''), \mathbf{x}_{m'',l'',j''})). \tag{13}$$

Define $\mathcal{D}_1(Q,P) = \{V_1, V_1' : D(V_1'\|W_1|Q,P) \leq D(V_1\|W_1|Q,P)\}$, and

$$\mathcal{D}_2(Q,P) = \{V_2, V_2' : D(V_2'\|W_2|Q,P) \leq D(V_2\|W_2|Q,P)\}.$$

Therefore

$$\begin{aligned}
e(f, g_1, W_1) &= \max_{m \in \mathcal{M}_N, l \in \mathcal{L}_N} \sum_{\mathbf{x}_{m,l,j} \in \Theta} W_1^N((g_1^{-1}(m,l))^c|\mathbf{x}_{m,l,j}) f(\mathbf{x}_{m,l,j}|m,l) = \\
&= \max_{m \in \mathcal{M}_N, l \in \mathcal{L}_N} \sum_{j \in \mathcal{J}} f(\mathbf{x}_{m,l,j}|m,l) \times \\
&\quad \times W_1^N\{ \bigcup_{V_1, V_1' \in \mathcal{D}_1(Q,P)} B_1(V_1, V_1') \bigcup B_2(V_1, V_1')|\mathbf{x}_{m,l,j}\} \leq^{(a)} \\
&\leq \max_{m \in \mathcal{M}_N, l \in \mathcal{L}_N} \sum_{j \in \mathcal{J}} f(\mathbf{x}_{m,l,j}|m,l) \times W_1^N(\mathbf{y}|\mathbf{x}_{m,l,j}) \times \\
&\quad \times \left| \bigcup_{V_1, V_1' \in \mathcal{D}_1(Q,P)} B_1(V_1, V_1') \bigcup B_2(V_1, V_1') \right| \leq^{(b)} \\
&\leq \max_{m \in \mathcal{M}_N, l \in \mathcal{L}_N} \sum_{V_1, V_1' \in \mathcal{D}_1(Q,P)} W_1^N(\mathbf{y}|\mathbf{x}_{m,l,j}) \sum_{j \in \mathcal{J}} f(\mathbf{x}_{m,l,j}|m,l) \times \\
&\quad \times [|B_1(V_1, V_1')| + |B_2(V_1, V_1')|] \leq^{(c)} \\
&\leq \max_{m \in \mathcal{M}_N, l \in \mathcal{L}_N} \sum_{V_1, V_1' \in \mathcal{D}_1(Q,P)} \exp\{-N[D(V_1\|W_1|Q,P) + H_{Q,P,V_1}(Y|X)]\} \times \\
&\quad \times \sum_{j \in \mathcal{J}} f(\mathbf{x}_{m,l,j}|m,l) \times [|B_1(V_1, V_1')| + |B_2(V_1, V_1')|].
\end{aligned} \tag{14}$$

where (a) is concluded from the defined error sets for decoding (11) and (12). taking into account that the $W_1^N(\mathbf{y}|\mathbf{x}_{m,l,j})$ is constant for fixed Q. V_1, we conclude (b); and (c) is concluded from (3). Similarly error probability of receiver 2 is upper bounded as follows

$$e(f, g_2, W_2) \leq \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{V_2, V_2'\in\mathcal{D}_2(Q,P)} \exp\{-N[D(V_2\|W_2|Q, P) + H_{Q,P,V_2}(Z|X)]\} \times$$

$$\times \sum_{j\in\mathcal{J}} f(\mathbf{x}_{m,l,j}|m, l) \times [|B_3(V_2, V_2')|].$$

We shall prove that there exists a code such that for every $m \in \mathcal{M}_N$, $l \in \mathcal{L}_N$. $j \in \mathcal{J}$ and any conditional types V_1, V_1'. and N large enough the following inequalities are valid

$$|B_i(V_1, V_1')| \leq \exp\{NH_{Q,P,V_1}(Y|X)\} \exp\{-N|E_1 - D(V_1'\|W_1|Q, P)|^+\},\ i = 1, 2, \qquad (15)$$

$$|B_3(V_2, V_2')| \leq \exp\{NH_{Q,P,V_2}(Z|X)\} \exp\{-N|E_2 - D(V_2'\|W_2|Q, P)|^+\}. \qquad (16)$$

Let us note that if the collection of vectors $\{(\mathbf{u}_m, \mathbf{x}_{m,l,j})\}_{m\in\mathcal{M}_N, l\in\mathcal{L}_N, j\in\mathcal{J}}$ satisfy (15), (16) for any V_i, V_i', $i = 1, 2$, then $(\mathbf{u}_{m'}, \mathbf{x}_{m',l',j'}) \neq (\mathbf{u}_m, \mathbf{x}_{m,l,j})$ for $(m', l', j') \neq (m, l, j)$. To prove that it is enough to choose $V_i = V_i'$ and $D(V_i'\|W_i|Q, P) < E_i$, $i = 1, 2$. If V_i' is such that $D(V_i'\|W_i|Q, P) \geq E_i$ then $\exp\{-N|E_i - D(V_i'\|W_i|Q, P)|^+\} = 1$, $i = 1, 2$, and (15), (16) are valid for any $|\mathcal{M}_N|$, $|\mathcal{L}_N|$, $|\mathcal{J}|$.
It remains to prove inequalities (15). (16) for V_i' so that $D(V_i'\|W_i|Q, P) \leq E_i$, i=1,2. Let us define $\mathcal{D}_i'(Q, P) = \{V_i' :\ D(V_i'\|W_i|Q, P) \leq E_i\}$. $i = 1, 2$.

To prove (15) and (16), it is sufficient to show that for N large enough

$$|\sum_{V_1} \sum_{V_1'\in\mathcal{D}_1'(Q,P)} \sum_{i=1,2} \mathbf{E}(|B_i(V_1, V_1')|) \times \exp\{-N(H_{Q,P,V_1}(Y|X) - E_1 - D(V_1'\|W_1|Q, P))\} +$$

$$+ \sum_{V_2} \sum_{V_2'\in\mathcal{D}_2'(Q,P)} \mathbf{E}(|B_3(V_2, V_2')|) \times \exp\{-N(H_{Q,P,V_2}(Z|X) - E_2 - D(V_2'\|W_2|Q, P))\}| \leq 1. \qquad (17)$$

To this end since the events in the brackets are independent we can write the following inequality

$$\mathbf{E}(|B_1(V_1, V_1')|) \leq \sum_{\mathbf{y}\in\mathcal{T}^N_{Q,P,V_1}(Y)} \sum_{m'\neq m} \Pr\{\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m, l), \mathbf{x}_{m,l,j})\} \times$$

$$\times \Pr\{\mathbf{y} \in \bigcup_{l'\in\mathcal{L}_N, j'\in\mathcal{J}} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'), \mathbf{u}_2(m', l'), \mathbf{x}_{m',l',j'})\}. \qquad (18)$$

The first probability in (18) is different from zero iff $\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1}(Y)$, then for N large enough

$$\Pr\{\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m, l), \mathbf{x}_{m,l,j})\} = \frac{|\mathcal{T}^N_{Q,P,V_1}(U_1U_2X|\mathbf{y})|}{|\mathcal{T}^N_Q(U_1U_2X)|} \leq$$

$$\leq (N+1)^{|\mathcal{X}|} \exp\{-N[I_{Q,P,V_1}(Y \wedge U_1U_2X)] \leq \exp\{-N[I_{Q,P,V_1}(Y \wedge X) - \frac{\delta}{4}]\}. \qquad (19)$$

The second probability in (18) can be estimated for N large enough as following

$$\Pr\{\mathbf{y} \in \bigcup_{l'\in\mathcal{L}_N, j'\in\mathcal{J}} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'), \mathbf{u}_2(m', l'), \mathbf{x}_{m',l',j'})\} \leq$$

$$\leq \Pr\{\mathbf{y} \in \bigcup_{\mathbf{u}_2\mathbf{x} \in \mathcal{T}^N_{Q,P}(U_2X|\mathbf{u}_1(m'))} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'), \mathbf{u}_2, \mathbf{x})\} \leq$$

$$\leq \Pr\{\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m'))\} = \frac{|\mathcal{T}^N_{Q,P,V_1}(U_1|\mathbf{y})|}{|\mathcal{T}^N_{Q_1}(U_1)|} \leq \exp\{-N[I_{Q,P,V_1'}(Y \wedge U_1) - \frac{\delta}{4}]\}. \quad (20)$$

From (7) for some V_1' we have

$$|\mathcal{M}_N| - 1 \leq \exp\{N[I_{Q,P,V_1'}(Y \wedge U_1) + D(V_1'\|W_1|Q,P) - E_1 - \delta]\}. \quad (21)$$

Thus by substituting (21) in (18) and from (19), (20) the conclusion is

$$\mathbf{E}(|\mathcal{B}_1(V_1, V_1')|) \times \exp\{N[-H_{Q,P,V_1}(Y|X) - D(V_1'\|W_1|Q,P) + E_1]\} \leq \exp\{-\frac{N\delta}{2}\}. \quad (22)$$

$\mathbf{E}(|\mathcal{B}_2(V_1, V_1')|)$ in (17) can be estimated as follows

$$\mathbf{E}(|\mathcal{B}_2(V_1, V_1')|) \leq \sum_{l'\neq l} \sum_{\mathbf{y}\in\mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_m)} \Pr\{\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l), \mathbf{x}_{m,l,j})\} \times$$

$$\times \Pr\{\mathbf{y} \in \bigcup_{j'\in\mathcal{J}} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l'), \mathbf{x}_{m,l',j'})\}. \quad (23)$$

We estimate the second probability as follows

$$\Pr\{\mathbf{y} \in \bigcup_{j'\in\mathcal{J}} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l'), \mathbf{x}_{m,l',j'})\} \leq$$

$$\leq \Pr\{\mathbf{y} \in \bigcup_{\mathbf{x}\in\mathcal{T}^N_{Q,P}(X|\mathbf{u}_1(m),\mathbf{u}_2(m,l'))} \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l'), \mathbf{x})\} \leq$$

$$\leq \Pr\{\mathbf{y} \in \mathcal{T}^N_{Q,P,V_1'}(Y|\mathbf{u}_1(m), \mathbf{u}_2(m,l'))\} \leq \exp\{-N[I_{Q,V_1'}(Y \wedge U_2|U_1) - \frac{\delta}{4}]\}. \quad (24)$$

By the same way we can prove that the first probability for N large enough can not exceed

$$\exp\{-N[I_{Q,P,V_1}(Y \wedge X|U_1) - \frac{\delta}{4}]\}. \quad (25)$$

Further from (8) for some V_1' we have

$$|\mathcal{L}_N| \leq \exp\{N[I_{Q,P,V_1'}(Y \wedge X|U_1) + D(V_1'\|W_1|Q,P) - E_1 - \delta]\}. \quad (26)$$

By substituting (26) in (23) and from (24) and (25) we obtain

$$\mathbf{E}(|\mathcal{B}_2(V_1, V_1')|) \times \exp\{N[-H_{Q,P,V_1}(Y|X) - D(V_1'\|W_1|Q,P) + E_1]\} \leq \exp\{-\frac{N\delta}{2}\}. \quad (27)$$

$\mathbf{E}(|\mathcal{B}_3(V_2, V_2')|)$ can be estimated similarly.

$$\mathbf{E}(|\mathcal{B}_3(V_2, V_2')|) \times \exp\{N[-H_{Q,P,V_2}(Z|X) - D(V_2'\|W_2|Q,P) + E_2]\} \leq \exp\{-\frac{N\delta}{2}\}. \quad (28)$$

From (22), (27), (28) and taking into account that the number of all V_1, V_1' does not exceed $(N+1)^{2|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{Z}|)}$ for N large enough (17) is concluded. So by substituting (15) in (14) for N large enough we obtain

$$e(f, g_1, W_1) \leq \max_{m\in\mathcal{M}_N, l\in\mathcal{L}_N} \sum_{V_1,V_1'\in\mathcal{D}_1(Q,P)} \exp\{-N[D(V_1\|W_1|Q,P) + H_{Q,P,V_1}(Y|X)]\} \times$$

$$\times 2\exp\{-N|-H_{Q,P,V_1}(Y|X) - D(V_1'\|W_1|Q,P) + E_1 + \delta|\} \times \sum_{j\in J} f(\mathbf{x}_{m,l,j}|m,l) \leq$$

$$\leq \sum_{V_1,V_1'\in \mathcal{P}_1(Q,P)} \exp\{-N(E_1 - \delta)\} \leq \exp\{-N(E_1 - \epsilon)\},\ \epsilon > 0,$$

where the last inequality is concluded from that the number of all possible V_1, V_1' does not exceed $(N+1)^{2|\mathcal{X}||\mathcal{Y}|}$. So the error probability of the receiver 1 decreases exponentially, while N increases

$$e(f, g_1, W_1) \leq \exp\{-N(E_1 - \epsilon)\}. \tag{29}$$

The error probability for the receiver 2 can be estimated similarly. Therefore for N large enough

$$e(f, g_2, W_2) \leq \exp\{-N(E_2 - \epsilon)\},\ \epsilon > 0.$$

It completes the proof.

4. Conclusion

We constructed an inner bound for E-capacity region of the discrete memoryless asymmetric broadcast channel with an additional point that "stochastic encoding" is applied. The method of types is used. This study can be useful through out future works which assume secrecy.

Acknowledgment

The author is indebted to professor E. A. Haroutunian for his helpful and undivided guidance and M.E. Haroutunian for her useful comments.

References

[1] T. M. Cover, "Broadcast channels", *IEEE Trans. Inform. Theory*, vol. IT-18, no 1, pp. 2-14, 1972.

[2] I. Csiszár and J. Körner, "Broadcast channel with confidential messages", *IEEE Transaction on IT*, vol. IT-24(3), pp. 339-348, 1978.

[3] I. Csiszár and J. Körner, "Information Theory: Coding Theorems for Discrete Memoryless Systems", *New York, Wiley*, 1981.

[4] E. A. Haroutunian, "Upper estimate of transmission rate for memoryless channel with countable number of output signals under given error probability exponent", *in 3rd All Union Conference on Theory of Information Transmisssion and Coding, Uzhgorod, Publishing House of the Uzbek Academy of sciences*, pp. 83-86, Tashkent, 1967.

[5] E. A. Haroutunian, "On the optimality of information transmission by a channel with finite number of states known at the input", (in Russian), *Izvestia Academii Nauk Armenii, Matematika*, vol. 4, no. 2, pp.81-90, 1969.

[6] E. A. Haroutunian, "On Bounds for E-Capacity of DMC", *IEEE Trans. Inform. Theory*, vol. IT-53, no. 11, pp. 4210-4220, 2007.

[7] E. A. Haroutunian, M. E. Haroutunian and A. N. Haroutunian, "Reliability criteria in information theory and in statistical hypothesis testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, nos. 2-3, 2008.

[8] M. E. Haroutunian. "Random coding bound for E-capacity region of the broadcast channel". *Mathematical problems of computer science*. no. 21. pp. 50-60. 2000.
[9] J. Körner and K. Marton. "An achievable rate region for the broadcast channel". *IEEE Trans. Inform. Theory*. vol. IT-23. pp. 751-761, 1977.
[10] J. Körner and K. Marton. "General broadcast channels with degraded message sets". *IEEE Trans. Inform. Theory*. vol. IT-23. pp. 60-64, 1977.
[11] C. E. Shannon, "A mathematical theory of communication". *Bell System Technical Journal*, vol. 27, no. 3. pp. 379-423. 1948.
[12] C. E. Shannon, "Probability of error for optimal codes in Gaussian channels". *Bell Syst. Tech. J.*, vol. 38, no 5, pp. 611-659. 1959.

Լայնասփյուռ անհամաչափ ստոխաստիկ կոդավորմամբ կապուղու E-ունակության տիրույթի պատահահան կոդավորման գնահատականը

Ն. Ավշար

Ամփոփում

Հոդվածում ուսումնասիրվում է լայնասփյուռ անհամաչափ ստոխաստիկ կոդավորմամբ կապուղին: Կառուցված է E-ունակության (արագություն-հուսալիություն) տիրույթի պատահական կոդավորման գնահատականը: