Mathematical Problems of Computer Science 33, 11–23, 2010.

Lower Bound of Rate-Reliability-Distortion Function for Generalized Channel With Side Information

Mariam E. Haroutunian and Arthur R. Muradyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: armar@ipia.sci.am

Abstract

In this paper we study a generalized model of discrete memoryless channel (DMC) with finite input and output alphabets and random state sequence (side information) partially known to the encoder, channel and decoder. The study includes the family of Gel'fand-Pinsker and information hiding coding problems as special cases. Information is to be reliably transmitted through the noisy channel selected by adversary. Reasoning from applications the actions of encoder and adversary are limited by distortion constraints. The encoder and decoder depend on a random variable (RV) which can be treated as cryptographic key. Two cases are considered, when the joint distribution of this RV and side information is given or this RV is independent from side information and it's distribution can be chosen for the best code generation. We investigate the rate-reliability-distortion function for the mentioned model and derive the lower bound for it.

1. Introduction

The DMC with random state information available to the encoder was studied by Gel'fand and Pinsker [1], they derived the capacity of this channel. The capacity of arbitrary varying channel with side information at the encoder was derived by Ahlswede [2]. Error exponents of single-user, multi-user and varying channels with side information were studied in [3, 4, 5, 6, 7].

It was discovered that embedding and hiding [8] is closely related to the channel with random parameter, where the cover signal plays the role of the state information. The difference between the two problems is that in various formulations of data-hiding and watermarking there are distortion constraints for the transmitter and a memoryless adversary and the channel is not fixed as it is chosen by adversary. Motivated by data-hiding applications several models are studied, where partial or no information of the state sequence is available to the encoder, channel designer and decoder. Results on capacity and error exponents problems have been obtained in [8, 9, 10, 11, 12, 13].

A unified framework for studying such problems was first suggested by Cover and Chiang [14], who considered the channel with two-sided state information, where the sender and the receiver have correlated but different state information. This model includes four possible situations of the channel with random parameter as special cases. They obtained the capacity of this channel and explored the duality with source coding problems. The random coding bound of E-capacity for this model was derived in [15].

Later Moulin and Wang [16] studied the generalized model with side information, where the degraded versions of side information are distributed among encoder, adversary and decoder. This model includes also the various cases of information hiding. They derived the capacity formulas and random coding exponents for compound discrete memoryless channels and channels with arbitrary memory.

In this paper we study a similar generalized model of discrete memoryless channel (DMC) with finite input and output alphabets and random state sequence (side information) partially known to the encoder, channel and decoder (fig. 1). Information is to be reliably transmitted through the noisy channel selected by adversary.

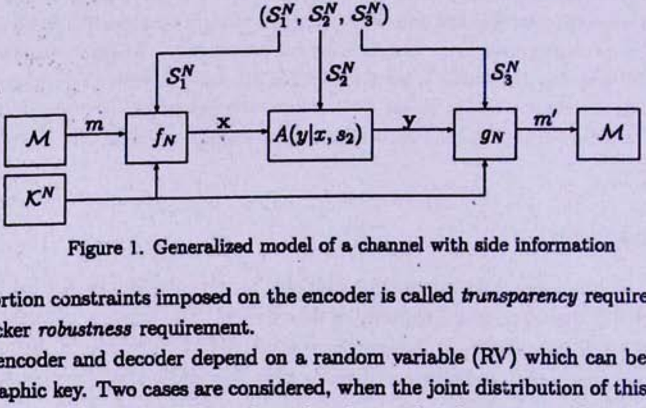

Figure 1. Generalized model of a channel with side information

Distortion constraints imposed on the encoder is called *transparency* requirement and on the attacker *robustness* requirement.

The encoder and decoder depend on a random variable (RV) which can be treated as a cryptographic key. Two cases are considered, when the joint distribution of this RV and side information is given or this RV is independent from side information and its distribution can be chosen for the best code generation.

We investigate the rate-reliability-distortion function for the mentioned model and derive the lower bound for it. This function expresses the dependence of the information hiding rate on reliability and distortion levels for information hider and attacker. This investigation is equivalent to studying of error exponents but sometimes is more expedient. The approach was first introduced by E. Haroutunian [17, 18, 19] and developed for various channels [4, 5, 7, 9, 10, 13, 15]. In this paper we derive the lower bound (random coding bound) of rate-reliability-distortion function.

The paper is organized as follows. Definitions of terms and notations used throughout the paper are described in section 2.. The formulation of the main result and its special cases are stated in the section 3.. The proof of the theorem appears in section 4..

2. Notations and Definitions

Capital letters are used for RV $K, S_1, S_2, S_3, U, X, Y$ taking values in the finite sets $\mathcal{K}, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{U}, \mathcal{X}, \mathcal{Y}$, correspondingly, and lower case letters $k, s_1, s_2, s_3, u, x, y$ for their realizations. Small bold letters are used for N-length vectors $\mathbf{x} = (x_1, ..., x_N) \in \mathcal{X}^N$. The cardinality of the set $\mathcal{X}$ we denote by $|\mathcal{X}|$. The notation $|a|^+$ will be used for $\max(a, 0)$.

The generalized model of a channel with side information is depicted in Figure 1. A message m to be transmitted through an attack channel to the receiver is uniformly distributed over the message set $\mathcal{M}$. The joint state sequence is described by random variable $S = (S_1, S_2, S_3)$ the components of which represent the partial information known to the encoder, adversary and decoder, correspondingly. Random variable K represents separate information known only to the encoder and decoder.

Two cases are considered, when the joint probability distribution

$$Q^* = Q_0^* \circ Q_1^* \circ Q_2^* \circ Q_3^* = \{Q^*(k, s_1, s_2, s_3) = Q_0^*(k)Q_1^*(s_1|k)Q_2^*(s_2|k, s_1)Q_3^*(s_3|k, s_1, s_2),$$
$$k \in \mathcal{K}, s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2, s_3 \in \mathcal{S}_3\}$$

is given or K is independent from side information and its distribution can be chosen for the best code generation.

It is assumed that:

$$Q^{*N}(\mathbf{k}, \mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3) = \prod_{n=1}^{N} Q^*(k_n, s_{1n}, s_{2n}, s_{3n}).$$

The transmitter encodes the message m using $\mathbf{s}_1$ and $\mathbf{k}$. The resulting codeword $\mathbf{x} \in \mathcal{X}^N$ is transmitted via attack channel $A(y|x, s_2)$. The attacker produces corrupted blocks $\mathbf{y} \in \mathcal{Y}^N$. The decoder does not know $A(y|x, s_2)$ selected by adversary and possessing $\mathbf{s}_3$ derives the message m'.

The following probability distributions are used in the paper:

$$Q = Q_0 \circ Q_1 \circ Q_2 \circ Q_3 = \{Q(k, s_1, s_2, s_3) = Q_0(k)Q_1(s_1|k)Q_2(s_2|k, s_1)Q_3(s_3|k, s_1, s_2),$$
$$k \in \mathcal{K}, s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2, s_3 \in \mathcal{S}_3\},$$
$$P = P_0 \circ P_1 = \{P(x, u|k, s_1) = P_0(u|k, s_1)P_1(x|u, k, s_1), x \in \mathcal{X}, u \in \mathcal{U}, k \in \mathcal{K}, s_1 \in \mathcal{S}_1\},$$
$$V = \{V(y|k, s_1, s_2, s_3, u, x), y \in \mathcal{Y}, k \in \mathcal{K}, s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2, s_3 \in \mathcal{S}_3, u \in \mathcal{U}, x \in \mathcal{X}\},$$
$$Q_3^* \circ A = \{Q_3^* \circ A(y, s_3|x, k, s_1, s_2) = Q_3^*(s_3|k, s_1, s_2)A(y|x, s_2),$$

$$y \in \mathcal{Y}, k \in \mathcal{K}, s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2, s_3 \in \mathcal{S}_3, x \in \mathcal{X}\}.$$

$$QP(x, s_2) = \sum_{k,s_1,u} Q_0(k)Q_1(s_1|k)Q_2(s_2|k, s_1)P(x, u|k, s_1).$$

For brevity we will write indices of Q separated by comma, when mentioning the product of respective probability distributions (or types), e.g. $Q_{0,1,2} = Q_0 \circ Q_1 \circ Q_2$.

For the information-theoretic quantities, such as entropy $H_{Q_0,Q_1,Q_2}(K, S_1, S_2)$, mutual information $I_{Q_0,Q_1,P_0}(U \wedge S_1)$, divergence $D(Q_0||Q_0^*)$ and for the notion of type we refer to [19, 20, 21, 22].

The following properties [20, 21] are used in proofs:
for $\mathbf{k} \in \mathcal{T}_{Q_0}(K)$, $\mathbf{s}_1 \in \mathcal{T}_{Q_0,Q_1}(S_1|\mathbf{k})$, $\mathbf{s}_2 \in \mathcal{T}_{Q_0,Q_1,Q_2}(S_2|\mathbf{k}, \mathbf{s}_1)$, $\mathbf{x} \in \mathcal{T}_{Q_0,Q_1,P}(X|\mathbf{k}, \mathbf{s}_1)$, $(\mathbf{y}, \mathbf{s}_3) \in \mathcal{T}_{Q,P,V}(Y, S_3|\mathbf{x}, \mathbf{k}, \mathbf{s}_1, \mathbf{s}_2)$,

$$Q_3^{*N} \circ A^N(\mathbf{y}, \mathbf{s}_3|\mathbf{k}, \mathbf{x}, \mathbf{s}_1, \mathbf{s}_2) = \exp\{-N(H_{Q,P,V}(Y, S_3|X, K, S_1, S_2) +$$

$$+ D(Q_3 \circ V||Q_3^* \circ A|Q_0, Q_1, Q_2, P)\}. \quad (1)$$

$$D(Q \circ P \circ V||Q^* \circ P \circ A) = D(Q_{0,1,2}||Q_{0,1,2}^*) + D(Q_3 \circ V||Q_3^* \circ A|Q_0, Q_1, Q_2, P), \quad (2)$$

$$D(Q||Q^*) = D(Q_0||Q_0^*) + D(Q_1||Q_1^*|Q_0) + D(Q_2||Q_2^*|Q_0, Q_1) + D(Q_3||Q_3^*|Q_0, Q_1, Q_2), \quad (3)$$

$$H_{Q,P,V}(Y, S_3|U, X, K, S_1, S_2) \le H_{Q,P,V}(Y, S_3|X, K, S_1, S_2). \quad (4)$$

All logarithms and exponents in the paper are of the base 2.

The mappings $d_1 : \mathcal{S}_1 \times \mathcal{X} \to \mathcal{R}^+$ and $d_2 : \mathcal{X} \times \mathcal{Y} \to \mathcal{R}^+$ are distortion functions over the encoder and attacker correspondingly. They are supposed to be symmetric ($d_1(s_1, x) = d_1(x, s_1)$ and $d_2(x, y) = d_2(y, x)$, $s_1 \in \mathcal{S}_1, x \in \mathcal{X}, y \in \mathcal{Y}$) and become 0 if $s_1 = x$ and $x = y$. Distortion functions for N-length vectors are defined as:

$$d_1^N(\mathbf{s}_1, \mathbf{x}) = \frac{1}{N}\sum_{n=1}^{N} d_1(s_{1n}, x_n), d_2^N(\mathbf{x}, \mathbf{y}) = \frac{1}{N}\sum_{n=1}^{N} d_2(x_n, y_n).$$

Let $\Delta_1 \ge 0$ be the number indicating the allowed distortion level for the encoder and $\Delta_2 \ge 0$ for the attacker.

The N-length *code* is a pair of mappings (f_N, g_N), where

$$f_N : \mathcal{M} \times \mathcal{K}^N \times \mathcal{S}_1^N \to \mathcal{X}^N,$$

is the encoding function which satisfies the following distortion constraint:

$$d_1^N(\mathbf{s}_1, f_N(m, \mathbf{k}, \mathbf{s}_1)) \le \Delta_1, \quad (5)$$

for all $m, \mathbf{k}, \mathbf{s}_1$ and

$$g_N : \mathcal{Y}^N \times \mathcal{K}^N \times \mathcal{S}_3^N \to \mathcal{M}.$$

is the decoding function.

Note that definition of the distortion constraint (5) means that the maximum distortion constraint is used, which is stronger condition than average distortion constraint over $m \in \mathcal{M}$, $\mathbf{k} \in \mathcal{K}^N$ and $\mathbf{s}_1 \in \mathcal{S}_1^N$ i.e. if we find f_N satisfying (5) it will also satisfy average distortion constraint.

N is called *code length* and $|\mathcal{M}|$ is called *code volume*. The nonnegative number $R = \frac{1}{N}\log|\mathcal{M}|$ is called the code rate.

The selected channel is memoryless, it means that for $\mathbf{x} \in \mathcal{X}^N$, $\mathbf{y} \in \mathcal{Y}^N$ and $\mathbf{s}_2 \in \mathcal{S}_2^N$:

$$A^N(\mathbf{y}|\mathbf{x}, \mathbf{s}_2) = \prod_{n=1}^{N} A(y_n|x_n, s_{2n})$$

and it satisfies the following distortion constraint for QP^N:

$$\sum_{\mathbf{s}_2, \mathbf{x}, \mathbf{y}} QP^N(\mathbf{x}, \mathbf{s}_2)A^N(\mathbf{y}|\mathbf{x}, \mathbf{s}_2)d_2(\mathbf{x}, \mathbf{y}) \leq \Delta_2. \quad (6)$$

A memoryless covert channel P, subject to distortion Δ_1, is probability distribution P such that for any $Q_{0,1}$:

$$\sum_{k, s_1, u, x} Q_{0,1}(s_1, k)P(x, u|k, s_1)d_1(s_1, x) \leq \Delta_1. \quad (7)$$

The set of probability distributions P satisfying condition (7) is denoted by $\mathcal{P}(Q_{0,1}, \Delta_1)$.

A memoryless attack channel A, subject to distortion Δ_2 is defined by probability distribution A such that for any $Q_{0,1,2}$ and P:

$$\sum_{k, s_1, s_2, u, x, y} Q_{0,1,2}(k, s_1, s_2)P(x, u|k, s_1)A(y|x, s_2)d_2(x, y) \leq \Delta_2. \quad (8)$$

The set of channels A satisfying condition (8) is denoted by $\mathcal{A}(Q_{0,1,2}, P, \Delta_2)$.

We will consider cases when the distribution of $\mathbf{k}$ is either given or it is independent of state sequences and it is not given but rather selected in a way to achieve the minimal error probability.

In the first case the probability of erroneous reconstruction of message m for $P \in \mathcal{P}(Q^*_{0,1}, \Delta_1)$, $A \in \mathcal{A}(Q^*_{0,1,2}, P, \Delta_2)$ is calculated in the following way:

$$e^1(m, A) = e(f_N, g_N, A, Q^*, \Delta_1, \Delta_2, m) =$$

$$= \sum_{\mathbf{k}, \mathbf{s}_1, \mathbf{s}_2} Q^{*N}_{0,1,2}(\mathbf{k}, \mathbf{s}_1, \mathbf{s}_2)Q^{*N}_3 \circ A^N(\mathcal{Y}^N \times \mathcal{S}^N_3 \backslash g^{-1}_{N,\mathbf{k}}(m)|f_N(m, \mathbf{k}, \mathbf{s}_1), \mathbf{k}, \mathbf{s}_1, \mathbf{s}_2),$$

where $g^{-1}_{N,\mathbf{k}}(m) = \{\mathbf{y}, \mathbf{s}_3 : g_N(\mathbf{y}, \mathbf{k}, \mathbf{s}_3) = m\}$.

In the second case the erroneous reconstruction probability can be calculated in the following way:

$$e^2(m, A) = e(f_N, g_N, A, Q^*, \Delta_1, \Delta_2, m) =$$

$$= \min_{Q_0} \sum_{\mathbf{k}, \mathbf{s}_1, \mathbf{s}_2} Q^N_0(\mathbf{k})Q^{*N}_{1,2}(\mathbf{s}_1, \mathbf{s}_2)Q^{*N}_3 \circ A^N(\mathcal{Y}^N \times \mathcal{S}^N_3 \backslash g^{-1}_{N,\mathbf{k}}(m)|f_N(m, \mathbf{k}, \mathbf{s}_1), \mathbf{s}_1, \mathbf{s}_2).$$

The maximal value of error probability of the code over all A for given message m is denoted by:

$$e^i(m) = e^i(f_N, g_N, Q^*, \Delta_1, \Delta_2, m) = \max_A e^i(m, A),\ \mathrm{i} = 1, 2.$$

The maximal error probability of the code over all $m \in \mathcal{M}$ is equal to:

$$e^i = e^i(f_N, g_N, Q^*, \Delta_1, \Delta_2) = \max_{m \in \mathcal{M}} e^i(m),\ \mathrm{i} = 1, 2$$

and the average error probability of the code over all $m \in \mathcal{M}$ is:

$$\overline{e^i} = \overline{e^i}(f_N, g_N, Q^*, \Delta_1, \Delta_2) = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} e^i(m).\ \mathrm{i} = 1, 2.$$

3. Formulation of Results

The rate-reliability-distortion function for maximal error probability is denoted by $C^i(E, Q^*, \Delta_1, \Delta_2)$ and is defined in the following way:

$$C^i(E, Q^*, \Delta_1, \Delta_2) = \overline{\lim_{N \to \infty}} \frac{1}{N} \log M^i(E, Q^*, \Delta_1, \Delta_2, N),$$

where

$$M^i(E, Q^*, \Delta_1, \Delta_2, N) = \sup_{f_N, g_N} \{|\mathcal{M}| : e^i \leq \exp(-NE)\},\ \mathrm{i} = 1, 2.$$

The rate-reliability-distortion function for the average error probability is denoted by $\overline{C^i}(E, Q^*, \Delta_1, \Delta_2)$.

We can observe that the rate-reliability-distortion function is a generalization of the capacity because it converges to channel capacity when $E \to 0$. To introduce the main theorem denote:

$$R(E, Q^*, A, Q, P, V) = I_{Q,P,V}(U \wedge S_3, Y|K) - I_{Q_0, Q_1, P_0}(U \wedge S_1|K) + D(Q \circ P \circ V || Q^* \circ P \circ A) - E.$$

$$R_r^1(E, Q^*, \Delta_1, \Delta_2) = \min_{Q_0, Q_1, Q_2} \max_{P \in \mathcal{P}(Q_{0,1}, \Delta_1)} \min_{A \in \mathcal{A}(Q_{0,1,2}, P, \Delta_2)} \min_{Q_3, V : D(Q \circ P \circ V || Q^* \circ P \circ A) \leq E} \left| R(E, Q^*, A, Q, P, V) \right|^+ \tag{9}$$

and

$$R_r^2(E, Q^*, \Delta_1, \Delta_2) = \max_{Q_0} \min_{Q_1, Q_2} \max_{P \in \mathcal{P}(Q_{0,1}, \Delta_1)} \min_{A \in \mathcal{A}(Q_{0,1,2}, P, \Delta_2)} \min_{Q_3, V : D(Q_{1,2,3} \circ P \circ V || Q^*_{1,2,3} \circ P \circ A | Q_0) \leq E} \left| R(E, Q^*, A, Q, P, V) \right|^+. \tag{10}$$

Theorem. *For generalized channel with distortion constraints imposed on the encoder and channel, for given Q^* and for all $E > 0$, $i = 1, 2$*

$$R_r^i(E, Q^*, \Delta_1, \Delta_2) \leq C^i(E, Q^*, \Delta_1, \Delta_2) \leq \overline{C^i}(E, Q^*, \Delta_1, \Delta_2).$$

The proof of the theorem is given in the next section.

Corollary 1. *When $E \to 0$, $i = 2$ we derive the capacity for both compound discrete memoryless channel and channel with arbitrary memory established in [16].*

$$C(Q^*, \Delta_1, \Delta_2) = \max_{P \in \mathcal{P}(Q_1^*, \Delta_1)} \min_{A \in \mathcal{A}(Q_{1,3}^*, P, \Delta_2)} [I_{Q^*, P, A}(U \wedge S_3, Y) - I_{Q_1^*, P_0}(U \wedge S_1)].$$

Corollary 2. *When $S_2 = (S_1, S_3), K = \emptyset$, channel is fixed, there are no distortion constraints we derive the E-capacity obtained in [15], which in its turn is generalization of the channels for four possible situations with random parameter.*

Corollary 3. *When $S_2 = \emptyset$, $S_1 \neq S_3$ we get the semiblind watermarking case [8] and for $S_2 = \emptyset, S_3 = \emptyset$ we get the public watermarking case [8, 12]. The lower bound of E-capacity for the public watermarking problem when $i = 1$ is established in [9] which also becomes a special case of the theorem.*

Corollary 4. *When $S_2 = S_1, S_3 = \emptyset, K = \emptyset$ we get the Gel'fand-Pinsker [1] coding problem.*

4. Proof of the Theorem

The proof of the theorem is based on the method of types. We use random bin coding technique [1] for encoding and minimum divergence method [18] for decoding. Then we estimate the error caused by both encoding and decoding.

To prove the random coding bound we must show the existence of R satisfying (9) or (10) (depending on the case we consider) and $e^i \leq \exp\{-N(E-\varepsilon)\}$, for any $0 < \varepsilon < E, i = 1, 2$. In the paper we present the proof for the case when $i = 1$. The proof for $i = 2$ case can be derived similarly.

In the proof we consider only state sequences types of which are not far (in sense of divergence) from the given Q^*. Other state sequences which are farther from Q^* more than E are ignored. This can be done because state sequences with farther types cause minor errors.

Denote:

$$\mathcal{Q}(Q^*, E) = \{Q : D(Q \| Q^*) \leq E\}$$

and

$$\mathcal{T}_{Q^*, E}^N(K, S) = \bigcup_{Q \in \mathcal{Q}(Q^*, E)} \mathcal{T}_Q^N(K, S).$$

We will construct the code only for $(\mathbf{k}, \mathbf{s}) \in \mathcal{T}_{Q^*, E}^N(K, S)$, because for sufficiently large N, the probability of $(\mathbf{k}, \mathbf{s}) \notin \mathcal{T}_{Q^*, E}^N(K, S)$ is exponentially small:

$$Q^{*N}\Big\{\bigcup_{Q \notin \mathcal{Q}(Q^*, E)} \mathcal{T}_Q^N(K, S)\Big\} = \sum_{Q \notin \mathcal{Q}(Q^*, E)} Q^{*N}\{\mathcal{T}_Q^N(K, S)\} \leq$$

$$\leq \sum_{Q \notin \mathcal{Q}(Q^*, E)} \exp\{-ND(Q \| Q^*)\} < (N+1)^{|K||S_1||S_2||S_3|} \exp\{-NE\} \leq \exp\{-N(E - \varepsilon_1)\}, \quad (11)$$

where ε_1 is positive and small enough. Considering (3) we can see that estimation (11) is true also for the probability of $(\mathbf{k}, \mathbf{s}_1) \notin \mathcal{T}^N_{Q^*_{0,1}, E}(K, S_1)$ and $(\mathbf{k}, \mathbf{s}_1, \mathbf{s}_2) \notin \mathcal{T}^N_{Q^*_{0,1,2}, E}(K, S_1, S_2)$.

Encoding Scheme

For given $\delta > 0$, $E > 0$, Q^*, any type $Q = Q_0 \circ Q_1 \circ Q_2 \circ Q_3 \in \mathcal{Q}(Q^*, E)$, $P = P_0 \circ P_1 \in \mathcal{P}(Q_{0,1}, \Delta_1)$ and $\mathbf{k} \in \mathcal{T}^N_{Q_0}(K)$ we choose randomly $|\mathcal{M}|$ collections $\mathcal{J}(m)$, $m \in \mathcal{M}$ of vectors $\mathbf{u}_j(m), j = \overline{1, J}$ from $\mathcal{T}^N_{Q_{0,1}, P_0}(U|\mathbf{k})$, where $J = \exp\{N(I_{Q_{0,1}, P_0}(S_1 \wedge U|K) + \delta/2)\}$.

Then for each $\mathbf{s}_1 \in \mathcal{T}^N_{Q_0, Q_1}(S_1|\mathbf{k})$ we choose such $\mathbf{u}_j(m)$ from $\mathcal{J}(m)$, that $\mathbf{u}_j(m) \in \mathcal{T}^N_{Q_0, Q_1, P_0}(U|\mathbf{k}, \mathbf{s}_1)$. Denote this vector by $\mathbf{u}(m, \mathbf{k}, \mathbf{s}_1)$.

If for some $\mathbf{s}_1 \in \mathcal{T}^N_{Q_0, Q_1}(S_1|\mathbf{k})$ there is no such $\mathbf{u}_j(m)$ in $\mathcal{J}(m)$, we randomly choose $\mathbf{u}(m, \mathbf{k}, \mathbf{s}_1)$ from $\mathcal{T}^N_{Q_0, Q_1, P_0}(U|\mathbf{k}, \mathbf{s}_1)$. Denote by $B_{Q_0, Q_1, P_0}(m, \mathbf{k}, \mathbf{s}_1)$ the probability of this event. It can be estimated in the following way:

$$B_{Q_0,Q_1,P_0}(m, \mathbf{k}, \mathbf{s}_1) = \Pr\Big\{ \bigcap_{j=1}^{J} \mathbf{u}_j(m) \notin \mathcal{T}^N_{Q_0,Q_1,P_0}(U|\mathbf{k}, \mathbf{s}_1) \Big\} \le$$

$$\le \prod_{j=1}^{J} \Big(1 - \Pr\Big\{\mathbf{u}_j(m) \in \mathcal{T}^N_{Q_0,Q_1,P_0}(U|\mathbf{k}, \mathbf{s}_1)\Big\}\Big) \le \Big(1 - \frac{|\mathcal{T}^N_{Q_0,Q_1,P_0}(U|\mathbf{k}, \mathbf{s}_1)|}{|\mathcal{T}^N_{Q_0,Q_1,P_0}(U|\mathbf{k})|}\Big)^J \le$$

$$\le (1 - \exp\{-N(I_{Q_0,Q_1,P_0}(S_1 \wedge U|K) + \delta/4\})^{\exp\{N(I_{Q_0,Q_1,P_0}(S_1 \wedge U|K) + \delta/2)\}} \le \exp\{-\exp\{N\delta/4\}\}. \quad (12)$$

The last inequality is true because for any n and $t \in (0, 1)$ we have $(1-t)^n \le \exp\{-nt\}$.

The codeword $\mathbf{x}$ is constructed in the following way. For each $m \in \mathcal{M}$ and $(\mathbf{k}, \mathbf{s}_1 \in \mathcal{T}^N_{Q_{0,1}}(K, S_1)$ we randomly choose $\mathbf{x}(m, \mathbf{k}, \mathbf{s}_1) \in \mathcal{T}^N_{Q_0, Q_1, P}(X|\mathbf{u}(m, \mathbf{k}, \mathbf{s}_1), \mathbf{k}, \mathbf{s}_1)$.

We must show that distortion caused be the encoder meets the requirement (5). Taking into account that $P \in \mathcal{P}(Q_{0,1}, \Delta_1)$ the distortion can be estimated in the following way:

$$d_1^N(\mathbf{s}_1, f_N(m.\mathbf{s}_1, \mathbf{k})) = \frac{1}{N} \sum_{s_1, x} N(s_1, x|\mathbf{s}_1, \mathbf{x}) d_1(s_1, x) =$$

$$= \sum_{x,u,s_1,k} Q_0(k) Q_1(s_1|k) P_0(u|s_1, k) P_1(x|u, s_1, k) d_1(s_1, x) \le \Delta_1,$$

where $N(s_1, x|\mathbf{s}_1, \mathbf{x})$ is the number of occurrences of s_1, x in the vector pair $\mathbf{s}_1, \mathbf{x}$.

We must also show that distortion caused by adversary meets the requirement (6). The channel A can variate in the set $\mathcal{A}(Q_{0,1,2}, P, \Delta_2)$. We have

$$\sum_{\mathbf{s}_2, \mathbf{x}, \mathbf{y}} QP^N(\mathbf{x}, \mathbf{s}_2) A^N(\mathbf{y}|\mathbf{x}, \mathbf{s}_2) d_2(\mathbf{x}, \mathbf{y}) = E d_2^N(X^N, Y^N) = \frac{1}{N} \sum_{n=1}^{N} E d_2(x_n, y_n) =$$

$$= \sum_{k, s_1, s_2, u, x, y} Q_{0,1,2}(k, s_1, s_2) P(x, u|k, s_1) A(y|x, s_2) d_2(x, y) \le \Delta_2.$$

Decoding Scheme

For brevity the pair of vectors $\mathbf{u}(m,\mathbf{k},\mathbf{s}_1),\mathbf{x}(m,\mathbf{k},\mathbf{s}_1)$ we denote by $\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1)$.
According to minimum divergence method each $\mathbf{y}$ and $\mathbf{s}_3$ are decoded to such m for which: $\mathbf{y},\mathbf{s}_3 \in \mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)$ and $Q = Q_0 \circ Q_1 \circ Q_2 \circ Q_3$, $P \in \mathcal{P}(Q_{0,1},\Delta_1)$, V are such that

$$\min_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} D(Q\circ P\circ V||Q^*\circ P\circ A)$$

is minimal.

The decoder g can make an error, when $m \in \mathcal{M}$ is transmitted in the case of $(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) \in \mathcal{T}^N_{Q_{0,1,2}}(K,S_1,S_2)$, but there exists $m' \neq m$, vector triple $(\mathbf{k}',\mathbf{s}_1',\mathbf{s}_2')$, types $Q' = Q_0'\circ Q_1'\circ Q_2'\circ Q_3'$, $P' \in \mathcal{P}(Q'_{0,1},\Delta_1)$, V' such that

$$\mathbf{y},\mathbf{s}_3 \in \mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\bigcap \mathcal{T}^N_{Q',P',V'}(Y,S_3|\mathbf{u}',\mathbf{x}'(m',\mathbf{k}',\mathbf{s}_1'),\mathbf{k}',\mathbf{s}_1',\mathbf{s}_2')$$

and

$$\min_{A\in\mathcal{A}(Q'_{0,1,2},P',\Delta_2)} D(Q'\circ P'\circ V'||Q^*\circ P'\circ A) \leq \min_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} D(Q\circ P\circ V||Q^*\circ P\circ A). \quad (13)$$

Error Estimation

Denote by $\mathcal{D} = \{Q,P,V,Q',P',V' : (13) \text{ is valid}\}$. The erroneous reconstruction of message $m \in \mathcal{M}$ maximal over all attack channels $A \in \mathcal{A}(Q_{0,1,2},P,\Delta_2)$ can be estimated in the following way:

$$e^1(m) = \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} \sum_{\mathbf{k},\mathbf{s}_1,\mathbf{s}_2} Q^{*N}_{0,1,2}(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) Q_3^{*N}\circ A^N(\mathcal{Y}^N\times \mathcal{S}_3^N\setminus g^{-1}_{N,\mathbf{k}}(m)|f_N(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2).$$

We can split the sum of the above formula into 2 parts with $(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) \notin \mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)$ and $(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) \in \mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)$. Taking into account (11) the first part can be estimated in the following way:

$$e_1^1(m) \leq \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} \sum_{(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\notin \mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)} Q^{*N}_{0,1,2}(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) \leq \exp\{-N(E-\varepsilon_1)\}. \quad (14)$$

The second part can be split again into 2 parts: error caused during encoding (e_2^1) and decoding (e_3^1) for $(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) \in \mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)$. Taking into account that number of $Q \in \mathcal{Q}(Q^*,E)$ does not exceed $(N+1)^{|\mathcal{K}||\mathcal{S}_1||\mathcal{S}_2||\mathcal{S}_3|}$ and (12) the e_2^1 can be estimated in the following way:

$$e_2^1(m) \leq \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} \sum_{(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\in \mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)} Q^{*N}_{0,1,2}(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) B_{Q_0,Q_1,P_0}(m,\mathbf{k},\mathbf{s}_1) \leq$$

$$\leq \exp\{-\exp\{N\delta/4\}+\varepsilon_2\}. \tag{15}$$

The estimation of e_3^1 is as follows:

$$e_3^1(m) \leq \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} \sum_{(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\in\mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)} Q^{*N}_{0,1,2}(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)$$

$$Q_3^{*N}\circ A^N\Big\{\bigcup_{\mathcal{D}}\mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\bigcap$$

$$\bigcup_{m'\neq m}\ \bigcup_{(\mathbf{k},\mathbf{s}'_1,\mathbf{s}'_2)\in\mathcal{T}^N_{Q'_{0,1,2},E}(K,S_1,S_2)} \mathcal{T}^N_{Q',P',V'}(Y,S_3|\mathbf{u}',\mathbf{x}'(m',\mathbf{k}',\mathbf{s}'_1),\mathbf{k}',\mathbf{s}'_1,\mathbf{s}'_2)\Big|\mathbf{x}(m,\mathbf{k},\mathbf{s}_1).\mathbf{k}.\mathbf{s}_1,\mathbf{s}_2\Big\}\leq$$

$$\leq \sum_{(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\in\mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)}\sum_{\mathcal{D}}\Big|\mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\bigcap$$

$$\bigcup_{m'\neq m}\ \bigcup_{(\mathbf{k}',\mathbf{s}'_1,\mathbf{s}'_2)\in\mathcal{T}^N_{Q'_{0,1,2},E}(K,S_1,S_2)} \mathcal{T}^N_{Q',P',V'}(Y,S_3|\mathbf{u}',\mathbf{x}'(m',\mathbf{k}',\mathbf{s}'_1),\mathbf{k}',\mathbf{s}'_1,\mathbf{s}'_2)\Big|\times$$

$$\times \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} Q^{*N}_{0,1,2}(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)Q_3^{*N}\circ A^N(\mathbf{y},\mathbf{s}_3|\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1.\mathbf{s}_2).$$

Packing Lemma. *For given Q^*, for any $E>\delta\geq 0$, types $Q=Q_0\circ Q_1\circ Q_2\circ Q_3\in\mathcal{Q}(Q^*,E)$, $P\in\mathcal{P}(Q_{0,1},\Delta_1)$ and set of channels $A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)$ there exists a code with*

$$|\mathcal{M}|\geq\exp\Big\{N\min_{Q,V:D(Q\circ P\circ V\|Q^*\circ P\circ A)\leq E}\Big|R(E,Q^*,A,Q,P,V)-\delta\Big|^+\Big\} \tag{16}$$

such that

1. for each $(\mathbf{k},\mathbf{s}_1)\in\mathcal{T}^N_{Q_{0,1}}(K,S_1)$ $\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1)$ are distinct for different $m\in\mathcal{M}$,

2. for sufficiently large N, for any $Q'\in\mathcal{Q}(Q^*,E)$, $P'\in\mathcal{P}(Q'_{0,1},\Delta_1)$ and conditional types V,V', for all $m\in\mathcal{M}$ and $(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\in\mathcal{T}^N_{Q_{0,1,2}}(K,S_1,S_2)$ the following inequality holds

$$\Big|\mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\bigcap$$

$$\bigcup_{m'\neq m}\ \bigcup_{(\mathbf{k}',\mathbf{s}'_1,\mathbf{s}'_2)\in\mathcal{T}^N_{Q'_{0,1,2},E}(K,S_1,S_2)} \mathcal{T}^N_{Q',P',V'}(Y,S_3|\mathbf{u}',\mathbf{x}'(m',\mathbf{k}',\mathbf{s}'_1),\mathbf{k}',\mathbf{s}'_1,\mathbf{s}'_2)\Big|\leq$$

$$\leq\Big|\mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\Big|\exp\Big\{-N\Big|E-\min_{A\in\mathcal{A}(Q'_{0,1,2},P',\Delta_2)}D(Q'\circ P'\circ V'\|Q^*\circ P'\circ A)\Big|^+\Big\}. \tag{17}$$

The Lemma can be proved by using the techniques established in [15]. Taking into account (1), (2), (4), (13) and (17) we can continue the estimation of e_3^1:

$$e_3^1(m)\leq\sum_{(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\in\mathcal{T}^N_{Q^*_{0,1,2},E}(K,S_1,S_2)}\sum_{\mathcal{D}}\Big|\mathcal{T}^N_{Q,P,V}(Y,S_3|\mathbf{u},\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)\Big|\times$$

$$\times \exp\left\{-N\left|E - \min_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} D(Q'\circ P'\circ V'||Q^*\circ P'\circ A)\right|^+\right\}\times$$

$$\times \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} Q_{0,1,2}^{*N}(\mathbf{k},\mathbf{s}_1,\mathbf{s}_2)Q_3^{*N}\circ A^N(\mathbf{y},\mathbf{s}_3|\mathbf{x}(m,\mathbf{k},\mathbf{s}_1),\mathbf{k},\mathbf{s}_1,\mathbf{s}_2) \leq$$

$$\leq \sum_{Q_{0,1,2}\in\mathcal{Q}(Q^*_{0,1,2},E)} \exp\{NH_{Q_0,Q_1,Q_2}(K,S_1,S_2)\}\sum_{\mathcal{D}}\exp\{NH_{Q,P,V}(Y,S_3|U,X,K,S_1,S_2)\}$$

$$\times \exp\left\{-N\left|E - \min_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} D(Q'\circ P'\circ V'||Q^*\circ P'\circ A)\right|^+\right\}\times$$

$$\times \max_{A\in\mathcal{A}(Q_{0,1,2},P,\Delta_2)} \exp\{-N(H_{Q_0,Q_1,Q_2}(K,S_1,S_2)+D(Q_{0,1,2}||Q^*_{0,1,2})+H_{Q,P,V}(Y,S_3|X,K,S_1,S_2)+$$

$$+D(Q_3\circ V||Q_3^*\circ A|Q_0,Q_1,Q_2,P))\} \leq (N+1)^{|\mathcal{K}||\mathcal{S}_1||\mathcal{S}_2|}\sum_{\mathcal{D}}\exp\{-N(E+H_{Q,P,V}(Y,S_3|X,K,S_1,S_2)-$$

$$-H_{Q,P,V}(Y,S_3|U,X,K,S_1,S_2))\} \leq (N+1)^{|\mathcal{K}||\mathcal{S}_1||\mathcal{S}_2|}\sum_{Q,P,V,Q',P',V'}\exp\{-NE\} \leq$$

$$\leq \exp\{-N(E-\varepsilon_3)\}. \tag{18}$$

Considering (14), (15) and (18) the overall error can be upper bounded:

$$e^1(m) = e_1^1(m) + e_2^1(m) + e_3^1(m) \leq \exp\{-N(E-\varepsilon_1)\} + \exp\{-\exp\{N\delta/4\}+\varepsilon_2\}+$$

$$+\exp\{-N(E-\varepsilon_3)\} \leq \exp\{-N(E-\varepsilon)\}.$$

Taking into account the continuity of all expressions when $N \to \infty$, arbitrary probability distributions can be considered instead of types. The theorem is proved.

References

[1] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters", *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19-31, 1980.

[2] R. Ahlswede, "Arbitrarily varying channels with states sequence known to the sender", *IEEE Transactions on Information Theory*, vol. IT-32, no. 5, pp. 621-629, 1986.

[3] E. A. Haroutunian, M. E. Haroutunian, "Channel with random parameter", *Proc. of XXII Prague conf. on Inform. Theory, Statistical Decision Functions, Random Processes*, pp. 99-101, 1994.

[4] M. E. Haroutunian, "New bounds for E-capacities of arbitrarily varying channel and channel with random parameter", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA, Mathematical Problems of Computer Sciences*, vol. 22, pp. 44-59, 2001.

[5] M. E. Haroutunian, "On multiple-access channel with random parameter", *Proc. of Int. conf. on Computer Science and Inform. Technologies*, Armenia, Yerevan, pp. 174 - 178, 2003.

[6] A. Somekh-Baruch and N. Merhav, "On the random coding error exponenets of the single-user and the multiple-access Gel'fand-Pinsker channels", *Proc. of IEEE International Symposium on Information Theory*, USA, Chicago, p. 448, 2004.

[7] M. E. Haroutunian, "Estimates of E-capacity and capacity regions for multiple-access channel with random parameter", *Lecture Notes in Computer Science*, vol. 4123, Springer Verlag, pp. 196-217, 2006.

[8] P. Moulin and J.A. O'Sullivan, "Information-theoretic analysis of information hiding", *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 563-593, Mar. 2003.

[9] M. E. Haroutunian, S. A. Tonoyan, "Random coding bound of information hiding E-capacity", *Proc. of IEEE International Symposium on Information Theory*, USA, Chicago, p. 536, 2004.

[10] M. E. Haroutunian, S. A. Tonoyan "On estimates of rate-reliability distortion function for information hiding system", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA, Mathematical Problems of Computer Science*, vol. 23, pp. 20-31, 2004.

[11] A. Somekh-Baruch, N. Merhav, "On the error exponent and capacity games of private watermarking systems", *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 537-562, 2003.

[12] A. Somekh-Baruch, N. Merhav, "On the capacity game of public watermarking systems", *IEEE Transactions on Information Theory*,vol. 50, no. 3, pp. 511-524, 2004.

[13] M. Haroutunian, S. Tonoyan, O. Koval, S. Voloshynovskiy, "On reversible information hiding system", *Proc. of IEEE International Symposium on Information Theory*, Canada, Toronto, pp. 940-944,2008.

[14] T. M. Cover and M. Chiang, "Duality between channel capacity and rate distortion with two-sided state information", *IEEE Transactions on Information Theory*, vol. 48, no. 6, pp. 1629-1638, 2002.

[15] M. Haroutunian, A. Muradyan, "Lower bound for E capacity of discrete memoryless channel with two-sided state information", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA, Mathematical Problems of Computer Sciences*, vol. 31, pp. 28-39, 2008.

[16] P. Moulin and Y. Wang, "Capacity and random-coding exponents for channel coding with side information", *IEEE Transactions on Information Theory*, vol. 53, no. 4, 2007.

[17] E. A. Haroutunian, "Upper estimate of transmission rate for memoryless channel with countable number of output signals under given error probability exponent", (in Russian), *3rd All-Union Conf. on Theory of Information Transmission and Coding, Uzhgorod, Publication house of Uzbek Academy of Sciences, Tashkent*, pp. 83-86, 1967.

[18] E. A. Haroutunian, "On bounds for E-capacity of DMC", *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4210-4220, 2007.

[19] E. A. Haroutunian, M. E. Haroutunian and A. N. Harutyunyan, "Reliability criteria in information theory and in statistical hypothesis testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, no 2-3, pp. 97-263, 2008.

[20] T. M. Cover and J. A. Thomas, "Elements of Information Theory", second edition, Wiley, New York, 2006.

[21] I. Csiszár and J. Körner, "Information Theory: Coding Theorems for Discrete Memoryless Systems", Academic Press, New York, 1981.

[22] I. Csiszár, "The method of types", *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505-2523, 1998.

Արագություն-հուսալիություն-շեղում ֆունկցիայի ստորին գնահատականը ընդհանրացված կողմնակի ինֆորմացիայով կապուղիների համար

Մ. Հարությունյան և Ա. Մուրադյան

Ամփոփում

Աշխատանքում ուսումնասիրված է ընդհատ առանց հիշողության կապուղու ընդհանրացված մոդելը, երբ պատահական վիճակի հաջորդականությունը (կողմնակի ինֆորմացիան) մասնակիորեն հայտնի է կոդավորիչին, կապուղուն և ապակոդավորիչին: Որպես դիտարկված մոդելի մասնավոր դեպք ստացվում են Գելֆանդ-Պինսկերի և ինֆորմացիայի թաքցման կոդավորման խնդիրները: Դիտարկված մոդելում ինֆորմացիան պետք է հուսալի ուղարկել հարձակվողի կողմից ընտրված աղմուկով կապուղու միջոցով: Կիրառություններից ելնելով կոդավորիչի և հարձակվողի գործողությունների վրա դրված են շեղման սահմանափակումներ: Կոդավորիչը և ապակոդավորիչը կախված են պատահական փոփոխականից, որը կարող է դիտարկվել որպես կոդավորման բանալի: Դիտարկվել են երկու դեպքեր, երբ պատահական փոփոխականի և կողմնակի ինֆորմացիայի համատեղ բաշխումը տրված է կամ պատահական փոփոխականը անկախ է կողմնակի ինֆորմացիայից և նրա բաշխումը կարող է ընտրվել լավագույն կոդի ստեղծման համար: Հետազոտվել է արագություն հուսալիություն շեղում ֆունկցիան նշված մոդելի համար և կառուցվել դրա ստորին գնահատականը:

Հոդվածում ստացված է երկու վիճակագրորեն կախյալ օբյեկտների հավանականային բաշխումների ասիմպտոտորեն օպտիմալ նույնականացման խնդրի լուծումը: Երկու անկախ օբյեկտների դեպքում խնդիրը լուծվել էր [5]-ում: