Mathematical Problems of Computer Science 21, 2000, 61–76.

On Branching Communication System Rates-Reliability-Distortions Region with Partial Secrecy under Distortion Criterion

Evgueni A. Haroutunian, Ashot N. Harutyunyan*, Anahit R. Ghazaryan†
and Edward C. van der Meulen

Institute for Informatics and Automation Problems of NAS RA and YSU
E-mail: evhar@ipia.sci.am, ashar@ipia.sci.am,
ecvdm@gauss.wis.kuleuven.ac.be

Abstract

A source coding problem for a one-stage branching communication system is considered. Messages of K correlated sources $\{X_1, \dots, X_K\} = X$ are encoded by a common encoder and two secondary encoders. At each receiver it is demanded: (i) to recover messages of a part of the sources within given distortion levels, (ii) to keep secret the outputs of another part of the sources for receivers connected to the secondary encoders; for this purpose corresponding distortions must be ensured to be sufficiently great, (iii) to disregard the information of the rest of the sources.

It is required that for a given reliabilty $E > 0$ at all receivers the error probabilities of the blocklength N code do not exceed 2^{-NE}.

Inner and outer bounds on the region of achievable rates are established, depending on the reliability E and permissible distortion and secrecy levels. The results are specialized to some particular communication systems, including those studied by Yamamoto and El Gamal and Cover.

1 Introduction

We study a problem of common encoding of K correlated sources for transmission to three destinations with respect to fidelity, security and reliability criteria for the one-stage branching communication system shown in Fig. 1.

The problem is a generalization of the encoding problem studied by Yamamoto [17] for a bidirectorial branching communication system.

Let X_n, $n = \overline{1,N}$ be a sequence of N discrete, independent, identically distributed (i.i.d.) random vectors (RV) with K components $X_n = (X_{1,n}, ..., X_{K,n})$. A random variable (Rv) $X_{k,n}$ represents the message of the k-th source at the n-th moment, $k = \overline{1,K}$, $n = \overline{1,N}$, with values in the finite set $\mathcal{X}_k$, $k = \overline{1,K}$, respectively. Let

$$\mathcal{X}_1 \times ... \times \mathcal{X}_K = \mathcal{X}, \quad (\mathcal{X}_1)^N \times ... \times (\mathcal{X}_K)^N = (\mathcal{X})^N.$$

*The work of the author was supported by INTAS YSF Grant 00-4162.
†The work of the author was supported by INTAS YSF Grant 00-4163.

For each receiver $m = 0, 1, 2$ the set of indices of sources $\{1, ..., K\}$ is divided into three groups:

$$\{1, ..., K\} = \mathcal{G}_1^m \bigcup \mathcal{G}_2^m \bigcup \mathcal{G}_3^m, \ \mathcal{G}_2^0 = \emptyset.$$

We denote by small letters the corresponding values of RV and Rv, such that

$$(x_{1,n}, ..., x_{K,n}) = x_n, \ (x_{k,1}, ..., x_{k,N}) = \mathbf{x}_k, \ k = \overline{1,K}, \ (\mathbf{x}_1, ..., \mathbf{x}_K) = \mathbf{x}.$$

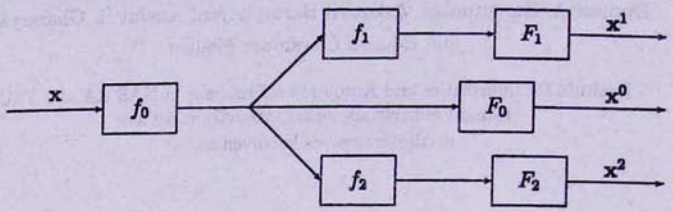

Fig. 1. One-stage threedirectorial branching communication system.

Let $X_{k,n}^m$ be the reconstruction of the n-th message of the k-th source at the m-th receiver, with values in a finite set $\mathcal{X}_k^m$, respectively, $n = \overline{1,N}$, $k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m$, $m = 0, 1, 2$. The sets $\mathcal{X}_k^m$ are the reconstruction alphabets and in general they are different from $\mathcal{X}_k$, $k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m$, $m = 0, 1, 2$. Let

$$(X_{k,n}^m, k \in \mathcal{G}_s^m) = X_{m,s,n}^m, \ (X_{m,s,1}^m, \ldots, X_{m,s,N}^m) = \mathbf{X}_{m,s}^m, \ s = 1, 2, \ m = 0, 1, 2.$$

We denote by $\mathcal{X}_{m,s}^m$ the Cartesian product of the sets $\mathcal{X}_k^m$, by $(\mathcal{X}_{m,s}^m)^N$ - the Cartesian product of the sets $(\mathcal{X}_k^m)^N$, $k \in \mathcal{G}_s^m$, $s = 1, 2$, $m = 0, 1, 2$. Let

$$\mathcal{X}_{m,1}^m \times \mathcal{X}_{m,2}^m = \mathcal{X}^m, \ (\mathcal{X}_{m,1}^m)^N \times (\mathcal{X}_{m,2}^m)^N = (\mathcal{X}^m)^N, \ m = 0, 1, 2.$$

For messages received at the outputs we use analogous notations, such as

$$(x_{k,n}^m, k \in \mathcal{G}_s^m) = x_{m,s,n}^m, \ (x_{m,1,n}^m, x_{m,2,n}^m) = x_n^m, \ (x_{k,1}^m, ..., x_{k,N}^m) = \mathbf{x}_k^m, \ k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m,$$

$$(\mathbf{x}_k^m, k \in \mathcal{G}_s^m) = \mathbf{x}_{m,s}^m, \ (\mathbf{x}_{m,1}^m, \mathbf{x}_{m,2}^m) = \mathbf{x}^m, \ s = 1, 2, \ m = 0, 1, 2.$$

The common probability distribution (PD) of the vector of messages of K sources is denoted by

$$P^* = \{P^*(x), \ x \in \mathcal{X}\}.$$

Since X_n, $n = \overline{1,N}$, is a sequence of i.i.d. RVs, we omit the subscript n in the sequel. Since the sources are assumed to be memoryless, we have that

$$P^{*N}(\mathbf{x}) = \prod_{n=1}^{N} P^*(x_n).$$

We assume the following distortion measures:

$$d_k^m : \mathcal{X}_k \times \mathcal{X}_k^m \to [0, \infty), \ k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m, \ m = 0, 1, 2.$$

The average distortions of N–vectors are defined by

$$d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) = N^{-1} \sum_{n=1}^{N} d_k^m(x_{kn}, x_{kn}^m),$$

where $\mathbf{x}_k \in (\mathcal{X}_k)^N$, $\mathbf{x}_k^m \in (\mathcal{X}_k^m)^N$, $k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m$, $m = 0, 1, 2$.

For the system considered, a code $(f, F) = (f_0, f_1, f_2, F_0, F_1, F_2)$ is a family of six mappings:

(i) three encoding functions

$$f_0 : (\mathcal{X})^N \to \{1, ..., M_0(N)\},$$

$$f_1 : \{1, ..., M_0(N)\} \to \{1, ..., M_1(N)\},$$

$$f_2 : \{1, ..., M_0(N)\} \to \{1, ..., M_2(N)\},$$

(ii) and three decoding functions

$$F_m : \{1, ..., M_m(N)\} \to (\mathcal{X}^m)^N, \ m = 0, 1, 2.$$

The tasks of the system are:

1) to restore the messages of the sources $\{X_k\}$ at the m-th receiver within given distortion levels Δ_k^m, $k \in \mathcal{G}_1^m$, $m = 0, 1, 2$,

2) to keep secret the messages of the sources $\{X_k\}$, $k \in \mathcal{G}_2^m$, from the m-th receiver, $m = 1, 2$, by ensuring the distortions between the transmitted and the received messages of the k-th source at the m-th output to be greater than a given level Δ_k^m, $k \in \mathcal{G}_2^m$, $m = 1, 2$.

Security evaluation by distortion measures was first considered by Yamamoto in [19] and later in [20] for the case of the Shannon cipher system with a broadcast channel. The problem of keeping the correlation information secret from the receiver was earlier considered by Yamamoto in [18] and later in [19] for a one-way communication system.

Let us consider the following sets:

$$\mathcal{A}_0 = \{\mathbf{x} : \ F_0(f_0(\mathbf{x})) = \mathbf{x}^0, \ d_k^0(\mathbf{x}_k, \mathbf{x}_k^0) \le \Delta_k^0, \ k \in \mathcal{G}_1^0\},$$

$$\mathcal{A}_m = \{\mathbf{x} : \ F_m(f_m(f_0(\mathbf{x}))) = \mathbf{x}^m, \ d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) \le \Delta_k^m, \ k \in \mathcal{G}_1^m,$$

$$d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) \ge \Delta_k^m, \ k \in \mathcal{G}_2^m\}, \ m = 1, 2.$$

For brevity we denote

$$(\Delta_k^m, \ k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m) = \Delta^m, \ (\Delta^0, \Delta^1, \Delta^2) = \mathbf{\Delta}.$$

The error probabilities of the code (f, F) are defined as follows:

$$e_m(f, F, \Delta^m) = 1 - P^{*N}(\mathcal{A}_m), \ m = 0, 1, 2.$$

A triplet of nonnegative numbers (R_0, R_1, R_2) is called $(E, \mathbf{\Delta})$-achievable for $E > 0$, $\Delta_k^m \ge 0$, $k \in \mathcal{G}_1^m \cup \mathcal{G}_2^m$, $m = 0, 1, 2$, if for any $\varepsilon > 0$ and N sufficiently large there exists a code (f, F) such that

$$N^{-1} \log M_m(N) \le R_m + \varepsilon,$$

$$e_m(f, F, \Delta^m) \le \exp(-NE), \ m = 0, 1, 2. \qquad (1)$$

(The logarithm and exponential functions are taken to the base 2.)

We call the set $\mathcal{R}(E,\Delta)$ of all (E,Δ)-achievable rates the rates-reliability-distortions and partial secrecy region. When $E \to 0$, $\mathcal{R}(E,\Delta)$ becomes the rates-distortions and partial secrecy region $\mathcal{R}(\Delta)$. If $\mathcal{G}_2^m \equiv \mathcal{G}_3^m \equiv \emptyset$, then $\mathcal{R}(E,\Delta)$ is the rates-reliability-distortions region, and $\mathcal{R}(\Delta)$ is the *rates-distortions region*. $\mathcal{R}(\Delta)$ in the case when the system has two correlated sources $\{X_1\}$ and $\{X_2\}$, the decoder F_0 is absent and at the decoder F_m only the messages of the source $\{X_m\}$ are reconstructed, $m = 1,2$, and no secrecy restrictions are present, was studied by Yamamoto [17], who called such scheme a bidirectorial branching communication system. If $\mathcal{G}_2^m \equiv \mathcal{G}_3^m \equiv \emptyset$, the system has one source $\{X\}$, and $R_0 = R_1 = R_2$, then $\mathcal{R}(\Delta)$ becomes the rate-distortions function for the robust description system, considered by El Gamal and Cover [7].

Inner and outer bounds for the rates-reliability-distortions and partial secrecy region $\mathcal{R}(E,\Delta)$ are formulated in the Theorem in the second section. Proofs are presented in the third Section and in the Appendix.

The preliminary results were presented at the 1999 International Conference on Computer Science and Information Technologies [15] and at the 2000 IEEE International Symposium on Information Theory [16].

2 Formulation of Results

Let

$$P = \{P(x_n),\ x_n \in \mathcal{X},\ n = \overline{1,N}\}$$

be a PD on $\mathcal{X}$,

$$Q = \{Q(x_n^0, x_n^1, x_n^2 \mid x_n),\ x_n \in \mathcal{X},\ x_n^m \in \mathcal{X}^m,\ n = \overline{1,N},\ m = 0,1,2\}$$

be a conditional PD on $\mathcal{X}^0 \times \mathcal{X}^1 \times \mathcal{X}^2$ for given x,

$$P_{k,n} = \{P(x_{k,n})\},\ n = \overline{1,N},\ k = \overline{1,K},$$

with

$$P(x_{k,n}) = \sum_{x_{r,n} \in \mathcal{X}_r,\ r=\overline{1,K},\ r \neq k} P(x_n).$$

We also need

$$Q_n^m = \{Q(x_n^m \mid x_n)\},\ n = \overline{1,N},\ m = 0,1,2,$$

with

$$Q(x_n^m \mid x_n) = \sum_{x_n^t \in \mathcal{X}^t,\ t=0,1,2,\ t \neq m} Q(x_n^0, x_n^1, x_n^2 \mid x_n),$$

and

$$Q_{k,n}^m = \{Q(x_{k,n}^m \mid x_{k,n})\},\ k = \overline{1,K},\ n = \overline{1,N},\ m = 0,1,2,$$

with

$$Q(x_{k,n}^m \mid x_{k,n}) = \sum_{x_{r,n} \in \mathcal{X}_r,\ x_{r,n}^m \in \mathcal{X}_r^m,\ r=\overline{1,K},\ r \neq k} P(x_{1,n}, \ldots, x_{k-1,n}, x_{k+1,n}, \ldots, x_{K,n} \mid x_{k,n}) Q(x_n^m \mid x_n).$$

Consider the set

$$\alpha(E) = \{P :\ D(P \parallel P^*) \leq E\}.$$

We denote by $\Phi(P,E,\Delta)=Q_P$ the function, which puts into correspondence with the PD P some PD Q_P such that for given Δ, if $P\in\alpha(E)$, the following three conditions are fulfilled:

$$\mathbf{E}_{P,Q_P}d_k^m(X_k,X_k^m)=$$

$$=\sum_{x_{k,n},x_{k,n}^m}P(x_{k,n})Q_P(x_{k,n}^m\mid x_{k,n})d_k^m(x_{k,n},x_{k,n}^m)\le\Delta_k^m,\ k\in\mathcal{G}_1^m,\ m=0,1,2, \tag{2}$$

$$\mathbf{E}_{P,Q_P}d_k^m(X_k,X_k^m)\ge\Delta_k^m,\ k\in\mathcal{G}_2^m,\ m=1,2. \tag{3}$$

Denote by $\mathcal{M}(P,E,\Delta)$ the set of all such functions $\Phi(P,E,\Delta)$ for given P, Δ and E, and by $\mathcal{M}(\Delta)$ – the set of all functions $\Phi(P^*,\Delta)$, for which (2) and (3) are valid for given Δ and P^*. Below we shall write for brevity simply $\Phi(P)$ and $\Phi(P^*)$.

Let us denote by $\Phi_i(P)$, $i=1,2$, those functions $\Phi(P)$, which are of the following forms:

$$\Phi_1(P)=Q_P(x^1\mid x)Q_P(x^2\mid x)Q_P(x^0\mid x^2,x),$$

$$\Phi_2(P)=Q_P(x^1\mid x)Q_P(x^2\mid x)Q_P(x^0\mid x^1,x).$$

Define the regions:

$\mathcal{D}_1=\mathcal{D}_1(E,\Delta,P,\Phi(P))=\{(R_0,R_1,R_2):$

$$R_0\ge I_{P,\Phi(P)}(X\wedge X_{0,1}^0,X_{1,1}^1,X_{2,1}^2),$$

$$R_1\ge I_{P,\Phi(P)}(X\wedge X_{1,1}^1),\ \ R_2\ge I_{P,\Phi(P)}(X\wedge X_{1,1}^1,X_{2,1}^2)\},$$

$\mathcal{D}_2=\mathcal{D}_2(E,\Delta,P,\Phi(P))=\{(R_0,R_1,R_2):$

$$R_0\ge I_{P,\Phi(P)}(X\wedge X_{0,1}^0,X_{1,1}^1,X_{2,1}^2),$$

$$R_1\ge I_{P,\Phi(P)}(X\wedge X_{1,1}^1,X_{2,1}^2),\ \ R_2\ge I_{P,\Phi(P)}(X\wedge X_{2,1}^2)\},$$

$\mathcal{D}_3=\mathcal{D}_3(E,\Delta,P,\Phi_1(P))=\{(R_0,R_1,R_2):$

$$R_0\ge I_{P,\Phi_1(P)}(X\wedge X_{1,1}^1)+I_{P,\Phi_1(P)}(X\wedge X_{2,1}^2)+I_{P,\Phi_1(P)}(X\wedge X_{0,1}^0\mid X_{2,1}^2),$$

$$R_1\ge I_{P,\Phi_1(P)}(X\wedge X_{1,1}^1),\ \ R_2\ge I_{P,\Phi_1(P)}(X\wedge X_{2,1}^2)\},$$

$\mathcal{D}_4=\mathcal{D}_4(E,\Delta,P,\Phi_2(P))=\{(R_0,R_1,R_2):$

$$R_0\ge I_{P,\Phi_2(P)}(X\wedge X_{1,1}^1)+I_{P,\Phi_2(P)}(X\wedge X_{2,1}^2)+I_{P,\Phi_2(P)}(X\wedge X_{0,1}^0\mid X_{1,1}^1),$$

$$R_1\ge I_{P,\Phi_2(P)}(X\wedge X_{1,1}^1),\ \ R_2\ge I_{P,\Phi_2(P)}(X\wedge X_{2,1}^2)\}.$$

Next consider the regions:

$$\mathcal{R}^-(E,\Delta,P,\Phi(P),\Phi_1(P),\Phi_2(P))=\bigcup_{i=1}^4\mathcal{D}_i$$

and

$\mathcal{R}^+(E,\Delta,P,\Phi(P))=\{(R_0,R_1,R_2):$

$$R_0\ge I_{P,\Phi(P)}(X\wedge X_{0,1}^0,X_{1,1}^1,X_{2,1}^2),$$

$$R_1 \geq I_{P,\Phi(P)}(X \wedge X^1_{1,1}),\ \ R_2 \geq I_{P,\Phi(P)}(X \wedge X^2_{2,1})\}.$$

We shall use as inner estimate for $\mathcal{R}(E,\Delta)$ the region

$$\mathcal{R}^-(E,\Delta) = \bigcap_{P\in\alpha(E)} \bigcup_{\Phi(P),\Phi_1(P),\Phi_2(P)\in\mathcal{M}(P,E,\Delta)} \mathcal{R}^-(E,\Delta,\Phi(P),\Phi_1(P),\Phi_2(P)),$$

and as outer estimate the region

$$\mathcal{R}^+(E,\Delta) = \bigcap_{P\in\alpha(E)} \bigcup_{\Phi(P)\in\mathcal{M}(P,E,\Delta)} \mathcal{R}^+(E,\Delta,\Phi(P)).$$

Then we can prove the following theorem.

Theorem: For $E > 0$, $\Delta^m_k \geq 0$, $k \in \mathcal{G}^m_1 \cup \mathcal{G}^m_2$, $m = 0,1,2,$

$$\mathcal{R}^-(E,\Delta) \subseteq \mathcal{R}(E,\Delta) \subseteq \mathcal{R}^+(E,\Delta).$$

From this theorem we deduce the following corollaries.

Corollary 1: When $E \to 0$, we obtain inner and outer bounds for the corresponding rates-distortions and partial secrecy region $\mathcal{R}(\Delta)$.

Corollary 2: When the system has two correlated sources $\{X_1\}$ and $\{X_2\}$, decoder F_0 is absent, at the first decoder only the messages of the source $\{X_1\}$ and at the second decoder only the messages of the source $\{X_2\}$ must be reconstructed, and no secrecy restrictions are present, then we arrive at the result of Yamamoto [17] for a bidirectorial branching communication system. But for this system our inner bound for the rates-distortions region is larger, because Yamamoto did not take into account the regions $\mathcal{D}_3$ and $\mathcal{D}_4$, which in this case coincide and take on the following form:

$\{(R_0,R_1,R_2)$:

$$R_0 \geq R(\Delta^1) + R(\Delta^2),$$

$$R_1 \geq R(\Delta^1),\ \ R_2 \geq R(\Delta^2)\}.$$

Corollary 3: If the system has two correlated sources $\{X_1\}$ and $\{X_2\}$, $R_2 = 0$, $\mathcal{G}^m_2 \cup \mathcal{G}^m_3 \equiv \emptyset$, $m = 0,1$, then it becomes the cascade communication system studied by Yamamoto [17], the rates-reliabilities-distortions region of which was specified in [8], [12].

Corollary 4: If $\mathcal{G}^m_2 \cup \mathcal{G}^m_3 \equiv \emptyset$, the system has only one source $\{X\}$, encoders f_1 and f_2 are absent, or $R_1 = R_2 = R_0$, then we arrive at the result of El Gamal and Cover [7] concerning multiple descriptions, see also [2]–[4], [7]–[11], [13], [14], [21].

Corollary 5: When the system has two correlated sources $\{X_1\}$ and $\{X_2\}$, encoder f_2, decoders F_0 and F_2 are absent, at the decoder F_1 only the messages of the source $\{X_1\}$ must be reconstructed, then the inner and outer bounds for the rates-reliability-distortions and partial secrecy function coincide:

$$R^-(E,\Delta^1) \equiv R^+(E,\Delta^1) \equiv R(E,\Delta^1) = \max_{P\in\alpha(E)} \min_{\substack{Q_P:\, \mathbf{E}_{P,Q_P} d_1(X_1,X^1_1) \leq \Delta^1_1,\\ \mathbf{E}_{P,Q_P} d_2(X_2,X^1_2) \geq \Delta^1_2}} I_{P,Q_P}(X \wedge X_1),$$

and specifically for the same problem with absence of reliability criterion we arrive at the result of Yamamoto [19] for an one-way communication system with correlated source outputs.

Corollary 6: If $X \to X^2_{2,1} \to X^1_{1,1}$ or $X \to X^1_{1,1} \to X^2_{2,1}$ form Markov chains and decoder F_0 is absent, then the inner and outer bounds for the rates-reliability-distortions and partial secrecy region coincide and give the rates-reliability-distortions and partial secrecy region:

$$\mathcal{R}(E,\Delta) = \bigcap_{P\in\mathcal{Q}(\mathcal{E})} \bigcup_{\Phi(P)\in\mathcal{M}(P,\mathcal{E},\Delta)} \{(R_0,R_1,R_2): R_0 \ge I_{P,\Phi(P)}(X \wedge X^0_{0,1}, X^1_{1,1}, X^2_{2,1}),$$

$$R_1 \ge I_{P,\Phi(P)}(X \wedge X^1_{1,1}),\ \ R_2 \ge I_{P,\Phi(P)}(X \wedge X^2_{2,1})\}.$$

Corollary 7: In the special case of absence of decoder F_0 for $R_0 = R(E,\Delta^1) + R(E,\Delta^2)$, where $R(E,\Delta^m)$, $m = 1,2$, are the rate-reliability-distortions and partial secrecy functions:

$$R(E,\Delta^m) = \max_{P\in\mathcal{Q}(\mathcal{E})} \min_{\substack{Q_P:\, \mathbf{E}_{P,Q_P} d^m_k(X_k,X^m_k) \le \Delta^m_k,\ k\in\mathcal{G}^m_1,\\ \mathbf{E}_{P,Q_P} d^m_k(X_k,X^m_k) \ge \Delta^m_k,\ k\in\mathcal{G}^m_2}} I_{P,Q_P}(X \wedge X^m_{m,1}),\ \ m = 1,2,$$

the inner and outer bounds for the rates-reliability-distortions and partial secrecy region coincide:

$$\mathcal{R}^-(E,\Delta) \equiv \mathcal{R}^+(E,\Delta) \equiv \mathcal{R}(E,\Delta) = \{(R_0,R_1,R_2):$$

$$R_0 \ge R(E,\Delta^1) + R(E,\Delta^2),\ \ R_1 \ge R(E,\Delta^1),\ \ R_2 \ge R(E,\Delta^2)\}.$$

Remarks: 1. The considered problem can be generalized by considering different reliabilities E_m at the different receivers, $m = 0,1,2$.

2. A similar problem can be considered for a multistage branching communication system [17].

3. Our inner and outer estimates $\mathcal{R}^-(E,\Delta)$ and $\mathcal{R}^+(E,\Delta)$ for $\mathcal{R}(E,\Delta)$ are not proved to be convex. Naturally, it is desired to receive the convex estimates for $\mathcal{R}(E,\Delta)$. But, the difficulty (which we were not able to overcome) is that the timesharing arguments may not be applied for the problem with reliability criterion.

3 Proof of the Theorem

We use the typical sequences technique [5], [6] and apply the following modification of covering lemma from [1], [5], [9], [11]:

Lemma: Let for fixed type P, conditional type Q and $\varepsilon > 0$

$$L_1(P,Q) = \exp\{N(I_{P,Q}(X \wedge X^1_{1,1}) + \varepsilon)\},$$

$$L_2(P,Q) = \exp\{N(I_{P,Q}(X \wedge X^2_{2,1} \mid X^1_{1,1}) + \varepsilon)\},$$

$$L_0(P,Q) = \exp\{N(I_{P,Q}(X \wedge X^0_{0,1} \mid X^1_{1,1}, X^2_{2,1}) + \varepsilon)\}.$$

Then for sufficiently large N there exist:

a collection of conditional types

$$\{\mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}),\ l_1 = \overline{1, L_1(P,Q)}\},$$

which is a covering for $\mathcal{T}_P(X)$,

for $l_1 = \overline{1, L_1(P,Q)}$ a collection of conditional types

$$\{\mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}),\ l_2 = \overline{1, L_2(P,Q)}\},$$

which is a covering for $\mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1})$,
for $l_1 = \overline{1, L_1(P,Q)}$, $l_2 = \overline{1, L_2(P,Q)}$ a collection

$$\{\mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}, \mathbf{x}^0_{0,1,l_1,l_2,l_0}),\ l_0 = \overline{1, L_0(P,Q)}\},$$

which is a covering for $\mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2})$.

Proof of the Lemma is given in Appendix.

We begin the proof of the theorem from the inclusion

$$\mathcal{R}^-(E,\Delta) \subseteq \mathcal{R}(E,\Delta). \tag{4}$$

Denote by $\mathcal{P}(X,N)$ the set of all distributions P, which for given N are types. Let us present $(\mathcal{X})^N$ as a family of disjoint types

$$(\mathcal{X})^N = \bigcup_{P \in \mathcal{P}(X,N)} \mathcal{T}_P(X).$$

Let some $\delta > 0$ be given. Then from [5] we have

$$P^{*N}[\bigcup_{P \notin \alpha(E+\delta)} \mathcal{T}_P(X)] \le (N+1)^{|\mathcal{X}|} \exp\{-N \min_{P \notin \alpha(E+\delta)} D(P \parallel P^*)\} \le$$

$$\le \exp\{-N(E+\delta) + |\mathcal{X}| \log(N+1)\} \le \exp\{-N(E+\frac{\delta}{2})\}.$$

Hence, to obtain error probabilities small enough, it is sufficient to construct good encoding functions only for the vectors of the types P from $\alpha(E+\delta)$.

For each type P from $\alpha(E+\delta)$ let us fix some $\Phi(P) \in \mathcal{M}(P,E,\Delta)$ and denote it by $\Phi(P) = Q_P$. According to the lemma there exists a covering

$$\{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}),\ l_1 = \overline{1, L_1(P,Q_P)}\}$$

for $\mathcal{T}_P(X)$. Let

$$\mathcal{B}(P,Q_P,l_1) = \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}) - \bigcup_{l_1' < l_1} \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1'}),\ l_1 = \overline{1, L_1(P,Q_P)}.$$

For any $l_1 = \overline{1, L_1(P,Q_P)}$ a covering

$$\{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}),\ l_2 = \overline{1, L_2(P,Q_P)}\}$$

for $\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1})$ exists. Let for $l_2 = \overline{1, L_2(P,Q_P)}$

$$\mathcal{B}(P,Q_P,l_1,l_2) = \mathcal{B}(P,Q_P,l_1) \bigcap \{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}) - \bigcup_{l_2' < l_2} \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2'})\}.$$

For any $l_1 = \overline{1, L_1(P,Q_P)}$, $l_2 = \overline{1, L_2(P,Q_P)}$ a covering

$$\{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}, \mathbf{x}^0_{0,1,l_1,l_2,l_0}),\ l_0 = \overline{1, L_0(P,Q_P)}\}$$

for $\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2})$ exists. Let for $l_0 = \overline{1, L_0(P,Q_P)}$

$$\mathcal{B}(P,Q_P,l_0,l_1,l_2) = \mathcal{B}(P,Q_P,l_1,l_2) \cap$$

$$\cap\{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}, \mathbf{x}^0_{0,1,l_1,l_2,l_0}) - \bigcup_{l_0'<l_0} \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}, \mathbf{x}^0_{0,1,l_2,l_2,l_0'})\}.$$

For $(R_0,R_1,R_2) \in \mathcal{D}_1$ we define a code $(f,F) = (f_0,f_1,f_2,F_0,F_1,F_2)$ as follows: encoding functions

$$f_0(\mathbf{x}) = \begin{cases} (l_1,l_2,l_0), & \text{when } \mathbf{x} \in \mathcal{B}(P,Q_P,l_0,l_1,l_2),\ P \in \alpha(E+\delta), \\ k', & \text{when } \mathbf{x} \in \mathcal{T}_P(X),\ P \notin \alpha(E+\delta), \end{cases}$$

$$f_1(l_1,l_2,l_0) = l_1,\ f_2(l_1,l_2,l_0) = (l_1,l_2),\ f_m(k') = k',\ m = 1,2,$$

decoding functions

$$F_0(l_1,l_2,l_0) = \mathbf{x}^0_{0,1,l_1,l_2,l_0},\ F_1(l_1) = \mathbf{x}^1_{1,1,l_1},\ F_2(l_1,l_2) = \mathbf{x}^2_{2,1,l_1,l_2},\ F_m(k') = \overline{\mathbf{x}}^m,\ m = 0,1,2.$$

According to the definition of the code (f,F), to the lemma and the inequalities (2) and (3) we have for $P \in \alpha(E+\delta)$

$$d^m_k(\mathbf{x}_k,\mathbf{x}^m_k) = N^{-1} \sum_{x_{k,n},x^m_{k,n}} n(x_{k,n},x^m_{k,n} \mid \mathbf{x}_k,\mathbf{x}^m_k) d^m_k(x_{k,n},x^m_{k,n}) =$$

$$= \sum_{x_{k,n},x^m_{k,n}} P(x_{k,n}) Q_P(x^m_{k,n} \mid x_{k,n}) d^m_k(x_{k,n},x^m_{k,n}) = \tag{5}$$

$$= \mathrm{E}_{P,Q_P} d^m_k(X_k,X^m_k) \le \Delta^m_k,\ k \in \mathcal{G}^m_1,\ m = 0,1,2,$$

$$d^m_k(\mathbf{x}_k,\mathbf{x}^m_k) = \mathrm{E}_{P,Q_P} d^m_k(X_k,X^m_k) \ge \Delta^m_k,\ k \in \mathcal{G}^m_2,\ m = 1,2. \tag{6}$$

We see that for the code, which has the following properties

$$M_0(N) \ge \exp\{N(I_{P,\Phi(P)}(X \wedge X^0_{0,1},X^1_{1,1},X^2_{2,1}) + 3\varepsilon)\},$$

$$M_1(N) \ge \exp\{N(I_{P,\Phi(P)}(X \wedge X^1_{1,1}) + \varepsilon)\}, \tag{7}$$

$$M_2(N) \ge \exp\{N(I_{P,\Phi(P)}(X \wedge X^1_{1,1},X^2_{2,1}) + 2\varepsilon)\}$$

for each type $P \in \alpha(E+\delta)$, the conditions (1)–(3) take place. For the case of $\mathcal{D}_2$ the proof is similar.

For the case of $\mathcal{D}_3$ according to the lemma there exist the coverings

$$\{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^m_{m,1,l_m}),\ l_m = \overline{1, K_m(P,Q_P)}, K_m(P,Q_P) = \exp\{N(I_{P,Q_P}(X \wedge X^m_{m,1}) + \varepsilon)\},\ m = 1,2$$

for $\mathcal{T}_P(X)$. Let

$$\mathcal{B}(P,Q_P,l_m) = \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^m_{m,1,l_m}) - \bigcup_{l_m'<l_m} \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^m_{m,1,l_m'}),\ l_m = \overline{1, K_m(P,Q_P)},\ m = 1,2.$$

For any $l_2 = \overline{1, K_2(P, Q_P)}$ a covering

$$\{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^2_{2,1,l_2}, \mathbf{x}^0_{0,1,l_2,l_0}),\ l_0 = \overline{1, K_0(P, Q_P)},$$

$$K_0(P, Q_P) = \exp\{N(I_{P,Q_P}(X \wedge X^0_{0,1} \mid X^2_{2,1}) + \varepsilon)\}$$

for $\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^2_{2,1,l_2})$ exists. Let for $l_0 = \overline{1, K_0(P, Q_P)}$

$$\mathcal{B}(P, Q_P, l_2, l_0) =$$

$$\mathcal{B}(P, Q_P, l_2) \cap \{\mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^2_{2,1,l_2}, \mathbf{x}^0_{0,1,l_2,l_0}) - \bigcup_{l'_0 < l_0} \mathcal{T}_{P,Q_P}(X \mid \mathbf{x}^2_{2,1,l_2}, \mathbf{x}^0_{0,1,l_2,l'_0})\}.$$

We define a code $(f, F) = (f_0, f_1, f_2, F_0, F_1, F_2)$ as follows:

$$f_0(\mathbf{x}) = \begin{cases} (l_1, l_2, l_0), & \text{when } \mathbf{x} \in \mathcal{B}(P, Q_P, l_1) \cap \mathcal{B}(P, Q_P, l_2, l_0),\ P \in \alpha(E + \delta), \\ k', & \text{when } \mathbf{x} \in \mathcal{T}_P(X),\ P \notin \alpha(E + \delta), \end{cases}$$

$$f_1(l_1, l_2, l_0) = l_1,\ f_2(l_1, l_2, l_0) = l_2,\ f_m(k') = k',\ m = 1, 2,$$

$$F_0(l_1, l_2, l_0) = \mathbf{x}^0_{0,1,l_1,l_2,l_0},\ F_1(l_1) = \mathbf{x}^1_{1,1,l_1},\ F_2(l_2) = \mathbf{x}^2_{2,1,l_2},\ F_m(k') = \overline{\mathbf{x}}^m,\ m = 0, 1, 2.$$

By analogy with the case of $\mathcal{D}_1$ we can show that the conditions (5)-(7) take place.

For the case of $\mathcal{D}_4$ the proof is similar to the case of $\mathcal{D}_3$.

Taking into account arbitrariness of ε and δ, continuity of all functions with respect to E, we obtain (4).

Now we shall prove the inclusion

$$\mathcal{R}(E, \Delta) \subseteq \mathcal{R}^+(E, \Delta). \tag{8}$$

Let $\varepsilon > 0$ be fixed and a given code (f, F) of blocklength N has (E, Δ)-achievable triplet (R_0, R_1, R_2) of rates. It is enough to show that for every type $P \in \alpha(E)$ and for some $\Phi(P) = Q_P(x^0_n, x^1_n, x^2_n \mid x_n) \in \mathcal{M}(P, E, \Delta)$, $n = \overline{1, N}$, we have

$$\frac{1}{N} \log M_0(N) + \varepsilon \geq I_{P,\Phi(P)}(X \wedge X^0_{0,1}, X^1_{1,1}, X^2_{2,1}),$$

$$\frac{1}{N} \log M_1(N) + \varepsilon \geq I_{P,\Phi(P)}(X \wedge X^1_{1,1}), \tag{9}$$

$$\frac{1}{N} \log M_2(N) + \varepsilon \geq I_{P,\Phi(P)}(X \wedge X^2_{2,1}),$$

when N is large enough.

For sufficiently large N and P from $\alpha(E - \varepsilon)$ the following inequality takes place

$$\left|\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X)\right| \geq \exp\{N(H_P(X) - \varepsilon/2)\} \tag{10}$$

(for the proof of (10) see Appendix).

To each $\mathbf{x} \in \mathcal{A}_0 \cap \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{T}_P(X)$ corresponds a unique $(\mathbf{x}^0_{0,1}, \mathbf{x}^1_{1,1}, \mathbf{x}^2_{2,1})$ such that $\mathbf{x}^0_{0,1} = F_0(f_0(\mathbf{x}))$, $\mathbf{x}^m_{m,1} = F_m(f_m(f(\mathbf{x})))$, $m = 1, 2$. These vectors determine type Q, for which

$$\mathbf{x} \in \mathcal{T}_{P,Q}(X \mid \mathbf{x}^0_{0,1}, \mathbf{x}^1_{1,1}, \mathbf{x}^2_{2,1}).$$

Since $\mathbf{x} \in \mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2$, then

$$\mathrm{E}_{P,Q} d_k^m(X_k, X_k^m) = d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) \le \Delta_k^m, \ k \in \mathcal{G}_1^m, \ m = 0, 1, 2,$$

$$\mathrm{E}_{P,Q} d_k^m(X_k, X_k^m) = d_k^m(\mathbf{x}_k, \mathbf{x}_k^m) \ge \Delta_k^m, \ k \in \mathcal{G}_2^m, \ m = 1, 2.$$

So $Q \in M(P, E, \Delta)$.

The set of all vectors $\mathbf{x} \in \mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X)$ is divided into classes corresponding to these conditional types Q. Let us select from them the class, which for given P contains the greatest number of $\mathbf{x}$. We denote corresponding conditional type Q by $Q_P = \Phi(P)$, and the class itself we denote by $(\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X))(\Phi(P))$.

Using polynomial upper estimate [5] of the number of conditional types Q we have

$$|\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X)| \le$$

$$\le (N+1)^{|\mathcal{X}| \cdot |\mathcal{X}^0| \cdot |\mathcal{X}^1| \cdot |\mathcal{X}^2|} \, |(\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X)(\Phi(P))| \le \tag{11}$$

$$\le \exp\{N\varepsilon/2\} \, |(\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X)(\Phi(P))|$$

for N large enough.

Let $\mathcal{D}_{0,1,2}$ be the set of all $(\mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1, \mathbf{x}_{2,1}^2)$, for which there exist vectors

$$\mathbf{x} \in \mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X), \quad \mathbf{x} \in \mathcal{T}_{P,\Phi(P)}(X \mid \mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1, \mathbf{x}_{2,1}^2),$$

such that $\mathbf{x}_{0,1}^0 = F_0(f_0(\mathbf{x}))$, $\mathbf{x}_{m,1}^m = F_m(f_m(f(\mathbf{x})))$, $m = 1, 2$. According to the definition of the code remark that

$$|\mathcal{D}_{0,1,2}| \le M_0(N).$$

We see that

$$|(\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X))(\Phi(P))| \le \sum_{(\mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1, \mathbf{x}_{2,1}^2) \in \mathcal{D}_{0,1,2}} \left| \mathcal{T}_{P,\Phi(P)}(X \mid \mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1, \mathbf{x}_{2,1}^2) \right| \le$$

$$\le M_0(N) \exp\{N H_{P,\Phi(P)}(X \mid X_{0,1}^0, X_{1,1}^1, X_{2,1}^2)\}. \tag{12}$$

From (11) and (12) we receive that

$$\left| \mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X) \right| \le M_0(N) \exp\{N(H_{P,\Phi(P)}(X \mid X_{0,1}^0, X_{1,1}^1, X_{2,1}^2) + \varepsilon/2)\}.$$

From the last inequality and from (10) it is not difficult to derive

$$M_0(N) \ge \exp\{N(I_{P,\Phi(P)}(X \wedge X_{0,1}^0, X_{1,1}^1, X_{2,1}^2) - \varepsilon)\}.$$

Hence

$$\frac{1}{N} \log M_0(N) \ge I_{P,\Phi(P)}(X \wedge X_{0,1}^0, X_{1,1}^1, X_{2,1}^2) - \varepsilon. \tag{13}$$

We can remark that

$$\left| \mathbf{x}_{1,1}^1, \exists \mathbf{x}_{0,1}^0, \mathbf{x}_{2,1}^2 : \ (\mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1, \mathbf{x}_{2,1}^2) \in \mathcal{D}_{0,1,2} \right| \le M_1(N),$$

$$\left| \mathbf{x}_{2,1}^2, \exists \mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1 : \ (\mathbf{x}_{0,1}^0, \mathbf{x}_{1,1}^1, \mathbf{x}_{2,1}^2) \in \mathcal{D}_{0,1,2} \right| \le M_2(N).$$

For the same $\Phi(P)$ as in (11) the following inclusions are valid

$$(\mathcal{A}_0 \cap \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{T}_P(X))(\Phi(P)) \subseteq \bigcup_{(x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \mathcal{T}_{P,\Phi(P)}(X \mid x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \equiv$$

$$\equiv \bigcup_{x^1_{1,1}, \exists x^0_{0,1}, x^2_{2,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \; \bigcup_{x^0_{0,1}, x^2_{2,1}, \exists x^1_{1,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \mathcal{T}_{P,\Phi(P)}(X \mid x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \subseteq$$

$$\subseteq \bigcup_{x^1_{1,1}, \exists x^0_{0,1}, x^2_{2,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \mathcal{T}_{P,\Phi(P)}(X \mid x^1_{1,1}), \tag{14}$$

which yields

$$|(\mathcal{A}_0 \cap \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{T}_P(X))(\Phi(P))| \leq$$

$$\leq \sum_{x^1_{1,1}, \exists x^0_{0,1}, x^2_{2,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \left| \mathcal{T}_{P,\Phi(P)}(X \mid x^1_{1,1}) \right| \leq \tag{15}$$

$$\leq M_1(N) \exp\{N H_{P,\Phi(P)}(X \mid X^1_{1,1})\}.$$

Taking into account (10) and (11) with (15) the inequality

$$M_1(N) \geq \exp\{N(I_{P,\Phi(P)}(X \wedge X^1_{1,1}) - \varepsilon)\}$$

holds. Therefore

$$\frac{1}{N} \log M_1(N) \geq I_{P,\Phi(P)}(X \wedge X^1_{1,1}) - \varepsilon. \tag{16}$$

For the same $\Phi(P)$ as in (11) similarly to (14) and (15) we obtain that

$$(\mathcal{A}_0 \cap \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{T}_P(X))(\Phi(P)) \subseteq$$

$$\subseteq \bigcup_{(x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \mathcal{T}_{P,\Phi(P)}(X \mid x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \equiv$$

$$\equiv \bigcup_{x^2_{2,1}, \exists x^0_{0,1}, x^1_{1,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \; \bigcup_{x^0_{0,1}, x^1_{1,1}, \exists x^2_{2,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \mathcal{T}_{P,\Phi(P)}(X \mid x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \subseteq$$

$$\subseteq \bigcup_{x^2_{2,1}, \exists x^0_{0,1}, x^1_{1,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \mathcal{T}_{P,\Phi(P)}(X \mid x^2_{2,1}),$$

therefore

$$|(\mathcal{A}_0 \cap \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{T}_P(X))(\Phi(P))| \leq$$

$$\leq \sum_{x^2_{2,1}, \exists x^0_{0,1}, x^1_{1,1} : (x^0_{0,1}, x^1_{1,1}, x^2_{2,1}) \in \mathcal{D}_{0,1,2}} \left| \mathcal{T}_{P,\Phi(P)}(X \mid x^2_{2,1}) \right| \leq$$

$$\leq M_2(N) \exp\{N H_{P,\Phi(P)}(X \mid X^2_{2,1})\}.$$

From (10) and (11) we have

$$M_2(N) \geq \exp\{N(I_{P,\Phi(P)}(X \wedge X^2_{2,1}) - \varepsilon)\},$$

hence

$$\frac{1}{N} \log M_2(N) \geq I_{P,\Phi(P)}(X \wedge X^2_{2,1}) - \varepsilon. \tag{17}$$

Since the inequalities (13), (16), (17) we can assert for each type P from $\alpha(E-\varepsilon)$ with certainly choosen $\Phi(P)$ (by the way discussed above), then taking into account arbitrariness of ε and continuity by E of all used above functions, we complete the proof of (9), hence of (8) too.

Appendix

Proof of Lemma: The first part of the assertion is proved in [9]. Using the method of random selection, by similarity with the proof of Lemma 4.1 [sec. 2, [5]], we show the existence of a covering for $\mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}), l_1 \in \{1,...,L_1(P,Q)\}$ with $L_1(P,Q)$ of elements. Let l_1 be fixed and $\{\zeta_{l_2}, l_2 = \overline{1, L_2(P,Q)}\}$ be a collection of Rv independent and identically distributed on $\mathcal{T}_{P,Q}(X^2_{2,1} \mid \mathbf{x}^1_{1,1,l_1})$. Denote by $\psi(\mathbf{x})$ the characteristic function of the complement of random set $\bigcup_{l_2=1}^{L_2(P,Q)} \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \zeta_{l_2})$:

$$\psi(\mathbf{x}) = \begin{cases} 1, & \text{if } \mathbf{x} \notin \bigcup_{l_2=1}^{L_2(P,Q)} \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \zeta_{l_2}), \\ 0, & \text{otherwise.} \end{cases}$$

It is necessary to show that for N sufficiently large

$$\Pr\left\{ \sum_{\mathbf{x} \in \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1})} \psi(\mathbf{x}) < 1 \right\} > 0,$$

since it is equivalent to the existence of the required covering. We have

$$\Pr\left\{ \sum_{\mathbf{x} \in \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1})} \psi(\mathbf{x}) \geq 1 \right\} \leq$$

$$\leq \left| \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}) \right| \Pr\left\{ \mathbf{x} \notin \bigcup_{l_2=1}^{L_2(P,Q)} \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \zeta_{l_2}) \right\}.$$

Taking into account the independence of Rv $\zeta_{l_2}, l_2 = \overline{1, L_2(P,Q)}$ and the polynomial estimate for numbers of conditional types [5] we have for N large enough

$$\Pr\left\{ \mathbf{x} \notin \bigcup_{l_2=1}^{L_2(P,Q)} \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \zeta_{l_2}) \right\} \leq$$

$$\leq \left(1 - \left| \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}, \mathbf{x}^2_{2,1,l_1,l_2}) \right| \left| \mathcal{T}_{P,Q}(X \mid \mathbf{x}^1_{1,1,l_1}) \right|^{-1} \right)^{L_2(P,Q)} \leq$$

$$\leq (1 - \exp\{NH_{P,Q}(X \mid X^1_{1,1}, X^2_{2,1}) -$$

$$- |\mathcal{X}||\mathcal{X}^1||\mathcal{X}^2| \log(N+1) - NH_{P,Q}(X \mid X^1_{1,1})\})^{L_2(P,Q)} \leq$$

$$\leq (1 - \exp\{-N(I_{P,Q}(X \wedge X^2_{2,1} \mid X^1_{1,1}) + \frac{\varepsilon}{2})\})^{L_2(P,Q)},$$

where $\varepsilon \geq N^{-1}|\mathcal{X}||\mathcal{X}^1||\mathcal{X}^2|\log(N+1)$. Applying the inequality $(1-t)^s \leq \exp\{-st\}$ (which holds for each $0 < t < 1$ and s) with

$$t = \exp\{-N(I_{P,Q}(X \wedge X^2_{2,1} \mid X^1_{1,1}) + \frac{\varepsilon}{2})\},$$

and $s = L_2(P,Q)$, we continue the estimation

$$\Pr\left\{\sum_{x \in \mathcal{T}_{P,Q}(X|x^1_{1,1,l_1})} \psi(x) \geq 1\right\} \leq$$

$$\leq \exp\{NH_{P,Q}(X \mid X^1_{1,1})\} \exp\{-L_2(P,Q) \exp\{-N(I_{P,Q}(X \wedge X^2_{2,1} \mid X^1_{1,1}) + \frac{\varepsilon}{2})\}\} =$$

$$= \exp\{NH_{P,Q}(X \mid X^1_{1,1}) - \exp\{N\frac{\varepsilon}{2}\}\},$$

and when N is large enough, then

$$\Pr\left\{\sum_{x \in \mathcal{T}_{P,Q}(X|x^1_{1,1,l_1})} \psi(x) \geq 1\right\} < 1.$$

For $l_1 = \overline{1, L_1(P,Q)}$, $l_2 = \overline{1, L_2(P,Q)}$ the existence of the covering

$$\{\mathcal{T}_{P,Q}(X \mid x^1_{1,1,l_1}, x^2_{2,1,l_1,l_2}, x^0_{0,1,l_1,l_2,l_0}),\ l_0 = \overline{1, L_0(P,Q)}\}$$

for $\mathcal{T}_{P,Q}(X \mid x^1_{1,1,l_1}, x^2_{2,1,l_1,l_2})$ may be demonstrated similarly.

Proof of the inequality (10): It is clear that

$$\left|\mathcal{A}_0 \bigcap \mathcal{A}_1 \bigcap \mathcal{A}_2 \bigcap \mathcal{T}_P(X)\right| = |\mathcal{T}_P(X)| - \left|\overline{\mathcal{A}_0} \bigcup \overline{\mathcal{A}_1} \bigcup \overline{\mathcal{A}_2} \bigcap \mathcal{T}_P(X)\right|.$$

For $P \in \alpha(E-\varepsilon)$ we have

$$\left|\overline{\mathcal{A}_0} \cup \overline{\mathcal{A}_1} \cup \overline{\mathcal{A}_2} \cap \mathcal{T}_P(X)\right| \leq \frac{P^{*N}(\overline{\mathcal{A}_0} \cup \overline{\mathcal{A}_1} \cup \overline{\mathcal{A}_2} \cap \mathcal{T}_P(X))}{P^{*N}(x)} \leq$$

$$\leq 3\exp(-NE)\exp\{N(H_P(X) + D(P \parallel P^*))\} \leq$$

$$\leq \exp\{N(H_P(X) - \varepsilon + \frac{\log 3}{N})\} \leq \exp\{N(H_P(X) - \varepsilon/2\}$$

for N large enough.

Then using the polynomial inner estimate [5] of the number of types P for N large enough we obtain that

$$|\mathcal{A}_0 \cap \mathcal{A}_1 \cap \mathcal{A}_2 \cap \mathcal{T}_P(X)| \geq (N+1)^{-|\mathcal{X}|}\exp\{NH_P(X)\} - \exp\{N(H_P(X) - \varepsilon/2)\} =$$

$$= \exp\{N(H_P(X) - \varepsilon/2)\}\left(\frac{\exp\{N\varepsilon/2\}}{(N+1)^{|\mathcal{X}|}} - 1\right) \geq \exp\{N(H_P(X) - \varepsilon/2)\}.$$

References

[1] R. Ahlswede, "Coloring hypergraphs. A new approach to multi-user source coding", I, II, *J. Combin. Inform. and Syst. Sci.*, vol. 4, no. 1, pp. 75-115, 1979; vol. 5, no. 2, pp. 220-268, 1980.

[2] R. Ahlswede, "The rate-distortion region for multiple descriptions without excess rate", *IEEE Trans. Inform. Theory*, vol. IT-31, no. 6, pp. 721-726, 1985.

[3] T. Berger and Z. Zhang, "New results in binary multiple descriptions", *IEEE Trans. Inform. Theory*, vol. 33, no. 4, pp. 502-521, 1987.

[4] T. Berger and Z. Zhang, "Multiple description source coding with no excess marginal rate", *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 349-357, 1995.

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

[6] T. M. Cover and J. A. Thomas, Elements of Information Theory, New York: Wiley, 1991.

[7] A. El Gamal and T. M. Cover, "Achievable rates for multiple descriptions", *IEEE Trans. Inform. Theory*, vol. IT-28, no. 6, pp. 851-857, 1982.

[8] A. R. Ghazaryan, "Multiterminal sources optimal coding rates depending on levels of reliability, distortion and secrecy", Candidate of Science thesis (in Russian), Institute for Informatics and Automation Problems of the NAS of RA and of the YSU, 1999.

[9] E. A. Haroutunian and R. Sh. Maroutian, "(E, Δ)-achievable rates for multiple descriptions of random varying source", *Problems of Control and Inform. Theory*, vol. 20, no. 2, pp. 165-178, 1991.

[10] A. N. Haroutunian and E. A. Haroutunian, "An achievable rates-reliabilities-distortions dependence for source coding with three descriptions", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA and of the Yerevan State University, Mathematical problems of computer science*, vol. 17, pp. 70-75, 1997.

[11] A. N. Harutyunyan, "Investigation of achievable interdependence between coding rates and reliability for several classes of sources", Candidate of Science thesis (in Russian), Institute for Informatics and Automation Problems of the NAS of RA and of the YSU, 1997.

[12] E. A. Haroutunian and A. R. Kazarian, "On cascade system coding rates with respect to distortion criteria and reliability", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA and of the Yerevan State University, Mathematical problems of computer science*, vol. 18, pp. 19-32, 1997.

[13] E. A. Haroutunian, A. N. Haroutunian and A. R. Kazarian, "On rate-reliabilities-distortions function of source with many receivers", *Proceedings of the 13-th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes*, vol. 1, pp. 217-220, 1998.

[14] E. A. Haroutunian, A. N. Haroutunian, A. R. Kazarian, "Rate-reliabilities-distortions dependence for source coding with many receivers", *Transactions of the Institute for Informatics and Automation Problems of the NAS of RA and of YSU, Mathematical Problems of Computer Science*, vol. 20, pp. 98-110, 1998.

[15] E. A. Haroutunian, A. N. Harutyunyan, A. R. Kazarian, and E. C. van der Meulen, "On branching system coding rates with respect to reliability, distortion and secrecy criteria", *Proceedings of 1999 International Conference on Computer Science and Information Technologies (CSIT 99)*, pp. 131-134, 1999.

[16] E. C. van der Meulen, E. A. Haroutunian, A. N. Harutyunyan, A. R. Kazarian, "On the Rates-reliability-distortions and partial secrecy region of a one-stage branching communication system", *Proceedings of the 2000 International Simposium on Information Theory (ISIT 2000)*, p. 211, 2000.

[17] H. Yamamoto, "Source coding theory for cascade and branching communication systems", *IEEE Trans. Inform. Theory*, vol. IT-27, no. 3, pp. 299-308, 1981.

[18] H.Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers", *IEEE Trans. Inform. Theory*, vol. IT-29, no. 6, pp. 918-923, 1983.

[19] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered", *IEEE Trans. Inform. Theory*, vol. IT-34, No. 4, pp. 835-842, 1988.

[20] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system", *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 827-835, 1997.

[21] R. Sh. Maroutian, "Achievable rates for multiple descriptions with given exponent and distortion levels" (in Russian), *Problems of Inform. Transm.*, vol. 26, no. 1, pp. 83-89, 1990.