ON RELIABILITY FUNCTION OF BSC: EXPANDING THE REGION, WHERE IT IS KNOWN EXACTLY

The region of rates (“straight-line”), where the BSC reliability function is known exactly, is expanded.

§ 1. Introduction and main results

In the paper notation from [11] is used. A binary symmetric channel (BSC) with crossover probability \(0 < p < 1/2\) and \(q = 1 - p\) is considered. Let \(F^n\) denote the set of all \(2^n\) binary \(n\)-tuples, and \(d(x, y), x, y \in F^n\) denote the Hamming distance between \(x\) and \(y\). A subset \(C = C(M, n) = \{x_1, \ldots, x_M\} \subseteq F^n\) is called a code of length \(n\) and cardinality \(M\). The minimum distance of the code \(C\) is \(d(C) = \min\{d(x_i, x_j) : i \neq j\}\). Code rate is \(R(C) = \frac{n - 1}{\log_2 M}\). Everywhere below \(\log z = \log_2 z\).

Cardinality of a set \(A\) is denoted by \(|A|\). Code spectrum (distance distribution) \(B(C) = (B_0, B_1, \ldots, B_n)\) is the \((n + 1)\)-tuple with components

\[
B_i = |C|^{-1} |\{(x, y) : x, y \in C, d(x, y) = i\}|, \quad i = 0, 1, \ldots, n.
\]

(1)

In other words, \(B_i\) is average number of codewords \(y\) on the distance \(i\) from the codeword \(x\). Clearly, \(B_0 + \ldots + B_n = |C|\). The total number of ordered codepairs \(x, y \in C\) with \(d(x, y) = i\) equals \(|C|B_i\).

The BSC reliability function \(E(R, p)\) is defined as follows [2, 3, 4]

\[
E(R, p) = \limsup_{n \to \infty} \frac{1}{n} \ln \frac{1}{P_e(R, n, p)},
\]

where \(P_e(R, n, p)\) – the minimal possible decoding error probability \(P_e\) for \((n, R)\)-code.

Introduce the function [3]

\[
G(\alpha, \tau) = 2 \alpha \frac{(1 - \alpha) - \tau(1 - \tau)}{1 + 2 \sqrt{\tau(1 - \tau)}} = \frac{1}{2} \sqrt{\tau(1 - \tau)} - \frac{(1 - 2\alpha)^2}{2 \left[ 1 + 2 \sqrt{\tau(1 - \tau)} \right]}
\]

(2)

and define the function \(\delta_{GV}(R) \leq 1/2\) (Gilbert-Varshamov bound) as

\[
1 - R = h_2(\delta_{GV}(R)), \quad 0 \leq R \leq 1,
\]

(3)

\footnote{Supported in part by the Russian Foundation for Basic Research (project nos. 15-01-08051) and by Russian Scientific Foundation (project nos. 13-01-12458 о_м2).}
where \( h_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \).

Define the value \( R = R(\alpha, \tau) \) by the formula

\[
R = 1 - h_2(\alpha) + h_2(\tau), \quad 0 \leq \tau \leq \alpha \leq 1/2. \tag{4}
\]

For \( R \in (0, 1) \) and \( \alpha \in [\delta_{GV}(R), 1/2] \) introduce also values

\[
\tau_R(\alpha) = h_2^{-1}(h_2(\alpha) - 1 + R) \leq \alpha,
\]

\[
\omega_R(\alpha) = G(\alpha, \tau_R(\alpha)) \tag{5}
\]

and

\[
\omega_R = \min_{\delta_{GV}(R) \leq \alpha \leq 1/2} \omega_R(\alpha) = \min\{G(\alpha, \tau) : h_2(\alpha) - h_2(\tau) = 1 - R\}. \tag{6}
\]

The best known upperbound for the maximal relative code distance \( \delta(R) \) (linear programming bound) has the form \([5, 6]\)

\[
\delta(R) \leq \delta_{LP}(R) = \omega_R. \tag{7}
\]

If \( R \leq R_0 \approx 0.30524 \) (\( R_0 \) is defined in \([28]\) and \([29]\)), then minimum in the right-hand side of \([6]\) is attained for \( \alpha = 1/2 \), and the formula \([7]\) takes simple form \([5, 6]\)

\[
\delta_{LP}(R) = \omega_R = \frac{1}{2} - \sqrt{\tau(1 - \tau)}, \quad R = h_2(\tau). \tag{8}
\]

Denote by \( \alpha_R, \tau_R \) optimal values of parameters \( \alpha, \tau \) in \([6]\), i.e.

\[
\omega_R = \omega_R(\alpha_R) = G(\alpha_R, \tau_R). \tag{9}
\]

The function \( \omega_R \) decreases monotonically for \( R \in (0, 1) \), and the function \( \alpha_R \) does not increases in \( R \).

Introduce critical rates \( R_{\text{crit}}(p), R_1(p) \) and \( R_2(p) \), beginning with well-known

\[
R_{\text{crit}}(p) = 1 - h_2 \left( \frac{\sqrt{p}}{\sqrt{p} + \sqrt{q}} \right). \tag{10}
\]

The rate \( R_1(p) \) was introduced in \([11, \text{ формулы (6)}]\)

\[
R_1(p) = h_2(\tau_1(p)), \quad \tau_1(p) = \frac{(1 - (4pq)^{1/4})^2}{2(1 + \sqrt{4pq})} \leq \frac{1}{2}. \tag{11}
\]

Introduce the important value

\[
\omega_1(p) = \frac{2\sqrt{pq}}{1 + 2\sqrt{pq}} = G(1/2, \tau_1(p)), \quad 0 \leq p \leq 1/2. \tag{12}
\]

Note that the value \( \omega_1(p) \) is defined by the condition \( t_1(\omega) = t_2(\omega, p) \) (см. \([5, 8]\)).
Introduce the critical rate $R_2 = R_2(p)$ by the formula
\[
\omega_{R_2} = \omega_1(p) = \frac{2\sqrt{pq}}{1 + 2\sqrt{pq}}, \quad 0 < p < 1/2,
\]
(13)

or, equivalently,
\[
R_2(p) = 1 - \max_{\alpha, \tau} \{ h_2(\alpha) - h_2(\tau) : G(\alpha, \tau) = \omega_1(p) \}.
\]
(14)

In other words, $R_2(p)$ is the minimal rate for which it is possible to have $G(\alpha, \tau) = \omega_1(p)$. On the contrary, $R_1(p)$ is the maximal such rate (it corresponds to $\alpha = 1/2$). Functions $R = R_2(p)$ and $R = R_1(p)$ decreases monotonically in $p \in [0, 1/2]$.

Introduce the value $p_0 \approx 0.036587$ as the unique root of the equation $R_2(p) = R_1(p)$. If $p < p_0$, then in the optimizing value $\alpha < 1/2$. If $p \geq p_0$, then the optimizing value $\alpha = 1/2$ and $R_2(p) = R_1(p)$. We also have $R_2(0) = R_1(0) = 1$ and $R_2(p_0) = R_1(p_0) = R_0 \approx 0.30524$, where $R_0$ is defined in (28)–(29).

Introduce also the value $p_1 \approx 0.0078176$ as the unique root of the equation $R_1(p) = R_{\text{crit}}(p)$. Then we have
\[
\begin{align*}
R_2(p) &< R_{\text{crit}}(p), \quad 0 < p < 1/2; \\
R_0 &< R_2(p) < R_1(p), \quad p < p_0; \\
R_2(p) &< R_1(p) < R_0, \quad p > p_0; \\
R_1(p) &< R_{\text{crit}}(p), \quad p > p_1; \\
R_1(p) &> R_{\text{crit}}(p), \quad p < p_1; \\
R_{\text{crit}}(p) &\leq R_0, \quad p \geq 0.05014.
\end{align*}
\]
(15)

In Fig. 1 plots of functions $R_1(p)$, $R_2(p)$, $R_{\text{crit}}(p)$ and $C(p)$ are shown.

Remark 1. Although notations $\omega_R(\alpha)$ and $\omega_1(p)$ (also $\tau_R(\alpha)$ and $\tau_1(p)$) are not well consistent, it should not imply any problems (for example, we always have $R < 1$).

In the region $R_{\text{crit}}(p) \leq R \leq C(p) = 1 - h_2(p)$ the function $E(R, p)$ is known since a long time ago \cite{2} and it coincides with the sphere-packing bound
\[
E(R, p) = E_{\text{sp}}(R, p), \quad R_{\text{crit}}(p) \leq R \leq C(p),
\]
(16)

where
\[
E_{\text{sp}}(R, p) = D(\delta_{\text{GV}}(R)\|p)), \quad D(x\|y) = x \log \frac{x}{y} + (1 - x) \log \frac{1 - x}{1 - y},
\]
\[
E_{\text{sp}}(0, p) = \frac{1}{2} \log \frac{1}{4pq} = 2E(0, p).
\]
(17)

The main result of the paper is

Theorem 1.1) For any $0 < p < 1/2$ the inequality holds
\[
E(R, p) = 1 - \log_2 (1 + 2\sqrt{pq}) - R, \quad R_2(p) \leq R \leq R_{\text{crit}}(p),
\]
(18)

where $R_2(p), R_{\text{crit}}(p)$ are defined in (13) and (10), respectively.
2) For any $0 < p < 1/2$ and $0 \leq R \leq \min \{ R_0, R_2(p) \}$ the bound is valid

\[ E(R, p) \leq \frac{\omega_R}{2} \log \frac{1}{4pq} - \mu(R, 1/2, \omega_R) = \frac{\omega_R}{2} \log \frac{1}{4pq} - h_2(\tau) - h(\omega_R) + 1, \]

\[ \omega_R = \frac{1}{2} - \sqrt{\tau(1 - \tau)}, \quad R = h_2(\tau), \]

where $\omega_R$ and $\mu(R, 1/2, \omega)$ are defined in (6) and (33), respectively.

3) If $p < p_0 \approx 0.036587$, then $R_0 < R_2(p)$ and for $R_0 \leq R \leq R_2(p)$ the bound holds

\[ E(R, p) \leq 1 + \min_{0 \leq \alpha \leq 1/2} \left\{ \frac{G(\alpha, \tau)}{2} \log \frac{1}{4pq} - L(G(\alpha, \tau)) \right\} - R \leq \]

\[ \leq 1 - R + \frac{\omega_R}{2} \log \frac{1}{4pq} - L(\omega_R), \]

where $t_1(\omega)$ is defined in (38).

\[ L(\omega) = 2h_2(t_1(\omega)) - \omega - (1 - \omega)h_2 \left[ \frac{2t_1(\omega) - \omega}{2(1 - \omega)} \right]. \] (21)

In other words, for any $0 < p < 1/2$ the function $E(R, p)$ is linear for $R_2(p) \leq R \leq R_{\text{crit}}(p)$. Earlier it was known only for $R_1(p) \leq R \leq R_{\text{crit}}(p)$, if $p$ is not too small [7]. Recall that $R_2(p) < R_1(p)$, $p < p_0$, and $R_2(p) = R_1(p)$, $p \geq p_0$. Also $R_2(p) \leq \min \{ R_1(p), R_{\text{crit}}(p) \}$, $0 < p < 1/2$ (see also [15]).

Notice also that improvement in the formula (18) with respect to [1] is attained due to using the values $\alpha < 1/2$ (in [1] only $\alpha = 1/2$ was used).

Inequalities (19)–(20) strengthen similar estimate form [1, теорема 1].

For comparison purpose, the best know lowerbound for $E(R, p)$ has the form [4]

\[ E(R, p) \geq -\delta_{GV}(R) \log (2\sqrt{pq}), \quad 0 \leq R \leq R_{\text{min}}(p), \] (22)

and

\[ E(R, p) \geq 1 - \log_2 (1 + 2\sqrt{pq}) - R, \quad R_{\text{min}}(p) \leq R \leq R_{\text{crit}}(p), \] (23)

where $\delta_{GV}(R)$ is defined in [4],

\[ R_{\text{min}}(p) = 1 - h_2 \left( \frac{2\sqrt{pq}}{1 + 2\sqrt{pq}} \right), \] (24)

and $R_{\text{min}}(p) < R_2(p) < R_{\text{crit}}(p)$, $0 < p < 1/2$.

Denote by $E_{\text{up}}(R, p)$ the right-hand sides of formulas (18)–(20), and by $E_{\text{low}}(R, p)$ the right-hand sides of formulas (22)–(23). Then for all $R, p$ we have

\[ E_{\text{low}}(R, p) \leq E(R, p) \leq E_{\text{up}}(R, p). \]

In Fig. 2 plots of functions $E_{\text{low}}(R, p)$ and $E_{\text{up}}(R, p)$ for $p = 0.01$ are shown. In that case $R_{\text{crit}} \approx 0.5591$, $R_1 \approx 0.5518$, $R_2 \approx 0.5370$, $R_{\text{min}} \approx 0.3516$, $C \approx 0.9192$. 

4
Notice that $E_{up}(R, p) - E_{low}(R, p) > 0$ for $R < R_2(p)$ and all $p$.

Upper bounds (19) and (20) have simple meaning: we should apply the union bound using the best known upperbound (7) for the value $\delta(R)$ and the best known lowerbound (26) for the number of code neighbors.

When proving Theorem 1 we will need the function [9]:

$$
\mu(R, \alpha, \omega) = h_2(\alpha) - 2 \int_0^{\omega/2} \log \frac{P + \sqrt{P^2 - 4Qy^2}}{Q} dy - (1 - \omega)h_2\left(\frac{\alpha - \omega/2}{1 - \omega}\right),
$$

(25)

where $\tau \leq 1/2$ such that $h_2(\tau) = h_2(\alpha) - 1 + R$.

Importance of the function $\mu(R, \alpha, \omega)$ and its relation to the code spectrum $\{B_i\}$ (see (11)) is described by the following variant [9, Theorem 5] (see also proof in [11]).

**Theorem 2.** For any $(R, n)$-code and any $\alpha \in [\delta_{GV}(R), 1/2]$ there exists $\omega, 0 \leq \omega \leq G(\alpha, \tau)$, where $h_2(\tau) = h_2(\alpha) - 1 + R$ and $G(\alpha, \tau)$ is defined in (2), such that

$$
\frac{1}{n} \log B_{\omega n} \geq \mu(R, \alpha, \omega) + o(1), \quad n \to \infty,
$$

(26)

where $\mu(R, \alpha, \omega) > 0$ is defined in (25) and for $\mu(R, \alpha, \omega)$ the nonintegral representation (82) holds.

It should be noted that the parameter $\alpha$ determines a constant weight on code, which replaces the original code (using Elias-Bassalygo lemma) [5, 9, 1].

For $0 \leq R \leq R_0$ the best in Theorem 2 is $\alpha = 1/2$ [8, Remark 4], since such $\alpha$ simultaneously minimizes $G(\alpha, \tau)$ and maximizes $\mu(R, \alpha, \omega)$ for all $\omega$. For $R > R_0$, probably, the optimal is $\alpha = \alpha_R$ (see [9]), i.e. minimization of $G(\alpha, \tau)$ over $\alpha < 1/2$ (at least, the value $G(\alpha, \tau)$ is in the estimate (20)). With $\alpha = \alpha_R$ we get from Theorem 2

**Corollary 1.** For any $(R, n)$-code there exists $\omega, 0 \leq \omega \leq \omega_R$ such that

$$
\frac{1}{n} \log B_{\omega n} \geq \mu(R, \alpha_R, \omega) + o(1), \quad n \to \infty,
$$

(27)

where $\omega_R$ and $\alpha_R$ are defined in (3) and (9), respectively.

**Remark 2.** Theorem 1 is based on the important feature of inequalities (26) and (27). Till 1999 the best upperbound for $E(R, p)$ followed from the best upperbound (7) for the maximal relative code distance $\delta(R) \leq \omega_R$ [5]. From that point of view inequalities (26)–(27) do not improve the estimate (7), but it follows from them that $\mu(R, \alpha_R, \omega_R) > 0$. In other words, there are an exponential number of codewords on the minimal (or smaller) code distance $\omega_R n$. That “correction” on $\mu(R, \alpha_R, \omega_R)$ in inequalities (19)–(20), essentially, constitutes Theorem 1. Notice also that the randomly chosen (“typical”) code has the spectrum $n^{-1} \log B_{\omega n} \approx h_2(\omega) - h_2(\delta_{GV}(R)), \omega \geq \delta_{GV}(R)$. It is possible to check
that for such code the maximal contribution (additive) to the decoding error probability $P_e$ is given by “neighbors” on the distance $\omega_1(p)n$ (see \cite{23}), from which the inequality \cite{24} follows for all $R, p$.

Introduce the value $R_0$ by the formula \cite{6,8}

$$R_0 = h_2(\tau_0) \approx 0, 30524,$$  \hspace{1cm} (28)

where $\tau_0 \approx 0, 054507$ – the unique root of the equation

$$(1 - 2\tau) \left[ 1 + \frac{1}{2\sqrt{\tau(1 - \tau)}} \right] - \ln \frac{1 - \tau}{\tau} = 0.$$  \hspace{1cm} (29)

For fixed $R$ we have

$$\frac{dG}{d\alpha} = \frac{2(1 - 2\alpha)}{1 + 2\sqrt{\tau(1 - \tau)}} - \frac{(1 - 2\tau)}{2\sqrt{\tau(1 - \tau)}} \left[ 1 - \frac{(1 - 2\alpha)^2}{2 \sqrt{\tau(1 - \tau)}} \right] \ln[(1 - \alpha)/\alpha] \ln[(1 - \tau)/\tau]$$  \hspace{1cm} (30)

For any $R$ and $0 < \omega < G(\alpha, \tau)$ we also have \cite{8} Proposition 1]

$$\mu'_\alpha(R, \alpha, \omega) > 0, \quad \delta_{GV}(R) \leq \alpha < 1/2.$$  

For $R \leq R_0$ the function $G(\alpha, \tau_R(\alpha))$ monotonically decreases in $\alpha \in [\delta_{GV}(R), 1/2]$ and $\alpha_R = 1/2$. If $R \in (R_0, 1)$ then values $0 < \tau_R < \alpha_R < 1/2$ are uniquely defined by the system of equations

$$\frac{dG}{d\alpha} = 0,$$  \hspace{1cm} (31)

$$h_2(\alpha) - h_2(\tau) = 1 - R.$$  \hspace{1cm} (32)

Also

$$\tau_R = \frac{1}{2} \left\{ 1 - \sqrt{1 - \left[ \sqrt{(1 - \omega_R)^2 - (1 - 2\alpha)^2} - \omega_R \right]^2} \right\}.$$  

For $\alpha \in (0, 1/2)$ denote by $\tau(\alpha)$ the unique root of the equation \cite{31}, such that $\tau(\alpha) < \alpha$. Denote also $R(\alpha) = 1 - h_2(\alpha) + h_2(\tau(\alpha))$, $\alpha \in (0, 1/2)$.

The function $\tau(\alpha)$ monotonically increases, and $R(\alpha)$ monotonically decreases on $\alpha$. Each $\alpha \in (0, 1/2)$ defines $R(\alpha) > R_0$ and $\tau(\alpha) < \alpha$. Similarly, each $R > R_0$ uniquely defines $\alpha < 1/2$ and $\tau(\alpha) < \alpha$. Note that

$$\lim_{\alpha \downarrow 1/2} \tau(\alpha) = \tau_0 \approx 0, 0545, \quad \lim_{\alpha \downarrow 1/2} R(\alpha) = R_0 \approx 0, 3055, \quad \lim_{\alpha \downarrow 1/2} p(\alpha) = p_0 \approx 0, 036587.$$  

For calculation purpose it is convenient first to set the parameter $\alpha \in (0, 1/2)$, and then find sequentially corresponding values $\tau(\alpha), R(\alpha)$ from \cite{31, 32} and $\omega(\alpha) = G(\alpha, \tau(\alpha))$. For $p = p(\alpha)$ (from \cite{13}) we have $R_2(p) = R(\alpha)$ and

$$p(\alpha) = \frac{1 - G - \sqrt{1 - 2G}}{2(1 - G)}, \quad G = G(\alpha, \tau(\alpha)).$$
In particular, for $\alpha \to 0$ we have

$$\tau \approx \alpha^2, \quad G(\alpha, \tau(\alpha)) \approx \alpha, \quad p(\alpha) \approx \frac{\alpha^2}{4}, \quad C(p(\alpha)) \approx 1 - \frac{\alpha^2}{2} \log \frac{1}{\alpha},$$

$$R_2(p(\alpha)) \approx 1 - \alpha \log \frac{1}{\alpha}, \quad R_{\text{crit}}(p(\alpha)) \approx 1 - \frac{\alpha}{2} \log \frac{1}{\alpha}.$$ 

Notice that due to Theorem 2 for a chosen $\alpha$ there exists $\omega$ such that $n^{-1} \log B_{\omega n} \geq \mu(R, \alpha, \omega) + o(1)$. In other words, the number of neighbors on the distance $\omega n$ for each codeword $x_i$ satisfies in average that lower bound. In fact, that property holds not only in average, but also for every codeword $x_i$ from an “essential” part of all $M$ codewords (i.e. for $Me^{o(n)}$, $n \to \infty$ codewords). That fact, established by the “cleaning procedure”, regularly was used in the papers [10, 8, 1] (and earlier) and will be also used in the proof of Theorem 1.

Remark 3. In the author’s paper [1] there are the following inaccuracies:

3a) There is a miscalculation in the formula (15) [1] for the function $\mu(R, 1/2, \omega)$, coming from the earlier paper [8, formula (23)]. The correct version of that formula is [8, формула (23)]. Правильный вид этой формулы

$$\mu(R, 1/2, \omega) = -2(1 - \omega) \log(1 - \omega) - \log \tau - 2(1 - \tau) \log(1 - \tau) + (1 - 2\tau) \log(\tau - \omega + g) + \log[1 - \omega - (1 - 2\tau)g] - 2\omega \log g - 2, \quad (33)$$

where

$$\tau = \tau(R) = h_2^{-1}(R), \quad g = g(\tau, \omega) = \frac{1 - 2\tau + \sqrt{(1 - 2\tau)^2 - 4\omega(1 - \omega)}}{2}.$$

From (33) the useful formula, which has already appeared in [1, formula (16)], follows

$$\mu(h_2(\tau), 1/2, G(1/2, \tau)) = h_2(\tau) + h_2(G(1/2, \tau)) - 1, \quad \tau \geq 0. \quad (34)$$

Due to importance of the formula (34), in Appendix its derivation is presented. In §4 the explicit (non-integral) representation for the function $\mu(R, \alpha, \omega)$ is obtained, from which the formula (33) can be received as well. There also the generalization of the formula (34) for arbitrary $\alpha$ is obtained (see (75)).

2b) There is the following inaccuracy in the formulation of Theorem 1 [1]: the function $W(\omega, \alpha, R, p)$ was defined, using the value $t_2(\omega, p)$ (for all $\omega$). In fact, the proof of Theorem 1 in [1] was performed using the right function $t(\omega, p)$ (and for that purpose the function $t(\omega, p)$ was introduced in [1] formula (29))). Due to the author’s fault, the definition [1, formula (9)]) (coming from the earlier paper [8]) remained in [1] §1. Those changes do not influence validity of the corollary 1 [1].

2c) There is an inaccuracy in the proof of the Theorem 1 (noted by Litsyn S., for which the author is grateful to him): the “cleaning” procedure in [1] §4 was performed in such a way that formally [1, formula (44)] does not yet follow from [1] formula
The same drawback remained in [14] as well. In §2 below we fix that inaccuracy, and, moreover, simplify the proof.

2d) The main difference of the paper with respect to [8] is that here it turned out possible to investigate the case $\alpha < 1/2$. An important role was played by the relation (75). Also some proof details were simplified.

In §2 connection between $P_e$ and a code spectrum is investigated. In §3 the proof of Theorem 1 is given. In §4 the non-integral representation for $\mu(R, \alpha, \omega)$ is derived. That representation is used in the proof of Theorem 1 in §3. Some calculations and proofs are presented in Appendix.

§ 2. Lower bound for $P_e$ and code spectrum

For $x_i \in C$ denote $d_i(y) = d(x_i, y)$ and for any integer $tn$, $t \in (0, 1)$, introduce the set

$$X_t(y) = \{ x_i \in C : d_i(y) = tn \} = (C + y)^{(tn)}, \quad y \in F^n.$$

Also for any integer $tn$, $t \in (0, 1)$ and each pair of codewords $x_i \neq x_j$ in the output space $F^n$ of the channel introduce the "ambiguity" set:

$$Y_{ij}(t) = Y_{ji}(t) = \{ y : d_i(y) = d_j(y) = tn \}$$

and for $i = 1, \ldots, M$ the set

$$Y_i(t) = \bigcup_{j \neq i} Y_{ij}(t) = \{ y : \text{there exists } x_j \neq x_i, \text{ such that } d_i(y) = d_j(y) = tn \}.$$

Next result is a variant of [1, Proposition 2, formulas (20), (21)] (see also [8, лемма 2]).

Lemma 1. For error probability $P_e$ the lower bound holds ($t = m/n$)

$$P_e \geq \frac{q^n}{2M} \sum_{m=1}^{n} \binom{p}{q}^m \sum_{y : |X_t(y)| \geq 2} |X_t(y)| = \frac{q^n}{2M} \sum_{m=1}^{n} \binom{p}{q}^m \sum_{i=1}^{M} |Y_i(t)|. \quad (35)$$

Proof. We explain only the equality in the formula (35) (it was not done in [1]). It is sufficient to check the relation

$$\sum_{y : |X_t(y)| \geq 2} |X_t(y)| = \sum_{i=1}^{M} |Y_i(t)|, \quad t = m/n > 0.$$

For any point $y$ with $|X_t(y)| \geq 2$ those $|X_t(y)|$ codewords $\{x_i\}$ give the same contribution $|X_t(y)|$ to the right-hand side of the equality. \qed

Since

$$\sum_{y : |X_t(y)| \geq 2} |X_t(y)| = \sum_{y} |X_t(y)| - \sum_{y : |X_t(y)| = 1} |X_t(y)| =$$

$$= M \left( \binom{n}{tn} \right) - \left| \{ y : |X_t(y)| = 1 \} \right|,$$
then, in particular, from (35) for any \( t \in (0, 1) \) we have
\[
P_e \geq \frac{q^n}{2M} \left( \frac{p}{q} \right)^{tn} M \left( \binom{n}{tn} \right) - |\{ y : |X_i(y)| \geq 1 \}|.
\] (36)

Using the inequality \( |\{ y : |X_i(y)| \geq 1 \}| \leq 2^n \) and optimizing over \( t \), we get from (36) the sphere-packing bound (see [1, §3])
\[
E(R, p) \leq E_{sp}(R, p), \quad 0 \leq R \leq C(p),
\] (37)
where \( E_{sp}(R, p) \) is defined in (17). From the inequality (37) and similar lower bound [2] we get the formula (16). In other words, for \( R \geq R_{crit}(p) \) the lowerbound (35) for \( P_e \) is logarithmically precise.

Important for us will be the following result, similar to Johnson’s bound [11, Theorems 17.2.2 and 17.2.4] (see proof in Appendix).

**Lemma 2.**
Let \( C = \{ x_1, \ldots, x_M \} \) – code of length \( n \) and constant weight \( tn \), \( t \leq 1/2 \). If for some \( \omega \leq 1/2 \) and some \( \delta \geq 0 \) the following condition is fulfilled
\[
\sum_{0<i<\omega n} B_i \leq \delta M,
\] (38)
and for some \( a > 0 \) the value \( t \) satisfies the inequality
\[
t \leq 1 - \frac{1 - 2(1 - \delta)\omega + 2a}{2},
\] (39)
then
\[
M \leq \frac{\omega}{a}.
\] (40)

In the sequel Lemma 2 will be used for small \( \delta, a \). Then (39) takes the form (see the definition of the value \( t_1(\omega) \) in (58))
\[
t \leq (1 - \sqrt{1 - 2\omega})/2 + o(1), \quad n \to \infty.
\]

Consider some values related to sums in the right-hand side of (35). For codewords \( x_i, x_j \) with \( d_{ij} = d(x_i, x_j) = \omega n \) introduce the set
\[
Z_{ij}(t, \omega) = \{ y : d_i(y) = d_j(y) = tn \}.
\] (41)
Since the cardinality \( |Z_{ij}(t, \omega)| \) does not depend on indices \((i, j)\), denote it simply \( Z(t, \omega) \). For the value \( Z(t, \omega), \omega/2 \leq t \leq 1/2 \) we have
\[
\frac{1}{n} \log_2 Z(t, \omega) = \frac{1}{n} \log_2 \left[ \left( \frac{(1 - \omega)n}{(t - \omega/2)n} \right)^{\omega n/2} \right] = u(t, \omega) - \delta(t, \omega),
\]
\[
u(t, \omega) = \omega + (1 - \omega)h_2 \left( \frac{2t - \omega}{2(1 - \omega)} \right),
\] (42)
\[
0 \leq \delta(t, \omega) \leq \frac{2}{n} \log_2 \frac{n + 2}{2},
\]
since for any $0 \leq k \leq n$ inequalities hold [12, formula (12.40)]

$$\frac{1}{n+1} 2^{nh(k/n)} \leq \binom{n}{k} \leq 2^{nh(k/n)}.$$ 

For the function $u(t, \omega)$ we have

$$u'_\omega = -\frac{1}{2} \log \frac{(1 - \omega)^2}{(2t - \omega)(2 - 2t - \omega)} \leq 0,$$

$$u''_{\omega\omega} = -\frac{(1 - 2t)^2}{(1 - \omega)(2t - \omega)(2 - 2t - \omega) \ln 2} \leq 0,$$

$$u'_t = \log \frac{2 - 2t - \omega}{2t - \omega} \geq 0, \quad t \leq \frac{1}{2},$$

$$u''_{tt} = \frac{4(1 - \omega)}{(2t - \omega)(2 - 2t - \omega) \ln 2} \leq 0.$$  

(43)

We call $(x_i, x_j)$ $\omega$–pair, if $d_{ij} = \omega n$. Then the total number of $\omega$–pairs in a code equals $MB_{\omega n}$. We say that a point $y$ is $(\omega, t)$–covered, if there exists $\omega$–pair $(x_i, x_j)$ such that $d_i(y) = d_j(y) = tn$. For the point $y$ denote by $K(y, \omega, t)$ the number of her $(\omega, t)$–coverings (taking into account multiplicity of coverings), i.e.

$$K(y, \omega, t) = | \{ (x_i, x_j) : d_{ij} = \omega n, d_i(y) = d_j(y) = tn \} |, \quad \omega > 0. \quad (44)$$

Then for any $t, y$

$$|X_t(y)|(|X_t(y)| - 1) = \sum_{\omega > 0} K(y, \omega, t),$$

and for any $t, \omega$ we get

$$|X_t(y)| \geq \sqrt{K(y, \omega, t)}. \quad (45)$$

Therefore from (35) and (45) for any $t, \omega$ we have

$$P_e \geq \frac{q^n}{2M} \left( \frac{p}{q} \right)^{tn} \sum_{y \in Y} \sqrt{K(y, \omega, t)}. \quad (46)$$

We modify the right-hand side of (46) as follows. For any set $A$ denote

$$K(A, \omega, t) = \sum_{y \in A} K(y, \omega, t), \quad (47)$$

where $K(y, \omega, t)$ is defined in (44). In other words, $K(A, \omega, t)$ is the total number of $(\omega, t)$–coverings of the set $A$.

Introduce the set $Y(\omega, t)$ of all $(\omega, t)$–covered points $y$, i.e.

$$Y(\omega, t) = \{ y : K(y, \omega, t) \geq 1 \} = \left\{ y : \begin{array}{l} \text{there exist } x_i, x_j, \text{ such that } \end{array} \\ d_{ij} = \omega n \text{ and } d_i(y) = d_j(y) = tn \right\}.$$
Since every $\omega$-pair $(x_i, x_j)$ $t$-covers $Z(t, \omega)$ points $y$, then

$$K(Y, \omega, t) = K(Y(\omega, t), \omega, t) = MB_{\omega n}Z(t, \omega).$$
(48)

For any subset $Y' \subseteq Y(\omega, t)$ introduce the value

$$K_{\text{max}}(Y', \omega, t) = \max_{y \in Y'} K(y, \omega, t).$$
(49)

Then for any $t, \omega$ and $Y' \subseteq Y(\omega, t)$ we have

$$P_e \geq q^n \left( \frac{p}{q} \right)^n \frac{K(Y', \omega, t)}{\sqrt{K_{\text{max}}(Y', \omega, t)}}.$$
(50)

Describe the scheme of proving Theorem 1 realized in the paper. Suppose that for chosen $\omega, t$ it is possible to choose also a set $Y'(\omega, t) \subseteq Y(\omega, t)$ such that the following two conditions are fulfilled:

$$K(Y'(\omega, t), \omega, t) \geq 2^{o(n)} K(Y(\omega, t), \omega, t), \quad n \to \infty$$
(51)

and

$$K(y, \omega, t) \leq 2^{o(n)}, \quad y \in Y'(\omega, t).$$
(52)

Then the inequality (50) can be continued as follows

$$P_e \geq 2^{o(n)} q^n \left( \frac{p}{q} \right)^n K(Y(\omega, t), \omega, t) = 2^{o(n)} q^n \left( \frac{p}{q} \right)^n B_{\omega n}Z(t, \omega).$$
(53)

Estimate (53) is the desired additive lowerbound for $P_e$ (for values $\omega, t$). After optimization of the right-hand side of (53) over $\omega, t$ Theorem 1 will be proved.

**Remark 4.** For a good code the value $K(y, \omega, t)$ in (52), probably, can not be exponential in $n$ for an essential part of all points $y$. In other words, for a good code it is unlikely that exponential number of codewords are more probable than the true codeword (!?).

We set some $\omega$ and $t = t(\omega)$. Due to (18) there exists a collection of $M_\omega$ points $\{y_1, \ldots, y_{M_\omega}\}$ such that

$$K(y_i, \omega, t) \sim \frac{MB_{\omega n}Z(t, \omega)}{M_\omega}, \quad i = 1, \ldots, M_\omega.$$

For that purpose it is sufficient to “quantize” all values $\ln K(y, \omega, t) \sim n$ with a step of order $o(n), n \to \infty$. At that $K(y_i, \omega, t)$ is the number of $\omega$-pairs on the $t$-sphere around the point $y_i$. The total number of various $\omega$-pairs on $t$-spheres around points $\{y_i\}$ has the order $MB_{\omega n}$, i.e. "all" (in exponential sense) $\omega$-pairs are located on those spheres. Therefore each $\omega$-pair belongs to $Z(t, \omega)$ $t$-spheres, i.e. it covers $Z(t, \omega)$ points $y_i$. Then, essentially, each $\omega$-pair covers only points $y_i$. 
If there are several such $M_\omega$ then choose the maximal one.

As a result, there are $N_\omega$ points on every $t$-sphere and each $t$-sphere there are $K(y_i, \omega, t)$ $\omega$-pairs. We investigate the right-hand side of the inequality (53). Denoting

$$b(\omega) = \frac{1}{n} \log B_{\omega n} + o(1), \quad n \to \infty,$$

represent (53) in an equivalent form ($n \to \infty$)

$$\frac{1}{n} \log \frac{1}{P_e} \leq c(\omega, t, p) - b(\omega) + o(1),$$

where

$$c(\omega, t, p) = t \log \frac{q}{p} - \log q - u(t, \omega),$$

and the function $u(t, \omega)$ is defined in (42). For the function $c(\omega, t, p)$ using (43) we have

$$c'_\omega = -u'_\omega = \frac{1}{2} \log \frac{(1 - \omega)^2}{(2t - \omega)(2 - 2t - \omega)} \geq 0,$$

$$c''_{\omega\omega} = \frac{(1 - 2t)^2}{(1 - \omega)(2t - \omega)(2 - 2t - \omega) \ln 2} \geq 0,$$

$$c'_t = \log \frac{q(2t - \omega)}{p(2 - 2t - \omega)} \leq 0, \quad t \leq t_2(\omega, p) = \frac{\omega}{2} + (1 - \omega)p,$$

$$c''_{tt} = \frac{4(1 - \omega)}{(2t - \omega)(2 - 2t - \omega) \ln 2} \geq 0.$$

The function $c(\omega, t, p)$ from (56) has a simple meaning. Suppose that we distinguish two codewords $x_i, x_j$ with $d(x_i, x_j) = \omega n$. Introduce the set of “ambiguity” $Z_{ij}(t, \omega)$ from (41). If $y \in Z_{ij}(t, \omega)$ then with probability $1/2$ decoding error occurs. Moreover,

$$P \left\{ y \in Z_{ij}(t, \omega) | x_i \right\} \sim 2^{-c(\omega, t, p)n}.$$

In order to choose the radius $t$ introduce functions (see. [1, formula (29)])

$$t_1(\omega) = \frac{1 - \sqrt{1 - 2\omega}}{2}, \quad t_2(\omega, p) = \frac{\omega}{2} + (1 - \omega)p.$$

The function $t_2(\omega, p)$ sometimes is called “Elias radius”. We set

$$t(\omega, p) = \min \{t_1(\omega), t_2(\omega, p)\} = \begin{cases} 
(1 - \sqrt{1 - 2\omega})/2, & \omega \leq \omega_1(p), \\
\omega/2 + (1 - \omega)p, & \omega \geq \omega_1(p),
\end{cases}$$

where $\omega_1(p)$ is defined in (12). The threshold value $\omega_1(p)$ will play very important role in the sequel.
It follows from (57) that the function \( c(\omega, t, p) \) monotonically decreases in \( t < t_2(\omega, p) \) and monotonically increases in \( t > t_2(\omega, p) \). In particular,

\[
\min_t c(\omega, t, p) = c(\omega, t_2(\omega, p), p) = \frac{\omega}{2} \log \frac{1}{4pq}.
\]

(60)

For any \( \omega \) we will always choose \( t \) such that the following condition is satisfied

\[
t \leq t(\omega, p).
\]

(61)

There are two reasons for such choice:
1) we would like to minimize the function \( c(\omega, t, p) \), which monotonically decreases in \( t < t_2(\omega, p) \);
2) the condition \( t \leq t_1(\omega) \) is necessary in order Lemma 2 be valid (and related with it the condition (52)).

§ 3. Proof of Theorem 1

For a given \( R \) choose some \( \alpha \) such that

\[
h^{-1}(1 - R) \leq \alpha \leq \frac{1}{2} \quad (\text{see Theorem 2})
\]

and set \( \tau = h^{-1}(h(\alpha) - 1 + R) \) (such \( \tau \) minimizes \( G(\alpha, \tau) \)). Due to Theorem 3 for some \( \delta \leq \delta_0 = G(\alpha, \tau) \) we have

\[
\frac{1}{n} \log B_{\delta n} \geq \mu(R, \alpha, \delta) + o(1), \quad n \to \infty.
\]

Since \( K(Y, \delta, s(\delta)) = MB_{\delta n}Z(s(\delta), \delta) \) for any radius \( s(\delta) \), there exists a collection of \( N_\delta \) points \( \{y_1, \ldots, y_{N_\delta}\} \) such that

\[
K(y_i, \delta, s(\delta)) = \frac{2^{o(n)}MB_{\delta n}Z(s(\delta), \delta)}{N_\delta}, \quad i = 1, \ldots, N_\delta.
\]

Therefore from (66) we get

\[
P_e \geq 2^{o(n)} \left( \frac{p}{q} \right)^{s(\delta)n} \sqrt{N_\delta B_{\delta n}Z(s(\delta), \delta)}.
\]

(62)

Now two cases are possible:
1) \( \ln K(y_i, \delta, s(\delta)) = o(n) \) for an essential part \( N_\delta \) of points \( \{y_i\} \) (i.t. the condition (52) is fulfilled);
2) \( \ln K(y_i, \delta, s(\delta)) \sim n \) for for an essential part \( N_\delta \) of points \( \{y_i\} \).

Consider sequentially those cases assuming \( s(\delta) \leq t_1(\delta) \).

1) If \( \ln K(y_i, \delta, s(\delta)) = o(n) \) for an essential part \( N_\delta \) of points \( \{y_i\} \), then the bound (62) takes additive form for \( \delta \) and \( t = s(\delta) \)

\[
P_e \geq 2^{o(n)} q^n \left( \frac{p}{q} \right)^{s(\delta)n} B_{\delta n}Z(s(\delta), \delta).
\]

(63)
2) If \( \ln K(\mathbf{y}_i, \delta, s(\delta)) \sim n \) for an essential part \( N_\delta \) of points \( \{\mathbf{y}_i\} \), then consider \( s(\delta) \)-spheres around each point \( \mathbf{y}_i \) from that essential part. We may assume that on every such \( s(\delta) \)-sphere there is the same number \( m_1 \) points and there are \( K(\mathbf{y}_i, \delta, s(\delta)) \) \( \delta \)-pairs. Denote by \( B'_{\omega n} \) analogues of numbers \( B_{\omega n} \) for \( s(\delta) \)-spheres. Then

\[
m_1 B'_{\omega n} = K(\mathbf{y}_i, \delta, s(\delta)) = \frac{2o(n) MB_{\delta n} Z(s(\delta), \delta)}{N_\delta}.
\]

Let for that essential part \( N_\delta \) точек \( \{\mathbf{y}_1, \ldots, \mathbf{y}_{N_\delta}\} \) the condition is satisfied

\[
\sum_{\omega < \delta} K(\mathbf{y}_i, \omega, s(\delta)) \leq K(\mathbf{y}_i, \delta, s(\delta))/n.
\]

Since \( s(\delta) \leq t_1(\delta) \), it follows from Lemma 2 that the number points \( m_1 \) on every such \( s(\delta) \)-sphere satisfies the inequality \((10)\), i.e. it is non-exponential. Therefore in that case the additive bound \((63)\) holds.

It remains to consider the case when for some \( \omega < \delta \) the condition \((63)\) is not satisfied, i.e. for an essential part \( N_\delta \) points \( \{\mathbf{y}_i\} \)

\[
K(\mathbf{y}_i, \omega, s(\delta)) > K(\mathbf{y}_i, \delta, s(\delta))/n^2.
\]

If necessary, choose the minimal one among all possible \( \omega < \delta \). Then we have (since \( K(Y, \omega, s) = MB_{\omega n} Z(s, \omega) \))

\[
\log [B_{\omega n} Z(s(\delta), \omega)] \geq \log [B_{\delta n} Z(s(\delta), \delta)] + o(n).
\]

Therefore for an essential part \( N_\delta \) of points \( \{\mathbf{y}_i\} \) we have \( \log B'_{\omega n} \geq \log B'_{\delta n} + o(n) \). We choose \( s(\omega) \leq t_1(\omega) \) such that the potential additive bound \( \omega \) will be not less than the right-hand side of \((63)\), i.e. the inequality holds

\[
\left(\frac{p}{q}\right)^{s(\delta)n} B_{\delta n} Z(s(\delta), \delta) \leq \left(\frac{p}{q}\right)^{s(\omega)n} B_{\omega n} Z(s(\omega), \omega).
\]

Due to \((66)\) for that purpose it is sufficient to have

\[
\left(\frac{p}{q}\right)^{s(\delta)n} Z(s(\delta), \omega) \leq \left(\frac{p}{q}\right)^{s(\omega)n} Z(s(\omega), \omega),
\]

or, equivalently,

\[
f = [s(\delta) - s(\omega)] \log \frac{q}{p} + u(s(\omega), \omega) - u(s(\delta), \omega) \geq 0,
\]

where \( u(t, \omega) \) is defined in \((12)\). Using \((43)\) we have

\[
\frac{\partial f}{\partial s(\omega)} = \log \frac{p[2 - 2s(\omega) - \omega]}{q[2s(\omega) - \omega]} \geq 0, \quad s(\omega) \leq t_2(p, \omega),
\]

\[
\frac{\partial f}{\partial s(\delta)} = \log \frac{q[2s(\delta) - \omega]}{p[2 - 2s(\delta) - \omega]} \geq 0, \quad s(\delta) \geq t_2(p, \omega).
\]
Therefore for all $\omega$ we set
\[
s(\omega) = t(p, \omega) = \min\{t_1(\omega), t_2(p, \omega)\}.
\]
Since $s(\omega) \leq s(\delta)$, the inequalities (68) and (67) will be fulfilled. It means that a descent from $\delta$ to $\omega$ does not decreases the potential additive bound. It should be noted that a further descent from $\omega$ on a lower level $\omega_1$ is not possible, since the level $\omega$ was chosen as the minimal possible one, for which the inequality (65) holds. It proves validity of the additive bound (63) for $s(\omega) = t(p, \omega)$, from which we get $(h_2(\tau) = h_2(\alpha) - 1 + R)$

**Proposition 1.** For any $0 \leq R < C(p)$ and $0 < p < 1/2$ the inequality holds
\[
E(R, p) \leq \min_{0 \leq \alpha \leq 1/2} \max_{\delta \leq G(\alpha, \tau)} \left\{ t(p, \delta) \log \frac{q}{p} - \log q - \mu(R, \alpha, \delta) - u(t(p, \delta), \delta) \right\}.
\]  (69)

That result coincides with [1, Theorem 1] in the most interesting region $0 \leq R \leq R_2(p)$ and improves that Theorem in the less interesting region $R_2(p) \leq R \leq C(p)$.

**Remark 5.** For large $R$ maximum over $\delta \leq G(\alpha, \tau)$ in (69) is attained not in the extreme point $\delta = G(\alpha, \tau)$.

We will get the paper main Theorem 1 as a corollary from the bound (69). For that purpose introduce the function
\[
W(\omega, \alpha, R, p) = \frac{\omega}{2} \log \frac{1}{4pq} - \mu(R, \alpha, \omega).
\]  (70)

As will be clear below, it is sufficient to consider the case $0 \leq R \leq R_2(p)$. Then
\[
\min_{0 \leq \alpha \leq 1/2} G(\alpha, \tau) \geq \omega_1(p) \quad \text{(see (6) and (13))}
\]
and then $t(p, \delta) = t_2(\delta, p)$. Since
\[
u(t_2(\delta, p), \delta) = \delta + (1 - \delta)h_2(p),
\]
then for $0 \leq R \leq R_2(p)$ we get from (69)
\[
E(R, p) \leq \min_{0 \leq \alpha \leq 1/2} \max_{\delta \leq G(\alpha, \tau)} W(\delta, \alpha, R, p),
\]  (71)
where the function $W(\delta, \alpha, R, p)$ is defined in (70).

We show that maximum over $\delta$ in the right-hand side of (71) is attained for $\delta = G(\alpha, \tau)$.

**Lemma 3.** For any $0 \leq \tau \leq \alpha \leq 1/2$ such that $R = 1 - h_2(\alpha) + h_2(\tau)$ and $G(\alpha, \tau) \geq \omega_1(p)$ the formula holds
\[
\max_{\lambda \leq G(\alpha, \tau)} W(\lambda, \alpha, R, p) = W(G(\alpha, \tau), \alpha, R, p) =
\]
\[= \frac{G(\alpha, \tau)}{2} \log \frac{1}{4pq} - \mu(R, \alpha, G(\alpha, \tau)).
\]  (72)
Proof. From (25) we have [8, Proposition 1] \((P = P(\omega/2), Q = Q(\omega/2), a_1 = 2[\alpha(1 - \alpha) - \tau(1 - \tau)])\)

\[
\mu'(R, \alpha, \omega) = \frac{1}{2} \log \frac{(1 - \omega)^2}{(\alpha - \omega/2)(1 - \alpha - \omega/2)} - \log \frac{P + \sqrt{P^2 - Q\omega^2}}{Q} = \\
= \log \frac{(1 - \omega)\sqrt{(2\alpha - \omega)(2 - 2\alpha - \omega)}}{a_1 - \omega(1 - \omega) + \sqrt{(1 - 2\tau)^2\omega^2 - 2a_1\omega + a_1^2}},
\]

(73)

For \(W(\omega, \alpha, R, p)\) we have from (70) and (73) [8, Proposition 2]

\[
W''(\omega, \alpha, R, p) < 0, \quad W'(\omega, \alpha, R, p) \bigg|_{\omega = G} = \log \frac{G}{\sqrt{4pq(1 - G)}}, \quad G = G(\alpha, \tau).
\]

Therefore, if \(G(\alpha, \tau) \geq \omega_1(p)\) then \(W''(\omega, \alpha, R, p) \bigg|_{\omega = G} \geq 0, \) and then maximum over \(\delta\) in the right-hand side of (72) is attained for \(\lambda = G(\alpha, \tau). \) \(\square\)

As a result, from (71) and (72) for \(0 \leq R \leq R_2(p)\) we get

\[
E(R, p) \leq \min_{0 \leq \alpha \leq 1/2} \left\{ \frac{G(\alpha, \tau)}{2} \log \frac{1}{4pq} - \mu(R, \alpha, G(\alpha, \tau)) \right\}.
\]

(74)

It remained us to get for \(\mu(R, \alpha, G(\alpha, \tau))\) from (74) an explicit expression. We use the following analytical result (see proof in Appendix).

Lemma 4. For any \(\alpha, \tau\) the formula holds

\[
\mu(R, \alpha, G(\alpha, \tau)) = L(G(\alpha, \tau)) + R - 1,
\]

(75)

where \(R = 1 - h_2(\alpha) + h_2(\tau)\) and the function \(L(\omega)\) is defined in (21).

Using (75) and (74) we get

\[
E(R, p) \leq 1 - R + \min_{0 \leq \alpha \leq 1/2} \left\{ \frac{G(\alpha, \tau)}{2} \log \frac{1}{4pq} - L(G(\alpha, \tau)) \right\} \leq \\
\leq 1 - R + \frac{\omega_R}{2} \log \frac{1}{4pq} - L(\omega_R),
\]

(76)

where \(\omega_R\) is defined in (6).

In particular, from (76) the formula (20) follows. Concerning the formula (19) recall that if \(R \leq R_0\), then the best is \(\alpha = 1/2\). The bound (19) follows from (74) with \(\alpha = 1/2\) and (34).

It remained us to prove the formula (18). Note that

\[
t_1(\omega_1(p)) = \frac{\sqrt{p}}{\sqrt{q} + \sqrt{p}}.
\]
Therefore if $G(\alpha, \tau) = \omega_1(p)$ then using (75) we get
\[
\mu(R, \alpha, \omega_1(p)) = \frac{\omega_1(p)}{2} \log \frac{1}{4pq} + R + \log(1 + 2\sqrt{pq}) - 1. \tag{77}
\]
Then for any rate $R$, for which it is possible to have $G(\alpha, \tau) = \omega_1(p)$, from (14) and (77) the inequality follows
\[
E(R, p) \leq 1 - \log(1 + 2\sqrt{pq}) - R. \tag{78}
\]
The rate $R = R_2(p)$ is the minimal of such rates (see (13)). For $R = R_{\text{crit}}(p)$ the formula holds \[2\] (see (16))
\[
E(R_{\text{crit}}, p) = E_{\text{sp}}(R_{\text{crit}}, p) = 1 - \log_2(1 + 2\sqrt{pq}) - R_{\text{crit}}. \tag{79}
\]
Therefore due to the “straight-line upper bound” \[3\] the inequality (78) holds for all $R$ such that $R_2(p) \leq R \leq R_{\text{crit}}(p)$, i.e.
\[
E(R, p) \leq 1 - \log(1 + 2\sqrt{pq}) - R, \quad R_2(p) \leq R \leq R_{\text{crit}}(p). \tag{80}
\]
On the other hand, for the function $E(R, p)$ the random coding lower bound is known \[2\]
\[
E(R, p) \geq 1 - \log_2(1 + 2\sqrt{pq}) - R, \quad 0 \leq R \leq R_{\text{crit}}(p). \tag{81}
\]
As result, from (80) and (81) the formula (18) follows, that completes Theorem 1 proof.

§ 4. Non-integral representation for $\mu(R, \alpha, \omega)$

Proof of the next result represents a standard integration using Euler’s substitution. That representation is used in deriving the formula (75) and in the proof of Theorem 1.

P r o p o s i t i o n 3. For the function $\mu(R, \alpha, \omega)$ the representation holds
\[
\mu(R, \alpha, \omega) = (1 - \omega) h_2 \left( \frac{\alpha - \omega/2}{1 - \omega} \right) - h_2(\alpha) + 2h_2(\omega) + \omega \log \frac{2\omega}{e} - T(A, B, \omega), \tag{82}
\]
where
\[
\tau = h_2^{-1}(h_2(\alpha) - 1 + R) \leq 1/2, \quad A = 1 - 2\alpha, \quad B = 1 - 2\tau, \quad B > A \geq 0,
\]
\[
T(A, B, \omega) = \omega \log(v - 1) - (1 - \omega) \log \frac{v^2 - A^2}{v^2 - B^2} + B \log \frac{v + B}{v - B} - A \log \frac{v + A}{v - A} - \frac{(v - 1)(B^2 - A^2)}{(v^2 - B^2) \ln 2}, \tag{83}
\]
and
\[
v = \sqrt{B^2\omega^2 - 2a_1\omega + a_1^2 + a_1}, \quad a_1 = 2[\alpha(1 - \alpha) - \tau(1 - \tau)]. \tag{84}
\]
Proof. Using notations (83) and the variable \( z = 2y \), we have from (25)

\[
\mu(R, \alpha, \omega) = h_2(\alpha) - \omega - (1 - \omega)h_2 \left( \frac{\alpha - \omega/2}{1 - \omega} \right) - \int_0^\omega \log \frac{f_1}{g_1} \, dz,
\]

\[
f_1 = z^2 - z + a_1 + \sqrt{B^2z^2 - 2a_1z + a_1^2}, \quad g_1 = (1 - z)^2 - A^2.
\]

Then

\[
\int_0^\omega \log g_1 \, dz = -2h_2(\alpha) - 2(1 - \omega) \log(1 - \omega) + 2(1 - \omega)h_2 \left( \frac{\alpha - \omega/2}{1 - \omega} \right) - 2\omega \log \frac{e}{2}.
\]

We also have

\[
\int_0^\omega \log f_1 \, dz = F(a_1, B, \omega) - F(a_1, B, 0),
\]

where \( F(a_1, B, z) \) — primitive function for \( \log f_1 \). In order to find \( F(a_1, B, z) \), we use Euler’s substitution

\[
\sqrt{B^2z^2 - 2a_1z + a_1^2} = zv - a_1,
\]

and then

\[
z = \frac{2a_1(v - 1)}{v^2 - B^2}, \quad z' = \frac{2a_1(2v - v^2 - B^2)}{(v^2 - B^2)^2}.
\]

Now

\[
F(a_1, B, z) \ln 2 = \int \ln f_1 \, dz = z \ln z - z + z(v) \ln[z(v) + v - 1] + \frac{a_1}{A} \ln \frac{v + A}{v - A} - 4a_1^2 I_1,
\]

where

\[
I_1 = \int \frac{(2v - v^2 - B^2)}{(v^2 - A^2)(v^2 - B^2)^2} \, dv.
\]

After standard integration we have

\[
\frac{(B^2 - A^2)^2 I_1}{2} = \ln \frac{v^2 - A^2}{v^2 - B^2} + \frac{(v - 1)(B^2 - A^2)}{(v^2 - B^2)^2} + \frac{B^2 + A^2}{2A} \ln \frac{v + A}{v - A} + B \ln \frac{v - B}{v + B}.
\]

Since \( 2a_1 = B^2 - A^2 \) and

\[
z(v) + v - 1 = \frac{(v - 1)(v^2 - A^2)}{v^2 - B^2},
\]

18
we get
\[
F(a_1, B, z) = z \log z - \frac{z}{\ln 2} + z \log(v - 1) - (1 - z) \log \frac{v^2 - A^2}{B^2} + 
\]
\[
+ B \log \frac{v + B}{v - B} - A \log \frac{v + A}{v - A} - \frac{(v - 1)(B^2 - A^2)}{(v^2 - B^2) \ln 2},
\]
where \( v \) is defined in (84). Since \( v \to \infty \) as \( u \to 0 \) и \( F(a, b, 0) = 0 \), then
\[
\mu(R, \alpha, \omega) = -h_2(\alpha) - 2(1 - \omega) \log(1 - \omega) - 2\omega \log e + 
\]
\[
+(1 - \omega)h_2 \left( \frac{\alpha - \omega / 2}{1 - \omega} \right) - F(a_1, B, \omega),
\]
from which Proposition 3 follows. \( \Box \)

**APPENDIX**

**Proof of formula (33).** For \( \omega \leq G(1/2, \tau) \) we have \[ formula (П. 2) \]
\[
\mu(R, 1/2, \omega) \ln 2 = -2\omega(1 - \ln 2) - 2(1 - \omega) \ln(1 - \omega) - I,
\]
\[
I = \int_0^{2\omega} \ln \left[ b + \sqrt{(1-z)^2 + b^2 - 1} \right] dz, \quad b = 1 - 2\tau > 0.
\]

In order to find the integral \( I \), we use variable \( u = \sqrt{(1-z)^2 + b^2 - 1} \). Then denoting
\[
A = \sqrt{(1-2\omega)^2 + b^2 - 1}, \quad v_1 = \frac{b}{\sqrt{1-b^2}}, \quad v_2 = \frac{A}{\sqrt{1-b^2}},
\]
and using integration by parts we have
\[
I = - \int_b^A \ln(b + u) d\sqrt{u^2 + 1 - b^2} =
\]
\[
= \ln(2b) - (1 - 2\omega) \ln(b + A) + \sqrt{1-b^2} \int_{v_1}^{v_2} \frac{\sqrt{1+v^2}}{v + v_1} dv.
\]

Since
\[
\int \frac{\sqrt{1+z^2}}{z + a} dz =
\]
\[
= \sqrt{1+z^2} - a \ln \left[ z + \sqrt{1+z^2} \right] - \sqrt{1+a^2} \ln \frac{\sqrt{(1+a^2)(1+z^2)} - za + 1}{z + a},
\]
then
\[
I = \ln(2b) - (1 - 2\omega) \ln(b + A) - 2\omega - b \ln \frac{1 - 2\omega + A}{1 + b} - \ln \frac{b(2 - 2\omega - b^2 - bA)}{(b + A)(1 - b^2)}.
\]
After standard algebra with \( g = (b + A)/2 \) we get the formula (33). □

**Proof of lemma 2.** Consider a code \( C \) average distance

\[
d_{av}(C) = M^{-2} \sum_{i=1}^{M} \sum_{j=1}^{M} d_{ij}.
\]

Similarly to Plotkin’s bound derivation [11, теорема 2.2.1] we have

\[
d_{av}(C) \leq 2t(1 - t)n, \quad 0 \leq t \leq 1.
\] (85)

Using the assumption (38) we can also lower bound the value \( d_{av}(C) \)

\[
d_{av}(C) \geq \frac{1}{M} \sum_{i \geq \omega n} iB_i \geq \omega n M \sum_{i \geq \omega n} B_i =
\]

\[
= \frac{\omega n}{M} \left( \sum_{i > 0} B_i - \sum_{0 < i < \omega n} B_i \right) \geq \frac{\omega(M - 1 - \delta M)n}{M}.
\]

Comparing that estimate with (85) we get the inequality (40). □

**Proof of formula (75).** We use the representation (82) and notations from (83) and (84). Since

\[
G(\alpha, \tau) = \frac{a_1}{1 + 2\sqrt{\tau(1 - \tau)}}, \quad a_1 = 2[\alpha(1 - \alpha) - \tau(1 - \tau)],
\]

then

\[
B^2G^2 - 2a_1G + a_1^2 = 0 \quad \text{и} \quad v = \frac{a_1}{G} = 1 + 2\sqrt{\tau(1 - \tau)}.
\]

Also

\[
v - B = 2\sqrt{\tau}v, \quad v + B = 2\sqrt{1 - \tau}v, \quad v^2 - B^2 = 4\sqrt{\tau(1 - \tau)} \left[ 1 + 2\sqrt{\tau(1 - \tau)} \right], \quad \frac{(v - 1)(B^2 - A^2)}{v^2 - B^2} = G,
\]

\[
v - A = 2 \left[ \sqrt{\tau(1 - \tau)} + \alpha \right], \quad v + A = 2 \left[ 1 + \sqrt{\tau(1 - \tau)} - \alpha \right].
\]

Therefore \((\omega = G(\alpha, \tau))\)

\[
T(A, B, G) = \frac{\omega}{2} \log \left[ \tau(1 - \tau) \right] - (1 - \omega) \log \left[ \frac{1 + \sqrt{\tau(1 - \tau)} - \alpha}{\sqrt{\tau(1 - \tau)}} \right] +
\]

\[
+ \frac{(1 - 2\tau)}{2} \log \frac{1 - \tau}{\tau} - (1 - 2\alpha) \log \frac{1 + \sqrt{\tau(1 - \tau)} - \alpha}{\sqrt{\tau(1 - \tau)} + \alpha} - \omega \left( \frac{1}{\ln 2} - 1 \right)
\]
\[ \mu(R, \alpha, G) = (1 - \omega)h_2 \left( \frac{\alpha - \omega/2}{1 - \omega} \right) + R - 1 + 2h_2(\omega) + \omega \log \omega + \]
\[ (1 - \omega) \log \frac{1 + \sqrt{\tau(1 - \tau) - \alpha}}{1 + 2\sqrt{\tau(1 - \tau)}} + \]
\[ +(1 - \omega) \log \frac{1 + \sqrt{\tau(1 - \tau) - \alpha}}{\sqrt{\tau(1 - \tau) + \alpha}}. \]

Using in the last expression formulas
\[ \frac{2\alpha - G}{2} = \left[ \frac{\sqrt{\tau(1 - \tau) + \alpha}}{1 + 2\sqrt{\tau(1 - \tau)}} \right]^2, \]
\[ 1 - G - \frac{2\alpha - G}{2} = \left[ \frac{1 + \sqrt{\tau(1 - \tau) - \alpha}}{1 + 2\sqrt{\tau(1 - \tau)}} \right]^2, \]
and also formulas
\[ ah(b/a) = a \ln a - b \ln b - (a - b) \ln(a - b), \]
\[ 2t_1(\omega) - \omega = 2t_1^2(\omega), \]
we get the formula (75).

REFERENCES

1. **Burnashev M. V.** Code spectrum and reliability function: binary symmetric channel // Probl. Inform. Transm. 2006. V. 42. № 4. P. 3–22.

2. **Elias P.** Coding for noisy channels // IRE Conv. Rec. 1955. March, P. 37–46. Reprinted in D. Slepian, Ed., Key papers in the development of information theory, IEEE Press, 1974, P. 102–111.

3. **Shannon C. E., Gallager R. G., Berlekamp E. R.** Lower Bounds to Error Probability for Codes on Discrete Memoryless Channels. I, II // Inform. and Control. 1967. V. 10. № 1. P. 65–103; № 5. P. 522–552.

4. **Gallager R.G.** A Simple Derivation of the Coding Theorem and some Applications // IEEE Trans. Inform. Theory. 1965. V. 11. P. 3–18.

5. **McEliece R. J., Rodemich E. R., Rumsey H., Jr., Welch L. R.** New Upper Bounds on the Rate of a Code via the Delsarte–MacWilliams Inequalities // IEEE Trans. Inform. Theory. 1977. V. 23. № 2. P. 157–166.
6. Levenstein V. I. On a straight line bound for the undetected error exponent // Probl. Inform. Transm. 1989. V. 25. № 1. P. 33–37.

7. Barg A., McGregor A. Distance Distribution of Binary Codes and the Error Probability of Decoding // IEEE Trans. Inform. Theory. 2005. V. 51. № 12. P. 4237–4246.

8. Burnashev M. V. Upper bound sharpening on reliability function of binary symmetric channel // Probl. Inform. Transm. 2005. V. 41. № 4. P. 3–22.

9. Litsyn S. New Bounds on Error Exponents // IEEE Trans. Inform. Theory. 1999. V. 45. No. 2. P. 385–398.

10. Burnashev M. V. On the relation between the code spectrum and the decoding error probability // Probl. Inform. Transm. 2000. V. 36. № 4. P. 3–24.

11. MacWilliams F. J., Sloane N. J. A. The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North Holland. 1977.

12. Cover T. M., Thomas J. A. Elements of Information Theory. New York: Wiley. 1991.

13. Levenshtein V. I. Bounds for packings of metric spaces and some applications // Probl. Kibern. M.: Nauka, 1983. V. 40. P. 43–110.

14. Burnashev M. V. Supplement to the paper: Code spectrum and reliability function: binary symmetric channel // Probl. Inform. Transm. 2007. V. 42. № 1. P. 28–31.

Burnashev Marat Valievich
Kharkevich Institute for Information Transmission Problems,
Russian Academy of Sciences, Moscow
burn@iitp.ru
Fig. 1. Plots of functions $R_1(p)$, $R_2(p)$, $R_{\text{crit}}(p)$ and $C(p)$
Fig. 2. Plots of functions $E_{\text{low}}(R, p)$ and $E_{\text{up}}(R, p)$ for $p = 0.01$.