Lower Bounds on the Code Rate for a Model of Data Transmission with Side Information *

Vladimir B. Balakirsky
Member, IEEE

The author is currently with the
Fakultät für Mathematik, Universität Bielefeld,
Postfach 100131, D-33501 Bielefeld 1, Germany
on leave from the Data Security Association "Confident",
193060 St.-Petersburg, Russia
E-mail addresses :
vbal@mathematik.uni-bielefeld.de
vbal@vbal.spb.su

Abstract Asymptotic lower bounds on the code rate when the encoder and decoder have some partial knowledge about the positions where errors may occur during transmission of a codeword are derived.

Key words :
Coding, Decoding, Localized Errors, Side Information

*The work was supported by the SFB-343, Universität Bielefeld, Germany

1 Introduction

Suppose that a message m of some source has to be delivered to the receiver using a q-ary block code of length n and at most t bits of the transmitted codeword can be changed. In particular, this situation may occur when the participants, Encoder and Decoder, are included into a network and another user transmits his data at t time instants $i_1, \ldots, i_t \in \{1, \ldots, n\}$ in accordance with some protocol. Obviously, Encoder and Decoder solve the communication problem by using a code with the minimal distance at least $2t + 1$. We consider possible extensions of this problem and assume that Encoder and Decoder know some sets $\mathcal{E}_{t_e}, \mathcal{E}_{t_d} \supseteq \{i_1, \ldots, i_t\}$ of fixed cardinalities $t_e, t_d \geq t$. The case $t_e = t$ and $t_d = n$ (Encoder knows all positions where errors may occur, while Decoder is ignorant) corresponds to data transmission over a channel with localized errors. The coding problem for this channel was formulated in [1] as a generalization of the problem for memories with defective cells [2] and it was intensively studied in recent years [3], [4], [5], [6] for $q = 2$. The case $t_e > t$ and $t_d = n$ was also considered [4] and called data transmission over a channel with partially localized errors.

A basic idea developed in the analysis of the situation when Encoder has side information is a reservation of lists of codewords for every message instead of one codeword. Having received $\mathcal{E}_{t_e}$, Encoder selects one of the entries of the list assigned to m and sends it. If Decoder is ignorant about $i_1, \ldots, i_t$, then he has to construct a union of the Hamming balls of radius t around all points of the Hamming space corresponding to codewords reserved for a particular message and considers this union as a decoding region for that message.

The case $t_d < n$ means that Decoder has some side information and can change decoding regions of every message depending on $\mathcal{E}_{t_d}$. In particular, if $t_d = t$, then he knows all positions where errors may occur, like for data transmission over erasure channel. Therefore he punctures positions belonging to $\mathcal{E}_t$ and looks for a codeword coinciding with the received word at the remaining positions. If, in addition, $t_e = t$, then Encoder also knows $\{i_1, \ldots, i_t\}$ and any of q^{n-t} messages can be noiselessly delivered. If $t_e = n$, then Encoder has to use a code with the minimal distance at least $t + 1$ (instead of $2t + 1$ as for the case $t_d = n$), since Decoder's side information makes it possible to find out all positions where the transmitted code symbols are not changed.

We will present a general and rather simple sufficient condition that allows us to classify a collection of lists as a $SI(t_e, t_d, t)$-code, i.e., Encoder and Decoder solve communication problem using this code for given t_e, t_d, and t (SI stands for Side Information). If $t_d = n$ and $q = 2$, then this condition is reduced to the known ones [1], [4]. However, we develop another approach and do not use a concept of "the worst error pattern" : in binary case, there is only one vector containing 1's at all positions where errors could occur which transforms the transmitted codeword to a vector at the Hamming distance t. As a result, we obtain a new lower bound for channels with localized errors when $q > 2$ reducing the general bound to the case $(t_e, t_d) = (t, n)$.

We will also address the following problem. Suppose we can transmit data over a channel with localized errors ($t_e = t$ and $t_d = n$) at some rate. Now, let Encoder know less meaning that t_e becomes greater than t. How should we change t_d to transmit data at the same rate ? This question can be also formulated as follows. Suppose we have a situation when the information about positions where errors may occur during data transmission has to be distributed among Encoder and Decoder. Which distribution maximizes the transmission rate ? We will consider this problem from the point of view of asymptotic lower bounds on the rate and come to a conclusion that Decoder's influence on communication process is more important.

The correspondence is organized as follows. We begin with some notations and formal statement of the problem in Section 2. After that we introduce a definition of the SI- codes in Section 3 which includes both the possibility of adaptation of the transmitted codeword to positions where errors may occur and modification of decoding regions depending on these positions. Then we present two auxiliary results in Section 4 and use them to prove a lower bound on the code rate in Section 5. Considerations concerning balance of knowledges of Encoder and Decoder are presented in Section 6.

2 Notations and Formal Statement of the Problem

Let us fix integers t, t_e, t_d, and n in such a way that $t \leq t_e, t_d \leq n$ and consider a model of data transmission system given in Fig.1. The E-Generator selects an $E \in \mathcal{E}_t$ and sends it to the E_e-Generator, E_d-Generator and Jammer, where

$$\mathcal{E}_t = \Big\{ \ E \subseteq [n] : \ |E| = t \ \Big\} \tag{2.1}$$

denotes the collection of the t-element subsets of the set $[n] = \{1, \ldots, n\}$. The generators select some sets $E_e \in \mathcal{F}_{t_e}(E)$ and $E_d \in \mathcal{F}_{t_d}(E)$ belonging to the collections of t_e- and t_d-element subsets of the set $[n]$ which contain a given $E \in \mathcal{E}_t$,

$$\begin{aligned} \mathcal{F}_{t_e}(E) \ &= \ \Big\{ \ E_e \in \mathcal{E}_{t_e} : \ E_e \supseteq E \ \Big\}, \\ \mathcal{F}_{t_d}(E) \ &= \ \Big\{ \ E_d \in \mathcal{E}_{t_d} : \ E_d \supseteq E \ \Big\}, \end{aligned} \tag{2.2}$$

where the sets $\mathcal{E}_{t_e}$ and $\mathcal{E}_{t_d}$ are defined similarly to (2.1). These sets are available to Encoder and Decoder, respectively, before the transmission of a q-ary codeword $\mathbf{x}_m(E_e) \in \mathcal{Q}^n$ corresponding to the message $m \in [M]$ begins; $\mathcal{Q} = \{0, 1, \ldots, q-1\}$, $[M] = \{1, \ldots, M\}$. Jammer selects one of the q-ary vectors $\mathbf{e} \in V(E)$, where

$$V(E) = \Big\{ \ \mathbf{e} \in \mathcal{Q}^n : \ e_i = 0, \ \text{for all } i \in E^c \ \Big\}, \tag{2.3}$$

$E^c = [n] \backslash E$, and uses it to corrupt the transmitted codeword in such a way that Decoder receives $\mathbf{y} = \mathbf{x}_m(E_e) \oplus \mathbf{e}$; the $\oplus$ sign denotes the component-wise addition modulo q. Decoder constructs an estimate $\hat{m} \in [M]$ of the message m taking into account the set E_d, and the encoding and decoding algorithms should be specified in such a way that $\hat{m} = m$ for all $E_e \in \mathcal{F}_{t_e}(E)$, $E_d \in \mathcal{F}_{t_d}(E)$, $\mathbf{e} \in V(E)$, $E \in \mathcal{E}_t$, and $m \in [M]$.

We are interested in the maximal code rate [1] $(\log M)/n$ that can be asymptotically attained for

$$(t, t_e, t_d) = (n\tau, n\tau_e, n\tau_d),$$

[1] All logarithms in the correspondence are to the base 2. We also set $0 \log 0 = 0$.

where τ, τ_e, and τ_d do not depend on n and satisfy the inequalities $0 \leq \tau \leq \tau_e, \tau_d \leq 1$. This rate will be denoted by $R_q(\tau, \tau_e, \tau_d)$ and a lower bound on $R_q(\tau, \tau_e, \tau_d)$ will be denoted by $r_q(\tau, \tau_e, \tau_d)$.

If $q = 2$ then the following equations are known,

$$r_2(\tau, \tau_e, \tau_d) = \begin{cases} 1 - \tau, & \text{if } (\tau_e, \tau_d) = (\tau, \tau), \\ 1 - h(\tau), & \text{if } (\tau_e, \tau_d) = (\tau, 1) \text{ or } (\tau_e, \tau_d) = (1, \tau), \\ 1 - h(2\tau), & \text{if } (\tau_e, \tau_d) = (1, 1), \end{cases} \tag{2.4}$$

where

$$h(p) = -p \log p - (1 - p) \log(1 - p), \quad \text{for all } p \in [0, 1],$$

is the binary entropy function. Furthermore, if the pair (τ_e, τ_d) is equal to either (τ, τ) or $(\tau, 1)$, equations are tight, i.e., we may substitute $R_2(\tau, \tau_e, \tau_d)$ for $r_2(\tau, \tau_e, \tau_d)$ in (2.4). The corresponding curves are shown in Fig.2.

Note that equations (2.4) for the cases $(\tau_e, \tau_d) \in \{(1, \tau), (1, 1)\}$ come from the Varshamov-Gilbert bound and that the case $(\tau_e, \tau_d) = (\tau, \tau)$ relates to data transmission over erasure channel. The lower bound for the case $(\tau_e, \tau_d) = (\tau, 1)$ and its tightness were proved in [1].

Our goal is to prove a formula for $r_q(\tau, \tau_e, \tau_d)$ containing (2.4) as special cases. In other words, for any r bounded from below by the value of the q-ary Varshamov-Gilbert bound ([7], p.550) at the point 2τ and from above by the maximal value of the code rate for the q-ary erasure channel :

$$\begin{aligned} r &\geq \log q - h(2\tau) - 2\tau \log(q - 1), \\ r &\leq \log q - \tau \log q, \end{aligned}$$

we want to find all pairs (τ_e, τ_d) such that there exist q-ary $SI(n\tau, n\tau_e, n\tau_d)$ codes having r as asymptotically achievable code rate.

3 SI-codes

Note that there are

$$\sum_{E \in \mathcal{E}_t} |\mathcal{F}_{t_e}(E)| \cdot |\mathcal{F}_{t_d}(E)| = \binom{n}{t} \cdot \binom{n-t}{t_e - t} \cdot \binom{n-t}{t_d - t}$$

possible triples (E, E_e, E_d) and $|V(E)| = q^t$ possibilities for the vector $\mathbf{e}$ for all $E \in \mathcal{E}_t$, where the sets $\mathcal{E}_t, \mathcal{F}_{t_e}(E), \mathcal{F}_{t_d}(E)$, and $V(E)$ are defined in (2.1), (2.2), and (2.3). Having received $E_d \in \mathcal{E}_{t_d}$, Decoder can construct all pairs $(\hat{E}, \hat{E}_e)$ matching E_d, i.e., all possible triples $(\hat{E}, \hat{E}_e, E_d)$. If $\mathbf{x}_m(\hat{E}_e)$ is the codeword for the m-th message and $\hat{E}$ is the set of positions where errors may occur, then

$$\mathbf{x}_m(\hat{E}_e) \oplus V(\hat{E}) = \bigcup_{\mathbf{e} \in V(\hat{E})} \{\mathbf{x}_m(\hat{E}_e) \oplus \mathbf{e}\}$$

is the set of possible received vectors $\mathbf{y}$. The sets $\mathbf{x}_m(\hat{E}_e) \oplus V(\hat{E})$ should be pairwise disjoint for different $m \in [M]$ and we give the following definition.

Definition *A collection $\mathcal{C}^{(n)} = (\mathcal{L}_1, \ldots, \mathcal{L}_M)$, whose entries are lists of binary vectors of length n, is a $SI(t, t_e, t_d)$-code iff there exists an encoding*

$$(m, E_e) \in [M] \times \mathcal{E}_{t_e} \quad \to \quad \mathbf{x}_m(E_e) \in \mathcal{L}_m$$

such that the sets $X_1(E_d), \ldots, X_M(E_d)$ are pairwise disjoint for all $E_d \in \mathcal{E}_{t_d}$, where

$$X_m(E_d) \;\; = \bigcup_{\hat{E} \in \mathcal{E}_t(E_d)} \; \bigcup_{\hat{E}_e \in \mathcal{F}_{t_e}(\hat{E})} \Big(\mathbf{x}_m(\hat{E}_e) \oplus V(\hat{E}) \Big), \quad m \in [M], \tag{3.1}$$

and

$$\begin{aligned} \mathcal{E}_t(E_d) &= \Big\{ \, E \in \mathcal{E}_t : \; E \subseteq E_d \, \Big\}, \\ \mathcal{F}_{t_e}(\hat{E}) &= \Big\{ \, \hat{E}_e \in \mathcal{E}_{t_e} : \; \hat{E}_e \supseteq \hat{E} \, \Big\}, \end{aligned} \tag{3.2}$$

i.e.,

$$\begin{aligned} m_1 \neq m_2 \implies \; & (\, \mathbf{x}_{m_1}(E_{e1}) \oplus V(E_1) \,) \bigcap (\, \mathbf{x}_{m_2}(E_{e2}) \oplus V(E_2) \,) = \emptyset, \\ & \textit{for all } \; E_{e1} \in \mathcal{F}_{t_e}(E_1), E_{e2} \in \mathcal{F}_{t_e}(E_2), \\ & \qquad E_1, E_2 \in \mathcal{E}_t(E_d), \;\; \textit{and } \; E_d \in \mathcal{E}_{t_d}. \end{aligned} \tag{3.3}$$

Let us illustrate (3.1)-(3.3) for two special cases : $(\tau_e, \tau_d) = (\tau, 1)$ and $(\tau_e, \tau_d) = (1, \tau)$. In the first case, Encoder knows positions where errors may occur and Decoder is ignorant (data transmission over a channel with localized errors). In the second case, Decoder is informed, while Encoder is ignorant. Omitting dependences on $[n]$, we simplify (3.1)-(3.3) as follows :

$(\tau_e, \tau_d) = (\tau, 1)$

$$\begin{aligned}
(E_e, E_d) &= (E, [n]); \\
\mathcal{E}_t(E_d) &= \mathcal{E}_t; \\
\mathcal{F}_{t_e}(\hat{E}) &= \{\hat{E}\}, \text{ for all } \hat{E} \in \mathcal{E}_t; \\
X_m &= \bigcup_{\hat{E}\in\mathcal{E}_t} \Big(\mathbf{x}_m(\hat{E}) \oplus V(\hat{E}) \Big), \ \ m \in [M]; \\
m_1 \neq m_2 &\Longrightarrow (\mathbf{x}_{m_1}(E_1) \oplus V(E_1)) \bigcap (\mathbf{x}_{m_2}(E_2) \oplus V(E_2)) = \emptyset, \\
&\quad\ \text{for all } E_1, E_2 \in \mathcal{E}_t \ ;
\end{aligned}$$

$(\tau_e, \tau_d) = (1, \tau)$

$$\begin{aligned}
(E_e, E_d) &= ([n], E); \\
\mathcal{E}_t(E_d) &= E; \\
\mathcal{F}_{t_e}(\hat{E}) &= \mathcal{E}_t, \text{ for all } \hat{E} \in \mathcal{E}_t; \\
X_m(E) &= \mathbf{x}_m \oplus V(E), \ \ m \in [M]; \\
m_1 \neq m_2 &\Longrightarrow (\mathbf{x}_{m_1} \oplus V(E)) \bigcap (\mathbf{x}_{m_2} \oplus V(E)) = \emptyset, \\
&\quad\ \text{for all } E \in \mathcal{E}_t.
\end{aligned}$$

4 Auxiliary Results

For all $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{x}' = (x'_1, \ldots, x'_n) \in \mathcal{Q}^n$, and $E \subseteq [n]$, let

$$d_E(\mathbf{x}, \mathbf{x}') = \sum_{i\in E} \chi\{ \ x_i \neq x'_i \ \}$$

be the Hamming distance between two vectors of length $|E|$ consisting of the components $x_i, i \in E$, and $x'_i, i \in E$; note that $d_{[n]}(\mathbf{x}, \mathbf{x}')$ is the Hamming distance between $\mathbf{x}$ and $\mathbf{x}'$. Hereafter, χ stands for the indicator function : $\chi\{S\} = 1$ if the statement S is true and $\chi\{S\} = 0$ otherwise.

Lemma 4.1 *If $E_1, E_2 \subseteq [n]$ and $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{Q}^n$ are assigned in such a way that*

$$\begin{cases} d_{E_1}(\mathbf{x}_1, \mathbf{x}_2) < d_{E_1^c}(\mathbf{x}_1, \mathbf{x}_2), \\ d_{E_2}(\mathbf{x}_1, \mathbf{x}_2) < d_{E_2^c}(\mathbf{x}_1, \mathbf{x}_2), \end{cases} \tag{4.1}$$

then the sets $\mathbf{x}_1 \oplus V(E_1)$ *and* $\mathbf{x}_2 \oplus V(E_2)$ *are disjoint, i.e.,*

$$(\mathbf{x}_1 \oplus V(E_1)) \bigcap (\mathbf{x}_2 \oplus V(E_2)) = \emptyset.$$

Proof Suppose that

$$\mathbf{x}_1 \oplus \mathbf{e}_1 = \mathbf{x}_2 \oplus \mathbf{e}_2, \ \text{ for some } \ (\mathbf{e}_1, \mathbf{e}_2) \in V(E_1) \times V(E_2)$$

and denote

$$(d_1, d^*, d_2) = (d_{E_1 \backslash E^*}(\mathbf{x}_1, \mathbf{x}_2), d_{E^*}(\mathbf{x}_1, \mathbf{x}_2), d_{E_2 \backslash E^*}(\mathbf{x}_1, \mathbf{x}_2)),$$

where $E^* = E_1 \cap E_2$. The i-th components of both $\mathbf{e}_1$ and $\mathbf{e}_2$ are equal to 0 for all $i \notin E_1 \cup E_2$. Therefore

$$(d_{E_1^c}(\mathbf{x}_1, \mathbf{x}_2), d_{E_2^c}(\mathbf{x}_1, \mathbf{x}_2)) = (d_2, d_1),$$

and (4.1) leads to the system of inequalities

$$\begin{cases} d_1 + d^* & < \ d_2, \\ d_2 + d^* & < \ d_1 \end{cases}$$

that does not hold since $d^* \geq 0$.

$\square$

For all $E_e \in \mathcal{E}_{t_e}$ and $\mathbf{x}, \mathbf{x}' \in \mathcal{Q}^n$, let us introduce a Boolean function $\varphi_{E_e}(\mathbf{x}, \mathbf{x}')$, which will be specified later, and denote

$$b_{E_e}(\mathbf{x}') = \left| \left\{ \mathbf{x} \in \mathcal{Q}^n : \ \varphi_{E_e}(\mathbf{x}, \mathbf{x}') = 0 \ \right\} \right|. \tag{4.2}$$

Lemma 4.2 *If*

$$b_{E_e}(\mathbf{x}') \leq c_n \cdot 2^{nf}, \ \textit{ for all } \ E_e \in \mathcal{E}_{t_e} \ \textit{ and } \ \mathbf{x}' \in \mathcal{Q}^n, \tag{4.3}$$

then there exists a code $\mathcal{C}^{(n)} = (\mathcal{L}_1, \ldots, \mathcal{L}_M)$ *with*

$$M \geq \frac{1}{2q(n+1)c_n} \cdot 2^{n(\log q - f)} \tag{4.4}$$

having the following property : for all $(m, E_e) \in [M] \times \mathcal{E}_{t_e}$*, one can find an* $\mathbf{x}_m(E_e) \in \mathcal{L}_m$ *such that*

$$\varphi_{E_e}(\mathbf{x}_m(E_e), \mathbf{x}') = 1, \ \ \textit{for all} \ \ \mathbf{x}' \in \mathcal{L}_{m'}, \ m' \in [M]\backslash\{m\}. \tag{4.5}$$

Proof Let us construct a collection consisting of M_0 lists $\hat{\mathcal{L}}_1, \ldots, \hat{\mathcal{L}}_{M_0}$ of size k in such a way that each component of every list is an independent random binary vector uniformly distributed over $\mathcal{Q}^n$. Given $m \in [M_0]$ and $E_e \in \mathcal{E}_{t_e}$, let us call $\hat{\mathcal{L}}_m$ a bad list for E_e if there exist $m' \in [M_0]\backslash\{m\}$ and $\mathbf{x}' \in \hat{\mathcal{L}}_{m'}$ such that $\varphi_{E_e}(\mathbf{x}, \mathbf{x}') = 0$ for all $\mathbf{x} \in \hat{\mathcal{L}}_m$. Let π_m denote the probability that $\hat{\mathcal{L}}_m$ is a bad list for at least one $E_e \in \mathcal{E}_{t_e}$.

If $\hat{\mathcal{L}}_{m'}, m' \in [M_0]\backslash\{m\}$, are fixed, then using (4.2) and (4.3) we can upperbound the number of possibilities to choose $\hat{\mathcal{L}}_m$ as a bad list for at least one $E_e \in \mathcal{E}_{t_e}$ as follows :

$$\sum_{E_e \in \mathcal{E}_{t_e}} \left[\sum_{\substack{m'=1 \\ m' \neq m}}^{M_0} \sum_{\mathbf{x}' \in \hat{\mathcal{L}}_{m'}} b_{E_e}(\mathbf{x}') \right]^k \leq q^n \cdot \left[M_0 k c_n \cdot 2^{nf} \right]^k.$$

This bound does not depend on $\hat{\mathcal{L}}_{m'}, m' \in [M_0]\backslash\{m\}$, and we obtain

$$\pi_m \leq (q^{-n})^k \cdot q^n \cdot \left[M_0 k c_n \cdot 2^{nf} \right]^k. \tag{4.6}$$

Let us assign

$$M_0 = \frac{1}{qkc_n} \cdot 2^{n(\log q - f)}, \ \ k = n + 1. \tag{4.7}$$

Then using (4.6) we get $\pi_m \leq 1/2$. Hence, the average number of lists $\hat{\mathcal{L}}_1, \ldots, \hat{\mathcal{L}}_{M_0}$ that are bad for at least one $E_e \in \mathcal{E}_{t_e}$ is not greater than $M_0/2$ and there exists a collection consisting of at least $M_0/2$ lists that are not bad for all $E_e \in \mathcal{E}_{t_e}$. These lists form a code with the desired property, and (4.4) follows from (4.7).

□

Note that the nonexponential coefficient in (4.4) can be improved, but this improvement does not affect asymptotics of lower bounds of the next section.

5 Lower Bounds on the Code Rate

Lemma 5.1 *Let $\mathcal{C}^{(n)} = (\mathcal{L}_1, \ldots, \mathcal{L}_M)$ be given. Suppose that, for all $(m, E_e) \in [M] \times \mathcal{E}_{t_e}$, there exists an $\mathbf{x} = \mathbf{x}_m(E_e) \in \mathcal{L}_m$ such that*

$$d_{E^c}(\mathbf{x}, \mathbf{x}') \le t_d - t,\ E \in \mathcal{E}_t(E_e) \implies d_E(\mathbf{x}, \mathbf{x}') < d_{E^c}(\mathbf{x}, \mathbf{x}'),$$

where $\mathbf{x}'$ is any element of $\mathcal{L}_{m'}$ with $m' \in [M]\backslash\{m\}$ and the set $\mathcal{E}_t(E_e)$ is defined similarly to (3.2). Then $\mathcal{C}^{(n)}$ is a $SI(t, t_e, t_d)$-code.

Proof Given an $E_e \in \mathcal{E}_{t_e}$, let us fix $(m_1, E_1), (m_2, E_2) \in [M] \times \mathcal{E}_t(E_e)$ and denote $\mathbf{x}_1 = \mathbf{x}_{m_1}(E_1)$, $\mathbf{x}_2 = \mathbf{x}_{m_2}(E_2)$. Suppose that

$$\mathbf{x}_1 \oplus \mathbf{e}_1 = \mathbf{x}_2 \oplus \mathbf{e}_2, \ \text{ for some } \ (\mathbf{e}_1, \mathbf{e}_2) \in V(E_1) \times V(E_2).$$

If $d_{E_1^c}(\mathbf{x}_1, \mathbf{x}_2) > t_d - t$, then this equation can be valid only if $|E_2 \backslash E_1| > t_d - t$. Then $|E_1 \cup E_2| > t_d$, and there is no $E_d \in \mathcal{E}_{t_d}$ such that $E_1, E_2 \in \mathcal{E}_t(E_d)$. The case when $d_{E_2^c}(\mathbf{x}_1, \mathbf{x}_2) > t_d - t$ is similar. At last, if $d_{E^c}(\mathbf{x}_1, \mathbf{x}_2) \le t_d - t$ for $E = E_1, E_2$, we use Lemma 4.1 with $\mathbf{x}_1 = \mathbf{x}_{m_1}(E_1)$, $\mathbf{x}_2 = \mathbf{x}_{m_2}(E_2)$ and complete the proof.

$\square$

Theorem

$$R_q(\tau, \tau_e, \tau_d) \ge r_q(\tau, \tau_e, \tau_d) - \frac{\log 2q(n+1)^3}{n},$$

where

$$\begin{aligned} r_q(\tau, \tau_e, \tau_d) &= \min_{(\alpha,\beta) \in \mathcal{D}_{\tau,\tau_e,\tau_d}} F_{q,\tau_e}(\alpha, \beta), \qquad (5.1) \\ \mathcal{D}_{\tau,\tau_e,\tau_d} &= \Big\{ (\alpha, \beta) \in [0, \tau_e] \times [0, 1 - \tau_e] : \ \alpha + \beta \le \tau_e, \\ &\qquad \alpha - \beta \ge \tau_e - \min\{2\tau, \tau_d\}, \\ &\qquad \beta \le \tau_d - \tau \Big\} \end{aligned}$$

and

$$\begin{aligned} F_{q,\tau_e}(\alpha, \beta) &= \log q - \tau_e \cdot h\left(\frac{\alpha}{\tau_e}\right) - (1 - \tau_e) \cdot h\left(\frac{\beta}{1 - \tau_e}\right) \qquad (5.2) \\ &\quad - (\tau_e - \alpha + \beta) \log(q - 1). \end{aligned}$$

Proof For all $E_e \in \mathcal{E}_{t_e}$ and $\mathbf{x}, \mathbf{x}' \in \mathcal{Q}^n$, let us define

$$\varphi_{E_e}(\mathbf{x}, \mathbf{x}') = 1 - \chi\left\{ \exists E \in \mathcal{E}_t(E_e) : \ d_E(\mathbf{x}, \mathbf{x}') \geq d_{E^c}(\mathbf{x}, \mathbf{x}'), \ d_{E^c}(\mathbf{x}, \mathbf{x}') \leq t_d - t \right\}.$$

Then using (4.2) we obtain

$$\begin{aligned} b_{E_e}(\mathbf{x}') \ = \ \sum_{\mathbf{x}} \chi \Big\{ \ \exists E \in \mathcal{E}_t(E_e) : \ d_E(\mathbf{x}, \mathbf{x}') \geq d_{E^c}(\mathbf{x}, \mathbf{x}'), \\ d_{E^c}(\mathbf{x}, \mathbf{x}') \leq t_d - t \quad \Big\}. \end{aligned} \tag{5.3}$$

Let us denote $i = d_{E_e}(\mathbf{x}, \mathbf{x}')$ and $j = d_{E_e^c}(\mathbf{x}, \mathbf{x}')$. If there exists an $E \in \mathcal{E}_{t_e}(E_e)$ such that

$$d_E(\mathbf{x}, \mathbf{x}') \geq d_{E^c}(\mathbf{x}, \mathbf{x}'), \ \ d_{E^c}(\mathbf{x}, \mathbf{x}') \leq t_d - t, \tag{5.4}$$

then

$$t \geq i - s_e \geq j + s_e, \ \ j + s_e \leq t_d - t, \tag{5.5}$$

where

$$s_e = d_{E_e \setminus E}(\mathbf{x}, \mathbf{x}'). \tag{5.6}$$

On the other hand, if one can find an integer $s_e \in \{0, \ldots, t_e - t\}$ satisfying (5.5), then there exists a set $E \in \mathcal{E}_{t_e}(E_e)$ such that (5.4) and (5.6) are valid. Therefore we continue (5.3) as follows :

$$\begin{aligned} b_{E_e}(\mathbf{x}') \ = \ \sum_{i=0}^{t_e} \sum_{j=0}^{n-t_e} \binom{t_e}{i} \binom{n-t_e}{j} (q-1)^{i+j} \cdot \chi \Big\{ \ \exists s_e \in \{0, \ldots, t_e - t\} : \\ t \geq i - s_e \geq s_e + j \ \text{ and } \ s_e + j \leq t_d - t \ \Big\}. \end{aligned}$$

Let $i' = t_e - i$. Since

$$\begin{aligned} t \geq i - s_e \ &\iff \ s_e \geq t_e - t - i', \\ i - s_e \geq s_e + j \ &\iff \ s_e \leq (t_e - i' - j)/2, \end{aligned}$$

the sum at the right hand side (5.3) is taken over all pairs (i, j) such that

$$\min\left\{ t_d - t - j, \frac{t_e - i' - j}{2} \right\} \geq \max\{ \ 0, t_e - t - i' \ \}.$$

Thus,

$$
\begin{aligned}
b_{E_e}(\mathbf{x}') &= \sum_{i'=0}^{t_e} \sum_{j=0}^{n-t_e} \binom{t_e}{i'} \binom{n-t_e}{j} (q-1)^{t_e-i'+j} \qquad (5.7) \\
& \cdot \chi \left\{ \, i'+j \le t_e, \;\; i'-j \ge t_e - \min\{2t, t_d\}, \;\; j \le t_d - t \, \right\}.
\end{aligned}
$$

Let $\alpha = i'/n$, $\beta = j/n$, $c_n = (n+1)^2$, and

$$
f = \max_{(\alpha,\beta)\in\mathcal{D}_{\tau,\tau_e,\tau_d}} \left[\; \log q - F_{q,\tau_e}(\alpha,\beta) \; \right],
$$

where $\mathcal{D}_{\tau,\tau_e,\tau_d}$ and $F_{q,\tau_e}(\alpha,\beta)$ are defined in (5.1) and (5.2). Since (see, for example [7], p.530)

$$
\binom{t_e}{i'} \le 2^{n\tau_e h(\alpha/\tau_e)}, \quad \binom{n-t_e}{j} \le 2^{n(1-\tau_e)h(\beta/(1-\tau_e))},
$$

we get (4.3) from (5.7), and complete the proof using Lemmas 4.2, 5.1.

□

Corollary

$$
\begin{aligned}
r_q(\tau,\tau,1) &= \begin{cases} F_{q,\tau}(\tau-\beta_q(\tau),\beta_q(\tau)), & \textit{if } \tau \le 1/2, \\ 0, & \textit{if } \tau > 1/2, \end{cases} \qquad (5.8) \\
r_q(\tau,1,\tau) &= \begin{cases} VG_q(\tau), & \textit{if } \tau \le \tau_0, \\ 0, & \textit{if } \tau > \tau_0, \end{cases} \qquad (5.9)
\end{aligned}
$$

where the function F is defined in (5.2),

$$
\begin{aligned}
\beta_q(\tau) &= \begin{cases} \tau(1-\tau), & \textit{if } q = 2, \\ \left(1 - \sqrt{1-4\omega_q\tau(1-\tau)}\right)/(2\omega_q), & \textit{if } q > 2, \end{cases} \qquad (5.10) \\
\omega_q &= \frac{(q-1)^2-1}{(q-1)^2},
\end{aligned}
$$

and

$$
VG_q(\tau) = \log q - h(\tau) - \tau \log(q-1)
$$

is the Varshamov-Gilbert bound on the rate of a code having the alphabet size q and minimal distance τn; the parameter τ_0 is defined by the equation $VG_q(\tau_0) = 0$.

If $q = 2$, then (5.8)-(5.9) are equivalent to the equation

$$r_2(\tau, \tau, 1) = r_2(\tau, 1, \tau) = 1 - h(\tau), \tag{5.11}$$

which was already presented in (2.4). Several examples of the function $r_2(\tau, \tau_e, \tau_d)$, where τ_e and τ_d linearly depend on τ, are given in Fig.3. However,

$$r_q(\tau, \tau, 1) < r_q(\tau, 1, \tau), \quad \text{for all} \quad q \geq 3, \tag{5.12}$$

and the corresponding curves are given in Fig.4 for $q = 3$, where we also show the curve corresponding to the lower bound $r_3'(\tau, \tau, 1)$ established in [5].

6 On the Balance of Knowledges of Encoder and Decoder

Let us fix $q \geq 2$ and $\tau \in [0, 1/2]$ and, for all $\delta_e \in [0, 1 - \tau]$, introduce $\delta_d(\delta_e)$ by the equation

$$r_q(\tau, \tau + \delta_e, \tau + \delta_d(\delta_e)) = r_q(\tau, \tau, 1). \tag{6.1}$$

Proposition 6.1 *If $\delta_e \in (0, 1 - \tau]$, then $\delta_d(\delta_e)$ is a monotone non-increasing function such that*

$$\delta_d(0) = 1 - \tau, \tag{6.2}$$

but

$$\lim_{\delta_e \to 0^+} \delta_d(\delta_e) = \beta_q(\tau), \tag{6.3}$$

where $\beta_q(\tau)$ is defined in (5.10).

Proof Using the definition (5.10) it is easy to check that there exists a $\delta(\tau) > 0$ such that

$$\beta_q(\tau + \delta) \leq \tau, \quad \text{for all} \quad \delta \in [0, \delta(\tau)].$$

Therefore, we analyze the case when $\delta_e \to 0^+$ assuming that

$$\beta_q(\tau + \delta_e) \leq \tau. \tag{6.4}$$

Note that

$$\frac{d}{d\delta} F_{q,\tau+\delta}(\tau + \delta - \beta_q(\tau), \beta_q(\tau)) > 0.$$

Hence,

$$F_{q,\tau+\delta_e}(\tau + \delta_e - \beta_q(\tau), \beta_q(\tau)) > F_{q,\tau}(\tau - \beta_q(\tau), \beta_q(\tau)) = r_q(\tau, \tau, 1)$$

and since

$$F_{q,\tau+\delta_e}(\tau + \delta_e - \beta_q(\tau + \delta_e), \beta_q(\tau + \delta_e)) < r_q(\tau, \tau, 1),$$

there exists a unique $\beta^* \in (\beta_q(\tau), \beta_q(\tau + \delta_e))$ such that

$$F_{q,\tau+\delta_e}(\tau + \delta_e - \beta^*, \beta^*) = r_q(\tau, \tau, 1).$$

Let us fix a $\beta \in (\beta^*, \beta_q(\tau + \delta_e)]$ and denote $\tau_d = \tau + \beta$ and $\alpha = \tau + \delta_e - \beta$. Then

$$\begin{aligned} \alpha + \beta &\leq \tau + \delta_e, \\ \alpha - \beta &\geq \tau + \delta_e - \tau_d \geq \tau + \delta_e - 2\tau, \\ \beta &\leq \tau_d - \tau, \end{aligned}$$

where (6.4) was used twice. Thus, $(\alpha, \beta) \in \mathcal{D}_{\tau,\tau+\delta_e,\tau+\beta}$ (see (5.1)) and

$$r(\tau, \tau + \delta_e, \tau + \delta_d) \leq F_{q,\tau+\delta_e}(\tau + \delta_e - \beta, \beta) < r_q(\tau, \tau, 1).$$

It means that $\delta_d(\delta_e) \leq \beta^*$. On the other hand, the pair $(\alpha^*, \beta^*) = (\tau + \delta_e - \beta^*, \beta^*)$ belongs to $\mathcal{D}_{\tau,\tau+\delta_e,\tau+\beta}$ and $\delta_d(\delta_e) = \beta^*$. When $\delta_e \to 0^+$, the length of the interval $(\beta_q(\tau), \beta_q(\tau + \delta_e))$ tends to zero. Hence, β^* tends to $\beta_q(\tau)$, and (6.3) is proved.

Equation (6.2) directly follows from (6.1).

$\square$

Based on (5.11)-(5.12), we conclude that the point $(1, \tau)$ belongs to the set of pairs $(\tau + \delta_e, \tau + \delta_d(\delta_e))$, $\delta_e \in [0, 1 - \tau]$, only if $q = 2$. Otherwise, the case when $\tau_e = 1$, i.e., Encoder is ignorant, corresponds to a pair $(1, \tau_d)$ with $\tau_d > \tau$, i.e., Decoder has to know some estimate of the set of positions where errors may occur during data transmission to make a balance. Note also that $\delta_d(\delta_e) < \delta_e$ for all $\delta_e < 1 - \tau$, which means that Decoder's knowledge gives a greater contribution to the increasing of the lower bound on the transmission rate caused by side information. The pairs $(\tau_e, \tau_d) = (\tau + \delta_e, \tau + \delta_d(\delta_e))$ are shown in Fig.5 for $q = 2, 3$.

The above considerations were based on the results of comparison of asymptotic lower bounds on the rate and cannot be viewed as a final conclusion concerning the roles of Encoder and Decoder. However, we can also take into account the following upper bound proved in [5]

$$R_q(\tau, \tau, 1) \leq VG_q(\tau) = r_q(\tau, 1, \tau),$$

i.e., the same function is simultaneously a lower bound for the case $(\tau_e, \tau_d) = (1, \tau)$ (see (5.8)) and the upper bound for the case $(\tau_e, \tau_d) = (\tau, 1)$. Note also that the Varshamov-Gilbert bound is not tight in general [8] and the exact value of $R_q(\tau, 1, \tau)$ is greater than $r_q(\tau, 1, \tau)$ at least for some q.

7 Acknowledgment

The work was initiated by the lectures of Professor Rudolf Ahlswede on coding problems for channels with localized errors. The author is also grateful to Professor Ahlswede for interesting and helpful discussions and the referees for careful reading of the manuscript and useful comments that have improved the presentation.

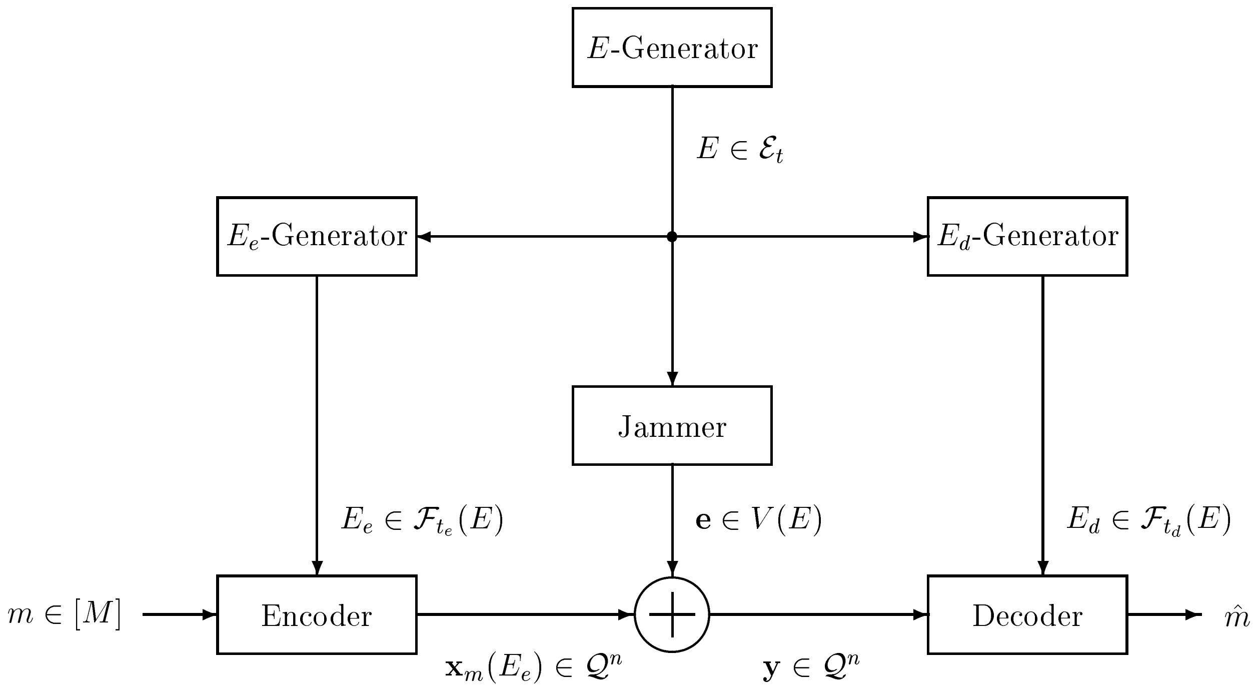

Figure 1: Model of a data transmission system with side information.

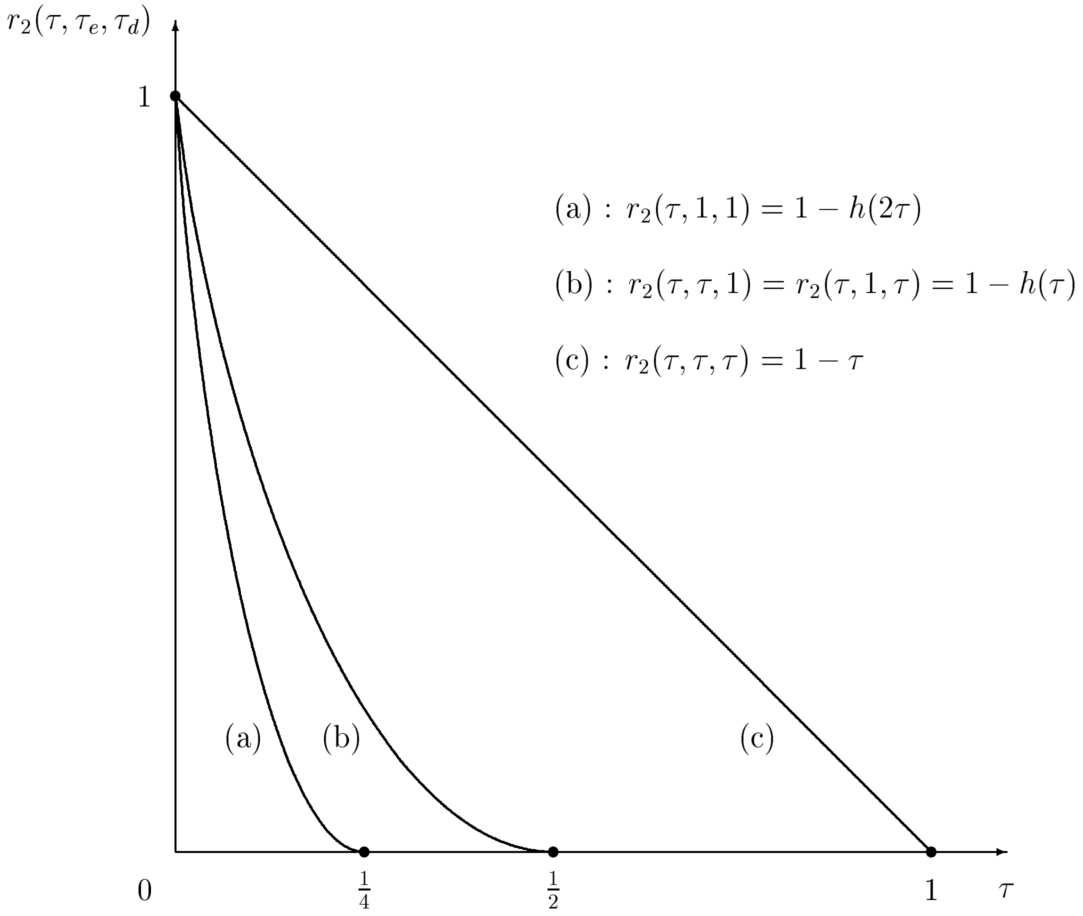

Figure 2: Lower bounds on the code rate for $\tau_e, \tau_d \in \{\tau, 1\}$ and $q = 2$. If $(\tau_e, \tau_d) = (\tau, 1), (\tau, \tau)$, then the bounds are tight.

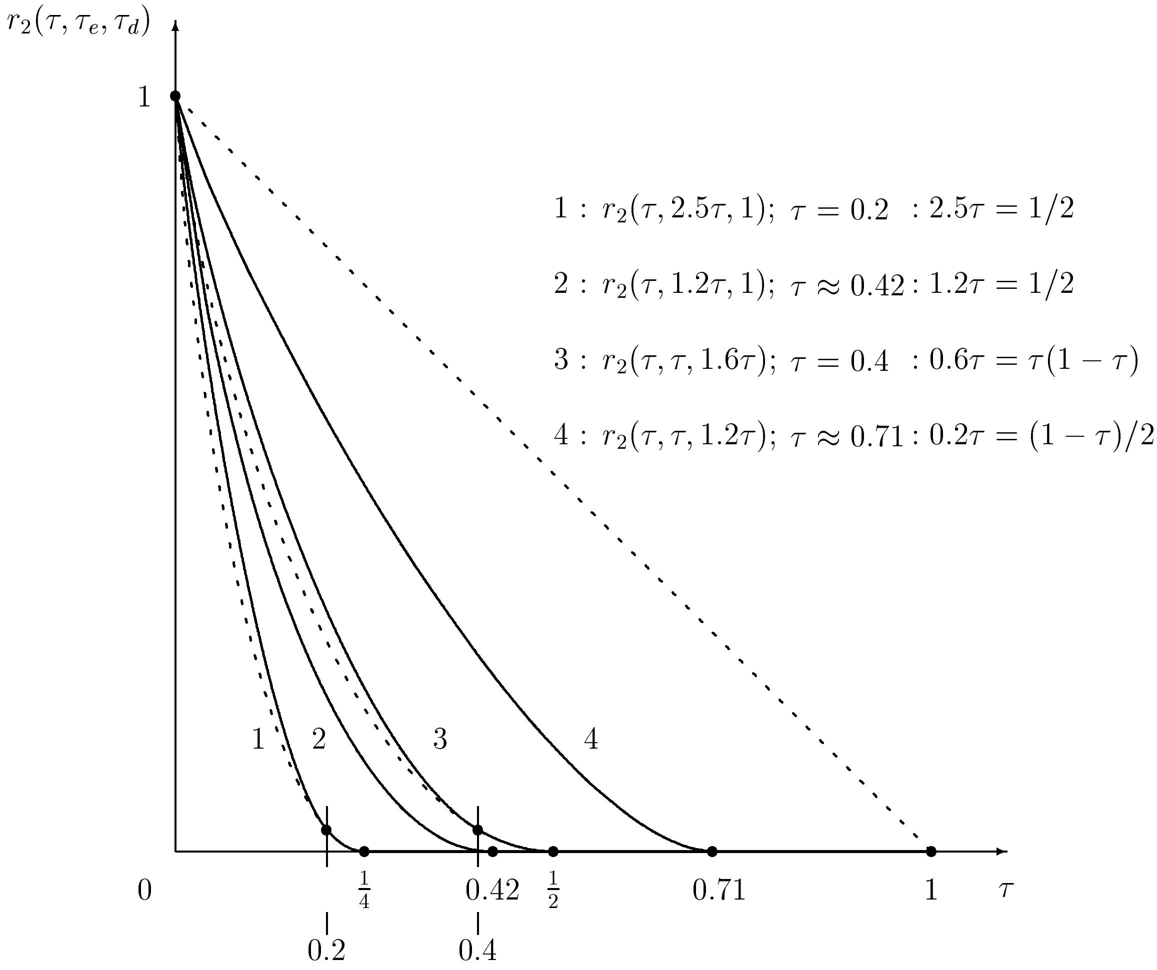

Figure 3: Lower bounds on the code rate for different $\tau_e, \tau_d \in [\tau, 1]$ and $q = 2$. The dotted curves correspond to the functions $1 - h(2\tau)$, $1 - h(\tau)$, and $1 - \tau$.

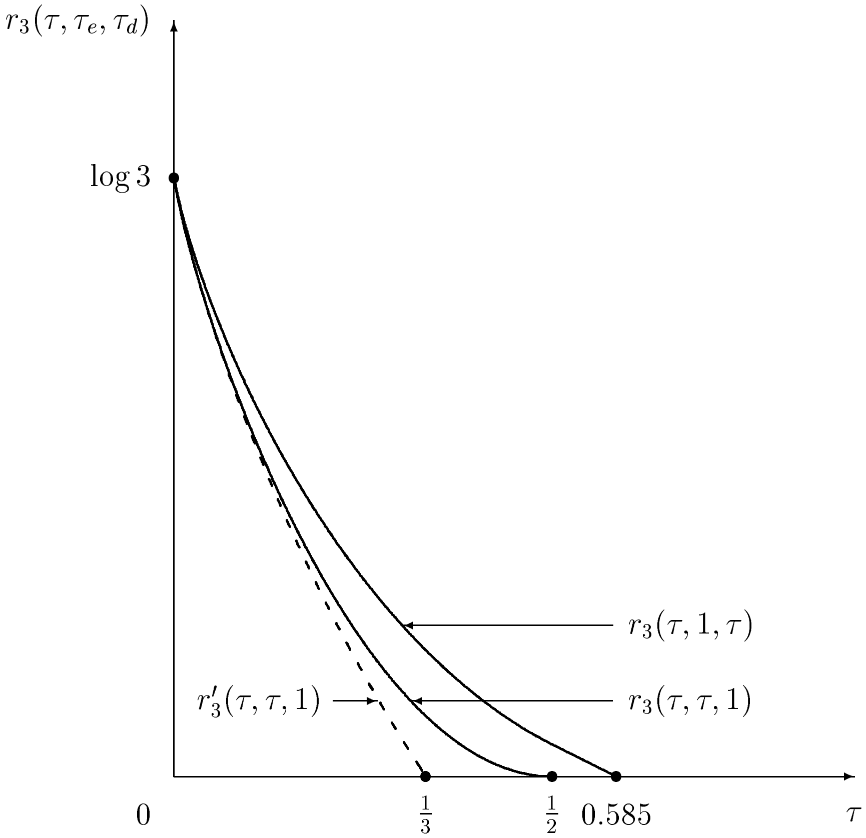

Figure 4: Lower bounds on the code rate for $(\tau_e, \tau_d) = (\tau, 1), (1, \tau)$ and $q = 3$.

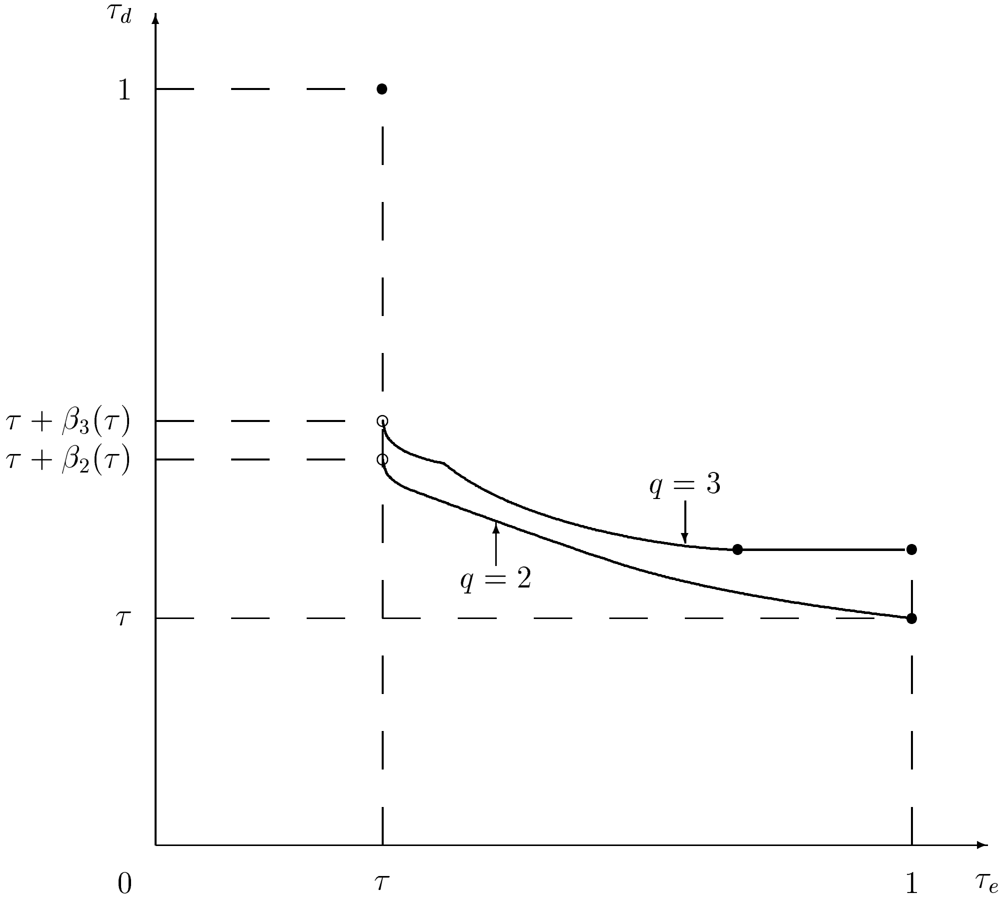

Figure 5: The pairs (τ_e, τ_d) such that $r_q(\tau, \tau_e, \tau_d) = r_q(\tau, \tau, 1)$ for $\tau = 0.3$ and $q = 2, 3$. The point $(\tau, 1)$ belongs to both curves.

References

[1] L.A.Bassalygo, S.I.Gelfand, and M.S.Pinsker, "Coding for channels with localized errors," In : *Proc. 4th Joint Swedish-Soviet Workshop Inform. Theory,* Sweden, pp.95-99, 1989.

[2] A.V.Kuznetsov and B.S.Tsybakov, "Coding in a memory with defective cells," *Problemy Peredachi Informatsii,* vol.10, no.2, pp.52-60, Apr.-June 1974.
English translation : *Probl.Inform.Transmission,* vol.10, pp.132-138, 1974.

[3] L.A.Bassalygo, S.I.Gelfand, and M.S.Pinsker, "Simple methods for deriving lower bounds in the theory of codes," *Problemy Peredachi Informatsii,* vol.27, no.4, pp.3-8, Oct.-Dec. 1991.
English translation : *Probl.Inform.Transmission,* vol.27, pp.277-281, 1991.

[4] L.A.Bassalygo, S.I.Gelfand, and M.S.Pinsker, "Coding for partially localized errors," *IEEE Trans.Inform.Theory,* vol.37, no.3, pp.880-884, May 1991.

[5] R.Ahlswede, L.A.Bassalygo, and M.S.Pinsker, "Nonbinary codes correcting localized errors," *IEEE Trans.Inform.Theory,* vol.39, no.4, pp.1413-1416, July 1993.

[6] R.Ahlswede, L.A.Bassalygo, and M.S.Pinsker, "Localized random and arbitrary errors in the light of arbitrary varying channels," *IEEE Trans.Inform.Theory,* vol.41, no.1, pp.14-25, Jan. 1995.

[7] R.G.Gallager, *Information Transmission and Reliable Communication,* New York: Wiley, 1968.

[8] M.A.Tsfasman, S.G.Vladuts, and Th.Zink, "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound," *Math.Nachr.,* vol.109, pp.21-28, 1982.