On the Hamming bound for nonbinary localized-error-correcting codes*

R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker

Abstract

For nonbinary codes it is proved that the Hamming bound is asymptotically sharp in some range of the code rate.

1. Introduction

In [1], we claimed that the transmission rate of a nonbinary (q-ary) code of length n which corrects τn localized errors asymptotically equals the Hamming bound on an interval $\tau \in [0, \tau_0]$, $\tau_0 \leq 1/2$, and conjectured that $\tau_0 = 1/2$ (transmission rate is zero if the number of errors is greater than or equal to $n/2$). Though, in recent years, we came somewhat nearer to $1/2$ and obtained τ_0 as a function of q which tends to $1/2$ with growing q, we have not succeeded in proving our conjecture. Therefore, it is apparently the right time to promulgate the derivation of the incomplete result on the Hamming bound, the more so, as the method of the proof itself is of independent interest (this is also prompted by the publication of [2], where a lower bound is presented which is everywhere significantly worse than the Hamming bound). The authors have already used a similar approach in [3], but in that paper it was accompanied by a number of additional tricks because of the complexity of the problem considered. In this paper, however, the approach is presented in a "pure" form; first, we explain the ideas only and after that proceed to formal definitions and proofs. The situation with localized errors is characterized by the following fact: to attain the Hamming bound asymptotically, it suffices to provide the decoder with "small" information (we have already used this in [4]). Indeed, let us divide the transmitted segment into a

*Supported in part by the Russian Fundamental Research Foundation (project No. 96-01-00884).

growing number of segments of equal length (the length is also growing) and arrange the segments in an ascending order with respect to the number of possible errors on them. The number of the first segment (i.e., of that with the least number of errors) and the number of a set that covers the positions of possible errors on this segment are precisely the "small" information that should be known to the decoder. Now, let us explain why this information is sufficient to attain the Hamming bound. On the first segment, outside the positions of the covering set, we transmit to the decoder the number of the second segment and the number of a set that covers the error positions on this segment. The remaining positions of the first segment are used for message transmission. On the second segment, outside the positions of the covering set, we transmit the number of the third segment and the number of a set that covers the possible errors on it; the remaining positions are used for message transmission, and so on. Surely, one can ask why we transmit covering sets but not the actual positions of possible errors, which, in fact, would leave more positions for message transmission. The answer is simple: with the optimal choice of covering sets, the gain due to their rather small number compensates the loss of positions for message transmission. Simple computations show that thus we attain the Hamming bound.

Thus, the main problem is to transmit the mentioned "small" information to the decoder. We overcome this problem (unfortunately, not for all values of the parameters) with the help of special encoding and decoding procedures. In encoding, we first construct three auxiliary code words from which the transmitted word is constructed (these auxiliary words are defined on some of n positions only and in the other positions they can be extended by zero symbols). In decoding, we construct three auxiliary "de-code" words from the word received and then reconstruct the transmitted message using them.

Transmission of "small" information is performed with the help of binary constant-weight codes that correct localized errors and defects (see [5]). To employ these codes, we proceed as follows: start the above-mentioned encoding procedure not from the first segment but from the $(k+1)$st, leaving the first k segments free (the choice of the parameter k, as well as all the other parameters, is a technical detail of the proof to which we do not turn our attention now; we note only that the total length of the first k segments is small). Then this encoding procedure generates the first q-ary codeword outside the first k segments and in positions outside the covering sets on the other segments. The unity positions of this q-ary codeword (i.e., the positions with the symbol 1 in them) are considered as the defect positions for the second binary codeword that we are going to construct (we can fix the number of unity positions of the first codeword beforehand—this is required for the paper [5] to be applicable). As the set of positions of localized errors

for the second word, we consider, together with actual such positions, all positions of the first k segments. According to [5], in this case we can choose the second binary word to be of small weight w (since, in fact, we have to transmit "small" information, namely, information of the $(k+1)$st segment and also the numbers of the first k segments), where these w unity symbols lie outside the positions of defects and localized errors. On the first k segments, we construct the third codeword of the binary localized-error-correcting code in order to transmit information of the location of w unity symbols of the second codeword and which q-ary symbols of the first codeword are in these positions. Now, from three codewords constructed (one q-ary word and two binary ones), we can construct a q-ary codeword to be transmitted:

(a) on the first k segments, we transmit the third codeword;

(b) from the second codeword, we transmit only w unity symbols;

(c) in the remaining positions, we transmit symbols of the first codeword.

In decoding, from the received word we first construct the second de-code binary word which corresponds to the second codeword transmitted over the above-described channel with defects and localized errors. To do this, we replace all symbols from 2 to $q-1$ of the received q-ary word by 0. From this word, the decoder reconstructs the "small" information to transmit which was the main difficulty. In particular, this "small" information includes the numbers of the first k segments which become known to the decoder, and thus he can construct the third de-code word which coincides on the first k segments with the received word. ¿From this word, the decoder reconstructs the symbols of the first codeword in those w positions where the unity symbols of the second codeword were transmitted. It is clear now how to construct the first de-code word: in these w positions it coincides with the first codeword and in the remaining positions outside the first k segments it coincides with the received word. Now, from this first de-code word, the decoder successively reconstructs the message starting from the $(k+1)$st segment since the "small" information previously reconstructed includes both the number of the $(k+1)$st segment and the number of the set that covers the possible error positions on this segment.

2. Statement of the problem and formulation of the main result

After explaining the ideas, let us proceed to strict statements. Let $Q = \{0, 1, \ldots, q-1\}$ be the alphabet, $\mathcal{B}$ be the set of q-ary sequences of length n, $\mathcal{M} = \{m\}$ be the set of messages ($|\mathcal{M}| = M$), $\mathcal{E}_t = \{E \mid E \subseteq [1, 2, \ldots, n], |E| = t\}$ be the set of all possible collections of error positions of multiplicity t ($|\mathcal{E}_t| = \binom{n}{t}$), $V(E)$ be the set of q-ary words of length n that are equal to zero in positions outside E ($|V(E)| = q^t$). Since, while encoding, we know those t positions where errors can occur, a codeword $x(m, E)$ depends on $m \in \mathcal{M}$ and $E \in \mathcal{E}_t$. A code $X = \{x(m, E),\ m \in \mathcal{M},\ E \in \mathcal{E}_t\}$ corrects t localized errors if the condition

$$x(m, E) + e \neq x(m', E') + e' \tag{1}$$

holds for all $E, E' \in \mathcal{E}_t$, $e \in V(E)$, $e' \in V(E')$, $m, m' \in \mathcal{M}$, $m \neq m'$ (addition in (1) is made modulo q). It is known [1] that the maximum transmission rate R of such code does not exceed the Hamming bound

$$R \leq 1 - h_q(\tau) - \tau \log_q(q-1),$$

where

$$h_q(\tau) = -\tau \log_q \tau - (1-\tau)\log_q(1-\tau), \quad t = \tau n \quad (0 \leq \tau \leq 1/2).$$

Theorem. *Let* $0 < \tau < 1/2 - \dfrac{q-2}{2q(2q-3)}$. *Then, for any* $\varepsilon > 0$, *there is a number* $n(\varepsilon)$ *such that for* $n > n(\varepsilon)$ *a code of length* n *with transmission rate* $1 - h_q(\tau) - \tau \log_q(q-1) - \varepsilon$ *exists which corrects* τn *localized errors.*

3. Proof of the theorem

Let $\varepsilon > 0$. Let us describe the encoding procedure for a given E. Divide the transmission length n into s consecutive segments $\mathcal{A}_1, \ldots, \mathcal{A}_s$ of length N ($\mathcal{A}_i = [(i-1)N + 1, \ldots, iN]$, $n = sN$, and we note in advance that both s and N tend to infinity with growing n). Denote the intersection of the ith segment $\mathcal{A}_i$ with E by E_i:

$$E_i = \mathcal{A}_i \cap E.$$

Denote the cardinality of E_i by a_i ($a_1 + \ldots + a_s = t$). Arrange the segments in an ascending order with respect to the number of possible errors on them:

$$\mathcal{A}_{i_1}, \mathcal{A}_{i_2}, \ldots, \mathcal{A}_{i_s} \quad (a_{i_1} \le a_{i_2} \le \ldots \le a_{i_s}).$$

Let us fix $\varepsilon_1, \varepsilon_2 > 0$. Put $s_1 = \varepsilon_1 s$ and define $s_1 + s_2$ as the maximum number of the segment the number of possible errors on which is not greater than $\left(\frac{q-1}{q} - \varepsilon_2\right) N$, i.e., $a_{i_{s_1+s_2}} \le \left(\frac{q-1}{q} - \varepsilon_2\right) N$ and $a_{i_{s_1+s_2+1}} > \left(\frac{q-1}{q} - \varepsilon_2\right) N$. Divide the set of the segments into three groups such that the first group consists of the first s_1 segments $\mathcal{A}_{i_1}, \ldots, \mathcal{A}_{i_{s_1}}$, the second group consists of the next s_2 segments $\mathcal{A}_{i_{s_1+1}}, \ldots, \mathcal{A}_{i_{s_1+s_2}}$, and the third group, of the remaining s_3 segments ($s_1 + s_2 + s_3 = s$). Denote by t_j, $j = 1, 2, 3$ the number of possible errors on the jth group ($t_1 + t_2 + t_3 = t$). It is clear that

$$t_1 \le \varepsilon_1 t \qquad \text{and} \qquad t_3 \ge \left(\frac{q-1}{q} - \varepsilon_2\right) N s_3. \tag{2}$$

Construction of the first codeword. Here we need the following well-known covering lemma (see, e.g., [6]).

Lemma. *Let $\mathcal{N}$ be a set with N elements and $\mathcal{N}_d$ be the set of all its subsets of cardinality d. For $d < \frac{q-1}{q} N$, a covering $C_q(\mathcal{N}_d)$ of the set $\mathcal{N}_d$ by subsets of cardinality $\frac{q}{q-1} d$ exists such that*

$$|C_q(\mathcal{N}_d)| \le N \binom{N}{d} \Big/ \binom{\frac{q}{q-1} d}{d}.$$

For $d \ge \frac{q-1}{q} N$, the covering consists of the set $\mathcal{N}$ itself, (i.e., $|C_q(\mathcal{N}_d)| = 1$).

Both the lemma and the method for constructing the first codeword have already been used in [4, Sec. V]; therefore, here we describe this procedure in brief. The first codeword is successively defined on the segments from the second group as follows: on a segment $\mathcal{A}_{i_{s_1+1}}$, we take an element of the covering $c(E_{i_{s_1+1}})$ of the set $E_{i_{s_1+1}}$ ($|c(E_{i_{s_1+1}})| = \dfrac{q}{q-1}a_{i_{s_1+1}}$) and in positions outside this element of the covering (i.e., on $\mathcal{A}_{i_{s_1+1}} \setminus c(E_{i_{s_1+1}})$) we write an arbitrary q-ary word with $\dfrac{1}{q}\left(N - \dfrac{q}{q-1}a_{i_{s_1+1}}\right)$ unity symbols; the number $B_{i_{s_1+1}}$ of such words equals

$$B_{i_{s_1+1}} = \begin{pmatrix} N - \dfrac{q}{q-1}a_{i_{s_1+1}} \\ \dfrac{1}{q}\left(N - \dfrac{q}{q-1}a_{i_{s_1+1}}\right) \end{pmatrix} (q-1)^{\left(1-\frac{1}{q}\right)\left(N-\frac{q}{q-1}a_{i_{s_1+1}}\right)}. \qquad (3)$$

These words are used to transmit the following information:

(a) the number of possible errors on the next segment, i.e., the value $a_{i_{s_1+2}}$ (there are at most N different values);

(b) the number of the set $c(E_{i_{s_1+2}})$ that covers the set $E_{i_{s_1+2}}$. By the lemma, there are at most

$$N\binom{N}{a_{i_{s_1+2}}} \Big/ \binom{\dfrac{q}{q-1}a_{i_{s_1+2}}}{a_{i_{s_1+2}}}$$

different numbers;

(c) "useful" information, i.e., information of the messages. According to (a) and (b), it accounts for at least $M_{i_{s_1+1}}$ words, where

$$M_{i_{s_1+1}} = B_{i_{s_1+1}} \binom{\dfrac{q}{q-1}a_{i_{s_1+2}}}{a_{i_{s_1+2}}} \Big/ N^2\binom{N}{a_{i_{s_1+2}}}. \qquad (4)$$

Then we pass to the segment $\mathcal{A}_{i_{s_1+2}}$ and repeat the same procedure on it, namely, consider the covering $c(E_{i_{s_1+2}})$ of the set $E_{i_{s_1+2}}$ and in positions outside this covering (i.e., on $\mathcal{A}_{i_{s_1+2}} \setminus c(E_{i_{s_1+2}})$) write an arbitrary q-ary word with $\dfrac{1}{q}\left(N - \dfrac{q}{q-1}a_{i_{s_1+2}}\right)$ unity symbols; the number $B_{i_{s_1+2}}$ of such words equals

$$B_{i_{s_1+2}} = \begin{pmatrix} N - \dfrac{q}{q-1}a_{i_{s_1+2}} \\ \dfrac{1}{q}\left(N - \dfrac{q}{q-1}a_{i_{s_1+2}}\right) \end{pmatrix} (q-1)^{\left(1-\frac{1}{q}\right)\left(N-\frac{q}{q-1}a_{s_1+2}\right)}. \qquad (5)$$

These words are used to transmit the following information:

(a) the number of possible errors on the next segment, i.e., the value $a_{i_{s_1+3}}$ (there are at most N different values);

(b) the number of the set $c(E_{i_{s_1+3}})$ that covers the set $E_{i_{s_1+3}}$. By the lemma, there are at most

$$N\binom{N}{a_{i_{s_1+3}}}\Big/\binom{\frac{q}{q-1}a_{i_{s_1+3}}}{a_{i_{s_1+3}}}$$

different numbers;

(c) "useful" information, i.e., information of the messages. According to (a) and (b), it accounts for at least $M_{i_{s_1+2}}$ words, where

$$M_{i_{s_1+2}} = B_{i_{s_1+2}}\binom{\frac{q}{q-1}a_{i_{s_1+3}}}{a_{i_{s_1+3}}}\Big/N^2\binom{N}{a_{i_{s_1+3}}}. \tag{6}$$

Denote by $\sigma(J)$ the total number of unity symbols in the first codeword constructed on J segments $\mathcal{A}_{i_{s_1+1}}, \ldots, \mathcal{A}_{i_{s_1+J}}$. According to our construction rule, $\sigma(J)$ depends not on a particular codeword, but only on the number of segments J (with E given):

$$\sigma(J) = \frac{1}{q}\left(JN - \frac{q}{q-1}\sum_{j=1}^{J} a_{i_{s_1+j}}\right). \tag{7}$$

The procedure of constructing the first codeword is terminated at the Jth step, where J is determined by the condition

$$\sigma(J) = T \stackrel{\triangle}{=} \frac{1}{q}\left((s-s_1)N - \frac{q}{q-1}t\right). \tag{8}$$

If the condition (8) is not fulfilled for any J, $J \le s_2$, then the procedure is extended on all the s_2 segments of the second group $\mathcal{A}_{i_{s_1+1}}, \ldots, \mathcal{A}_{i_{s_1+s_2}}$, and the deficit (to T) unities of the first codeword are written in error-free positions of the segments of the third group, i.e., in positions

$$\mathcal{A}_{i_{s_1+s_2+1}} \setminus E_{i_{s_1+s_2+1}},\ \ldots,\ \mathcal{A}_{i_s} \setminus E_{i_s}.$$

This is possible since

$$s_3N - t_3 + \frac{1}{q}\left(s_2N - \frac{q}{q-1}t_2\right) \ge \frac{1}{q}\left((s-s_1)N - \frac{q}{q-1}t\right).$$

Remark 1. It should be noted here that we are only interested in the behavior of the information rate, i.e., exponential behavior of the number of messages (see the statement of the theorem), but since $n = Ns$ where both N and s grow with n, a change in a finite number of symbols on segments of length N have no effect on the behavior of the rate. Therefore, though we deal only with integer numbers in formulas like (3)–(8) (and in the latter formula, we even have the equality which, generally speaking, may hold with accuracy to the length N of the segment), we do not specify this anywhere since the corresponding formal precise definitions only make the text awkward but do not affect the result.

Thus, the total number of messages that can be transmitted on the segments of the first group is not less than

$$M_1 = \prod_{j=1}^{J} M_{i_{s_1+j}}. \tag{9}$$

Also, since

$$B_{i_{s_1+j}} \geq N^{-1} q^{N - \frac{q}{q-1} a_{i_{s_1+j}}} \tag{10}$$

and

$$q^{-\frac{q}{q-1} a_{i_{s_1+j}}} \binom{\frac{q}{q-1} a_{i_{s_1+j}}}{a_{i_{s_1+j}}} \geq N^{-1} (q-1)^{-a_{i_{s_1+j}}}, \tag{11}$$

we have

$$M_1 \geq N^{-4J} q^{NJ} \Big/ \prod_{j=1}^{J} \binom{N}{a_{i_{s_1+j}}} (q-1)^{a_{i_{s_1+j}}} \geq N^{-4J} q^{NJ} V_q^{-1} \left(NJ, \sum_{j=1}^{J} a_{i_{s_1+j}} \right), \tag{12}$$

where by $V_q(B, r)$ we denote the volume of a sphere of radius r in the q-ary Hamming space of length B:

$$V_q(B, r) = \sum_{k=0}^{r} \binom{B}{k} (q-1)^k. \tag{13}$$

In the last inequality in (12), we used the obvious relation

$$V_q(B_1 + B_2, r_1 + r_2) \geq V_q(B_1, r_1) V_q(B_2, r_2). \tag{14}$$

By virtue of this relation and the inequality

$$q^B \leq B V_q \left(B, \frac{q-1}{q} B \right) \tag{15}$$

we obtain from (12) that

$$\begin{aligned} M_1 &\geq n^{-1}N^{-4J}q^{NJ+N(s-s_1-J)} \\ &\quad \times \left[V_q\left(NJ, \sum_{j=1}^{J} a_{i_{s_1+j}}\right) V_q\left(N(s-s_1-J), \frac{q-1}{q}N(s-s_1-J)\right)\right]^{-1} \\ &\geq n^{-1}N^{-4J}q^{N(s-s_1)}/V_q\left(N(s-s_1), \sum_{j=1}^{J} a_{i_{s_1+j}} + \frac{q-1}{q}N(s-s_1-J)\right) \\ &= n^{-1}N^{-4J}q^{N(s-s_1)}/V_q(N(s-s_1), t) \qquad \text{for } J \leq s_2, \end{aligned}$$

and (16)

$$\begin{aligned} M_1 &\geq n^{-1}N^{-4J}q^{Ns_2+Ns_3}/V_q(Ns_2, t_2)V_q\left(Ns_3, \frac{q-1}{q}Ns_3\right) \\ &\geq n^{-1}N^{-4J}q^{N(s_2+s_3)}/V_q(N(s_2+s_3), t_2+t_3+\varepsilon_2 Ns_3) \quad \text{otherwise.} \end{aligned}$$

For the final lower estimate of M_1, we need the following simple statement.

Claim. *Let ρ and ε_3 be positive constants and $B \to \infty$. Then a positive constant ε_4 exists such that for B large enough, the inequality*

$$V_q(B, \rho B) \leq V_q(B - \varepsilon' B, \rho B - \varepsilon'' B)q^{\varepsilon_3 B}$$

holds if $|\varepsilon'| \leq \varepsilon_4$, $|\varepsilon''| \leq \varepsilon_4$.

¿From this claim and the estimate (16) we obtain that there exist the numbers ε_1 and ε_2 (see (2)) such that for n large enough, the inequality

$$M_1 \geq \frac{q^n}{V_q(n, \tau n)}q^{-\frac{\varepsilon}{2}n} \geq q^{n\left(1-h_q(\tau)-\tau\log_q(q-1)-\varepsilon\right)} \tag{17}$$

holds. Thus, the first codeword is actually defined only in positions $\mathcal{A}_{i_{s_1+1}} \setminus c(E_{i_{s_1+1}})$, $\ldots$, $\mathcal{A}_{i_{s_1+J}} \setminus c(E_{i_{s_1+J}})$, the number of unity symbols in it equals T (see (8)), and the number of the corresponding messages satisfies the estimate (17).

Construction of the second codeword. This word belongs to a constant-weight binary code of length n with weight $w = \omega n$ which corrects $t + s_1 N = (\tau + \varepsilon_1)n$ localized errors and T single defects, where T is defined in (8), namely, $T = \frac{1}{q}\left(1 - \varepsilon_1 - \frac{q\tau}{q-1}\right)n$. Such codes were constructed in [4]; it is proved there that the rate R'' of such a code equals

$$R'' = \left(1 - \frac{1}{q}\left(1 - \varepsilon_1 - \frac{q\tau}{q-1}\right)\right)$$

$$\times \left(h_2 \left(\frac{\omega + \tau + \varepsilon_1}{1 - \frac{1}{q}\left(1 - \varepsilon_1 - \frac{q\tau}{q-1}\right)} \right) - h_2 \left(\frac{\tau + \varepsilon_1}{1 - \frac{1}{q}\left(1 - \varepsilon_1 - \frac{q\tau}{q-1}\right)} \right) \right), \quad (18)$$

where

$$0 < \omega < \frac{1}{2} - \tau - \varepsilon_1 - \frac{1}{2q}\left(1 - \varepsilon_1 - \frac{q\tau}{q-1}\right) = \frac{1}{2} - \frac{1}{2q} - \frac{(2q-3)\tau}{2(q-1)} - \varepsilon_1\left(1 - \frac{1}{2q}\right). \quad (19)$$

Moreover, it was proved in [5] that a codeword can be chosen in such a way that all of its w unity positions be outside the positions of localized errors and defects. In our case, besides the actual t positions of localized errors, we regard as localized errors all the $s_1 N$ positions of the first s_1 segments. As single defects, we regard T positions of unity symbols of the first codeword. Our attention to the precise number of single defects is due to the fact that in [5] the decoder must know the number of single defects, and the number T is known to the decoder since he knows the numbers N, s, and s_1.

Let us now specify the information that we transmit to the decoder with the help of the second codeword:

(a) the set of numbers of the first $(s_1 + 1)$ segments $i_1, i_2, \ldots, i_{s_1}, i_{s_1+1}$. The total number of different sets equals $\binom{s}{s_1+1} \le 2^s$;

(b) the number of the covering set on the (s_1+1)st segment. The total number of covering sets is not greater than $N\binom{N}{a_{i_{s_1}+1}} \Big/ \binom{\frac{q}{q-1}a_{i_{s_1}+1}}{a_{i_{s_1}+1}} \le 2^N$.

It follows from (18) that for any arbitrarily small, but fixed, ω and sufficiently large n, we can transmit this information with the help of the second codeword; the restriction on τ in the condition of the theorem follows from (19).

Construction of the third codeword. This word is constructed on the segments of the first group $\mathcal{A}_{i_1}, \ldots, \mathcal{A}_{i_{s_1}}$ and belongs to a binary code of length $s_1 N$ which corrects $\varepsilon_1 s_1 N$ localized errors. As is known [7], the rate R''' of such a code equals

$$R''' = 1 - h_2(\varepsilon_1). \quad (20)$$

Let us now specify the information transmitted to the decoder with the help of the third codeword:

(a) the number of the set of those w positions where the second codeword has unities. The number of such sets is $\binom{n}{w}$;

(b) the number of the ordered collection of symbols of the first codeword in these positions. The number of such collections is not greater than $(q-1)^w$ since, first, the first codeword can be defined on not all of w positions (we write zero symbols in positions where it is not defined) and, second, it cannot have a unity symbol in these positions according to the rule of the construction of the third codeword.

It follows from (20) that for ω small enough,

$$h_2(\omega) + \omega \log_2(q-1) < \varepsilon_1(1 - h_2(\varepsilon_1)),$$

we can transmit this information with the help of the third codeword.

Encoding and decoding. From the three codewords constructed, we can now construct the codeword to be transmitted:

(a) on the first s_1 segments $\mathcal{A}_{i_1}, \ldots, \mathcal{A}_{i_{s_1}}$, it coincides with the third codeword;

(b) it coincides with w unity positions of the second codeword;

(c) in the other positions, it coincides with the first codeword and in the positions where the first codeword is not defined, it equals zero.

After the encoding procedure is described in detail, decoding of a received word should not require a more detailed description than that given in the introduction. Indeed, if we substitute 0 for all symbols from 2 to $q-1$ in the received q-ary word, we obtain a binary word which could be received upon the transmission of the second codeword through the described-above channel with $t_1 + s_1 N$ localized errors and T single defects. Hence, the decoder can reconstruct the information transmitted with the help of the second codeword and thus reconstruct the numbers of the first $(s_1 + 1)$ segments and the covering set on the $(s_1 + 1)$st segment. Then, on the first s_1 segments, the decoder can reconstruct from the received word the information transmitted with the help of the third codeword and thus reconstruct the symbols of the first codeword in w unity positions of the second codeword. Then, starting from the (s_1+1)st segment, the decoder successively reconstructs the message from the symbols of the first codeword since all of these symbols are in error-free positions and the decoder, due to the construction of the first codeword, can reconstruct these positions on a succeeding segment from the preceding one. By (17), the number of messages satisfies the Hamming bound with accuracy to ε if $\tau + \dfrac{\tau}{2(q-1)} < \dfrac{1}{2} - \dfrac{1}{2q}$ (this restriction on τ follows from (19)). $\triangle$

Remark 2. For $\frac{1}{2} - \frac{q-2}{2q(2q-3)} \le \tau < \frac{1}{2}$, we cannot obtain the Hamming bound, but we can obtain a worse bound by decreasing the number of unity symbols in the first codeword. Taking this number to be $\lambda\Big(N(s-s_1)-\frac{qt}{q-1}\Big)$, where $0 \le \lambda \le \frac{1}{q}$, we obtain for each τ such that

$$\tau + \frac{\lambda q \tau}{2(q-1)} < \frac{1}{2} - \frac{\lambda}{2}$$

the following bound:

$$R \ge \left(1 - \frac{q}{q-1}\tau\right) h_q(\lambda) + (1-\lambda)\left(1 - \frac{q}{q-1}\tau\right)\log_q(q-1) - h_q(\tau) + \frac{q\tau}{q-1} h_q\left(\frac{1}{q}\right) - \varepsilon.$$

REFERENCES

1. R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker, "Nonbinary codes correcting localized errors," *IEEE Trans. Inf. Theory*, **39**, No. 4, 1413–1416 (1993).
2. V. B. Balakirsky, "Lower bounds on the code rate for a model of data transmission with side information," *IEEE Trans. Inf. Theory*, **44**, No. 4, 1642–1648 (1998).
3. R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker, "Asymptotically optimal binary codes of polynomial complexity correcting localized errors," *Probl. Inf. Trans.*, **31**, No. 2, 162–168 (1995).
4. R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker, "Localized random and arbitrary errors in the light of arbitrarily varying channel theory," *IEEE Trans. Inf. Theory*, **41**, No. 1, 14–25 (1995).
5. R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker, "Binary constant-weight codes correcting localized errors and defects," *Probl. Inf. Trans.*, **30**, No. 2, 102–104 (1994).
6. P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest (1974).
7. L. A. Bassalygo, S. I. Gelfand, and M. S. Pinsker, "Coding for channels with localized errors," *Proc. 4th Joint Swedish–Soviet Int. Workshop Inf. Theory*, Gotland, Sweden (1989), pp. 95–99.