ISSN 1064-2269, Journal of Communications Technology and Electronics, 2016, Vol. 61, No. 12, pp. 1440–1455. © Pleiades Publishing, Inc., 2016.
Original Russian Text © V.B. Afanassiev, A.A. Davydov, D.K. Zigangirov, 2016, published in Informatsionnye Protsessy, 2016, Vol. 16, No. 1, pp. 41–60.

THEORY AND METHODS OF INFORMATION PROCESSING

Design and Analysis of Codes with Distance 4 and 6 Minimizing the Probability of Decoder Error[1]

V. B. Afanassiev*, A. A. Davydov, and D. K. Zigangirov*****

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, 127051 Russia

**e-mail: afanv@iitp.ru*

***e-mail: adav@iitp.ru*

****e-mail: zig@iitp.ru*

Received March 10, 2016

Abstract—The problem of minimization of the decoder error probability is considered for shortened codes of dimension 2^m with distance 4 and 6. We prove that shortened Panchenko codes with distance 4 achieve the minimal probability of decoder error under special form of shortening. This shows that Hamming codes are not the best. In the paper, the rules for shortening Panchenko codes are defined and a combinatorial method to minimize the number of words of weight 4 and 5 is developed. There are obtained exact lower bounds on the probability of decoder error and the full solution of the problem of minimization of the decoder error probability for [39,32,4] and [72,64,4] codes. For shortened BCH codes with distance 6, upper and lower bounds on the number of minimal weight codewords are derived. There are constructed [45,32,6] and [79,64,6] BCH codes with the number of weight 6 codewords close to the lower bound and the decoder error probabilities are calculated for these codes. The results are intended for use in memory devices.

Keywords: binary code, probability of decoder error, code weight spectrum

DOI: 10.1134/S1064226916120020

1. INTRODUCTION

A nature of electronic memory devices, large and very large capacity, is a gradual degradation (monotonic deterioration) of their functional characteristics. Irreversible degradation of the cells is associated with the degradation (depletion) of insulating material and conductive microstructures. For example, in a cell of capacitive type with repeated cycles of read-write its charge corresponding to a binary (or multi-valued) state can be eroded. The logical state of the cell is restored after recording, but rebuilt physical condition may differ from the standard, which leads to a gradual increase of the error probability.

The article deals with the problem of constructing the best code to correct one and two errors in the random access memory (RAM) of computer systems. RAM is not suitable for long time storage and has a maximal data rate changes. Essentially, each computing operation ends by recording the result in memory. Under these conditions, there is no time to accumulate errors and the task for coding is correction of rare errors occurring due to impulse noise (effects) during recording or reading process of memory cell state. Typical structure of memory is associated with the word of standard length 32, 64, 128, 256 bits. Some check bits are added to the word to ensure the correction of one (or two) error and detection of the maximum possible number of error combinations of a greater weight. Using error-correcting codes in RAM is reviewed in many publications, for example, in [1–3]. Note that codes of distance 4 and 6 are commonly used in RAM.

As it is known the probability of decoder error depends on the code weight spectrum. Asymptotic estimates of linear code spectrum were considered in many papers, for example, in [4–6]. The exact values for individual weights of nonshortened linear codes and the full spectrum of the nonshortened Hamming code are considered, for example, in [7–9]. Algorithms to calculate the full range of weights of nonshortened cyclic codes are proposed in [10], where the values of small weights are given for BCH codes of length of 63 and 127.

In this article, *the exact values* of weights in *shortened* codes are considered.

Two classes of codes: Panchenko codes with distance 4 and Bose–Chaudhuri–Hocquenghem (BCH) codes with distance 6 are investigated. For nonshortened Panchenko code it is known only that it has the least number of words of weight 4 in comparison with

[1] The article was translated by the authors.

other codes, see [11, 12]. BCH codes are subject of interest since their decoding algorithms are well developed [7–9, 13]. For these codes, combinatorial problems of minimization of the number of small weight (4, 5, 6) codewords defining, in essence, the decoder error probability are unresolved until now.

The paper is devoted to the problem of minimization of decoder error probability for shortened codes of dimension 2^m. The special rules for shortening codes are formulated, the estimates of their weight spectrum are derived, and the results of calculation are given for the decoder error probability of shortened codes with the improved weight spectrum. For Panchenko codes, a combinatorial approach is developed that reduces the number of weight 5 codewords, under condition that the number of weight 4 words is minimal. In this paper, weight spectra of shortened and nonshortened codes are founded. The exact formula on the number of weight 5 codewords for the nonshortened code is obtained. We derive exact and achievable lower bounds on the decoder error probability for codes with 32 and 64 information bits at a given error probability in the channel. Thus, for shortened Panchenko codes the full solution of the problem of minimization of the decoder error probability is given.

For shortened BCH codes of dimension 32 and 64, we propose upper and lower estimates on the number of minimum weight 6 words and themselves shortened codes in which the number of the weight 6 words is between these estimates and fairly close to the lower bound. Such minimization of the decoder error probability seems to be practically useful.

List of notations: n—length of a code; d—minimum code distance; $d^{\perp}$—minimum distance of the dual code; $t = \left\lfloor \frac{d-1}{2} \right\rfloor$—the number of errors corrected by a code; A_w—the number of codewords of weight w; $A_w^{\perp}$—the number of codewords of weight w in the dual code; P— the error probability in the channel by symbol; $[n,k,d]$—a binary linear code of length n, dimension k, and distance d; $[n,n-r,d]$—a binary linear code of length n, redundancy r, and distance d; s—the number of non-zero weights in the code; $s^{\perp}$—the number of non-zero weights in the dual code; important constants

$$D = 2^{r-4}; \quad \overline{D} = 2^{r-4} - 1; \quad E = 5 \cdot 2^{r-5}.$$

The paper is organized as follows. Section 2 addresses codes with distance $d = 4$. The formulas for calculating the decoder error probability by code weight spectrum are given. Weight spectra of nonshortened and shortened Panchenko code and its dual code are calculated. Shortening algorithms minimizing the probability of decoder error are given. Section 3 deals with codes of distance $d = 6$. Estimates of the number of minimum weight words and BCH codes satisfying these estimates are described. In Sections 2 and 3 in a wide range of the probabilities of errors in the memory cells, for codes with the number of information symbols 32 and 64, values of the decoder error probability are calculated. Appendix rendered proofs of some theorems.

2. CODES WITH DISTANCE 4

2.1. The Probability of Decoder Error for a Code with $d = 4$

Let us consider decoding of a binary code up to its constructive distance in the binary symmetric channel with independent errors.

Let us define the *probability p_c of correct decoding* of an $[n,k,d]$, $d > 2t$, code correcting up to t errors as

$$p_c = (1-P)^n + nP(1-P)^{n-1} + \ldots + \binom{n}{t} P^t (1-P)^{n-t}. \tag{2.1}$$

Let the *probability p_e of decoding error* (or *decoder error*) be the probability that the result of errors correction is an erroneous codeword. Let the *probability p_r of decoding failure* (or *decoder rejection*) be the probability that decoder does not found a codeword at distance $\le t$ from the received word. For any code the following equality holds

$$p_c + p_e + p_r = 1. \tag{2.2}$$

Let the *probability p_{ic} of incorrect decoding* be the probability of union of the events: decoder error and decoder rejection; it is equal to

$$p_{ic} = p_e + p_r = 1 - p_c.$$

The probability of decoding error of linear block codes is considered in papers [8, 13, 14]. In the following theorem the exact formulas are given, in a form convenient for the aims of the present work.

Theorem 2.1. *The probability p_e of decoder error of a binary $[n,k,4]$ code in the binary symmetric channel with the probability P of error by symbol is equal to*

$$p_e = \sum_{w=4}^{n} A_w \left(P^{w-1}(1-P)^{n-w+1} w + P^w (1-P)^{n-w} + P^{w+1}(1-P)^{n-w-1}(n-w)\right) \tag{2.3}$$

or, equivalently,

$$p_e = P^3(1-P)^{n-3} \cdot 4A_4 + P^4(1-P)^{n-4}\left(A_4 + 5A_5\right) + \sum_{h=5}^{n} P^h (1-P)^{n-h}\left((n-h+1)A_{h-1} + A_h + (h+1)A_{h+1}\right). \tag{2.4}$$

Proof. For a linear code with code distance $d = 4$, formulas (2.3) and (2.4) can be obtained by the direct combinatorial consideration for the case of the zero word transmission. In (2.3), the expression in brackets, which is multiplied by A_w, consists of 3 terms exhausting, for a code with $d = 4$, all situations of incorrect decoding of the zero word to a weight w word. Such situations occur in the case when codeword weight is in the region $\{w-1, w, w+1\}$. In (2.4), the expression in brackets, which is multiplied by $P^h(1-P)^{n-h}$, consists of 3 terms exhausting all cases of incorrect decoding of the zero word under condition that the error multiplicity is equal to h. Such situations occur if multiplicity of error combination is in the region $\{h-1, h, h+1\}$.

If weight spectrum is unknown, it can be calculated for relatively small k or small $n-k$. In the last case we look for weight spectrum $A_w^{\perp}$ of the dual code and then use MacWilliams identities [9].

For codes of $d = 4$, that are used for error correction in RAM, we have $n-k = 7, 8, 9, 10$ and, hence, it is possible to calculate weight spectrum of the dual code. Note also that from (2.3), (2.4) it follows that for estimation of the probability p_e of decoder error it is sufficient to consider only the first components of spectrum A_4, A_5 and may be component A_6.

Let $\Delta_h(r)$ be the ratio of the number of error combinations of weight h detected by a code to the total number of errors of weight h. From (2.3), (2.4) it follows that for an $[n, n-r, 4]$ code the following equations hold:

$$\Delta_3(r) = 1 - \frac{4A_4}{\binom{n}{3}}, \quad \Delta_4(r) = 1 - \frac{A_4 + 5A_5}{\binom{n}{4}}. \qquad (2.5)$$

From Theorem 2.1 and equations (2.1), (2.2), (2.5) it follows that minimum of the decoder error probability is achieved by minimization of the number of codewords of small weights 4, 5, and 6.

2.2. The Binary Panchenko Code Π_r and Its Basic Properties

The code Π_r was proposed by V.I. Panchenko in paper [11]. The nonshortened $[n, n-r, 4]$ code Π_r has length $n = 5 \cdot 2^{r-4}$, redundancy $r \geq 5$, and code distance $d = 4$. In paper [12] the code Π_r is denoted as Π. Covering radius of the nonshortened code Π_r is equal to 2, therefore the nonshortened code Π_r is quasi-perfect.

Introduce notations. Let $B_k = [b_k \ldots b_k]$ be the matrix of identical columns b_k, where b_k is the binary representation of the integer k with the most significant bit (MSB) at the upper position. The number of rows and columns of matrix B_k will be clear from the context. Let us define matrix G as

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}. \qquad (2.6)$$

The parity check $(r \times 5 \cdot 2^{r-4})$ matrix P_r of the nonshortened code Π_r has the form

$$P_r = \begin{bmatrix} B_0 & B_1 & B_2 & \ldots & B_{\overline{D}} \\ G & G & G & \ldots & G \end{bmatrix}. \qquad (2.7)$$

In paper [12], the shortening algorithms of the code Π_r are proposed. They intend for minimization of the number A_4 of codewords of weight 4 in the following intervals of code length:

$$\max\{5 \cdot 2^{r-4} - 8, 9 \cdot 2^{r-5} - 1, 17 \cdot 2^{r-6} + 1\} \leq n \leq 5 \cdot 2^{r-4}, \qquad (2.8)$$

$$\max\{5 \cdot 2^{r-4} - 25, 17 \cdot 2^{r-6} + 1\} \leq n \leq 5 \cdot 2^{r-4}. \qquad (2.9)$$

The interval (2.8) includes $[39, 32, 4]$ and $[72, 64, 4]$ codes; the interval (2.9) includes $[137, 128, 4]$ codes.

Algorithm 1. *Shortening the matrix P_r by $i \leq 8$ columns:* for any $i \leq 8$ remove i columns strictly in the following order (from left to right):

$$\begin{bmatrix} b_\gamma \\ g_{15} \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_8 \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_4 \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_2 \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_1 \end{bmatrix}, \begin{bmatrix} b_\delta \\ g_{15} \end{bmatrix}, \begin{bmatrix} b_\nu \\ g_8 \end{bmatrix}, \begin{bmatrix} b_H \\ g_4 \end{bmatrix}, \qquad (2.10)$$

where g_u is the column of the matrix G which coincides with the binary representation of the integer u with MSB at the upper position; the columns $b_\gamma, b_\delta, b_\nu, b_H$ are different to each other.

Algorithm 2. *Shortening the matrix P_r by $i \leq 25$ columns:* remove entirely $(r \times 5)$ submatrices $\begin{bmatrix} B_u \\ G \end{bmatrix}$, where $u = k_v$, $v = 1, \ldots, f$, $f = \left\lfloor \frac{i}{5} \right\rfloor$. If $i \neq 5f$, partially remove one of the $(r \times 5)$ submatrices. Any 3 and 4 columns from the set $\{b_{k_1}, b_{k_2}, \ldots, b_{k_f}\}$ must be linear independent.

In the paper [12, Theorems 2 and 3] with using the results of paper [15] the following is proved.

Theorem 2.2. [12]

(i) *In the interval* (2.8), *a shortened by Algorithm* 1 $[n, n-r, 4]$ *code* Π_r *has the minimal number* A_4 *of weight* 4 *words and the maximal probability* $\Delta_3(r)$ *of detection of triple independent errors among all existent* $[n, n-r, 4]$ *codes including any other* (*not coinciding with Algorithm* 1) *shortenings of the code* Π_r.

(ii) *In the interval* (2.9), *a shortened by Algorithm* 2 $[n, n-r, 4]$ *code* Π_r *has the minimal number* A_4 *of weight* 4 *words and the maximal probability* $\Delta_3(r)$ *of detection of triple independent errors among all shortenings of existent codes nonequivalent to the code* Π_r. *In principle, shortenings, better than these produced by Algorithm* 2, *are possible for the code* Π_r.

Algorithm 1 can produce different variants depending on the choice of the columns $b_\gamma, b_\delta, b_\nu, b_H$. For all variants of shortening by Algorithm 1 the number of weight 4 words is the same while for other weights (5, 6 etc.) the number of words can be changed.

Algorithm 2 also has variability, but in this case the number of weight 4 words can be different for distinct variants of shortening.

2.3. Weight Spectrum of the Nonshortened Code Π_r

Theorem 2.3. *The number* $A_4^{\Pi}(r)$ *of weight* 4 *words of the nonshortened code* Π_r *is equal to*

$$A_4^{\Pi}(r) = \frac{5 \cdot 2^{r-6}(2^{r-4}-1)(2^{r-2}+5\cdot 2^{r-5}-1)}{3}. \quad (2.11)$$

Proof. From [12, equations (8),(10)] it follows that $A_4^{\Pi}(r) = \frac{1}{3}\left(10D\binom{D}{2} + \overline{D}\binom{E}{2}\right)$, whence (2.11) can be obtained by simple transformations.

Theorem 2.4. *The number* $A_5^{\Pi}(r)$ *of weight* 5 *words of the nonshortened code* Π_r *is equal to*

$$A_5^{\Pi}(r) = 2^{4r-16}. \quad (2.12)$$

Proof. The proof is presented in Appendix A.

Theorem 2.5. *Weight spectrum of the code* $\Pi_r^{\perp}$, *dual to the nonshortened code* Π_r, *is the following*

$$\begin{gathered} A_0^{\perp} = 1, \quad A_{2^{r-3}}^{\perp} = 10, \\ A_{5\cdot 2^{r-5}}^{\perp} = 2^r - 16, \quad A_{2^{r-2}}^{\perp} = 5. \end{gathered} \quad (2.13)$$

Proof. Consider the parity check matrix P_r of the code Π_r as a generator matrix of the dual code $\Pi_r^{\perp}$. It is easy to see that linear combinations of four bottom rows of this matrix has weight either $2 \cdot 2^{r-4}$ (10 combinations of one or two rows) or $4 \cdot 2^{r-4}$ (combinations of 3 or 4 rows). All linear combinations, which include at least one from upper $r/2$ rows, have weight $5 \cdot 2^{r-5}$. The number of such combinations is equal to $2^4(2^{r-4}-1)$.

Example 1. From Theorem 2.5 we see that weight spectrum of the nonshortened code $\Pi_7^{\perp}$ has the form

$$A_0^{\perp} = 1, \quad A_{16}^{\perp} = 10, \quad A_{20}^{\perp} = 112, \quad A_{32}^{\perp} = 5, \quad (2.14)$$

and weight spectrum of the nonshortened code $\Pi_8^{\perp}$ is

$$A_0^{\perp} = 1, \quad A_{32}^{\perp} = 10, \quad A_{40}^{\perp} = 240, \quad A_{64}^{\perp} = 5. \quad (2.15)$$

Now weight spectrum of the nonshortened code Π_r can be calculated using MacWilliams equations [9].

Corollary 2.1. *The words of any given weight in the nonshortened codes* Π_r *and* $\Pi_r^{\perp}$ *form a* T*-design with* $T \geq 1$.

Proof. According [9, Chapter 6], if $d^{\perp} - s \geq 1$ or $d - s^{\perp} \geq 1$, then codewords of any given weight form a T-design with T not less than $d^{\perp} - s$ or $d - s^{\perp}$. From Theorem 2.5 for the nonshortened code Π_r it holds that $d - s^{\perp} = 4 - 3 = 1$.

2.4. Weight Spectrum of the Code Π_r, *Shortened by One Symbol*

The matrix G, see. (2.6), after removing the column that is the binary representation of the integer m with MSB in the upper row, is denoted as $G_{\setminus m}$. For example,

$$G_{\setminus 4} = \begin{bmatrix} 1&0&0&1 \\ 0&0&0&1 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix}, \quad G_{\setminus 8} = \begin{bmatrix} 0&0&0&1 \\ 1&0&0&1 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix}, \quad G_{\setminus 15} = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix}. \quad (2.16)$$

Let $\Pi_{r,1}$ and $\Pi_{r,1}^{\perp}$ be the codes Π_r and $\Pi_r^{\perp}$, respectively, shortened by one symbol.

Theorem 2.6. *Weight spectrum of a code* $\Pi_{r,1}^{\perp}$, *dual to the code* Π_r *shortened by one symbol, is independent of the position of the removed symbol and has the form*

$$\begin{gathered} A_0^{\perp} = 1, \quad A_{2^{r-3}-1}^{\perp} = 4, \quad A_{2^{r-3}}^{\perp} = 6, \\ A_{5\cdot 2^{r-5}-1}^{\perp} = A_{5\cdot 2^{r-5}}^{\perp} = 2^{r-1} - 8, \\ A_{2^{r-2}-1}^{\perp} = 4, \quad A_{2^{r-2}}^{\perp} = 1. \end{gathered} \quad (2.17)$$

Proof. According to Corollary 2.1, after removing of any symbol, the number of "destroyed" and "saved" words of any given weight is independent of the removed position. Let us consider the variant of shortening defined by the parity check matrix

$$P_{r,1} = \begin{bmatrix} B_0 & B_1 & B_2 & \dots & B_{\overline{D}} \\ G_{15} & G & G & \dots & G \end{bmatrix}. \quad (2.18)$$

Let us consider three types of linear combinations of rows.

(a) Linear combination of $(r-4)$ upper rows of the matrix $P_{r,1}$.

(b) Linear combination of 4 lower rows of the matrix $P_{r,1}$.

(c) Linear combination of $(r-4)$ upper rows and 4 lower rows of the matrix $P_{r,1}$.

Denote by $L_w^{(u)}$ the number of linear combinations of rows of type u (u is a or b, or c) with weight w. From the direct consideration of matrix (2.18) it is easy to see that all possible variants of weights are given by the following list:

$$L_E^{(a)} = \overline{D}, \quad L_{2^{r-3}-1}^{(b)} = L_{2^{r-2}-1}^{(b)} = 4, \quad L_{2^{r-3}}^{(b)} = 6,$$
$$L_{2^{r-2}}^{(b)} = 1, \quad L_{E-1}^{(c)} = 8L_E^{(a)}, \quad L_E^{(c)} = 7L_E^{(a)},$$

whence the relation (2.17) follows.

Now weight spectrum of the shortened code $\Pi_{r,1}$ may be calculated using MacWilliams equations [9].

Example 2. According to (2.17), weight spectrum of a code $\Pi_{7,1}^{\perp}$, dual to the code Π_7 shortened by one symbol, is

$$A_0^{\perp} = 1, \quad A_{15}^{\perp} = 4, \quad A_{16}^{\perp} = 6,$$
$$A_{19}^{\perp} = 56, \quad A_{20}^{\perp} = 56, \quad A_{31}^{\perp} = 4, \quad A_{32}^{\perp} = 1.$$

Weight spectrum of the shortened code $\Pi_{7,1}$, calculated by MacWilliams identities, has the form

$$[A_0, A_1, \dots, A_{10}, \dots] = [1, 0, 0, 0, 1071, 3584, 26656, 118272, 481828, 1666560, 4935840, \dots]$$

2.5. Weight Spectrum of the Code Π_8, Shortened by 8 Symbols with Algorithm 1

Let $\Pi_{r,8}^{(i)}$ be the i-th variant of the code Π_r, shortened by 8 symbols with Algorithm 1. Let us denote the corresponding parity check matrix by $P_{r,8}^{(i)}$.

Theorem 2.7. (i) *The weight spectrum of the code Π_r, shortened by 8 symbols with Algorithm 1, depends only on the number of linear independent columns among the columns $b_\gamma, b_\delta, b_\nu, b_H$.*

(ii) *The code, dual to a code obtained by shortening the code Π_8 by 8 symbols with Algorithm 1, has weight spectrum of one of three types presented in Table 1.*

Proof. The proof is presented in Appendix B. Let us mention here that all columns $b_\gamma, b_\delta, b_\nu, b_H$ are different to each other and one of them may be all-zero. Therefore, among these columns can be 2, 3 or 4 linearly independent. All these cases are presented in Table 1: codes of type I (3 linear independent columns); codes of type II (2 linear independent columns); codes of type III (4 linear independent columns).

Corollary 2.2. (i) *A code, obtained by shortening the code Π_8 by 8 symbols with Algorithm 1, has one of three weight spectra the first components of which are presented in Table 2.*

(ii) *Among codes, obtained by shortening the code Π_8 by 8 symbols with Algorithm 1, the smallest number of weight 5 words is provided by a code for which the column set $b_\gamma, b_\delta, b_\nu, b_H$ contains one the zero column and exactly two columns of the rest are linear independent.*

Proof. Table 2 is obtained from Table 1 with the help of MacWilliams formulas [9]. By Table 2, a code of type II has the smallest number of weight 5 words. The structure of such code is given in the proof of Theorem 2.7 in Appendix B.

Remark. The approach applied for investigation of the code Π_8, shortened by 8 symbols with Algorithm 1, can be used for studying of shortening the code Π_9 by Algorithm 2.

2.6. The Probability of Decoder Error of a Shortened Code Π_r

In Tables 3 and 4, the results of calculations by formula (2.4) for the [39,32] code $\Pi_{7,1}^{(1)}$ and the [72,64] code $\Pi_{8,8}^{(7)}$, respectively, are given. For the calculations, weight spectra of the code $\Pi_{7,1}^{(1)}$ of Example 2 and the code $\Pi_{8,8}^{(7)}$ of Table 2 (spectrum of type II) are used. Introduce the notation

$$p_e(h) = P^h(1-P)^{n-h} \times \left((n-h+1)A_{h-1} + A_h + (h+1)A_{h+1}\right).$$

The sum $\sum_{h=3}^{8} p_e(h)$ is a lower estimate of the probability p_e of decoder error. In the considered region of input probabilities P this estimate is reasonable. An entry of the form e-b means 10^{-b}.

Table 1. Weight spectrum of codes $\Pi_{r,8}^{(i)\perp}$, dual to codes $\Pi_{r,8}^{(i)}$

Weight (general case)	The number of words, spectrum of type I	The number of words, spectrum of type II	The number of words, spectrum of type III	Weight ($r = 8$)	The number of words, spectrum of type I	The number of words, spectrum of type II	The number of words, spectrum of type III
$2^{r-3} - 4$	3	3	3	28	3	3	3
$2^{r-3} - 3$	6	6	6	29	6	6	6
$2^{r-3} - 2$	1	1	1	30	1	1	1
$E - 8$	0	0	2^{r-8}	32	0	0	1
$E - 7$	$5 \cdot 2^{r-7} - 2$	$2 \cdot 2^{r-6} - 2$	$8 \cdot 2^{r-8} - 2$	33	8	6	6
$E - 6$	$15 \cdot 2^{r-7} - 3$	$9 \cdot 2^{r-6} - 3$	$28 \cdot 2^{r-8} - 3$	34	27	33	25
$E - 5$	$25 \cdot 2^{r-7}$	$12 \cdot 2^{r-6}$	$56 \cdot 2^{r-8}$	35	50	48	56
$E - 4$	$35 \cdot 2^{r-7} - 3$	$15 \cdot 2^{r-6} - 3$	$70 \cdot 2^{r-8} - 3$	36	67	57	67
$E - 3$	$31 \cdot 2^{r-7} - 6$	$18 \cdot 2^{r-6} - 6$	$56 \cdot 2^{r-8} - 6$	37	56	66	50
$E - 2$	$13 \cdot 2^{r-7} - 1$	$7 \cdot 2^{r-6} - 1$	$28 \cdot 2^{r-8} - 1$	38	25	27	27
$E - 1$	$3 \cdot 2^{r-7}$	0	$8 \cdot 2^{r-8}$	39	6	0	8
E	$1 \cdot 2^{r-7} - 1$	$2^{r-6} - 1$	$1 \cdot 2^{r-8} - 1$	40	1	3	0
$2^{r-2} - 7$	2	2	2	57	2	2	2
$2^{r-2} - 6$	3	3	3	58	3	3	3

Table 2. Weight spectra of codes $\Pi_{8,8}^{(i)}$

Weight	The number of words, spectrum of type I	The number of words, spectrum of type II	The number of words, spectrum of type III
4	6654	6654	6654
5	38587	38586	38588
6	695798	695799	695798
7	5350816	5350848	5350784
8	48245552	48245520	48245552
9	328360512	328360016	328361008
10	2102899496	2102899992	2102899496
11	11795458880	11795463840	11795453920

For input error probabilities $P \le 0.0001$ from Tables 3 and 4 one can see that the sum $\sum_{h=3}^{8} p_e(h)$ is essentially smaller than P. Moreover, for the [39,32] code $\Pi_{7,1}^{(1)}$ the following holds.

$$\sum_{h=3}^{8} p_e(h) < 4.3 \times 10^{-(6+3j)} = 4.3P^3 \times 10^3 \quad \text{for } P = 10^{-(3+j)} \le 10^{-4}, \quad j = 1,\ldots,7. \tag{2.19}$$

For the [72, 64] code $\Pi_{8,8}^{(7)}$ the relations hold

$$\sum_{h=3}^{8} p_e(h) < 2.7 \times 10^{-(5+3j)} = 2.7P^3 \times 10^4 \quad \text{for } P = 10^{-(3+j)} \le 10^{-4}, \quad j = 1,\ldots,7. \tag{2.20}$$

It is important to note that in case $P \le 0.0001$, the summand $p_e(3)$ gives the main contribution to the

Table 3. The probability of decoder error of the [39,32] code $\Pi_{7,1}^{(1)}$ at the error probability P

P	0.0001	1.0e-05	1.0e-06	1.0e-07	1.0e-08	1.0e-09	1.0e-10
$p_e(3)$	4.27e-09	4.28e-12	4.28e-15	4.28e-18	4.28e-21	4.28e-24	4.28e-27
$p_e(4)$	1.89e-12	1.90e-16	1.90e-20	1.90e-24	1.90e-28	1.90e-32	1.90e-36
$p_e(5)$	2.00e-15	2.01e-20	2.01e-25	2.01e-30	2.01e-35	2.01e-40	2.01e-45
$p_e(6)$	9.73e-19	9.76e-25	9.76e-31	9.76e-37	9.76e-43	9.76e-49	9.76e-55
$p_e(7)$	4.84e-22	4.75e-29	4.85e-36	4.85e-43	4.85e-50	4.85e-57	4.85e-64
$p_e(8)$	1.92e-25	1.92e-33	1.93e-41	1.93e-49	1.93e-57	1.93e-65	1.93e-73
$\sum_{h=3}^{8} p_e(h)$	4.27e-09	4.28e-12	4.28e-15	4.28e-18	4.28e-21	4.28e-24	4.28e-27

Table 4. The probability of decoder error of the [72,64] code $\Pi_{8,8}^{(7)}$ at the error probability P

P	0.0001	1.0e-05	1.0e-06	1.0e-07	1.0e-08	1.0e-09	1.0e-10
$p_e(3)$	2.64e-08	2.66e-11	2.66e-14	2.66e-17	2.66e-20	2.66e-23	2.66e-26
$p_e(4)$	1.98e-11	1.99e-15	2.00e-19	2.00e-23	2.00e-27	2.00e-31	2.00e-35
$p_e(5)$	4.63e-14	4.66e-19	4.66e-24	4.67e-29	4.67e-34	4.67e-39	4.67e-44
$p_e(6)$	4.05e-17	4.07e-23	4.07e-29	4.07e-35	4.07e-41	4.07e-47	4.07e-53
$p_e(7)$	4.34e-20	4.37e-27	4.37e-34	4.37e-41	4.37e-48	4.37e-55	4.37e-62
$p_e(8)$	3.33e-23	3.35e-31	3.35e-39	3.35e-47	3.35e-55	3.35e-63	3.35e-71
$\sum_{h=3}^{8} p_e(h)$	2.64e-08	2.66e-11	2.66e-14	2.66e-17	2.66e-20	2.66e-23	2.66e-26

sum $\sum_{h=3}^{8} p_e(h)$. For the [39,32] code $\Pi_{7,1}^{(1)}$ and [72,64] code $\Pi_{8,8}^{(7)}$ the following holds.

$$\frac{p_e(3)}{p_e(h)} \approx 10^{(j+2)(h-3)}$$
$$\text{for } P = 10^{-(3+j)} \le 10^{-4}, \quad j = 1,\ldots,7. \tag{2.21}$$

We point out that for the codes $\Pi_{8,8}^{(1)}$ and $\Pi_{8,8}^{(10)}$, weight distribution of which is given in Table 2 (spectra of type I and III), the probabilities of decoder error practically coincide with those for the code $\Pi_{8,8}^{(7)}$ in Table 4. Hence, among possible variants of shortening $\Pi_{8,8}^{(i)}$ one should choose a variant more convenient for implementation.

3. CODES WITH DISTANCE 6

3.1. Estimates of the Minimum Number of Fixed Weight Words in a Shortened BCH Code with $d = 6$

Basing on the approaches of work [16], we consider *upper estimates* of the number of codewords

Theorem 3.1. *Let a binary linear $[n_0, n_0 - r, d]$ code C_{n_0} of length n_0 contain $A_w(n_0)$ words of weight w. Then there exists a shortened $[n, n-r, d]$ code C_n of length $n < n_0$ containing $A_w(n)$ words of weight w, where*

$$A_w(n) \le A_w(n_0)\frac{\binom{n_0 - w}{n - w}}{\binom{n_0}{n}}. \tag{3.1}$$

Proof. We perform shortening by removing columns from a parity check matrix H_{n_0} of the code C_{n_0}. As a result, we obtain a parity check matrix H_n of the code C_n. Every word of weight w of the code C_{n_0} corresponds to some set of w linear dependent columns of the nonshortened parity check matrix H_{n_0}. This set is saved without changes in $\binom{n_0-w}{n-w}$ shortened matrices H_n. Hence, the total number of weight w words over all shortened codes C_n is equal to $A_w(n_0)\binom{n_0-w}{n-w}$. There are $\binom{n_0}{n}$ shortened codes. By averaging over all the shortened codes we obtain (3.1).

Denote by $A_w^{\min}(n)$ the minimum possible number of weight w words in a code BCH with $d = 6$ of length n.

Corollary 3.1. *The upper bound on the minimum number of weight 6 words in an $[n, n-r, 6]$ code BCH with $d = 6$ of length $n \le n_0 = 2^m$, where $m = \frac{r-1}{2}$, is as follows*

$$A_6^{\min}(n) \le \begin{cases} \binom{n}{6}\dfrac{2^m-8}{(2^m-3)(2^m-4)(2^m-5)}, & \text{if } m \text{ odd} \\ \binom{n}{6}\dfrac{2^m-4}{(2^m-2)(2^m-3)(2^m-5)}, & \text{if } m \text{ even} \end{cases}. \tag{3.2}$$

Proof. In [7], it is shown that for nonshortened BCH codes of length $n_0 = 2^m$ we have

$$A_6(n_0 = 2^m) \le \begin{cases} \dfrac{2^m(2^m-1)(2^m-2)(2^m-8)}{720}, & \text{if } m \text{ odd} \\ \dfrac{2^m(2^m-1)(2^m-4)^2}{720}, & \text{if } m \text{ even} \end{cases}. \tag{3.3}$$

Relation (3.2) follows from (3.1) and (3.3).

In work [16], with using the results of [17], a *lower bound* on the value $A_6(n)$ is obtained by linear programming methods.

Theorem 3.2. [16] *For binary $[n, n-r, 6]$ codes with distance $d = 6$ and even distances between codewords the following estimate holds.*

$$A_6^{\min}(n) \ge \begin{cases} \dfrac{n(n-1)(n-2)(n^3-3n^2+8n-3\cdot 2^r)}{720(2^{r-1}-n)}, & \text{if } n \text{ even}, \\ \dfrac{n(n-1)(n-2)(n^3-2n^2+3n+6-3\cdot 2^r)}{720(2^{r-1}-n-1)}, & \text{if } n \text{ odd} \end{cases}. \tag{3.4}$$

3.2. Parity Check Matrices of Shortened BCH Codes with Distance $d = 6$

For error correction in a memory the following shortened codes have the most importance: $[n_m, n_m - r, 6]$ codes of length

$$n_m = 2^{m-1} + 2m + 1 = \frac{n_0}{2} + r, \quad m = \frac{r-1}{2}. \tag{3.5}$$

The number of information symbols k_m of such code is equal to a power of two:

$$k_m = n_m - r = 2^{m-1} = \frac{n_0}{2}.$$

Denote by ℓ_i the locator of the i-th position of a codeword. Let F_{2^m} be the Galois field of 2^m elements. A parity check matrix of an $[n_m, n_m - r, 6]$ BCH code with $d = 6$ can be written in the form

$$H = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \ell_1 & \ell_2 & \dots & \ell_{n_m} \\ \ell_1^3 & \ell_2^3 & \dots & \ell_{n_m}^3 \end{bmatrix} = \begin{bmatrix} J \\ H_1 \\ H_2 \end{bmatrix}, \tag{3.6}$$

$$\ell_i \in F_{2^m}, \quad n_m = 2^{m-1} + 2m + 1, \quad m = \frac{r-1}{2}.$$

In common manner, we represent the elements of the field F_{2^m} in the form of a polynomial of degree $m-1$ with binary coefficients, using degrees of a field primitive element.

In Table 5, decimal equivalents of binary columns of the matrix H_1 for $m = 6, 7$ and the corresponding

Table 5. Parity check matrices of shortened BCH codes

m	n	r	k	H_1	Lower bound $A_6^{\min}(n) \geq$	A_6	Upper bound $A_6^{\min}(n) \leq$
6	45	13	32	2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 30, 31, 34, 35, 36, 37, 40, 41, 46, 47, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63	1894	2170	2190
7	79	15	64	1, 2, 3, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 48, 49, 50, 51, 52, 53, 54, 55, 58, 59, 62, 63, 68, 69, 84, 85, 86, 87, 92, 93, 94, 95, 96, 97, 100, 101, 102, 103, 104, 105, 108, 109, 110, 111, 122, 123, 124, 125, 126, 127	16452	17375	17495

[45,32,6] and [79,64,6] BCH codes are given. The matrices are obtained by computer search. The codes under consideration have 2170 and 17375 weight 6 words, respectively; these values are smaller than the upper bound and greater than the lower bound, see (3.2), (3.4).

3.3. The Probability of Decoder Error for a Binary Code with Distance $d = 6$

Theorem 3.3. *The probability p_e of decoder error for a binary $[n,k,6]$ code in the binary symmetric channel with the probability P of error by symbol is equal to*

$$p_e = \sum_{w=6}^{n} A_w \left(P^{w-2}(1-P)^{n-w+2}\binom{w}{2} + P^{w-1}(1-P)^{n-w+1}w + P^{w}(1-P)^{n-w} \times (1+w(n-w)) + P^{w+1}(1-P)^{n-w-1}(n-w) + P^{w+2}(1-P)^{n-w-2}\binom{n-w}{2}\right) \quad (3.7)$$

or, equivalently,

$$p_e = \sum_{h=4}^{n} P^{h}(1-P)^{n-h}\left(\binom{n-h+2}{2}A_{h-2} + (n-h+1)A_{h-1} + (1+h(n-h))A_h + (n-h-1)A_{h+1} + \binom{h+2}{2}A_{h+2}\right). \quad (3.8)$$

Proof. For a linear code, formulas (3.7) and (3.8) can be obtained by the direct combinatorial consideration for the zero word transmission. In (3.7), the expression in brackets, which is multiplied by A_w, contains 5 summands exhausting all situations of incorrect decoding of the zero word to a weight w word. Such situations occur if codeword weights are in the interval $w-2 \ldots w+2$. In (3.8), the expression in brackets, which is multiplied by $P^h(1-P)^{n-h}$, contains 5 summands exhausting all situations of incorrect decoding of the zero word under condition that the error multiplicity is equal to h. Such situations occur if error multiplicity is in the interval $h-2 \ldots h+2$.

Corollary 3.2. *The probability p_e of decoder error for a binary $[n,k,6]$ code with even weights in the binary symmetric channel with the probability P of error by symbol is equal to*

$$p_e = \sum_{j=3}^{\lfloor n/2 \rfloor} A_{2j}\left(P^{2j-2}(1-P)^{n-2j+2}\binom{2j}{2} + P^{2j-1}(1-P)^{n-2j+1}\cdot 2j + P^{2j}(1-P)^{n-2j} \times (1+2j(n-2j)) + P^{2j+1}(1-P)^{n-2j-1}(n-2j) + P^{2j+2}(1-P)^{n-2j-2}\binom{n-2j}{2}\right) \quad (3.9)$$

or, equivalently,

$$p_e = P^4(1-P)^{n-4}\cdot 15A_6 + P^5(1-P)^{n-5}(n-6)A_6 + P^6(1-P)^{n-6}(6n-35)A_6 + 28A_8) + \sum_{h=7}^{n} P^h(1-P)^{n-h} \times \begin{cases} \binom{n-h+2}{2}A_{h-2} + (1+h(n-h))A_h + \binom{h+2}{2}A_{h+2}, & h \text{ even} \\ (n-h+1)A_{h-1} + (n-h-1)A_{h+1}, & h \text{ odd} \end{cases}. \quad (3.10)$$

Table 6. The probability of decodser error for the [45,32] code

P	0.001	0.0001	0.00001	0.000001	1.0 e-7	1.0 e-8	1.0 e-9	1.0 e-10
$p_e(4)$	3.124e-08	3.241e-12	3.253e-16	3.254e-20	3.254e-24	3.254e-28	3.254e-32	3.254e-36
$p_e(5)$	8.130e-11	8.429e-16	8.459e-21	8.462e-26	8.462e-31	8.462e-36	8.462e-41	8.462e-46
$\sum_{h=4}^{5} p_e(h)$	3.132e-08	3.242e-12	3.253e-16	3.254e-20	3.254e-24	3.254e-28	3.254e-32	3.254e-36

Table 7. The probability of decodser error for the [79,64] code

P	0.001	0.0001	0.00001	0.000001	1.0e-7	1.0 e-8	1.0 e-9	1.0 e-10
$p_e(4)$	2.417e-07	2.588e-11	2.604e-15	2.606e-19	2.606e-23	2.606e-27	2.606e-31	2.606e-35
$p_e(5)$	1.177e-09	1.259e-14	1.267e-19	1.268e-24	1.268e-29	1.268e-34	1.268e-39	1.268e-44
$\sum_{h=4}^{5} p_e(h)$	2.429e-07	2.588e-11	2.604e-15	2.606e-19	2.606e-23	2.606e-27	2.606e-31	2.606e-35

3.4. The Probability of Decoder Error of Shortened BCH Codes with Distance $d = 6$

The results of calculations by formula (3.10) for the [45,32] and [79,64] BCH codes are given in Tables 6 and 7, respectively. The number A_6 of weight 6 words is taken from Table 5. The notations $p_e(4) = P^4(1-P)^{n-4} \cdot 15A_6$, $p_e(5) = P^5(1-P)^{n-5}(n-6)A_6$ are used. The sum $\sum_{h=4}^{5} p_e(h)$ is a lower estimate of the probability p_e of decoder error. In the considered range of input probabilities P this estimate is reasonable.

For the input error probabilities $P \le 0.001$ from Tables 6 and 7 one can see that the sum $\sum_{h=4}^{5} p_e(h)$ is essentially smaller than P. Moreover, for the [45,32] code the following relations hold

$$\sum_{h=4}^{5} p_e(h) < 3.26 \times 10^{-(4+4j)} = 3.26P^4 \times 10^4 \quad \text{for } P = 10^{-(3+j)} \le 10^{-3}, \ j = 0,1,\ldots,7, \tag{3.11}$$

whereas for the [79,64] code we have

$$\sum_{h=4}^{5} p_e(h) < 2.61 \times 10^{-(3+4j)} = 2.61P^4 \times 10^5 \quad \text{for } P = 10^{-(3+j)} \le 10^{-3}, \ j = 0,1,\ldots,7. \tag{3.12}$$

It is important to note that for case $P \le 0.001$, the summand $p_e(4)$ gives the main contribution to the sum $\sum_{h=4}^{5} p_e(h)$. For the [45,32] code the relation holds

$$\frac{p_e(4)}{p_e(5)} \approx 10^{j+3} \quad \text{for } P = 10^{-(3+j)} \le 10^{-3}, \ j = 0,1,\ldots,7. \tag{3.13}$$

For the [79,64] code it holds that

$$\frac{p_e(4)}{p_e(5)} \approx 10^{j+2} \quad \text{for } P = 10^{-(3+j)} \le 10^{-3}, \ j = 0,1,\ldots,7. \tag{3.14}$$

4. CONCLUSIONS

Usually the problem of ensuring a high reliability of computer system memory is provided by applying error-correcting coding with correction of one or two errors in words, having 32, 64, or 128 information bits and from 6 to 14 check bits, via shortened Hamming codes and Bose-Chaudhuri-Hocquenghem (BCH) codes.

In this paper it is proved that shortened Panchenko codes with distance 4 provide the smallest probability of decoder errors under the special shortening. This shows that the Hamming codes are not the best for minimization of the decoder error probability. In the paper, the rules of shortening Panchenko codes are defined and the exact probabilities of decoder error are calculated. To obtain these results, we developed a special combinatorial approach minimizing the number of words of weight 4 as well as the number of weight 5 words. Weight spectra of nonshortened and short-

ened codes are obtained. The exact formula of the number of weight 5 words in the nonshortened code is developed. The proposed approach is applied to [39,32,4] and [72,64,4] codes. For these codes, exact lower bounds of the probability of decoder error are obtained and the problem of minimization of the decoder error probability is completely solved. The approach developed here seems to be perspective for further investigation of Panchenko codes, in particular, for obtaining effective shortening the [160,151,4] code Π_9 up to a [137,128,4] code.

For the BCH codes with distance 6, upper and lower bounds of the number of the minimum weight codewords are derived. Codes [45,32,6] and [79,64,6] are constructed for which the number of weight 6 words is between these estimates sufficiently close to the lower bound. The values of the decoder error probability for the constructed codes are calculated. The results are practically useful.

APPENDIX

A. Proof of Theorem 2.4

Consider some useful properties of the binary $\left[2^m-1, 2^m-1-m, 3\right]$ Hamming code. Denote by $A_w^H(m)$ the number of weight w words in this code. It is known [9] that

$$A_3^H(m) = \frac{1}{3}\binom{2^m-1}{2}, \quad A_4^H(m) = \frac{1}{2^m-3}\binom{2^m-1}{4}, \qquad (A.1)$$
$$A_5^H(m) = \frac{2^m-4}{5}\left(A_4^H(m) - A_3^H(m)\right).$$

Denote by $\tilde{A}_w^H(m)$ the number of weight w words in the binary $\left[2^m-1, 2^m-1-m, 3\right]$ Hamming code shortened by one symbol by removing a column of a parity check matrix.

Lemma 1. *The value $\tilde{A}_w^H(m)$ does not depend on the removed column. It holds that*

$$\tilde{A}_w^H(m) = A_w^H(m)\frac{2^m-1-w}{2^m-1}. \qquad (A.2)$$

Proof. In accordance with [9, Section 6.5, Example (E.2) (continue)], the words of every given weight w of the nonshortened $\left[2^m-1, 2^m-1-m, 3\right]$ Hamming code form a $2-(v,k,\lambda)$ design of b blocks. Just note that by definition of design parameters, we have $v = 2^m-1$, $k = w$, $b = A_w^H(m)$. According to [9, Section 2.5, Corollary (10)], in a $t-(v,k,\lambda)$ design, consisting from b blocks, every element appears exactly in $\frac{bk}{v}$ blocks. Hence, *every* column of a parity check matrix is involved in forming of exactly $\frac{A_w^H(m)\cdot w}{2^m-1}$ weight w words which will be corrupted if this column is removed. So, the value $\tilde{A}_w^H(m)$ does not depend on the removed column. Moreover, $\tilde{A}_w^H(m) = A_w^H(m) - \frac{A_w^H(m)\cdot w}{2^m-1} = A_w^H(m)\frac{2^m-1-w}{2^m-1}$.

Corollary 1. It holds that the following:

$$\tilde{A}_3^H(m) = \frac{(2^m-4)(2^{m-1}-1)}{3};$$
$$\tilde{A}_4^H(m) = \frac{(2^m-2)(2^m-4)(2^m-5)}{2\cdot 3\cdot 4}; \qquad (A.3)$$
$$\tilde{A}_5^H(m) = \left(A_4^H(m) - A_3^H(m)\right)\frac{(2^m-4)(2^m-6)}{5(2^m-1)}.$$

Proof. The validity of the formulas in (A.3) follows from (A.1), (A.2).

Lemma 2. *The last four rows of every five linear dependent columns of the parity check matrix P_r are (up to a permutation of columns) the matrix G.*

Proof. The validity of the lemma follows directly from (2.6), (2.7).

We introduce notations: $A_5^{\Pi}(r)$—the number of weight 5 words in the nonshortened code Π_r; $T_i(r)$—the number of weight 5 words of the code Π_r with the i-th structure, where i is number of the word structure; $B_k^{(i)}$—an $(r\times i)$ submatrix of the $(r\times 5)$ matrix $\begin{bmatrix} B_k \\ G \end{bmatrix}$, $1 \le i \le 5$; $\#B_k^{(i)}$—the number of possible variants of submatrix $B_k^{(i)}$ under condition that the previous submatrices of the structure are given; $\#\left[B_{k_1}^{(i)}\ldots B_{k_u}^{(j)}\right]$—the number of possible variants of submatrix $\left[B_{k_1}^{(i)}\ldots B_{k_u}^{(j)}\right]$ under condition that the previous submatrices of the structure are given; $\oplus$—the sign of binary bitwise addition of columns modulo 2.

Now we consider all possible structures of weight 5 words of the nonshortened code Π_r and find the number of words of every structure. All the arguments and calculations follow directly from (2.6), (2.7). Put $k, k_i > 0$.

Structure 1. The word of the form B_0^5. $T_1(r) = 1$.

Structure 2. Words of the form $\left[B_0^{(3)}B_k^{(2)}\right]$, $\forall k$. Here $\#B_0^{(3)} = \binom{5}{3}$, $\#B_k^{(2)} = 1$, $\#\{k\} = \overline{D}$. Therefore $T_2(r) = 10\overline{D}$.

Structure 3. Words of the form $\left[B_0^{(2)}B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}\right]$, $k_1\oplus k_2\oplus k_3 = 0$. Here $\#B_0^{(2)} = \binom{5}{2}$. For the given

triple (k_1, k_2, k_3) and the given pair of columns in B_0 it holds that $\#\left[B_{k_1}^{(1)} B_{k_2}^{(1)} B_{k_3}^{(1)}\right] = 3!$. The number of distinct triples (k_i, k_j, k_m) such that $k_i \oplus k_j \oplus k_m = 0$ is equal to $A_3^H(r-4) = \frac{1}{3}\binom{\overline{D}}{2}$. Therefore $T_3(r) = \binom{5}{2}\frac{3!}{3}\binom{\overline{D}}{2} = 20\binom{\overline{D}}{2}$.

Structure 4. Words of the form $\left[B_0^{(1)} B_k^{(4)}\right]$, $\forall k$. Here $\#B_0^{(1)} = \binom{5}{1}$, $\#B_k^{(4)} = 1$, $\#\{k\} = \overline{D}$. Therefore $T_4(r) = \binom{5}{1} \cdot 1 \cdot \overline{D} = 5\overline{D}$.

Structure 5. Words of the form $\left[B_0^{(1)} B_{k_1}^{(2)} B_{k_2}^{(2)}\right]$, $\forall k_1, k_2$. Here $\#B_0^{(1)} = \binom{5}{1}$. Also, for the given pair (k_1, k_2) and the given column in B_0 it holds that $\#\left[B_{k_1}^{(2)} B_{k_2}^{(2)}\right] = \binom{4}{2}$. The number of distinct pairs (k_1, k_2) is equal to $\binom{\overline{D}}{2}$. Therefore $T_5(r) = \binom{5}{1}\binom{4}{2}\binom{\overline{D}}{2} = 30\binom{\overline{D}}{2}$.

Structure 6. Words of the form $\left[B_0^{(1)} B_{k_1}^{(1)} B_{k_2}^{(1)} B_{k_3}^{(1)} B_{k_4}^{(1)}\right]$, $k_1 \oplus k_2 \oplus k_3 \oplus k_4 = 0$. Here $\#B_0^{(1)} = \binom{5}{1}$. Also, for the given quadruple (k_1, k_2, k_3, k_4) and the given column in B_0 it holds that $\#\left[B_{k_1}^{(1)} B_{k_2}^{(1)} B_{k_3}^{(1)} B_{k_4}^{(1)}\right] = 4!$. The number of distinct quadruples (k_i, k_j, k_m, k_u) such that $k_i \oplus k_j \oplus k_m \oplus k_u = 0$ is equal to $A_4^H(r-4) = \frac{1}{\overline{D}-2}\binom{\overline{D}}{4}$. Therefore $T_6(r) = \binom{5}{1} 4! A_4^H(r-4) = \binom{5}{1}\frac{4!}{\overline{D}-2}\binom{\overline{D}}{4} = \frac{120}{\overline{D}-2}\binom{\overline{D}}{4}$.

Structure 7. Words of the form $\left[B_{k_1}^{(3)} B_{k_2}^{(1)} B_{k_3}^{(1)}\right]$, $k_1 \oplus k_2 \oplus k_3 = 0$. Here for the given triple (k_1, k_2, k_3) it holds that $\#\left[B_{k_i}^{(3)} B_{k_j}^{(1)} B_{k_v}^{(1)}\right] = 3 \cdot \binom{5}{3} \cdot 2!$. The number of distinct triples (k_1, k_2, k_3) such that $k_1 \oplus k_2 \oplus k_3 = 0$ is equal to $A_3^H(r-4) = \frac{1}{3}\binom{\overline{D}}{2}$. Therefore $T_7(r) = 6\binom{5}{3}\frac{1}{3}\binom{\overline{D}}{2} = 20\binom{\overline{D}}{2}$.

Structure 8. Words of the form $\left[B_{k_1}^{(2)} B_{k_2}^{(1)} B_{k_3}^{(1)} B_{k_4}^{(1)}\right]$, $\forall k_1$, $k_2 \oplus k_3 \oplus k_4 = 0$. Here for the given quadruple (k_1, k_2, k_3, k_4) it holds that $\#\left[B_{k_1}^{(2)} B_{k_2}^{(1)} B_{k_3}^{(1)} B_{k_4}^{(1)}\right] = \binom{5}{2} \cdot 3! = 60$. Also, $\#\{k_1\} = \overline{D}$. The number of distinct triples $k_2 \oplus k_3 \oplus k_4 = 0$ for a chosen k_1 is equal to $\tilde{A}_3^H(r-4)$. Hence, the number of distinct quadruples is $\overline{D} \cdot \tilde{A}_3^H(r-4)$. As the result, $T_8(r) = 60\overline{D} \cdot \tilde{A}_3^H(r-4) = 20\overline{D}(2^{r-4}-4)(2^{r-5}-1)$.

Structure 9. Words of the form $\left[B_{k_1}^{(1)} B_{k_2}^{(1)} B_{k_3}^{(1)} B_{k_4}^{(1)} B_{k_5}^{(1)}\right]$, $k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 = 0$. Here for the given quintuple $(k_1, k_2, k_3, k_4, k_5)$ it holds that $\#\left[B_{k_1}^{(1)} B_{k_2}^{(1)} B_{k_3}^{(1)} B_{k_4}^{(1)} B_{k_5}^{(1)}\right] = 5!$. The number of distinct quintuples $(k_1, k_2, k_3, k_4, k_5)$ such that $k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 = 0$ is equal to $A_5^H(r-4)$. Therefore $T_9(r) = 120 A_5^H(r-4)$.

Now relation (2.12) can be obtained by addition of the values $T_i(r)$ and simple transformations. Theorem 2.4 is proved.

B. Proof of Theorem 2.7

From the structure of the parity check matrix P_r of (2.7) one can see that for shortening by Algorithm 1, weight spectrum of the dual code depends on the following facts: if columns $b_\gamma, b_\delta, b_\nu, b_H$ are zero or nonzero and if linear dependent column triples present among them. Below we write the list of variants of shortening by Algorithm 1 that, in principle, could give distinct spectra of the dual code. Number of a variant is denoted by i.

$i = 1$. $b_\gamma = 0$, $b_\delta \oplus b_\nu \oplus b_H \neq 0$.

$i = 2$. $b_\gamma \neq 0$, $b_\delta = 0$, $b_\gamma \oplus b_\nu \oplus b_H \neq 0$.

$i = 3$. $b_\gamma \neq 0$, $b_\nu = 0$, $b_\gamma \oplus b_\delta \oplus b_H \neq 0$.

$i = 4$. $b_\gamma, b_\delta, b_\nu, b_H \neq 0$, $b_\delta \oplus b_\nu \oplus b_H = 0$.

$i = 5$. $b_\gamma, b_\delta, b_\nu, b_H \neq 0$, $b_\gamma \oplus b_\delta \oplus b_\nu = 0$.

$i = 6$. $b_\gamma, b_\delta, b_\nu, b_H \neq 0$, $b_\gamma \oplus b_\nu \oplus b_H = 0$.

$i = 7$. $b_\gamma = 0$, $b_\delta \oplus b_\nu \oplus b_H = 0$.

$i = 8$. $b_\gamma \neq 0$, $b_\delta = 0$, $b_\gamma \oplus b_\nu \oplus b_H = 0$.

$i = 9$. $b_\gamma \neq 0$, $b_\nu = 0$, $b_\gamma \oplus b_\delta \oplus b_H = 0$.

$i = 10$. $b_\gamma, b_\delta, b_\nu, b_H \neq 0$, $b_\gamma, b_\delta, b_\nu, b_H$ linear independent.

From (2.6)–(2.10) one can see that for $r = 8$ this list is exhaustive.

We consider weight spectra of dual shortened code for the variants noted. Denote by $W(A)$ the matrix of all linear combinations of rows of a matrix A. If $A = B_i B_j B_k$, the number of rows and columns in submatrices B_u, as usually, is clear by the context. Note that matrices $W(GGGG)$, $W(G_{1\backslash 5}GG_{8\backslash}G_{4\backslash})$, and $W(GG_{1\backslash 5}G_{8\backslash}G_{4\backslash})$ are identical for all codes $\Pi^{(i)}_{r,8}$. Entries of type $B_{\backslash}$ mean that the submatrix B is removed for shortening a code. In tables for weight spectrum, denote by Ai, Bi, Ci data for the following objects.

Ai: linear combination of $(r-4)$ top rows of a matrix $P^{(i)}_{r,8}$.

Bi: linear combination of 4 bottom rows of a matrix $P^{(i)}_{r,8}$.

Ci: linear combination of $(r-4)$ top rows and 4 bottom rows of a matrix $P^{(i)}_{r,8}$.

$i = 1$. $b_\gamma = 0$, $b_\delta \oplus b_\nu \oplus b_H \neq 0$. Spectrum of type I.

The shortened parity check matrix has the form

$$P^{(1)}_{r,8} = \begin{bmatrix} B_{0\backslash} & B_1 & B_2 & \dots & B_{\delta\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\overline{D}} \\ G_{\backslash} & G & G & \dots & G_{1\backslash 5} & \dots & G_{8\backslash} & \dots & G_{4\backslash} & \dots & G \end{bmatrix}.$$

Condition $b_\delta \oplus b_\nu \oplus b_H \neq 0$ means that columns b_δ, b_ν, b_H are linear independent. Taking into account (2.6)–(2.10), (2.16) and the structure of the matrix $P^{(1)}_{r,8}$, it can be shown that matrix $W(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ with $b_\delta \oplus b_\nu \oplus b_H \neq 0$ has size $(2^{r-4}-1)\times 12$ and consists of 2^{r-7} sections. Everyone from $2^{r-7}-1$ identical bottom sections has size 8×12 and contains the zero top row. The top section of size 7×12 does not contain this zero row. Table 8 follows from the structures of matrices $W(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$, $W(GGGG)$, $W(GG_{1\backslash 5}G_{8\backslash}G_{4\backslash})$, $P^{(1)}_{r,8}$, and $W(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$.

$i = 2$. $b_\gamma \neq 0$, $b_\delta = 0$, $b_\gamma \oplus b_\nu \oplus b_H \neq 0$. Spectrum of type I.

The shortened parity check matrix has the form

$$P^{(2)}_{r,8} = \begin{bmatrix} B_{\delta=0} & B_1 & B_2 & \dots & B_{\gamma\neq 0\backslash} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\overline{D}} \\ G_{1\backslash 5} & G & G & \dots & G_{\backslash} & \dots & G_{8\backslash} & \dots & G_{4\backslash} & \dots & G \end{bmatrix}.$$

Condition $b_\gamma \oplus b_\nu \oplus b_H \neq 0$ means that columns b_γ, b_ν, b_H are linear independent. Taking into account (2.6)–(2.10), (2.16) and the structure of the matrix $P^{(2)}_{r,8}$, it can be shown that matrix $W(B_{\delta=0}B_{\gamma\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ with $b_\gamma \oplus b_\nu \oplus b_H \neq 0$ has size $(2^{r-4}-1)\times 17$ and consists of 2^{r-7} sections. Everyone from $2^{r-7}-1$ identical bottom sections has size 8×17 and contains the zero top row. The top section of size 7×17 does not contain this zero row. Table 9 follows from the structures of matrices $W(GGGG)$, $W(G_{1\backslash 5}GG_{8\backslash}G_{4\backslash})$, $P^{(2)}_{r,8}$, and $W(B_{\delta=0}B_{\gamma\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ for the case $b_\gamma \oplus b_\nu \oplus b_H \neq 0$.

$i = 7$. $b_\gamma = 0$, $b_\delta \oplus b_\nu \oplus b_H = 0$. Spectrum of type II.

The shortened parity check matrix has the form

$$P^{(7)}_{r,8} = \begin{bmatrix} B_{0\backslash} & B_1 & B_2 & \dots & B_{\delta\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\overline{D}} \\ G_{\backslash} & G & G & \dots & G_{1\backslash 5} & \dots & G_{8\backslash} & \dots & G_{4\backslash} & \dots & G \end{bmatrix}.$$

Condition $b_\delta \oplus b_\nu \oplus b_H = 0$ means that columns b_δ, b_ν, b_H are linear dependent. Taking into account (2.6)–(2.10), (2.16) and the structure of the matrix $P^{(7)}_{r,8}$, it can be shown that matrix $W(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ with $b_\delta \oplus b_\nu \oplus b_H = 0$ has size $(2^{r-4}-1)\times 12$ and consists of 2^{r-6} sections. Everyone from $2^{r-6}-1$ identical bottom sections has size 4×12 and contains the zero top row. The top section of size 3×12 does not contain this zero row. Table 10 follows from the structures of matrices $W(GGGG)$, $W(GG_{1\backslash 5}G_{8\backslash}G_{4\backslash})$, $P^{(7)}_{r,8}$, and $W(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ for the case $b_\delta \oplus b_\nu \oplus b_H = 0$.

$i = 10$. $b_\gamma, b_\delta, b_\nu, b_H \neq 0$, $b_\gamma, b_\delta, b_\nu, b_H$ linear independent. Spectrum of type III.

The shortened parity check matrix has the form

$$P^{(10)}_{r,8} = \begin{bmatrix} B_0 & B_1 & \dots & B_{\gamma\neq 0\backslash} & \dots & B_{\delta\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\overline{D}} \\ G & G & \dots & G_{\backslash} & \dots & G_{1\backslash 5} & \dots & G_{8\backslash} & \dots & G_{4\backslash} & \dots & G \end{bmatrix}.$$

Taking into account (2.6)–(2.10), (2.16) and the structure of matrix $P^{(10)}_{r,8}$, it can be shown that matrix $W(B_{\gamma\neq 0}B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ for the case, when $b_\gamma, b_\delta, b_\nu, b_H$ are linear independent, has size $(2^{r-4}-1)\times 17$ and consists of 2^{r-8} sections. Everyone from $2^{r-8}-1$ identical bottom sections has size 16×17 and contains the

Table 8. Weight spectrum of the code dual to the code $\Pi_{r,8}^{(1)}$. Spectrum of type I

Weight (general case)	A1 the number of words	B1 the number of words	C1 the number of words	Sum of the number of words	Weight $r = 8$	Sum of the number of words $r = 8$
$2^{r-3} - 4$		3		3	28	3
$2^{r-3} - 3$		6		6	29	6
$2^{r-3} - 2$		1		1	30	1
$E - 7$			$5 \cdot 2^{r-7} - 2$	$5 \cdot 2^{r-7} - 2$	33	8
$E - 6$			$15 \cdot 2^{r-7} - 3$	$15 \cdot 2^{r-7} - 3$	34	27
$E - 5$			$25 \cdot 2^{r-7}$	$25 \cdot 2^{r-7}$	35	50
$E - 4$			$35 \cdot 2^{r-7} - 3$	$35 \cdot 2^{r-7} - 3$	36	67
$E - 3$	$1 \cdot 2^{r-7}$		$30 \cdot 2^{r-7} - 6$	$31 \cdot 2^{r-7} - 6$	37	56
$E - 2$	$3 \cdot 2^{r-7}$		$10 \cdot 2^{r-7} - 1$	$13 \cdot 2^{r-7} - 1$	38	25
$E - 1$	$3 \cdot 2^{r-7}$			$3 \cdot 2^{r-7}$	39	6
E	$1 \cdot 2^{r-7} - 1$			$1 \cdot 2^{r-7} - 1$	40	1
$2^{r-2} - 7$		2		2	57	2
$2^{r-2} - 6$		3		3	58	3

Table 9. Weight spectrum of the code dual to the code $\Pi_{r,8}^{(2)}$

Weight (general case)	A2 the number of words	B2 the number of words	C2 the number of words	Sum of the number of words	Weight $r = 8$	Sum of the number of words $r = 8$
$2^{r-3} - 4$		3		3	28	3
$2^{r-3} - 3$		6		6	29	6
$2^{r-3} - 2$		1		1	30	1
$E - 7$	$1 \cdot 2^{r-7}$		$4 \cdot 2^{r-7} - 2$	$5 \cdot 2^{r-7} - 2$	33	8
$E - 6$	$2 \cdot 2^{r-7}$		$13 \cdot 2^{r-7} - 3$	$15 \cdot 2^{r-7} - 3$	34	27
$E - 5$	$1 \cdot 2^{r-7}$		$24 \cdot 2^{r-7}$	$25 \cdot 2^{r-7}$	35	50
$E - 4$			$35 \cdot 2^{r-7} - 3$	$35 \cdot 2^{r-7} - 3$	36	67
$E - 3$			$31 \cdot 2^{r-7} - 6$	$31 \cdot 2^{r-7} - 6$	37	56
$E - 2$	$1 \cdot 2^{r-7}$		$12 \cdot 2^{r-7} - 1$	$13 \cdot 2^{r-7} - 1$	38	25
$E - 1$	$2 \cdot 2^{r-7}$		$1 \cdot 2^{r-7}$	$3 \cdot 2^{r-7}$	39	6
E	$1 \cdot 2^{r-7} - 1$			$1 \cdot 2^{r-7} - 1$	40	1
$2^{r-2} - 7$		2		2	57	2
$2^{r-2} - 6$		3		3	58	3

Table 10. Weight spectrum of the code dual to the code $\Pi_{r,8}^{(7)}$

Weight (general case)	A7 the number of words	B7 the number of words	C7 the number of words	Sum of the number of words	Weight $r = 8$	Sum of the number of words $r = 8$
$2^{r-3} - 4$		3		3	28	3
$2^{r-3} - 3$		6		6	29	6
$2^{r-3} - 2$		1		1	30	1
$E - 7$			$2 \cdot 2^{r-6} - 2$	$2 \cdot 2^{r-6} - 2$	33	6
$E - 6$			$9 \cdot 2^{r-6} - 3$	$9 \cdot 2^{r-6} - 3$	34	33
$E - 5$			$12 \cdot 2^{r-6}$	$12 \cdot 2^{r-6}$	35	48
$E - 4$			$15 \cdot 2^{r-6} - 3$	$15 \cdot 2^{r-6} - 3$	36	57
$E - 3$			$18 \cdot 2^{r-6} - 6$	$18 \cdot 2^{r-6} - 6$	37	66
$E - 2$	$3 \cdot 2^{r-6}$		$4 \cdot 2^{r-6} - 1$	$7 \cdot 2^{r-6} - 1$	38	27
E	$2^{r-6} - 1$			$2^{r-6} - 1$	40	3
$2^{r-2} - 7$		2		2	57	2
$2^{r-2} - 6$		3		3	58	3

Table 11. Weight spectrum of the code dual to the code $\Pi_{r,8}^{(10)}$

Weight (general case)	A10 the number of words	B10 the number of words	C10 the number of words	Sum of the number of words	Weight $r = 8$	Sum of the number of words $r = 8$
$2^{r-3} - 4$		3		3	28	3
$2^{r-3} - 3$		6		6	29	6
$2^{r-3} - 2$		1		1	30	1
$E - 8$	$1 \cdot 2^{r-8}$			2^{r-8}	32	1
$E - 7$	$3 \cdot 2^{r-8}$		$5 \cdot 2^{r-8} - 2$	$8 \cdot 2^{r-8} - 2$	33	6
$E - 6$	$3 \cdot 2^{r-8}$		$25 \cdot 2^{r-8} - 3$	$28 \cdot 2^{r-8} - 3$	34	25
$E - 5$	$1 \cdot 2^{r-8}$		$55 \cdot 2^{r-8}$	$56 \cdot 2^{r-8}$	35	56
$E - 4$			$70 \cdot 2^{r-8} - 3$	$70 \cdot 2^{r-8} - 3$	36	67
$E - 3$	$1 \cdot 2^{r-8}$		$55 \cdot 2^{r-8} - 6$	$56 \cdot 2^{r-8} - 6$	37	50
$E - 2$	$3 \cdot 2^{r-8}$		$25 \cdot 2^{r-8} - 1$	$28 \cdot 2^{r-8} - 1$	38	27
$E - 1$	$3 \cdot 2^{r-8}$		$5 \cdot 2^{r-8}$	$8 \cdot 2^{r-8}$	39	8
E	$1 \cdot 2^{r-8} - 1$			$1 \cdot 2^{r-8} - 1$	40	0
$2^{r-2} - 7$		2		2	57	2
$2^{r-2} - 6$		3		3	58	3

zero top row. The top section of size 15×17 does not contain this zero row. Table 11 follows from the structures of matrices $W(GGGG)$, $W(GG_{15}G_8G_4)$, $P_{r,8}^{(10)}$, and $W(B_{\gamma\neq0}B_{\delta\neq0}B_{\nu\neq0}B_{H\neq0})$ for the case when $b_\gamma, b_\delta, b_\nu, b_H$ are linear independent.

Spectra of codes $\Pi_{r,8}^{(i)}$ with $i = 3,4,5,6,8,9$ can be obtained similarly to above-said. Spectra of codes with $i = 1,\ldots,6$ are the same; we call them spectra of type I. Spectra of codes with $i = 7,8,9$ are identical to each other; we call them spectra of type II. Finally, the code with $i = 10$ has type III. Table 1 gives the summary of all the results.

Theorem 2.7 is proved.

ACKNOWLEDGMENTS

The work was carried out at the IITP RAS at the expense of the Russian Science Foundation (project no. 14-50-00150).

REFERENCES

1. E. Fujiwara, *Code Design for Dependable Systems Theory and Practical Applications. USA* (Wiley, New Jersey, 2006).
2. R. Micheloni, A. Marelli, and R. Ravasio, *Error Correction Codes for Non-Volatile Memories* (Springer-Verlag, Qimonda Italy, 2008).
3. Yu. L. Sagalovich, "Code protection of computer random access memory from errors," Avtom. Telemekh. **52** (5), 3–45 (1991).
4. V. M. Sidel'nikov, "On spectrum of weights of binary Bose–Chaudhuri–Hocquenghem codes," Probl. Peredachi Inf. **7** (1), 14–22 (1971).
5. T. Kasami, T. Fujiwara, and S. Lin, "An approximation to the weight destitution of binary linear codes," IEEE Trans. Inf. Theory **31**, 769–780 (1985).
6. I. Krasikov and S. Litsyn, "On Spectra of BCH Codes," IEEE Trans. Inf. Theory **41**, 786–788 (1995).
7. E. R. Berlekamp, *Algebraic Coding Theory* (McGrow-Hill, New-York, 1968; Mir, Moskow, 1971).
8. T. Kassami, N. Tokura, E. Ivadari, and Ya. Inagaki, *Coding Theory* (Mir, Moscow, 1978).
9. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Publ. Company, Amsterdam, 1977).
10. A. Barg and I. Dumer, "On Computing the Weight Spectrum of Cyclic Codes," IEEE Trans. Inf. Theory **38**, 1382–1386 (1992).
11. V. I. Panchenko, "On optimization of linear code with distance 4," in *Proc. 8th All-Union Conf. on Coding Theory and Communications, Kuibyshev, 1981*, Part 2: *Coding Theory* (Moscow, 1981), pp. 132–134 [in Russian].
12. A. A. Davydov and L. M. Tombak, "An alternative to the Hamming code in the class of SEC-DED codes in semiconductor memory," IEEE Trans. Inf. Theory **37**, 897–902 (1991).
13. R. E. Blahut, *Theory and Practice of Error Control Codes* (Addison-Wesley, Reading, 1984; Mir, Moscow, 1986).
14. V. D. Kolesnik, *Error-Correcting Coding for Transmission and Storage of Information (Algebraic Theory of Block Codes)* (Vysshaya Shkola, Moscow, 2009) [in Russian].
15. A. A. Davydov and L. M. Tombak, "Quasi-perfect linear binary codes with minimal distance 4 and full caps in projective geometry," Probl. Peredachi Inf. **25** (4), 11–23 (1989).
16. A. A. Davydov, A. Yu. Drozhzhina-Labinskaya, and L. M. Tombak, "Supplementary correcting possibilities of BCH codes, correcting double and triple errors," in *Problems of Cybernetics. Complex Engineering of Elemental and Assembly Base of Super Computer*, Ed. by V. A. Mel'nikov and Yu. I. Mitropol'skii (VINITI, Moscow, 1988), pp. 86–112 [in Russian].
17. S. A. Ashmanov, *Linear Programming* (Nauka, Moscow, 1981) [in Russian].