

Weight Spectrum of Quasi-Perfect Binary Codes with Distance 4

Valentin B. Afanassiev

Institute for Information Transmission Problems
(Kharkevich institute), Russian Academy of Sciences
GSP-4, Moscow, 127994, Russian Federation
afanv@iitp.ru

Alexander A. Davydov

Institute for Information Transmission Problems
(Kharkevich institute), Russian Academy of Sciences
GSP-4, Moscow, 127994, Russian Federation
adav@iitp.ru

Abstract—We consider the weight spectrum of a class of quasi-perfect binary linear codes with code distance 4. For example, extended Hamming code and Panchenko code are the known members of this class. Also, it is known that in many cases Panchenko code has the minimal number of weight 4 codewords. We give exact recursive formulas for the weight spectrum of quasi-perfect codes and their dual codes. As an example of application of the weight spectrum we derive a lower estimate for the conditional probability of correction of erasure patterns of high weights (equal to or greater than code distance).

I. INTRODUCTION

Calculation or estimation of the weight spectrum of linear code is one of very old unresolved problem that gives rise a long list of other unresolved problems in coding theory. Binary quasi-perfect codes has a long history in investigation but with a “hole” in area of weight distribution for the most of the codes. We caught a happy chance to find a “simple” solution for weight spectrum of a whole class of binary quasi-perfect codes.

The other and real motivation for the research was to search most effective encoding and decoding schemes for error correction and error detection in computer memory. The physical volume of contemporary memory cells tends to “zero” but the probability of error or defect in a cell tends to be very critical for a whole memory device. As a consequence of this trend we need more and more effective encoding schemes for correction of independent errors and their collections in the form of two dimensional blots.

The binary quasi-perfect extended Hamming code is traditional choice for memory devices. We suggest as a better choice Panchenko code in original and product forms (for blot correction). The main our improvement over the traditional solution is the extension of the decoding area due to correction of detected errors as erasure patterns of weights equal to or greater than the code distance.

II. QUASI-PERFECT CODES CREATED BY THE DOUBLING CONSTRUCTION

Let an $[n, n - r, d]$ be a linear binary code of length n , redundancy r , and minimum distance d . For a code with redundancy r we introduce also the following notations: n_r is length of the code, H_r is its parity check matrix of size $r \times n_r$, and d_r is code distance.

Definition 1. The *doubling construction* creates a parity check matrix H_r of an $[n_r, n_r - r, d_r]$ code from a parity check matrix H_{r-1} of an $[n_{r-1}, n_{r-1} - (r-1), d_{r-1}]$ code as follows

$$H_r = \left[\begin{array}{ccc|ccc} 0 & \dots & 0 & 1 & \dots & 1 \\ \hline & & & & & \\ & & & & & \\ & & & & & \\ H_{r-1} & & & & & \\ \hline & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ H_{r-1} & & & & & \end{array} \right]. \quad (1)$$

By (1) we have $n_r = 2n_{r-1}$.

Let us define matrices S and M as

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Denote by H_r^{EH} a parity check matrix of the extended Hamming $[2^{r-1}, 2^{r-1} - r, 4]$ code, $r \geq 3$. By (1), if $H_{r-1} = M$ (resp. $H_{r-1} = H_{r-1}^{\text{EH}}$) then $H_r = H_3^{\text{EH}}$ (resp. $H_r = H_r^{\text{EH}}$). If in (1) we have $d_{r-1} = 3$ then $d_r = 3$ since the left part of H_r contains 3 linear dependent columns provided by the structure of H_{r-1} . Finally, let h_i (resp. $[0h_i]^T$ or $[1h_i]^T$) be a column of H_{r-1} (resp. H_r). If in (1) $d_{r-1} \geq 4$ then $d_r = 4$ as the sum of columns $[0h_i]^T + [0h_j]^T + [1h_i]^T + [1h_j]^T$, $i \neq j$, is equal to zero.

Definition 2. A code correcting t errors is *quasi-perfect* if its covering radius is equal to $t + 1$.

In particular, a quasi-perfect code with distance $d = 4$ has covering radius 2. Minimum distance of any code correcting t errors is equal to $2t + 1$ or $2t + 2$. A linear quasi-perfect code is “non-extendable” in the sense that addition of any column to a parity check matrix decreases the code distance. Any linear $[n, n - r, 2t + 2]$ code with $2t + 2 \geq 4$ is either a quasi-perfect one or shortening of some quasi-perfect code of redundancy r and distance $2t + 2$.

Theorem 3. [1] Let $n_r \geq 2^{r-2} + 2$, $r \geq 3$, and let an $[n_r, n_r - r, 4]$ code be quasi-perfect. Then a parity check matrix H_r of the code can be presented in the form (1) where matrix H_{r-1} is given in one of the following three variants only:

- H_{r-1} is a parity check matrix of an $[n_{r-1}, n_{r-1} - (r-1), 4]$ quasi-perfect code with $n_{r-1} = \frac{1}{2}n_r$;
- $H_{r-1} = S$;
- $H_{r-1} = M$.

Corollary 4. [1] Let $n_r \geq 2^{r-2} + 2$, $r \geq 5$, and let an $[n_r, n_r - r, 4]$ code be quasi-perfect. Then length n_r can take any value from the sequence

$$n_r = 2^{r-2} + 2^{r-2-g} \text{ for } g = 0, 2, 3, 4, 5, \dots, r-3. \quad (2)$$

Moreover, for each $g = 0, 2, 3, 4, 5, \dots, r-3$, there exists an $[n_r, n_r - r, 4]$ quasi-perfect code with $n_r = 2^{r-2} + 2^{r-2-g}$. Also, n_r may not take any other value that is not noted in (2).

Now we give a general description of a parity check matrix for whole class of quasi-perfect codes with distance 4. Let

$$B_{k,g} = [b_k \dots b_k], \quad g \in \{0, 2, 3, 4, 5, \dots, r-3\},$$

be the $(r-g-2) \times (2^g + 1)$ matrix of identical columns b_k , where $r \geq 5$ is code redundancy, b_k is the binary representation of the integer k (with the most significant bit at the top position).

Corollary 5. [1] Let $n_r = 2^{r-2} + 2^{r-2-g}$, $r \geq 5$, $g \in \{0, 2, 3, 4, 5, \dots, r-3\}$, and let an $[n_r, n_r - r, 4]$ code be quasi-perfect. Then a parity check matrix H_r of the code can be presented in the form

$$H_r = \left[\begin{array}{c|c|c|c} B_{0,g} & B_{1,g} & \dots & B_{D,g} \\ \hline \dots & \dots & \dots & \dots \\ \hline H_{g+2} & H_{g+2} & \dots & H_{g+2} \end{array} \right], \quad (3)$$

where $D = 2^{r-g-2} - 1$, $H_2 = M$, $H_4 = S$, H_{g+2} is a parity check matrix of a quasi-perfect $[2^g + 1, 2^g + 1 - (g+2), 4]$ code if $g \geq 3$.

Remark 6. By Corollary 5 a parity check matrix of any quasi-perfect binary code with length $2^{r-2} + 2^{r-2-g}$ and redundancy r can be created by $(r-g-2)$ -fold applying of the doubling construction.

As it is noted above, an arbitrary $[n, n-r, 4]$ code is either a quasi-perfect code or shortening of some quasi-perfect code with $d=4$ and redundancy r . Therefore Theorem 3, Corollaries 4, 5, and Remark 6, in fact, describe all binary linear codes with $d=4$ and length $\geq 2^{r-2} + 2$. It is why weight spectrum of codes obtained by the doubling construction (1) is an important problem.

The class of codes, say \mathcal{D} , obtained by the doubling construction is sufficiently wide. By (1), the $[2^r - 1, 2^r - 1 - r, 3]$ Hamming code and many its shortenings are included in \mathcal{D} . It follows from Theorem 3 that $[2^{r-1}, 2^{r-1} - r, 4]$ extended Hamming code and Panchenko code Π_r (see below) belong to \mathcal{D} . Other numerous non-equivalent codes of \mathcal{D} can be obtained by multiple application of the doubling construction to distinct quasi-perfect $[2^g + 1, 2^g + 1 - (g+2), 4]$ codes \mathcal{C}_0 with $g \in \{0, 2, 3, 4, 5, \dots, r-3\}$, see (3). Examples of codes \mathcal{C}_0 can be found in [1]–[3] in algebraic and in geometrical forms.

For instance, we give a parity check matrix of a quasi-perfect $[9, 9-5, 4]$ code.

$$\left[\begin{array}{c|c} 00000 & 1111 \\ 10001 & 0000 \\ 01001 & 1001 \\ 00101 & 0101 \\ 00011 & 0011 \end{array} \right].$$

The quasi-perfect codes Π_r were proposed by V.I. Panchenko in paper [4]. The $[n, n-r, 4]$ code Π_r has length $n = 5 \cdot 2^{r-4}$, redundancy $r \geq 5$, and code distance $d=4$. (In paper [5] the code Π_r is denoted as Π .)

The parity check $r \times 5 \cdot 2^{r-4}$ matrix P_r of Panchenko code Π_r is the matrix H_r of (3) with $g=2$, $D = 2^{r-4} - 1$, and $H_{g+2} = S$. So,

$$P_r = \left[\begin{array}{c|c|c|c|c} B_{0,2} & B_{1,2} & B_{2,2} & \dots & B_{D,2} \\ \hline S & S & S & \dots & S \end{array} \right]. \quad (4)$$

Remind the known [4]–[6] and important properties of Panchenko code and its shortenings:

- For all r and n , there exist a shortened Panchenko code in which the number of weight 4 codewords is close to the theoretical lower bound.

- Independently of shortening algorithm, for all r and n , the number of weight 4 codewords in Panchenko code and its shortenings is smaller than in a shortened extended Hamming code.

- For $r=7$, $n \in \{32, 33, \dots, 40\}$, and $r=8$, $n \in \{72, 73, \dots, 80\}$, Panchenko code and its shortenings by a special algorithm have the minimal number of weight 4 codewords among all other codes of the same length and redundancy.

As the consequence of this property, Panchenko code has a small (often the minimal) probability of undetected error since this probability is essentially defined by the number of weight 4 codewords. In particular, it is important for error correction in computer memory [5], [6].

III. WEIGHT SPECTRUM OF CODES CREATED BY THE DOUBLING CONSTRUCTION

By Section II, a parity check matrix of any quasi-perfect binary code with $d=4$ can be created by multiple application of the doubling construction. Therefore, Theorems 7 and 8 allow us to obtain weight spectrum of such code (and its dual) starting from weight spectrum of a short code.

We use notations introduced in the previous section. Also, for a code with redundancy r we denote by $A_w^{(r)}$ the number of codewords of weight w and by $A_w^{(r)\perp}$ the number of codewords of weight w in the dual code.

Theorem 7. Let $d_r \leq 4$. Assume that an $[n_r, n_r - r, d_r]$ code \mathcal{C}_r is created from a $[\frac{1}{2}n_r, \frac{1}{2}n_r - r + 1, d_{r-1}]$ code \mathcal{C}_{r-1} by the doubling construction (1). Then weight spectrum $\{A_w^{(r)}, d_r \leq w \leq n_r\}$ of \mathcal{C}_r can be obtained from weight spectrum $\{A_w^{(r-1)}, d_{r-1} \leq w \leq \frac{1}{2}n_r\}$ of \mathcal{C}_{r-1} as follows:

$$A_{2v}^{(r)} = \Delta_v^{(r)} + \sum_{j=0}^{v-2} 2^{2v-2j-1} A_{2v-2j}^{(r-1)} \binom{\frac{1}{2}n_r - 2v + 2j}{j} \quad (5)$$

where

$$\Delta_v^{(r)} = \begin{cases} 0 & \text{if } v \text{ odd} \\ \binom{\frac{1}{2}n_r}{v} & \text{if } v \text{ even} \end{cases};$$

$$A_{2v+1}^{(r)} = \sum_{j=0}^{v-2} 2^{2v-2j} A_{2v+1-2j}^{(r-1)} \binom{\frac{1}{2}n_r - 2v - 1 + 2j}{j}. \quad (6)$$

Proof. We consider structures of weight w codewords and the structures of the corresponding sets of w columns of a parity check matrix.

Let $u \in \{r, r-1\}$. Let $c_{w,u}$ be a weight w codeword of the code \mathcal{C}_u . Denote by $H_{r-1}(c_{w,u})$ the set of w columns of the matrix H_u corresponding to the codeword $c_{w,u}$. By definition, the sum of all columns of $H_u(c_{w,u})$ is equal to zero.

We describe column sets of H_r in (1) with the help of column sets of H_{r-1} placed in the left and right sides of (1).

(i) Let us consider all possible structures of codewords $c_{2v,r}$ of **even weight** $2v$ and the corresponding column sets $H_r(c_{2v,r})$ in the matrix H_r of (1). Every such column set consists of the following components:

- A column set $H_{r-1}(c_{2v-2j,r-1})$ partitioned by two parts that are placed in the left and right sides of H_r .
- Two sets of the same j columns of H_{r-1} placed in the left and right sides of H_r . (These column sets are not connected with any codewords of \mathcal{C}_{r-1} .)

For $j = 0, 1, \dots, v-2$ and for every codeword $c_{2v-2j,r-1}$ of even weight, we explain summands of the formula (5).

- The summand $\sum_{j=0}^{v-2} 2^{2v-2j-1} A_{2v-2j}^{(r-1)} \binom{\frac{1}{2}n_r - 2v + 2j}{j}$ of (5).

A column set $\Gamma = H_{r-1}(c_{2v-2j,r-1})$ is partitioned by two parts. Every part contains an odd (resp. even) number of columns if j is odd (resp. even). The partition is executed by all possible ways. The number of the partitions is equal to $2^{2v-2j-1}$. The obtained parts are placed in the left and right sides of H_r .

Also, in every of two submatrices H_{r-1} of (1) we take the same set of j columns that do not belong to Γ . The number of such j -sets is equal to $\binom{\frac{1}{2}n_r - 2v + 2j}{j}$. As a result, in the right side of H_r we always take an even number of columns.

- The summand $\Delta_v^{(r)} = \binom{\frac{1}{2}n_r}{v}$ of (5).

If v is even then in every of two submatrices H_{r-1} of (1) we take the same set of v columns. The number of variants is equal to $\binom{\frac{1}{2}n_r}{v}$.

(ii) Let us consider all possible structures of codewords $c_{2v+1,r}$ of **odd weight** $2v+1$ and the corresponding column sets $H_r(c_{2v+1,r})$ in the matrix H_r of (1). Every such column set consists of the following components:

- A column set $H_{r-1}(c_{2v+1-2j,r-1})$ partitioned by two parts that are placed in the left and right sides of H_r .
- Two sets of the same j columns of H_{r-1} placed in the left and right sides of H_r . (These column sets are not connected with any codewords of \mathcal{C}_{r-1} .)

For $j = 0, 1, \dots, v-2$ and for every codeword $c_{2v+1-2j,r-1}$ of odd weight, we explain the formula (6).

A column set $\Gamma = H_{r-1}(c_{2v+1-2j,r-1})$ is partitioned by two parts. One part, say A_{odd} , contains an odd number of

columns, another part, say B_{even} , contains an even number of columns. The partition is executed by all possible ways. The number of the partitions is equal to 2^{2v-2j} .

If j is odd then the part B_{even} (resp. A_{odd}) is placed in the left (resp. right) side of H_r .

If j is even or $j = 0$ then the part A_{odd} (resp. B_{even}) is placed in the left (resp. right) side of H_r .

Also, in every of two submatrices H_{r-1} of (1) we take the same set of j columns that do not belong to Γ . The number of such j -sets is equal to $\binom{\frac{1}{2}n_r - 2v - 1 + 2j}{j}$. As a result, in the right side of H_r we always take an even number of columns. \square

Now we give the weight spectrum for duals to quasi-perfect codes.

Theorem 8. Let $d_r \leq 4$. Assume that an $[n_r, n_r - r, d_r]$ code \mathcal{C}_r is created from a $[\frac{1}{2}n_r, \frac{1}{2}n_r - r + 1, d_{r-1}]$ code \mathcal{C}_{r-1} by the doubling construction (1). Then weight spectrum $\{A_w^{(r)\perp}, w \leq n_r\}$ of the $[n_r, r, d_r^\perp]$ code dual to \mathcal{C}_r can be obtained from weight spectrum $\{A_w^{(r-1)\perp}, w \leq \frac{1}{2}n_r\}$ of the $[\frac{1}{2}n_r, r-1, d_{r-1}^\perp]$ code dual to \mathcal{C}_{r-1} as follows:

$$A_{2v}^{(r)\perp} = A_v^{(r-1)\perp} + \begin{cases} 0 & \text{if } 2v \neq \frac{1}{2}n_r \\ 2^{r-1} & \text{if } 2v = \frac{1}{2}n_r \end{cases}. \quad (7)$$

Proof. We consider matrix (1) as a generator matrix of the dual code. If codeword of the dual code is created without inclusion the top row, then its weight is equal to the doubled weight of the corresponding word formed from rows of matrix H_{r-1} . If the top row is included into codeword, its weight is equal to $\frac{1}{2}n_r$. \square

IV. ON CORRECTION OF ERASURE PATTERNS OF HIGH WEIGHT

Knowledge of the weight spectrum of a code opens a way for calculation of very important probabilities for the code, like conditional probability of correct decoding of erasure patterns, probability of undetected error and so on. In binary codes, the number of parity check bits is larger than code distance. That is a good reason to investigate a total ability of codes to correct erasure patterns of high weights (equal to or greater than code distance).

The necessary condition for correction of weight ρ erasure patterns is the full rank of submatrix, consisting of columns of a code parity check matrix, corresponding to erased positions.

Let S_ρ be the number of erasure patterns of weight ρ , which can be corrected by a code (equivalently, for a code parity check matrix, S_ρ is the number of distinct sets of ρ linear independent columns or the number of distinct $r \times \rho$ submatrices of the full rank).

For a code of length n , let $\delta_\rho = \frac{S_\rho}{\binom{n}{\rho}}$ be the conditional probability of correct decoding of erasure patterns of weight ρ .

In further, for $[n, n - r, d]$ code with weight spectrum A_0, A_1, \dots, A_n we introduce the function

$$\Psi(n, d, \rho) = \binom{n}{\rho} - \sum_{w=d}^{\rho} A_w \binom{n-w}{\rho-w}, \quad d \leq \rho \leq r. \quad (8)$$

This function gives a lower estimate of S_ρ , see [7], [8].

Theorem 9. For an $[n, n-r, d]$ code, the conditional probability δ_ρ and the value S_ρ satisfy the following lower estimates:

$$\delta_\rho \geq \frac{\Psi(n, d, \rho)}{\binom{n}{\rho}}, \quad S_\rho \geq \Psi(n, d, \rho), \quad d \leq \rho \leq r. \quad (9)$$

In particular, the following equalities

$$\delta_\rho = \frac{\Psi(n, d, \rho)}{\binom{n}{\rho}}, \quad S_\rho = \Psi(n, d, \rho),$$

hold under the condition

$$\rho \leq d + \frac{d-1}{2}.$$

The proof of Theorem 9 is based on the fact that the value S_ρ is equal to the difference between the total number of sets of ρ columns of a parity check matrix and the number of patterns of ρ linear dependent columns.

Now we use the known binomial approximation of weight spectrum of a binary linear code [9]–[11] $A_w \approx 2^{-z} \binom{n}{w}$, $r-1 < z \leq r$, $w \geq d$, where z is a real value taking into account (in principle) correction terms in the mentioned approximations and the weight region $w \geq d$. We obtain the following approximation of the function S_ρ for the region $d \leq \rho \leq r$.

$$\begin{aligned} S_\rho &\geq \binom{n}{\rho} - \sum_{w=d}^{\rho} A_w \binom{n-w}{\rho-w} \\ &\approx \binom{n}{\rho} - 2^{-z} \sum_{w=d}^{\rho} \binom{n}{w} \binom{n-w}{\rho-w} \\ &= \binom{n}{\rho} - 2^{-z} \binom{n}{\rho} \sum_{w=d}^{\rho} \binom{\rho}{w}. \end{aligned}$$

From here, using [11, Lemma 10.8], we obtain an estimate of the conditional probability δ_ρ of correct decoding of erasure patterns of high weight ρ .

$$\begin{aligned} \delta_\rho &\geq \frac{S_\rho}{\binom{n}{\rho}} \approx 1 - 2^{-z} \sum_{w=d}^{\rho} \binom{\rho}{w} \\ &\approx 1 - 2^{-z} \cdot 2^{\rho H(d/\rho)} \geq 1 - 2^{\rho-z}, \quad d \leq \rho < z, \end{aligned}$$

where $H(d/\rho)$ is the binary entropy.

The proposed estimate shows that for a fixed r , the probability δ_ρ decreases exponentially with growth of ρ . Therefore the reasonable extended region of correctable erasure patterns is $\rho < 2d$.

The following lemma allows us to improve estimates of Theorem 9 using a recursive approach.

Lemma 10. Any set of ρ linear dependent columns of a parity check matrix is an union of w columns with the zero sum (corresponding to a weight w codeword) and a set of $\rho-w$ linear independent columns, where $d \leq w \leq \rho$.

We give a recursive form of function of type (8) :

$$\tilde{\Psi}(n, d, \rho) = \binom{n}{\rho} - \sum_{w=d}^{\rho} A_w(n) \tilde{\Psi}(n-w, d, \rho-w),$$

where $A_w(n)$ is the number of weight w words in a (shortened) code of length n .

A recursive estimate of the conditional probability of correct decoding of erasure patterns of weight ρ and the first and second steps of the recursion has the form, respectively,

$$\begin{aligned} \tilde{\delta}(n, d, \rho) &= \frac{\tilde{\Psi}(n, d, \rho)}{\binom{n}{\rho}} \\ &= 1 - \sum_{w=d}^{\rho} A_w(n) \tilde{\delta}(n-w, d, \rho-w) \frac{\binom{n-w}{\rho-w}}{\binom{n}{\rho}}; \\ \tilde{\delta}_2(n, d, \rho) &= 1 - \sum_{w_1=d}^{\rho} A_{w_1}(n) \frac{\binom{n-w_1}{\rho-w_1}}{\binom{n}{\rho}} \times \\ &\times \left[1 - \sum_{w_2=d}^{\rho-w_1} A_{w_2}(n-w_1) \frac{\binom{n-w_1-w_2}{\rho-w_1-w_2}}{\binom{n-w_1}{\rho-w_1}} \right]. \end{aligned}$$

V. APPLICATION TO MEMORY

An important area for application of quasi-perfect codes is computer memory (Flash or SSD). Their ability to correct a big number of erasures instead of one error and very low probability of undetected error gives us a strong incentive to investigate the conditional probability of correct decoding for erasure patterns of high weight. As an example, useful for application, we give two tables: the first one for conditional probability of correct decoding for erasure patterns of weights higher the code distance and the second one for the probability (unconditional) of decoding failure in memory channel with different error probability for the product of Panchenko codes.

Decoding algorithm for product of Panchenko codes consists of following steps.

- 1) Error detection in rows and columns of the received word (in parallel).
- 2) Check (in parallel) of the detected row (column) list for correctability as erasure pattern.
- 3) Correction of the chosen erasure pattern (row or column) and output.

Check for correctability is executed in extended area up to d^+ erasures.

Table I gives a comparison between Hamming and Panchenko codes with 7 and 8 parity symbols. We can see from the table that extended decoding with correction of 4, 5, 6, 7 erasures has decreasing probability from 1 up to 1/2 (approximately).

Table II demonstrates fast decreasing of the probability of decoding failure for fixed number of parity bits with extension of the decoding area for product of two Panchenko codes. We can see from the second table fast decreasing of the failure probability with extension of the decoding area from 3 up to 6 erasures.

TABLE I
CONDITIONAL PROBABILITY δ_ρ OF CORRECT DECODING OF ERASURE
PATTERNS OF WEIGHT ρ FOR HAMMING AND PANCHENKO CODES

code	r	$\rho = d = 4$	$\rho = 5$	$\rho = 6$	$\rho = 7$
Hamming	7	0.9836	0.9180	0.7469	0.4121
Panchenko	7	0.9870	0.9287	0.7656	0.4306
Hamming	8	0.9920	0.9600	0.8741	0.6879
Panchenko	8	0.9934	0.9647	0.8830	0.6996

TABLE II
FAILURE PROBABILITY FOR PRODUCT OF PANCHENKO CODES [72, 64, 4]

p	10^{-1}	10^{-2}	$5 \cdot 10^{-3}$	10^{-3}	$5 \cdot 10^{-4}$
$d^+ = 3$	1	0,996	0,250	1,1e-09	2,3e-14
$d^+ = 4$	1	0,988	0,092	1,6e-12	5,1e-18
$d^+ = 5$	1	0,967	0,027	7,0e-14	1,045e-18
$d^+ = 6$	1	0,926	0,008	5,8e-14	1,029e-18

ACKNOWLEDGMENT

The research was carried out at the IITP RAS at the expense of the Russian Foundation for Sciences (project 14-50-00150).

REFERENCES

- [1] A. Davydov and L. Tombak, "Quasiperfect linear binary codes with minimal distance 4 and complete caps in projective geometry," *Problems of Information Transmission*, vol. 25, no. 4, pp. 265–275, Dec. 1989.
- [2] A. Bruen and D. Wehlauf, "Long binary linear codes and large caps in projective space," *Designs, Codes and Cryptography*, vol. 17, no. 1, pp. 37–60, Dec. 1999.
- [3] D. Wehlauf, "Complete caps in projective space which are disjoint from a codimension 2 subspace," in *Finite Geometries*, ser. Developments in Mathematics, A. Blokhuis, J. Hirschfeld, D. Jungnickel, and J. Thas, Eds. Dordrecht: Kluwer Academic Publishers, 2001, vol. 3, pp. 347–361, corrected version: <https://arxiv.org/abs/math/0403031>.
- [4] V. Panchenko, "On optimization of linear code with distance 4," in *Proceedings 8th All-Union Conference on Coding Theory and Communications, Part 2: Coding Theory*, Kuibyshev (Moscow), USSR, 1981, pp. 132–134, (in Russian).
- [5] A. Davydov and L. Tombak, "An alternative to the Hamming code in the class of SEC-DED codes in semiconductor memory," *IEEE Trans. Inf. Theory*, vol. IT-37, no. 3, pp. 897–902, May 1991.
- [6] V. Afanassiev, A. Davydov, and D. Zigangirov, "Design and analysis of codes with distance 4 and 6 minimizing the probability of decoder error," *Journal of Communications Technology and Electronics*, vol. 61, no. 12, pp. 1440–1455, Dec. 2016.
- [7] —, "Estimation of the conditional probability of correct decoding of erasure patterns for linear codes," *Informatsionnye Protessy*, vol. 16, no. 4, pp. 382–404, Dec. 2016, (in Russian).
- [8] O. Popov, "On estimate of ability of linear codes to correct erasures and to detect errors when erasures are," *Electrosvyaz*, vol. 10, 1967, (in Russian).
- [9] K. Cheung, "The weight distribution and randomness of linear codes," Jet Propulsion Lab., California Institute of Technology, Pasadena, CA, USA, TDA Progress Report 42-97, 1989. [Online]. Available: <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890018521.pdf>
- [10] I. Krasikov and S. Litsyn, "On spectra of bch codes," *IEEE Trans. Inf. Theory*, vol. IT-41, no. 3, pp. 786–788, May 1995.
- [11] F. MacWilliams and N. Sloane, *The Theory Error-Correcting Codes*. Amsterdam, New-York: North-Holland Publishing Company, 1977.