OPTIMIZATION OF SHORTENED HAMMING CODES

A. A. Davydov, L. N. Kaplan,
Yu. B. Smerkis, and G. L. Tauglikh

UDC 621.391.15

Optimization is treated as reduction of the number of words of weight d, where d is the code distance. For d = 3, the authors propose methods of synthesizing codes of arbitrary length with minimum number of words of weight 3. For expanded codes with d = 4, asymptotically coincident upper (guaranteed attainable) and lower bounds are constructed for the minimum number of words of weight 4. Classes of codes that attain the lower bound or are close to it are indicated.

1. Introduction

Shortened binary Hamming codes are extensively employed in practice, e.g., in computer storage devices [1-3]. One widespread mode of use involves correction of a single error with simultaneous deduction of multiple errors. In this case the probability of erroneous decoding basically depends on $A_d(n, r)$, the number of words of minimum weight d in the shortened Hamming code of length n obtained from the complete Hamming code with r check symbols. To optimize the code, therefore, it is necessary to minimize $A_d(n, r)$.

Papers [1, 4-8] posed the problem of choosing a check matrix for a shortened Hamming code to reduce $A_d(n, r)$. For some lengths, inspection algorithms were employed to obtain the corresponding matrices for Hamming codes proper (H-codes) with d = 3 [5, 7] and for expanded Hamming codes (EH-codes) with d = 4 having a common parity check [4, 7].

In this paper we investigate some properties of these codes. For H-codes we derive a formula that enables us to determine the minimum value (for specified n and r) of $A_3(n, r)$. Constructive methods for setting up the corresponding matrix are given.

For EH-codes, we prove a property of $A_4(n, r)$ that simplifies its minimization and estimation. A lower bound for $A_4(n, r)$ is obtained by using the MacWilliams relations and linear programming. Classes of codes that attain this bound or are close to it are pointed out. By averaging over all codes, an upper bound is obtained for the minimum value of $A_4(n, r)$ that can be achieved by stepwise optimization. It is shown that the upper and lower bounds coincide asymptotically.

We introduce some notation. For the initial code (the code to be shortened), r is the redundancy; N is the length; and $H_N^{(r)}$ is the check matrix. For the shortened code, n is the length $(r+1 \le n \le N)$, $H_n^{(r)}$ is the check matrix. We denote by $H_{N-n}^{(r)}$ the "complementary" matrix to $H_n^{(r)}$ in the sense that $\|H_n^{(r)} H_{N-n}^{(r)}\| = H_N^{(r)}$. The number of words of weight d in specific codes specified by check matrices $H_n^{(r)}$ and $H_{N-n}^{(r)}$ will be denoted by $A_d(n, r)$ and $A_d(N-n, r)$ respectively. The minimum (over all n, n − r)-codes) of $A_d(n, r)$ will be denoted by $a_d(n, r)$.

2. Minimization of $A_3(n, r)$ in Shortened H-Codes

For an H-code $N = 2^r - 1$, d = 3.

LEMMA 1. Among matrices $H_n^{(r)}$ of minimum rank* $]\log_2 (n+1)[$ there is a matrix with maximum (for given n) value of $A_3(n, r)$.

LEMMA 2. For any n and r we have†

$$A_3(n, r) + A_3(N-n, r) = (C_n^3 + C_{2^r-1-n}^3)/(2^r-3).$$

* $]x[$ is the nearest integer not larger than x.

† The proofs of the lemmas are given in the Appendix.

Translated from Problemy Peredachi Informatsii, Vol. 17, No. 4, pp. 63-72, October-December, 1981. Original article submitted September 5, 1979; revision submitted March 30, 1981.

0032-9460/81/1704-0261$07.50

Remark. Lemma 2 is equivalent to the following assertion. Assume that the space of binary vectors of length r is arbitrarily divided into two subsets M_1 and M_2 of cardinality n and (2^r-n), respectively. Then the sum of the number of linearly dependent (LD) triples of vectors in set M_1 and of the number of LD triples of vectors in M_2 is completely determined by r and n and is independent of the specific vectors that appear in M_1 and M_2.

Now we can determine $a_3(n, r)$ by employing the following considerations. In accordance with Lemma 2, to minimize $A_3(n, r)$ we should maximize $A_3(N-n, r)$; this can be done by taking (in accordance with Lemma 1) matrix $H^{(r)}_{N-n}$ of minimum possible rank $r' =]\log_2 (N-n+1)[$. Then, if we consider an H-code of length $N' = 2^{r'}-1$ with redundancy r' and again use Lemma 2, we can reduce the problem to optimization of a "strongly" shortened H-code of length less than $N'/2$. This optimization can readily be performed by taking a check matrix that does not contain LD triples of columns (e.g., a matrix all of whose columns have an odd number of 1's).

THEOREM 1. The minimum number of words of weight 3 in a shortened $(n, n-r)$ Hamming code is

$$a_3(n, r) = {}^1/_6 (2^r - 2^{r'})(2^{r'} + 3n - 2^{r'+1}), \tag{1}$$

where $r' =]\log_2(2^r - n)[$. To attain $a_3(n, r)$ it is sufficient to take $H^{(r)}_{N-n} = \left\| \begin{matrix} 0 \\ G \end{matrix} \right\|$, where 0 is a null matrix of dimensions $(r-r') \times (N-n)$; $G = \| G_1 G_2 \|$; G_1 is an $r' \times (2^{r'-1}-1)$ matrix; and all columns of G_1 contain an even number of 1's.

Proof. It follows from Lemma 2 that $a_3(n, r) = F_3(n, r) - \max A_3(N-n, r)$, where $F_3(n, r) = (C_n^3 + C^3_{2^r-1-n})/(2^r - 3)$; $\max A_3(N-n, r)$ is the maximum (over all $N-n$, $N-n-r$)-codes) of $A_3(N-n, r)$. Taking account of Lemma 1, to attain $\max A_3(N-n, r)$ is it sufficient to consider matrices $H^{(r)}_{N-n}$ of rank $r' =]\log_2(N-n+1)[=]\log_2(2^r-n)[$.

In $H^{(r)}_{N-n} = \left\| \begin{matrix} 0 \\ G \end{matrix} \right\|$ we eliminate zero rows and consider the resultant matrix G as the check matrix $H^{(r')}_{n'}$ of a shortened $(n', n'-r')$ Hamming code, where $n' = N-n$. The corresponding "complementary" matrix $H^{(r')}_{N'-n'}$ (where $N' = 2^{r'}-1$ and $N'-n' < {}^1/_2 N'$) consists only of columns with an odd number of 1's, since all nonzero columns of length r' with an even number of 1's appear in G_1. Therefore, matrix $H^{(r')}_{N'-n'}$ does not contain LD triples of columns. Consequently, $A_3(N-n', r') = 0$ and taking account of Lemma 2 for matrix $G = H_{n'}(r')$ we obtain $\max A_3(n', r') = F_3(n', r') = F_3(N-n, r')$. But this means that for matrix $H^{(r)}_{N-n} = \left\| \begin{matrix} 0 \\ G \end{matrix} \right\|$ we have obtained $\max A_3(N-n, r) = \max A_3(n', r') = F_3(N-n, r')$. Consequently, $A_3(n, r)$ has been minimized, where

$$a_3(n, r) = F_3(n, r) - F_3(N-n, r'),$$

and from this, after some manipulations, we obtain (1). The theorem is thus proved.

It is not hard to see that Theorem 1 is also valid when the requirement on G is formulated more generally: i.e., matrix $H^{(r')}_{N'-r'}$ does not contain LD triples of columns. Let us consider two cases.

1. Assume that matrix G_1 to which a zero column has been ascribed in a subspace of dimension $r'-1$ of the space of columns of length r'. In this case all columns of $H^{(r')}_{N'-n'}$ belong to a coset with respect to the subspace, and hence $H^{(r')}_{N'-n'}$ does not contain LD triples of columns. This generalization does not generate new codes, since the corresponding matrices G_1 are equivalent to matrix G_1 described in the theorem. With this approach, however, we can readily set up differing matrices $H^{(r)}_n$, for which $a_3(n, r)$ is attained and which are convenient from certain particular standpoints (simplicity of implementation, convenience of description, etc.). For example, we can require that all columns of G_1 contain an even number of 1's in l fixed positions. For $l = 1$ we have the following.

COROLLARY 1. The minimum number of words of weight 3 is attained in a shortened Hamming code for which the columns of the check matrix are the binary representation of numbers from $2^r - n$ to $2^r - 1$.

In the case under consideration, nonequivalent codes can be obtained by different choice of the columns for generating G_2.

2. The case in which $n = 2^{r-1} + r$ is of importance from the standpoint of use in working storages. Here $r' = r - 1$ and expression (1) yields

$$a_3(2^{r-1}+r, r)=r2^{r-2}.$$

In this case the form of the check matrix can be as stated in the following corollary.

COROLLARY 2. If $n = 2^{r-1} + r$, then to attain $a_3(n, r)$ it is sufficient that matrix $H_n^{(r)}$ contains 2^{r-1} columns with a 1 in the first position, $r - 1$ linearly independent (LIN) columns with 0 in the first position, and one column that is the sum of the indicated $r - 1$ LIN columns.

For the proof, it is sufficient to note that the last r columns of $H_n^{(r)}$ make up matrix $H_{N'-n'}^{(r')}$ in this case; obviously, for $r \geq 4$ it does not contain LD triple of columns.

There is reason to assume that for $n = 2^{r-1} + r$, from among all nonequivalent matrices $H_n^{(r)}$ described in Corollary 2 yields the minimum value of $A_4(n, r)$ as well. This hypothesis is valid at least for $r = 6, 7$.

3. Minimization of $A_4(n, r)$ in Shortened EH-Codes

For EH-codes $N = 2^{r-1}$, $d = 4$.

LEMMA 3. For any n and r we have

$$A_4(n, r)-A_4(N-n, r)=(C_n^4-C_{2^{r-1}-n}^4)/(2^{r-1}-3).$$

It can be seen from Lemma 3 that the problem of minimizing $A_4(n, r)$ is equivalent to that of minimizing $A_4(N - n, r)$.

We introduce the following notation:

$$F_4(n, r)=(C_n^4-C_{2^{r-1}-n}^4)/(2^{r-1}-3).$$

COROLLARY 3. $a_4(n, r) = a_4(N - n, r) + F_4(n, r)$.

COROLLARY 4. We have the bound

$$A_4(n, r)\geqslant\max\{0; F_4(n, r)\}. \tag{2}$$

This bound is attained in the following cases: (assuming that $r \geq 7$):*

$$n\leqslant 2^{(r-1)/2}+1 \ (r \text{ odd}),\ n\leqslant 2^{(r-2)/2}+2^{[r/4]} \ (r \text{ even}), \tag{3}$$

$$n\geqslant 2^{r-1}-2^{(r-1)/2}-1 \ (r \text{ odd}),\ n\geqslant 2^{r-1}-2^{(r-2)/2}-2^{[r/4]} \ (r \text{ even}). \tag{4}$$

Proof. In case (3) we have $F_4(m, r) < 0$ and it is sufficient to take $H_n^{(r)}$ to be the check matrix of the expansion of a BCH code with minimum distance $d = 5$ [9]. Here the shortened EH-code has $d = 6$ and $A_4(n, r) = 0$. In case (4) it is sufficient to use the matrix in question as $H_{N-n}^{(r)}$. Then we obtain $A_4(N - n, r) = 0$ and $A_4(n, r) = F_4(n, r) > 0$.

If linear codes are known with $d = 5$ and a length greater than for the corresponding BCH code, relations (3) and (4) can be improved. As an example, we note that the codes cited in [9] enable us to attain bound (2) for the following values of r and n: $r = 10$, $n \leq 24$ and $n \geq 2^9 - 24$; $r = 14$, $n \leq 75$ and $n \geq 2^{13} - 75$; $r = 18$, $n \leq 279$ and $n \geq 2^{17} - 279$. Note also that for $r = 5.6$ bound (2) is attained for $n = r + 1$ and $n \geq 2^{r-1} - r - 1$. For those n and r for which a code with $d = 5$ cannot be found (or cannot be constructed), a lower bound is obtained using the MacWilliams relations and linear programming (LP).

We denote by $\{A_j(n, r)\}$ and $\{A_j'(n, r)\}$ $(j = \overline{0, n})$ the weight spectra of the shortened EH-code and its dual code, respectively. The MacWilliams relations for these spectra have the form

$$A_k(n, r)=\frac{1}{2^r}\sum_{j=0}A_j'(n, r)P_k(j) \qquad (k=\overline{0, n}), \tag{5}$$

where $P_k(x)$ is a Kravchuk polynomial [9].

LEMMA 4. Among matrices $H_n^{(r)}$ of maximum rank r there is a matrix with minimal value (for given n and r) of $A_4(n, r)$.

* [x] is the integer part of x.

On the basis of Lemmas 3 and 4 we can conclude that to minimize $A_4(n, r)$ it is sufficient to consider the case in which the ranks of matrices $H_n^{(r)}$ and $H_{N-n}^{(r)}$ are equal to r. This is the case that will be considered below.

Allowing for the fact that the rank of $H_n^{(r)}$ is equal to r and that the dual code contains a word consisting of all 1's, we can write

$$A_0'(n,r)=A_n'(n,r)=1; \quad A_j'(n,r)=A'_{n-j}(n,r) \tag{6}$$
$$(j=\overline{1,m};\ m=[n/2]); \quad A_m'(2m,r) \text{ odd}.$$

It follows from (6) that the number of different spectral components in (5) can be halved. We introduce the variable

$$x_j=\begin{cases} A_j'(n,r) & \text{for} \quad j=\overline{1,[(n-1)/2]}, \\ {}^1/_2 A_j'(n,r) & \text{for} \quad j=m,\ n=2m. \end{cases} \tag{7}$$

Now, allowing for the fact that

$$A_0(n,r)=1,\ A_2(n,r)=0,\ A_{2i+1}(n,r)=0 \ \text{ and } \ A_i(n,r)\geqslant 0, \tag{8}$$

we can formulate the LP problem for bounding the minimum of $A_4(n, r)$ (i.e., for bounding $a_4(n, r)$): minimize the functional

$$A_4(n,r)=\frac{n^4}{12\cdot 2^r}-\frac{3n^2-2n}{24}+\frac{1}{12\cdot 2^r}\sum_{j=1}^{m}(n-2j)^4 x_j \tag{9}$$

under the following constraints:

$$\sum_{j=1}^{m} x_j=2^{r-1}-1; \quad \sum_{j=1}^{m}(n-2j)^2 x_j=(2^{r-1}-n)n; \quad x_j\geqslant 0 \ \ (j=\overline{1,m}); \tag{10}$$

$$A_{2i}(n,r)=\frac{1}{2^{r-1}}\left(C_n^{2i}+\sum_{j=1}^{m}P_{2i}(j)x_j\right)\geqslant 0; \tag{11}$$

$$A_{2m}(n,r)=\frac{1}{2^{r-1}}\left(n^v+(-1)^m x_m+\sum_{j=1}^{m-1}(-1)^j(n-2j)^v x_j\right)=0 \ \text{ or } \ 1; \tag{12}$$

x_j, $A_{2i}(n, r)$ are integers; $i=\overline{1, m}$; $j=\overline{1, m}$; $m=[n/2]$; $v=n-2m$.

Expressions (9)-(11) were obtained from (5) using (6)-(8) and simple manipulations. Constraint (12) follows from (5)-(8) and from the relation $A_{n-1}(n, r)+A_n(n, r)\leq 1$, which is valid for any linear code with $d\geq 3$.

We denote the solution of LP problem (9)-(12) by $\bar{A}_4(n, r)$. It is understood that $a_4(n,r)\geq \bar{A}_4(n, r)$.

LEMMA 5. We have the following lower bound:

$$\bar{A}_4(n,r)\geqslant L(n,r)=\max\{0; A_4^{(I)}(n,r); A_4^{(II)}(n,r)\},$$

where $A_4^{(I)}(n, r)=2^{2-r}(gn^v+{}^1/_3(m+2)m(m-2)(m+2v))-C_{m-1}^2-gv$; $g=m-2[m/2]$;

$$A_4^{(II)}(n,r)=\frac{n^4}{12\cdot 2^r}-\frac{3n^2-2n}{24}+\frac{1}{12\cdot 2^r}(n(2^{r-1}-n)(s^2+(s-2)^2)-(2^{r-1}-1)s^2(s-2)^2); \ s=n-2u;$$
$$u=\left[\frac{1}{2}(n-\sqrt{(2^{r-1}-n)n(2^{r-1}-1)^{-1}})\right].$$

COROLLARY 5. We have the lower bound

$$a_4(n,r)\geqslant M(n,r)=\max\{L(n,r); L(N-n,r)+F_4(n,r)\}. \tag{13}$$

Bound (13), which follows from Lemma 5 and Corollary 3, is useful for n values of practical interest. The asymptotic behavior of the lower bound can be conveniently studied using the relation

$$a_4(n,r)\geqslant A_4^{(II)}(n,r)\geqslant D(n,r)=\frac{n^4}{12\cdot 2^r}-\frac{3n^2-2n}{24}+\frac{n^2(2^{r-1}-n)^2}{(2^{r-1}-1)\cdot 12\cdot 2^r} \tag{14}$$

obtained by transforming the expression for $A_4^{(II)}(n, r)$. By averaging over all matrices $H_n^{(r)}$, we can readily obtain the following upper bound for $a_4(n, r)$.

LEMMA 6.

$$a_4(n, r) \leqslant C_n^4/(2^{r-1}-3). \tag{15}$$

Lemma 6 and expression (14) imply that the upper and lower bounds for $a_4(n, r)$ are asymptotically coincident.

THEOREM 2. Let $n^{-1}2^{r-1} = o(n)$. Then

$$\lim_{n\to\infty} a_4(n, r)\, 2^{r-1}/C_n^4 = 1.$$

Let us return to the construction of codes with minimal or quasiminimal value of $A_4(n, r)$. It can be seen from (7), (9) that to construct a "good" matrix $H_n^{(r)}$ it is desirable that the spectrum of nonzero weights of the corresponding binary code (except for a word of all 1's) lie in the range $n/2 \pm \delta$, where δ is relatively modest. This property is possessed [9] by codes that are dual to the BCH codes with d = 5, employed in Corollary 4. Other classes of codes with this spectrum are also known. By using the generating matrices of such codes as matrix $H_n^{(r)}$ and $H_{N-n}^{(r)}$ (and adding, if necessary, a word of all 1's), we can obtain values of $A_4(n, r)$ less than upper bound (15) and close to lower bound (13).

Examples. 1. Let r = 7. As $H_{21}^{(7)}$ we take the generating matrix of the (21, 7)-code obtained from the (21, 6)-code of [9, Sec. 8.4] by adding a word of all 1's. Then $A_0'(21,7) = A_{21}'(21,7) = 1$; $A_8'(21,7) = A_{13}'(21,7) = 21$; $A_9'(21,7) = A_{12}'(21,7) = 42$, i.e., $\delta = 2.5 < 0.55\sqrt{n}$. In this case $A_4(21, 7) = 84$ and it attains bound (13). Other similar examples can be constructed by using the codes considered in [9, secs. 8.4 and 15.4].

2. We generate matrix $H_{N-n}^{(r)}$, by adding a row of all 1's to the check matrix of the code of Example 4 in [10]. As a result we obtain an EH-code of length $n = 2^{b-1}(2b + 1)$ with $r = 2b + 1$, $b \geq 1$. The weight spectrum of the binary code $A_0'(n, r) = A_n'(n, r) = 1$; $A_{j_1}'(n, r) = A_{j_2}'(n, r) = 2^{2b}-1$, where $j_1 = n/2 - 2^{b-2}$, $j_2 = n/2 + 2^{b-2}$, i.e., $\delta = 2^{b-1} \leqslant 2^{-1}/2\sqrt{n}$.

This code is interesting in that for any b we have $A_4(n, r) = A_4^{(II)}(n, r) = D(n, r)$, i.e., bound (13) is attained.

3. Consider codes of the following class: the generating matrix of (n, k)-code $W^{(k)}(i_1, i_2, \ldots, i_e)$ consists of all columns of weight $i_1, i_2, \ldots, i_e$ ($e \geqslant 1$, $n = \sum_{u=1}^{e} C_k$). Simple combinatorial considerations yield that code $W^{(k)}(i_1, i_2, \ldots, i_e)$ contains C_k^v words of weight $\sum_{u=1}\sum_{j} C_{k-v}^{i_u-2j-1} C_v^{2j+1}$, where $v = \overline{0, k}$.

As $H_{36}^{(7)}$ we take the generating matrix of (36,7)-code $W^{(7)}(3,7)$. Then $A_0'(36,7) = A_{36}'(36,7) = 1$; $A_{16}'(36,7) = A_{20}'(36,7) = 63$, i.e., $\delta = 2 = \sqrt{n}/3$. Here $A_4(36,7) = 945$ and the code attains bound (13).

In the general case, attainment of upper bound (15) is guaranteed with stepwise optimization: at each step a column that yields the smallest number of LD quadruples is added to some initial array of columns.

Indeed, assume that after the i-th step $A_4(i, r) = C_i^4/(2^{r-1} - 3) - \varepsilon_i$, where $\varepsilon_i \geq 0$. At the (i + 1)-th step we can generate $2^{r-1} - i$ different matrices $H_n^{(r)}$. The total number of "additional" LD quadruples columns in all these matrices (i.e., quadruples containing a new (i + 1)-th column) amounts to $C_i^3 - 4A_i(i, r)$. Averaging the "addition" over all matrices, we obtain

$$A_4(i+1, r) \leqslant [A_4(i, r) + (C_i^3 - 4A_4(i, r))/(2^{r-1}-i)] = [C_{i+1}^4/(2^{r-1}-3) - \varepsilon_{i+1}],$$

i.e., $\varepsilon_{i+1} = \varepsilon_i(1 - 4/(2^{r-1} - i))$. With allowance for Corollary 4, we have $\varepsilon_{i+1} \geq 0$, and this proves that bound (15) is attained with stepwise optimization.

In practice, stepwise optimization allows us to come fairly close to lower bound (13) as well, and sometimes to attain it. This fact is illustrated by the accompanying table, which gives computer-obtained matrices $H_n^{(r)}$ using stepwise optimization and the corresponding values of $A_4(n, r)$, $A_4(N - n, r)$. Each column of the matrix, considered as a binary number, is replaced by the corresponding decimal number (e.g., the number 39 corresponds to column [100111]T). A notation of the form 64-69 means that the matrix includes columns 64, 65, 66, 67, 68, 69.

TABLE 1

r	n	$N-n$	$H_n^{(r)}$	$A_4(n, r)$	$A_4(N-n, r)$	$\bar{A}_4(n, r)$	$M(n, r)$
6	16	16	34–42, 44, 48–50, 53, 56, 57	59	59	59	59
6	17	15	33–42, 44, 48–50, 53, 56, 57	79	44	79	79
6	18	14	33–42, 44, 48–50, 53, 56, 57, 63	102	31	102	102
6	19	13	33–42, 44, 45, 48–50, 53, 56, 57, 63	131	22	131	131
6	20	12	33–42, 44, 45, 48–51, 53, 56, 57, 63	164	14	164	164
6	21	11	33–42, 44–46, 48–51, 53, 56, 57, 63	204	9	204	204
6	22	10	32–34, 36–43, 45, 46, 48–52, 54, 56, 57, 60	250	5	250	250
6	23	9	33–46, 48–51, 53, 54, 56, 57, 63	304	3	304	304
6	24	8	33–46, 48–54, 56, 57, 63	365	1	365	365
7	39	25	64–69, 72, 74, 76–78, 80–82, 85, 87–93, 96–102, 106, 108, 110–114, 116, 120, 127	1335	194	1332	1332
8	72	56	128–139, 141–147, 149, 150, 153, 154, 156, 160–164, 166, 168, 170, 175, 177, 178, 181, 182, 184, 186, 188, 189, 192–194, 196, 197, 199, 202, 204, 211, 212, 214, 215, 218–221, 224–227, 232, 234, 236, 237, 241, 245, 248, 249, 252–254	8166	2874	8157	8151

We should note that for the shortened (72, 64) EH-code that is important in practical applications (e.g., for protection of the working storage of Unified Series computers [3]), we have obtained the bound a_4 (72.8) $\geq \bar{A}_4$ (56,8) + F_4 (72,8) = 8157, and have found a (72, 64)-code with A_4 (72,8) = 8166 (see Table 1). Papers [4, 6, 3, 2] gave (72, 64)-codes with A_4 (72,8) values of 8175, 8392, 8754, 9251, respectively.

The authors are grateful to G. A. Kabatyanskii for useful discussions and remarks, and in particular for Corollary 1 which was proposed by him.

APPENDIX

Proof of Lemma 1. If $n \geq 2^{r-1}$, then the rank of $H_n^{(r)}$ is always equal to r, and the validity of the lemma is obvious. Now let $n < 2^{r-1}$. The quantity $A_3^{(\rho)}$ (n, r) is equal to the number of LD triples of columns in matrix $H_n^{(r)}$ of rank ρ. First we construct from $H_n^{(r)}$ the matrix $\bar{H}_n^{(r)} = \| H_{n0} H_{n1} \ldots H_{nV} \|$ of rank (r − 1) with different nonzero columns, for which A_3^{r-1} (n, r) $\geq A_3^{(r)}$ (n, r) , $V > 0$. Matrix H_{n_0} consists of columns $c_{0j}^{(0)} \in H_n^{(r)}$ (the superscript is equal to the value of the first digit of the column). Matrix H_{nj} consists of all columns of the form $c_{ij}^{(0)} = c_{ij}^{(1)} + c_i^{(1)}$, where $c_{ij}^{(1)} \in H_n^{(r)}$; $c_{ij}^{(0)} \overline{\in} H_{n_s}$, $s = \overline{0, i-1}$; $i = \overline{1, V}$. It is possible to do this, since if we allow for the fact that $r >]\log_2 (n+1)[$ we have $\sum_s n_s < n < 2^{r-1}$; in other words, there always exists a column $c_i^{(0)} \overline{\in} H_{n_s}$, and hence a column $c_i^{(1)} = c_{i_1}^{(1)} + c_{i_1}^{(0)}$ ($s = \overline{0, i-1}$, $i = \overline{1, V}$).

Thus, LD triple of column $(c_{0j_1}^{(0)}, c_{0j_2}^{(0)}, c_{0j_3}^{(0)}$ from $H_n^{(r)}$ corresponds to an analogous LD triple from $\bar{H}_n^{(r)}$; LD triple $(c_{0j_1}^{(0)}, c_{ij_2}^{(1)}, c_{ij_3}^{(0)})$ from $H_n^{(r)}$ corresponds to LD triple $(c_{0j_1}^{(0)}, c_{ij_2}^{(0)}, c_{ij_3}^{(0)})$ from $\bar{H}_n^{(r)}$; LD triple $(c_{0j_1}^{(0)}, c_{sj_2}^{(0)}, c_{ij_3}^{(0)})$ from $H_n^{(r)}$ corresponds to LD triple $(c_{0j_1}^{(0)}, c_{qj_4}^{(0)}, c_{sj_2}^{(0)})$ from $\bar{H}_n^{(r)}$. Column $c_{qj_4}^{(0)} = c_{ij_3}^{(1)} + c_s^{(1)}$ always exists in H_{nq}, since otherwise this column would appear in H_{n_1}, $0 \leq q < s < i$. On the other hand, given this construction two different LD triples of columns from $H_n^{(r)}$ do not become the same LD triples of columns from $\bar{H}_n^{(r)}$. Assume, for example, that LD triple $(c_{0j_5}^{(0)}, c_{sj_6}^{(1)}, c_{i_1 j_7}^{(1)})$ from $H_n^{(r)}$ has become $(c_{0j_1}^{(0)}, c_{qj_4}^{(0)}, c_{sj_2}^{(0)})$. Then, by definition, $c_{0j_5}^{(0)} = c_{0j_1}^{(0)}$, $c_{sj_6}^{(1)} = c_{sj_2}^{(1)}$, and consequently, $(c_{0j_5}^{(0)}, c_{sj_6}^{(1)}, c_{i_1 j_7}^{(1)}) = (c_{0j_1}^{(0)}, c_{sj_2}^{(1)}, c_{ij_3}^{(1)})$. Thus, $A_3^{(r-1)}(n, r) \geq A_3^{(r)}(n, r)$ and obviously, $A_3^{(r-1)}(n, r) \geq \max A_3^{(r)}(n, r)$, where the maximum is taken over all matrices of rank r − 1 and r, respectively. If we similarly reduce the rank of $H_n^{(r)}$ to the minimum possible value, we can prove the lemma.

Proof of Lemma 2. Since $A_3(n, r)$ and $A_3(N-n, r)$ are, respectively, the numbers of LD triples of columns in $H_n^{(r)}$ and $H_{N-n}^{(r)}$, we have $A_3(n, r) + A_3(N-n, r) = S_3 - s_3$, where S_3 is the number of words of weight 3 in H-codes, s_3 is the number of LD triples containing columns of both matrices. We have $S_3 = (2^r - 1)(2^r - 2)/6$ [9]. To determine s_3 we assume that we have written out all possible pairs of columns $(c_i, \bar{c}_i)$, $c_i \in H_n^{(r)}$,

$\bar{c}_i \in H_{N-n}^{(r)}$; their number is $n(N-n) = n(2^r - 1 - n)$. Then, to obtain an LD triple, by adding a single column to fixed pair $(c_i, \bar{c}_i)$ (e.g., $c_j \in H_n^{(r)}$), we will eliminate pair $(c_j, \bar{c}_i)$ from consideration each time. Therefore, $s_3 = n(2^r - 1 - n)/2$, and, after some manipulations, we obtain the statement of the lemma.

Proof of Lemma 3. For $n = 0$ the assertion of the lemma is valid, since in EH-code the number of LD quadruples is equal to $(-F_4(0, r))$. Let us assume that the assertion is valid for $n = i - 1 > 0$. We transfer column c_i from matrix $H_{N-i+1}^{(r)}$ to $H_{i-1}^{(r)}$ and consider the new matrices $H_{N-i}^{(r)}$ and $H_i^{(r)}$. We will show that

$$F_4(i, r) = F_4(i-1, r) + F_3(i-1, r-1), \tag{A1}$$

where $F_3(n, r) = (C_n^3 + C_{2^r-1-n}^3)/(2^r - 3)$ (see Lemma 2). Obviously, $F_4(i, r) = F_4(i-1, r) + \Delta$, where Δ is the number of LD quadruples containing column c_i and three columns that belong simultaneously to $H_i^{(r)}$ or $H_{N-i}^{(r)}$. Adding column c_i to matrices $H_i^{(r)}$ and $H_{N-i}^{(r)}$, we obtain that Δ is equal to the overall number of LD triples of columns that appear entirely in $H_{i-1}^{(r-i)}$ or $H_{2^{r-1}-1-i}^{(r-1)}$ in H code of length $2^{r-1} - 1$, i.e., $\Delta = F_3(i-1, r-1)$. Now, after transforming (A1), we obtain the assertion of the lemma for $n = 1$.

Proof of Lemma 4. If $n > 2^{r-2}$, then the rank of $H_n^{(r)}$ is always r and the validity of the lemma is obvious. Now let $n \leq 2^{r-2}$. The value of $A_4(n, r)$ is equal to the number of LD quadruples of columns in $H_n^{(r)}$. Assume that matrix $H_n^{(r)}$ of minimum rank r' contains $A_4^{(r')}(n, r)$ LD quadruples of columns, where the minimum is taken over all matrices of rank r'. We transform $H_n^{(r)}$ in such a way that it contains a zero row. The number of LD quadruples of columns remains unaltered. We replace the zero row by a nonzero one that does not appear in the linear span of $H_n^{(r)}$. In the new matrix of rank $r' + 1$ the number of LD quadruples of columns $A_4^{(r'+1)}(n, r)$ is obviously unaltered. Consequently, $\min A_4^{(r'+1)}(n, r) \leq \min A_4^{(r')}(n, r)$. By similarly increasing the rank of $H_n^{(r)}$ to the maximum rank r, we can prove the lemma.

Proof of Lemma 5. To obtain analytic bounds for $\bar{A}_4(n, r)$, we consider functional (9) in two cases: I) only with constraint (10) and (12); II) only with constraint (10). In case I the basis unknowns are fixed: x_{m-2}, x_{m-1}, x_m. In case II the basis unknowns are taken to be x_u, x_{u+1}. For both cases, in the expression of the target function $A_4(n, r)$ in terms of free unknowns, the coefficients for them are nonnegative. Consequently, by setting the free unknowns equal to zero [11], we obtain values $A_4^{(I)}(n, r)$ (in case I), and $A_4^{(II)}(n, r)$ (in case II) that bound the optimal solution from below.

LITERATURE CITED

1. M. Y. Hsiao, "A class of optimal minimum odd weight column SEC-DED codes," IBM J. Res. Dev., 14, No. 4, 395-401 (1970).
2. R. Schürba, "Chip cuts parts count in error correction networks," Electronics, 51, No. 23, 130-133 (1978).
3. A. S. Samarskii and V. G. Belyaev, "Economical design of a memory-error correction unit and its efficiency," Vopr. Radioelektron. Ser. EVT, No. 11, 59-67 (1977).
4. S. Azumi and T. Kasami, "On optimal modified Hamming codes," Trans. Inst. Electron. Commun. Eng. Jpn., A58, No. 6, 325-330 (1975).
5. S. Sanyual and K. N. Venkataraman, "Single error correcting code maximizes memory system efficiency," Comput. Des., 17, No. 5, 175-184 (1978).
6. K. Iwasaki, T. Kasami, and S. Yamamura, "Optimal (72, 64) modified Hamming codes in the sense of Hsiao," Trans. Inst. Electron. Commun. Eng. Jpn., A61, No. 3, 270-271 (1978).
7. C. E. Sandberg, "Properties of transparent shortened codes for memories with stuck-at faults," IEEE Trans. Comput., 28, No. 9, 686-690 (1979).
8. A. A. Shostak, "On the determination of the optimal linear correcting code for specified redundancy," in: Automation and Computer Engineering [in Russian], No. 4, Visha Shkola, Minsk (1974), pp. 250-255.
9. F. J. MacWilliams and N. J. Sloane, The Theory of Error Correcting Codes, Elsevier.
10. M. G. Karpovsky, "On the weight distribution of binary linear codes," IEEE Trans. Inf. Theory, 25, No. 1, 105-109 (1979).
11. F. I. Karpelevich and L. E. Sadovskii, Elements of Linear Algebra and Linear Programming [in Russian], Nauka, Moscow (1965).