An Alternative to the Hamming Code in the Class of SEC–DED Codes in Semiconductor Memory

Alexander A. Davydov and Leonid M. Tombak

Abstract —**The Π code constructed by Panchenko is studied. The Π code to be an alternative to the Hamming code in the class of single-error correcting and double-error detecting codes (SEC–DED codes) is also considered. The Π code has a smaller number of words of weight 4 and provides a larger probability of the triple-independent-error detection than the shortened Hamming code with the same parameters. In this work shortening algorithms for the Π code are proposed, and parity check matrices of the [39,32], [72,64], [137,128] shortened Π codes are constructed. The codes obtained can detect byte errors of length 4.**

I. Introduction

Every word of a semiconductor memory is usually encoded by an error correcting code [20]. Errors appearing in the memory are classified to be either independent errors or byte errors [1]–[8], [13]–[18]. In this correspondence the following strategies for memory protection [1]–[10], [13]–[18], [21, p. 177–182] are considered.

1) A linear code of length n, minimum distance $d=4$ and redundancy $r=\lceil \log_2 n \rceil + 1$ is used. All single errors are corrected and all double errors and some triple errors are detected.
2) In addition to Strategy 1 the same code detects all byte errors of length 4.

Let Δ_3 be the ratio of the number of triple independent errors that may be detected by a code to the total number of triple errors. Denote by A_4 the number of words of weight 4 in a code. For Strategies 1 and 2, the memory reliability substantially depends on the value of Δ_3. It is known that $\Delta_3 = 1 - 4A_4/\binom{n}{3}$ [13]. Hence, it is useful to decrease the value of A_4.

It should be noted that the maximum number of 1's in rows of a parity check matrix and regular structure of the matrix are also important for memory protection systems [4], [6], [7], [13]–[18], [21].

Manuscript received May 10, 1990; revised January 16, 1991. This work was presented in part at the II All Union Conference on Actual Problems of Informatics and Computers (INFORMATICS–87), Erevan, U.S.S.R., October 1987, and at the VIII Conference of International COMPCONTROL Committee on Computer Applications in Production Management and Engineering (COMPCONTROL–87), Moscow, U.S.S.R., October 1987.

The authors are with the Institute for Problems of Cybernetics of Academy of Sciences of the U.S.S.R., Vavilov Street 37, 117312 Moscow, U.S.S.R.

IEEE Log Number 9143294.

The Hamming code is the most well known of codes with $d=4$. The problem of A_4 minimization for the shortened Hamming code was considered in [3], [4], [9], [11], [13], [14], and [21]. (Throughout this correspondence the word "shortened" may be omitted in a code name.) Let $a_4^H(n,r)$ be the minimum of A_4 over all $[n, n-r]$ Hamming codes. In [9] evaluations of $a_4^H(n,r)$ were obtained.

There are linear codes with $d=4$ that are not equivalent to the Hamming code [10], [12], [19]. Let $a_4^L(n,r)$ be the minimum of A_4 over all linear $[n, n-r]$ codes with $d=4$. In [11], [19] evaluations of $a_4^L(n,r)$ were obtained. In [19] Panchenko constructed the Π code that is not equivalent to the Hamming code and has $A_4 < a_4^H(n,r)$.

Let $N_r = 17 \cdot 2^{r-6}$. In [12] it is proved that there exist only three nonequivalent quasiperfect binary linear codes with $d=4$, $n > N_r$: the Hamming code with $n = 2^{r-1}$, the Π code with $n = 5 \cdot 2^{r-4}$, and the Ω code with $n = 9 \cdot 2^{r-5}$. Any binary linear code with $d=4$, $n > N_r$, is a shortening of one of these codes.

Let $B_k = [b_k, \cdots, b_k]$ be a matrix consisting of equal columns b_k, where b_k is the binary representation of k. Let $D = 2^{r-4}$, $M = 2^{r-5}$,

$$G = \begin{bmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{bmatrix}, \qquad Q = \begin{bmatrix} 00000 & 1111 \\ 10001 & 0000 \\ 01001 & 1001 \\ 00101 & 0101 \\ 00011 & 0011 \end{bmatrix}. \tag{1}$$

The parity check matrix P_r of the nonshortened $[n, n-r]$ Π code with $n = 5 \cdot 2^{r-4}$, $r \ge 5$, has the following form:

$$P_r = \left[\begin{array}{c|c|c|c|c} B_0 & B_1 & B_2 & \cdots & B_{D-1} \\ \hline G & G & G & \cdots & G \end{array} \right], \tag{2}$$

where B_k is a $(r-4)\times 5$ matrix.

For example, the parity check matrix of the [40,33] Π code is

$$P_7 = \left[\begin{array}{c|c|c|c|c|c|c|c} 00000 & 00000 & 00000 & 00000 & 11111 & 11111 & 11111 & 11111 \\ 00000 & 00000 & 11111 & 11111 & 00000 & 00000 & 11111 & 11111 \\ 00000 & 11111 & 00000 & 11111 & 00000 & 11111 & 00000 & 11111 \\ \hline 10001 & 10001 & 10001 & 10001 & 10001 & 10001 & 10001 & 10001 \\ 01001 & 01001 & 01001 & 01001 & 01001 & 01001 & 01001 & 01001 \\ 00101 & 00101 & 00101 & 00101 & 00101 & 00101 & 00101 & 00101 \\ 00011 & 00011 & 00011 & 00011 & 00011 & 00011 & 00011 & 00011 \end{array} \right]. \tag{3}$$

The parity check matrix Q_r [12] of the nonshortened $[n, n-r]$ Ω code with $n = 9 \cdot 2^{r-5}$ has the following form:

$$Q_r = \left[\begin{array}{c|c|c|c|c} B_0 & B_1 & B_2 & \cdots & B_{M-1} \\ \hline Q & Q & Q & \cdots & Q \end{array} \right], \tag{4}$$

where B_k is a $(r-5)\times 9$ matrix.

Codes with $n = 2^{r-2} + r$, $r \le 9$, used in a memory, have $n > N_r$.

In Section II we construct two shortening algorithms for the Π code. We consider the following ranges of code length n:

$$\max\{5 \cdot 2^{r-4} - 8, 9 \cdot 2^{r-5} - 1, 17 \cdot 2^{r-6} + 1\} \le n \le 5 \cdot 2^{r-4}. \tag{5}$$

$$\max\{5 \cdot 2^{r-4} - 25, 17 \cdot 2^{r-6} + 1\} \le n \le 5 \cdot 2^{r-4}. \tag{6}$$

The range (5) includes [39,32] and [72,64] codes. In the range (5) the first algorithm gives the global minimum of A_4, i.e., $A_4 = a_4^L(n,r)$. The range (6) includes [137,128] codes. In the

0018-9448/91/0500-0897$01.00

TABLE I
VALUES OF A_4 FOR THE Π CODES SHORTENED BY ALGORITHM 1 AND LOWER BOUNDS OF A_4 FOR THE SHORTENED HAMMING CODES

i	n ($r=7$)	Π Code $A_4=$	Hamming Code $A_4\geq$	n ($r=8$)	Π Code $A_4=$	Hamming Code $A_4\geq$
0	40	1190	1480	80	10300	12578
1	39	1071	1332	79	9785	11944
2	38	959	1191	78	9285	11335
3	37	854	1063	77	8800	10748
4	36	756	945	76	8330	10185
5	35	665	838	75	7875	9644
6				74	7455	9124
7				73	7048	8626
8				72	6654	8157

range (6) the second algorithm provides smaller values of A_4 in comparison with the Hamming code and the Ω code. However, this algorithm does not give the best shortened Π code. In Section II we construct the parity check matrices of the [39,32], [72,64], and [137,128] shortened Π codes for strategy I.

In Section III we construct the parity check matrices of the [72,64] and [137,128] shortened Π codes for the strategy II.

Structures of the obtained matrices are regular. Therefore, these matrices are suitable for VLSI implementation.

All obtained parity check matrices of the Π code have a larger value of Δ_3 than corresponding matrices of the Hamming code and the Ω code. Therefore, the Π code for strategies I, II provides the best reliability of the memory in the class of linear codes with $n=2^{r-2}+r$.

Some results of this work are introduced (without proofs) in [10].

II. THE SHORTENED Π CODES WITH THE BEST DETECTING CAPABILITY IN THE CLASS OF BINARY LINEAR CODE WITH $d=4$

In order to count A_4 we represent a nonzero column s_t, which does not belong to the parity check matrix of an $[n, n-r]$ code ("external" column), as the sum of two columns $h_{t,j}$ and $h_{t,j+1}$, which belong to the matrix [14], [19]. Denote by $m(t)$ the number of various representations of the column s_t. Then the following relations hold:

$$s_t = h_{t,1}+h_{t,2} = h_{t,3}+h_{t,4} = \cdots = h_{t,2m(t)-1}+h_{t,2m(t)}, \quad (7)$$

where

$$t=\overline{1,\cdots,2^r-1-n}, \qquad m(t)\in\overline{\{0,\cdots,\lfloor n/2\rfloor\}}.$$

$$A_4 = \frac{1}{3}\sum_{t=1}^{2^r-1-n}\binom{m(t)}{2} = \frac{1}{3}\sum_{j=2}^{\lfloor n/2\rfloor}\binom{j}{2}F_j, \quad (8)$$

where F_j is the number of external columns s_t, for which $m(t)=j$.

The main idea of proposed algorithms is to decrease $F_{\lfloor n/2\rfloor}$.

Algorithm 1: We shorten the matrix P_r by i columns, $i\leq 8$. We delete columns of P_r in the following order:

$$\begin{bmatrix} b_\gamma \\ \hline g_{15}\end{bmatrix}, \begin{bmatrix} b_\gamma \\ \hline g_8\end{bmatrix}, \begin{bmatrix} b_\gamma \\ \hline g_4\end{bmatrix}, \begin{bmatrix} b_\gamma \\ \hline g_2\end{bmatrix}, \begin{bmatrix} b_\gamma \\ \hline g_1\end{bmatrix}, \begin{bmatrix} b_\delta \\ \hline g_{15}\end{bmatrix}, \begin{bmatrix} b_\nu \\ \hline g_8\end{bmatrix}, \begin{bmatrix} b_{\mathscr{H}} \\ \hline g_4\end{bmatrix}, \quad (9)$$

where g_v is a column of matrix G, corresponding to the binary representation of v, and columns $b_\gamma, b_\delta, b_\nu, b_{\mathscr{H}}$ are distinct.

Throughout this correspondence the expression $j=\{a,b\}$, $F_j=\{c,d\}$ means that $F_a=c$, $F_b=d$. Let $E=5\cdot 2^{r-5}$.

Theorem 1: For $r\times n$ matrices with $n=5\cdot 2^{r-4}-i$ obtained by Algorithm 1 the nonzero values F_j can be represented as follows:

$$\begin{aligned}
&i=0: j=\{D,E\}, && F_j=\{10D, D-1\}.\\
&i=1: j=\{D-1,D,E-1\}, && F_j=\{4D,6D,D-1\}.\\
&i=2: j=\{D-2,D-1,D,E-2\}, && F_j=\{D-1,6D+1,3D,D-1\}.\\
&i=3: j=\{D-2,D-1,D,E-3\}, && F_j=\{3D-3,6D+3,D,D-1\}.\\
&i=4: j=\{D-2,D-1,E-4\}, && F_j=\{6D-6,4D+6,D-1\}.\\
&i=5: j=\{D-2,D-1,E-5\}, && F_j=\{10D-10,10,D-1\}.\\
&i=6: j=\{D-3,D-2,D-1,E-6,E-5\}, && F_j=\{4D-8,6D+2,6,D-2,1\}.\\
&i=7: j=\{D-4,D-3,D-2,D-1,E-7,E-6\}, && F_j=\{D-4,6D-8,3D+9,3,D-3,2\}.\\
&i=8: j=\{D-4,D-3,D-2,D-1,E-8,E-7\}, && F_j=\{3D-12,6D,D+11,1,D-4,3\}.
\end{aligned} \quad (10)$$

Proof: See the Appendix. □

Denote by $\Delta_3^L(n,r)$ and $\Delta_3^H(n,r)$ the maximum of Δ_3 over all linear $[n,n-r]$ codes with $d=4$ and over all $[n,n-r]$ Hamming codes respectively.

Theorem 2: In the range (5) the $[n,n-r]$ Π code obtained by Algorithm 1 has the minimum number of words of weight 4 and the maximum probability of triple-independent-error detection over all linear $[n,n-r]$ codes with $d=4$, i.e., this Π code has $A_4=a_4^L(n,r)$ and $\Delta_3=\Delta_3^L(n,r)$.

Proof: See the Appendix. □

Using the relations (8), (10) and results of [9] we obtain Table I.

In order to shorten the matrices P_7 and P_8 we use Algorithm 1. Let $r=7$, $i=1$, and $\gamma=7$. Then the parity check matrix H_{39} of the [39,32] Π code is the matrix P_7 with the last column omitted. Take $r=8$, $i=8$, $\gamma=15$, $\delta=14$, $\nu=13$, and $\mathscr{H}=12$. The parity check matrix H_{72} of the [72,64] Π code has the following form:

$$H_{72}=\left[\begin{array}{c|c|c|c|c|c|c|c}
00000 & 00000 & 00000 & 00000 & 00000 & 00000 & 00000 & 00000\\
00000 & 00000 & 00000 & 00000 & 11111 & 11111 & 11111 & 11111\\
00000 & 00000 & 11111 & 11111 & 00000 & 00000 & 11111 & 11111\\
00000 & 11111 & 00000 & 11111 & 00000 & 11111 & 00000 & 11111\\
\hline
10001 & 10001 & 10001 & 10001 & 10001 & 10001 & 10001 & 10001\\
01001 & 01001 & 01001 & 01001 & 01001 & 01001 & 01001 & 01001\\
00101 & 00101 & 00101 & 00101 & 00101 & 00101 & 00101 & 00101\\
00011 & 00011 & 00011 & 00011 & 00011 & 00011 & 00011 & 00011
\end{array}\right.$$

$$\left.\begin{array}{|c|c|c|c|c|c|c}
11111 & 11111 & 11111 & 11111 & 11\ 11 & 111\ 1 & 1111\\
00000 & 00000 & 00000 & 00000 & 11\ 11 & 111\ 1 & 1111\\
00000 & 00000 & 11111 & 11111 & 00\ 00 & 000\ 0 & 1111\\
00000 & 11111 & 00000 & 11111 & 00\ 00 & 111\ 1 & 0000\\
\hline
10001 & 10001 & 10001 & 10001 & 10\ 01 & 100\ 1 & 1000\\
01001 & 01001 & 01001 & 01001 & 01\ 01 & 010\ 1 & 0100\\
00101 & 00101 & 00101 & 00101 & 00\ 01 & 001\ 1 & 0010\\
00011 & 00011 & 00011 & 00011 & 00\ 11 & 000\ 1 & 0001
\end{array}\right]. \tag{11}$$

For H_{39}:

$$A_4=a_4^L(39,7)=1071, \qquad \Delta_3=\Delta_3^L(39,7)=0.5312.$$

For the Hamming code [9]:

$$a_4^H(39,7)\geq 1332, \qquad \Delta_3^H(39,7)\leq 0.4170.$$

For H_{72}:

$$A_4=a_4^L(72,8)=6654, \qquad \Delta_3=\Delta_3^L(72,8)=0.5537.$$

For the Hamming code [9]:

$$a_4^H(72,8)\geq 8157, \qquad \Delta_3^H(72,8)\leq 0.4529.$$

Denote by Γ the maximum number of 1's in rows of a parity check matrix. Matrices H_{39} and H_{72} have $\Gamma=19$ and $\Gamma=34$, respectively. The parity check matrices of the [39,32] and [72,64] Hamming codes constructed in [13], [14] have $\Gamma=15$ and $\Gamma=27$, $A_4=8392$, $\Delta_3=0.4361$.

Algorithm 2: We shorten matrix P_r by i columns, where $i\leq 25$. We delete submatrices $\left[\begin{smallmatrix}B_u\\G\end{smallmatrix}\right]$, where $u=k_\nu$, $\nu=1,\cdots,q=\lfloor i/5\rfloor$, any three and four columns of the set $\{b_{k_1},b_{k_2},\cdots,b_{k_q}\}$ are linearly independent. If $i\neq 5q$, then one submatrix is deleted incompletely.

For $r\times n$ matrices with $n=5\cdot 2^{r-4}-5q$ obtained by Algorithm 2 the nonzero values of F_j can be represented as follows:

$$\begin{aligned}
j&=\{D-2q,D-2q+2,D-q,E-5q,E-5q+5\},\\
F_j&=\{10D-10-5q(q-1),5q(q-1),10,\\
&\qquad D-1-q(q-1)/2,q(q-1)/2\}.
\end{aligned} \tag{12}$$

This relation can be proved similar to Theorem 1.

Theorem 3: In the range (6) the $[n,n-r]$ Π code obtained by Algorithm 2 has a smaller value of A_4 than any $[n,n-r]$ codes with $d=4$ obtained by shortening of linear codes nonequivalent to the Π code.

Proof: See the Appendix. □

Let $r=9$, $i=23$, $q=5$, $k_1=31$, $k_2=30$, $k_3=29$, $k_4=27$, and $k_5=23$. The parity check matrix H_{137} of the [137,128] code obtained from P_9 by Algorithm 2 has the following form:

$$H_{137}=\left[\begin{array}{c|c|c|c|c|c|c|c|c}
B_0 & B_1 & \cdots & B_{22} & \hat{B}_{23} & B_{24} & B_{25} & B_{26} & B_{28}\\
\hline
G & G & \cdots & G & \hat{G} & G & G & G & G
\end{array}\right], \tag{13}$$

where $\hat{B}_{23}=[b_{23}b_{23}]$ is 5×2 matrix; $\hat{G}=[g_1g_2]$ is 4×2 matrix.

For H_{137}: $A_4=45488$, $\Delta_3=0.5660$, $\Gamma=62$. (Note that we construct the parity check matrix of the [137,128] Π code with $A_4=45443$, but this matrix does not have a regular structure).

For the Hamming code:

$$a_4^H(137,9)\geq 15182,\ \Delta_3^H(137,9)\leq 0.4735,\ \Gamma\geq 54,$$

[4], [9]. [13]. In [4] the parity check matrix of the [137,128] Hamming code with $A_4=56252$, $\Delta_3=0.4733$, $\Gamma=55$ is described.

Algorithm 2 gives matrices with more regular structure than Algorithm 1. For example, the parity check matrix H_{72}^* of the [72,64] Π code obtained by Algorithm 2 is more regular than H_{72}. For H_{72}^*: $A_4=6657$, $\Gamma=35$.

III. Parity Check Matrices of the Π Codes Detecting Byte Errors of Length 4

The parity check matrix H_{72}^4 of the [72,64] Π code detecting byte errors of length 4 has the following form:

$$H_{72}^4=\left[\begin{array}{c|c|c|c|c|c|c|c|c}
0000 & 0000 & 0000 & & 1111 & 1111 & 1111 & 0001 & 0001\\
0000 & 0000 & 0000 & \cdots & 1111 & 1111 & 1111 & 0010 & 0110\\
0000 & 0000 & 1111 & & 0000 & 1111 & 1111 & 0100 & 1011\\
0000 & 1111 & 0000 & & 1111 & 0000 & 1111 & 1000 & 1100\\
\hline
1000 & 1000 & 1000 & & 1000 & 1000 & 1000 & 1111 & 1111\\
0100 & 0100 & 0100 & \cdots & 0100 & 0100 & 0100 & 1111 & 1111\\
0010 & 0010 & 0010 & & 0010 & 0010 & 0010 & 1111 & 1111\\
0001 & 0001 & 0001 & & 0001 & 0001 & 0001 & 1111 & 1111
\end{array}\right]. \tag{14}$$

The syndromes of byte errors of length 4 are not identical with any column of the matrix H_{72}^4. For H_{72}^4: $A_4 = 7221$, $\Delta_3 = 0.5156$, $\Gamma = 36$.

Corresponding matrices for the Hamming code have $A_4 = 8408$, $\Delta_3 = 0.4363$, $\Gamma = 27$ [4] and $A_4 = 8200$, $\Delta_3 = 0.45$, $\Gamma = 31$ [15].

The parity check matrix H_{137}^4 of the [137,128] Π code detecting the byte errors of length 4 has the following form:

$$H_{137}^4 = \left[\begin{array}{c|c} 0\cdots 0 & 1\cdots 1 \\ \hline H_{72}^4 & H_{65}^4 \end{array}\right], \tag{15}$$

where H_{65}^4 is the matrix H_{72}^4 with the last 7 columns omitted. For H_{137}^4: $A_4 = 54885$, $\Delta_3 = 0.4763$, $\Gamma = 68$. For the Hamming code the corresponding matrix $H^{(10)}$ in [4] has $A_4 = 57339$, $\Delta_3 = 0.4529$, $\Gamma = 65$.

Conclusion

The Π code proposed by Panchenko belongs to the class of SEC–DED codes. In this correspondence we construct the parity check matrices of the [39,32], [72,64], and [137,128] shortened Π codes. The obtained matrices provide a smaller number of words of weight 4 and a larger probability of triple-independent-error detection as compared with the Hamming codes.

The constructed [39,32] and [72,64] shortened Π codes have the minimum number of words of weight 4 in the class of all linear codes with the same parameters.

On the other hand, the parity check matrices of the Π code have more 1's in rows than corresponding matrices of the Hamming code.

The Π code is a reasonable alternative to the Hamming code in the class of SEC–DED codes.

Acknowledgment

The authors thank the referees for their helpful suggestions.

Appendix

Notations and Definitions.

The set of numbers F_j (see (8)) is called an *F spectrum*. If external columns are partitioned into noncross groups, then $F_j^{(v)}$ denotes the number of columns belonging to vth group, for which $m(t) = j$. The set of numbers $F_j^{(v)}$ is called a *partial F spectrum*. Obviously,

$$F_j = \sum_v F_j^{(v)}. \tag{A.1}$$

Denote by $G_i = [g_i \ g_i \cdots g_i]$ a matrix consisting of equal columns g_i, where g_i is the binary 4-bit representation of i. Let $B^* = [b_0 b_1 \cdots b_{D-1}]$ be a $(r-4)\times 2^{r-4}$ matrix consisting of all distinct columns b_j of length $r-4$, where b_j is the binary representation of j. Denote by $B^*(d_1,\cdots,d_k)$ the matrix B^* with columns $b_{d_1},\cdots,b_{d_k}$ omitted. Let

$$A_0 = \left[\frac{B^*(0)}{G_0}\right], \qquad A_i = \left[\frac{B^*}{G_i}\right],$$

$$A_i(d_1,\cdots,d_k) = \left[\frac{B^*(d_1,\cdots,d_k)}{G_i}\right], \qquad i = 1,\cdots,15.$$

The matrix P_r can be represented as follows:

$$P_r = [A_1 A_2 A_4 A_8 A_{15}].$$

Let $Y = \{1,2,4,8,15\}$, $U = \{3,5,6,7,9,10,11,12,13,14\}$.

Definition: Let

$$a = \left[\frac{b_{i_a}}{g_k}\right] \in A_k, \ k \in \{0,\cdots,15\}.$$

Then b_{i_a} is called the locator of column a, and g_k is called the indicator of column a.

Proof of Theorem 1: We consider the case $i = 8$. For $i \neq 8$ the proof is analogous.

For $i = 8$ the Π code shortened by Algorithm 1 has the following parity check matrix:

$$H_{5D-8} = [A_1(\gamma)A_2(\gamma)A_4(\gamma,\mathscr{H})A_8(\gamma,\nu)A_{15}(\gamma,\delta)].$$

The deleted columns of P_r are external for a shortened matrix, but these columns cannot be represented in the form (7). Hence, the F spectrum does not depend on the deleted columns. All sums of the form $g_i + g_j$ for $i,j \in Y$, $i \neq j$, are distinct:

$$\begin{aligned} &g_1 + g_2 = g_3;\ g_4 + g_8 = g_{12},\ g_4 + g_{15} = g_{11},\ g_8 + g_{15} = g_7; \\ &g_1 + g_4 = g_5,\ g_1 + g_8 = g_9,\ g_1 + g_{15} = g_{14}, \\ &g_2 + g_4 = g_6,\ g_2 + g_8 = g_{10},\ g_2 + g_{15} = g_{13}. \end{aligned} \tag{A.2}$$

For any external column $a \in A_k$, $k \neq 0$, in every sum of the relation (7) one summand belongs to a matrix A_i and the other summand belongs to a matrix A_s, where $i,s \in Y$, $g_i + g_s = g_k$. For $a \in A_0$ both summands belong to a matrix A_i, $i \in Y$. For the matrix H_{5D-8} we partition external columns into 4 groups: 1) the matrix A_0, 2) the matrix A_3, 3) the matrices $A_5, A_6, A_9, A_{10}, A_{13}, A_{14}$, 4) the matrices A_7, A_{11}, A_{12}. Partial F spectrums of external columns belonging to different matrices of one group are equal (see (A.2)). The partial F spectrums of the groups of columns are as follows:

$$\begin{aligned} &j = \{E-8, E-7\},\ F_j^{(1)} = \{D-4, 3\}; \\ &j = \{D-2, D-1\},\ F_j^{(2)} = \{D-1, 1\}; \\ &j = \{D-4, D-3\},\ F_j^{(3)} = \{3D-12, 12\}; \\ &j = \{D-3, D-2\},\ F_j^{(4)} = \{6D-12, 12\}. \end{aligned} \tag{A.3}$$

For example, we calculate $F_j^{(3)}$. Columns $b_\gamma, b_\nu, b_{\mathscr{H}}$ are distinct, so columns of A_{12} with locators $b_\gamma + b_\gamma = b_0, b_\gamma + b_\nu, b_\gamma + b_{\mathscr{H}}, b_\nu + b_{\mathscr{H}}$ can be obtained by $D-3$ ways as a sum of columns belonging to $A_4(\gamma,\mathscr{H})$ and $A_8(\gamma,\nu)$. Everyone of the other $D-4$ columns of A_{12} is obtained in $D-4$ ways. We may consider A_{11} and A_7 in the same way. Therefore, in the third group of external columns $m(t) = D-3$ for $3\cdot 4 = 12$ columns and $m(t) = D-4$ for $3(D-4) = 3D-12$ columns.

So it is important that columns $b_\gamma, b_\delta, b_\nu, b_{\mathscr{H}}$ are distinct but the F spectrum does not depend on concrete values of $\gamma, \delta, \nu, \mathscr{H}$.

The proof of necessity can be obtained from (A.1) and (A.3). □

Proof of Theorem 2: According to [12], in the range (5) the following linear binary codes with $d = 4$ exist: the Π code and its shortenings, the shortened Hamming codes, the Ω code and its shortenings.

We show that the shortened Π code obtained by Algorithm 1 is the best code over all shortened Π codes. For $n-1$ external columns the number of representations $m(t)$ is reduced by one if the code of length n is shortened by one symbol. According to (8), in order to minimize the value of A_4 in a shortened code we should reduce the maximal values of $m(t)$. For the nonshortened Π code external columns can be partitioned into 2 groups: 1) the matrix A_0, 2) the matrices A_k, $k \in U$. The partial F spectrums of these groups of columns are as follows:

$$j=\{E\}, F_j^{(1)}=\{D-1\}; \mathscr{H}=\{D\}, F_{\mathscr{H}}^{(2)}=\{10D\}. \quad \text{(A.4)}$$

Therefore, in the range (5) for any shortening of the Π code by $i \le 8$ symbols we have $j > \mathscr{H}$.

Denote by Π^f a shortened Π code. For the code Π^f we introduce the following notations. Let X^f be the set of deleted columns of P_r and let X_i^f be the set of deleted columns with the indicator g_i, $i \in Y$. Obviously,

$$X^f = \bigcup_{i \in Y} X_i^f.$$

Let the column

$$\begin{bmatrix} \dfrac{b_{k_i}}{g_i} \end{bmatrix}$$

be a representative of the set X_i^f. Denote by X_*^f a set containing one representative of every $X_i^f \neq \varnothing$, $i \in Y$. Let $|X|$ be the cardinality of a set X. Evidently, $X_*^f \subseteq X^f$, $|X_*^f| \le 5$. Let the set of numbers $F_k^{(v,f)}$ be the partial F spectrum of columns belonging to the matrix A_v, $v \in U$. Denote by $F^{(v,f)}$ this partial F spectrum.

Lemma 1: For any X^f, X_*^f there exists on equivalent the matrix P_r for which all columns of X_*^f have equal locators.

Proof: We give the algorithm of this equivalent transformation. Assume that $X_i^f \neq \varnothing$, $i \in Y$, i.e., $|X_*^f| = 5$. Let $u(j) = 2^{j-1}$.

1) For $j = 2,3,4$ we sum the $(r+1-j)$th row of P_r with the rows in which $b_{k_{u(j)}}$ differs from b_{k_1}. As a result four columns of X_*^f have locator b_{k_1} and the fifth one has a locator $b_{k_{15}}^*$.
2) We add the sum of the 4 lower rows of P_r to the rows in which b_{k_1} differs from $b_{k_{15}}^*$. Now all columns of X_*^f have locator $b_{k_{15}}^*$. □

Let

$$X_{\max}^f = \max_{i \in Y} |X_i^f|, \; X_{\min}^f = \min_{i \in Y} |X_i^f|.$$

A set X^f is called nonoptimal if $X_{\max}^f - X_{\min}^f \ge 2$. Denote by $A_4(\Pi^f)$ the number of words of weight 4 in Π^f.

Lemma 2: Let Π^1 be a code such that the set X^1 is nonoptimal and $|X^1| \le 8$. Then there is a code Π^2 with $|X^2| = |X^1|$, $A_4(\Pi^2) < A_4(\Pi^1)$.

Proof: Let $X_{\min}^1 = |X_1^1|$, $X_{\max}^1 = |X_2^1|$.

Since X^1 is a nonoptimal set and $|X^1| \le 8$, we have $X_{\min}^1 = |X_1^1| \le 1$. So we should consider two cases: $X_{\min}^1 = 0$ and $X_{\min}^1 = 1$. We consider the first case. (The second case can be studied in much the same way.)

For $i = 2,4,8,15$ we assume that $|X_i^1| > 0$. Let

$$X_i^1 = \left\{ \frac{b_{k_i}}{g_i}, \cdots, \frac{b_{r_i}}{g_i} \right\}, \qquad i \in \{2,4,8,15\}.$$

By Lemma 1, $b_{k_2} = b_{k_4} = b_{k_8} = b_{k_{15}}$. Let Π^2 be the code with

$$X^2 = X^1 \cup \left\{ \frac{b_{r_2}}{g_1} \right\} \Big\backslash \left\{ \frac{b_{r_2}}{g_2} \right\}. \quad \text{(A.5)}$$

From (A.5), it follows that

$$|X^1| = |X^2|, \; X_i^2 = X_i^1, \qquad i = 4,8,15,$$

$$X_2^2 = X_2^1 \Big\backslash \left\{ \frac{b_{r_2}}{g_2} \right\}, \qquad X_1^2 = X_1^1 \cup \left\{ \frac{b_{r_2}}{g_1} \right\} = \left\{ \frac{b_{r_2}}{g_1} \right\}.$$

Constructions of codes Π^1, Π^2 result in

$$F^{(7,1)} = F^{(7,2)}, \; F^{(11,1)} = F^{(11,2)}, \; F^{(12,1)} = F^{(12,2)}. \quad \text{(A.6)}$$

According to (8), (A.1), it holds that

$$A_4(\Pi^f) = \frac{1}{3} \sum_{v \in U} \sum_{k=2}^{[n/2]} \binom{k}{2} F_k^{(v,f)}. \quad \text{(A.7)}$$

Let

$$\Phi_v \triangleq \sum_{k=2}^{[n/2]} \binom{k}{2} \left(F_k^{(v,1)} - F_k^{(v,2)} \right).$$

From (A.6), it follows that $\Phi_v = 0$ for $v = 7,11,12$. Now we can compare the partial $F^{(0,f)}$ spectrums. For this comparison we use the code Π^3 with

$$X^3 = X^1 \Big\backslash \left\{ \frac{b_{r_2}}{g_2} \right\} = X^2 \Big\backslash \left\{ \frac{b_{r_2}}{g_1} \right\}.$$

For the code Π^1, we see there are (resp. Π^2) $2^{r-4} - |X_1^2|$ (resp. $2^{r-4} - 1$) columns of A_0 for which the value of $m(t)$ is decreased by one with respect to the code Π^3.

Let $C = |X_2^1| - 1$, $N_j = 2^{r-4} - |X_j^1|$. For a code Π^f denote by $k(v,f,u)$ the number of representations in (7) of the uth column belonging to A_v. From the constructions of codes Π^1, Π^2 it follows that $|k(v,1,u) - k(v,2,u)| \le 1$. Consequently,

$$\Phi_0 = \sum_{u=1}^{C} \left(\binom{k(0,1,u)}{2} - \binom{k(0,1,u)-1}{2} \right)$$
$$= \sum_{u=1}^{C} \left(k(0,1,u) - 1 \right). \quad \text{(A.8)}$$

Reasoning along similar lines, we obtained (A.9)–(A.12).

$$\Phi_3 = \sum_{u=1}^{C} \left(k(3,1,u) - 1 \right). \quad \text{(A.9)}$$

$$\Phi_5 + \Phi_6 = \sum_{u=1}^{N_4} \left(k(5,1,u) - k(6,1,u) \right) > 0. \quad \text{(A.10)}$$

The last formula follows from relations $|X_2^1| > |X_1^1| + 1 = |X_1^2|$, $|X_4^1| = |X_4^2|$. From these statements we can obtain that $k(5,1,u) > k(6,1,u)$ for any u. In addition, the columns

$$\begin{bmatrix} \dfrac{b_{r_2}}{g_2} \end{bmatrix}, \qquad \begin{bmatrix} \dfrac{b_{r_2}}{g_1} \end{bmatrix}$$

have equal locators. In much the same way we have

$$\Phi_9 = \Phi_{10} = \sum_{u=1}^{N_8} (k(9,1,u) - k(10,1,u)) > 0, \quad \text{(A.11)}$$

$$\Phi_{13} + \Phi_{14} = \sum_{u=1}^{N_{15}} (k(14,1,u) - k(13,1,u)) > 0. \quad \text{(A.12)}$$

Let $\pi > 0$. From (A.7)–(A.12), it follows that

$$A_4(\Pi^1) - A_4(\Pi^2) = \sum_{u=1}^{|X_2^1|} k(0,1,u) - \sum_{m=1}^{|X_2^1|} k(3,1,m) + \pi. \quad \text{(A.13)}$$

From (A.4), it follows that $k(0,1,u) > k(3,1,m)$ for any $m, u \in \{1,\cdots,2^{r-4}\}$. Consequently, $A_4(\Pi^1) > A_4(\Pi^2)$. □

According to Lemmas 1 and 2, the code obtained by Algorithm 1 is optimal for any $i \leq 6$. If $i = 7$, we should consider two nonequivalent shortened Π codes: 1) the code obtained by Algorithm 1; 2) the code obtained by deleting the following columns:

$$Z \triangleq \left\{ \frac{b_\gamma}{g_{15}}, \frac{b_\gamma}{g_8}, \frac{b_\gamma}{g_4}, \frac{b_\gamma}{g_2}, \frac{b_\gamma}{g_1}, \frac{b_\delta}{g_{15}}, \frac{b_\delta}{g_8} \right\}. \quad \text{(A.14)}$$

If $i = 8$, we should consider three nonequivalent shortened Π codes: 1) the code obtained by Algorithm 1; 2) and 3) the codes obtained by deleting of the following columns:

$$\left\{ Z, \frac{b_\nu}{g_4} \right\} \text{ and } \left\{ Z, \frac{b_\delta}{g_4} \right\} \text{ respectively.} \quad \text{(A.15)}$$

We obtain the F spectrums in the cases (A.14), (A.15) and conclude that the Π code obtained by Algorithm 1 has a smaller value of A_4 than other Π codes.

According to [19], in the range (5) for any length n there exists a shortened $[n, n-r]$ Π code that has a smaller value of A_4 in comparison with any shortened $[n, n-r]$ Hamming code. Hence, the Π code shortened by Algorithm 1 has a smaller value of A_4 than any shortened Hamming code with the same parameters.

The range (5) contains the Ω code only for $r = 6, 7, 8$. In the range (5) we obtained the values of A_4 for the Ω code using a computer. These values are larger than the Π codes shortened by Algorithm 1. For example, the [72,64] Ω code has $A_4 = 7742$ (compare with Table I). This finishes the proof of Theorem 2. □

Proof of Theorem 3: According to [12], we consider the Hamming code, the Π code, and the Ω code.

The range (6) includes the Ω code only for $r = 6, \cdots, 9$. We obtained the value of A_4 for the Ω code with $r = 6, 7, 8$, by hand and for $r = 9$, $n \geq 141$ by computer. Algorithm 2 gives smaller values. The F spectrum of the $[144, 144-9]$ Ω code is as follows: $j = \{72, 48, 16\}$, $F_j = \{15, 112, 240\}$. Hence, any shortened [137,128] Ω code cannot be better than the [137,128] Ω code with F spectrum of the form $j = \{65, 41, 16, 15\}$, $F_j = \{15, 112, 149, 91\}$ and with $A_4 = 50159$. But according to (12), the [140,131] Π code shortened by Algorithm 2 with $i = 20$ has $A_4 = 49670$.

The Hamming code is a code with even weights. According to [9] and [11, formula (3)], it follows that for shortened Hamming codes $A_4 > \binom{n}{2}\left(\binom{n}{2}/2^{r-1} - 1\right)/6$. It can be verified that in the range (6) for the shortened Hamming codes the values of A_4 are larger than for the Π code shortened by Algorithm 2. □

References

[1] F. J. Aichelmann, Jr., "Fault-tolerant design techniques for semiconductor memory applications," *IBM J. Res. Develop.*, vol. 28, no. 2, pp. 177–183, Mar. 1984.

[2] J. Arlat and W. C. Carter, "Implementation and evaluation of a (b, k)-adjacent error-correcting/detecting scheme for supercomputer systems," *IBM J. Res. Develop.*, vol. 28, no. 2, pp. 159–169, Mar. 1984.

[3] S. Azumi and T. Kasami, "Of optimal modified Hamming codes," *Trans. Inst. Electr. Commun. Eng. Jap.*, vol. A58, no. 6, pp. 325–330, 1975.

[4] I. M. Boyarinov, A. A. Davydov, and B. M. Shabanov, "Error correction in main memory of a high-capacity computer," *Automat. Remote Contr.*, vol. 48, no. 7, pt. 2, pp. 956–965, 1987. (Transl. from Russian.)

[5] C. L. Chen, "Error-correcting codes with byte error detection capability," *IEEE Trans. Comput.*, vol. C-32, no. 7, pp. 615–621, July 1983.

[6] C. L. Chen, "Byte oriented error-correcting codes for semiconductor memory systems," *IEEE Trans. Comput.*, vol. C-35, no. 7, pp. 646–648, July 1986.

[7] C. L. Chen and M. Y. Hsiao, "Error-correcting codes for semiconductor memory applications: A state-of-art review," *IBM J. Res. Develop.*, vol. 28, no. 2, pp. 124–134, Mar. 1984.

[8] A. A. Davydov and A. Yu. Drozhzhina-Labinskaya, "Correction of error bytes of length 4 and double independent errors by the Bose–Chaudhuri–Hocquenghem code in semiconducting memory units," *Avtomatika i Telemechanika*, no. 11, pp. 135–146, Nov. 1989 (in Russian).

[9] A. A. Davydov, L. N. Kaplan, Yu. B. Smerkis, and G. L. Tauglikh, "Optimization of shortened Hamming codes," *Probl. Inform. Transm.*, vol. 17, no. 4, pp. 261–267, Oct.–Dec. 1981 (transl. from Russian).

[10] A. A. Davydov and L. M. Tombak, "The alternative to the Hamming codes for a correction of single errors in memory units of supercomputers," in *Proc. II All Union Conference Actual Probl. Informatics and Comput.* (INFORMATICS–87), Erevan, U.S.S.R., Oct. 1987, pp. 23–25 (in Russian).

[11] ____, "Number of minimal-weight words in block codes," *Probl. Inform. Transm.*, vol. 24, no. 1, pp. 7–18, Jan.–Mar. 1988 (transl. from Russian).

[12] ____, "Quasiperfect linear binary codes with minimum distance 4 and complete caps in projective geometry," *Probl. Peredach. Inform.*, vol. 25, no. 4, pp. 11–23, Oct.–Dec. 1989 (in Russian).

[13] M. Y. Hsiao, "A class of optimal minimum odd-weight-column SEC–DED codes," *IBM J. Res. Develop.*, vol. 14, no. 4, pp. 395–401, July 1970.

[14] K. Iwasaki, T. Kasami, and S. Yamamura, "Optimal (72,64) modified Hamming codes in the sense of Hsiao," *Trans. Inst. Electr. Commun. Eng. Jap.*, vol. A61, no. 3, pp. 270–271, 1978.

[15] S. Kaneda, "A class of odd-weight-column SEC–DED–SbED codes for memory system applications," *IEEE Trans. Comput.*, vol. C-33, no. 8, pp. 737–739, Aug. 1984.

[16] ____, "A class of SEC–DED–SbED codes for semiconductor memory systems," *Syst. Comput. Jap.*, vol. 16, no. 5, pp. 88–96, 1985.

[17] S. Kaneda and E. Fujiwara, "Single-byte error-correcting double-byte error-detecting codes for memory systems," *IEEE Trans. Comput.*, vol. C-31, no. 7, pp. 596–602, July 1982.

[18] S. Lin and D. J. Costello, *Error control coding: Fundamentals and Applications*, Englewood Cliffs, NJ: Prentice-Hall, 1983.

[19] V. I. Panchenko, "On optimization of linear code with minimum distance 4," in *Proc. VIII All Union Conf. Coding Theory Inform. Transm., pt. II: Coding theory*, Moscow–Kuibyshev, U.S.S.R., pp. 132–134, 1981 (in Russian).

[20] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[21] A. A. Davydov, S. I. Samoilenko, V. V. Zolotarev, and E. I. Tretiakova, *Computer Networks: Adaptability, Noise Immunity, Reliability*. Moscow: Nauka, 1981.