TABLE III
$q = 9$

Theorem	t	m	l	n	k	d	d_B
2.6	1	3	2	37	6	27	25
2.6	1	4	3	37	10	22	20
2.6	1	5	4	37	15	17	16
2.6	1	6	5	37	21	12	11
2.6	1	7	6	37	28	7	6
2.6	3	3	2	39	6	28	26
2.6	3	4	3	39	10	23	22
2.6	3	5	4	39	15	18	17
2.6	3	6	5	39	21	13	12
2.6	3	7	6	39	28	8	7
2.6	5	4	3	41	10	24	23
2.6	5	7	6	41	28	9	8
2.6	7	5	4	43	15	20	19
2.6	7	6	5	43	21	15	14
2.6	9	3	2	45	6	33	31
2.6	9	4	1	45	8	29	28
2.6	9	4	2	45	9	28	27
2.6	9	4	3	45	10	27	26
2.6	9	6	5	45	21	16	15
-	-	-	-	-	-	-	-

we just use Theorem 2.6 in our tables. However, for even q, Theorem 2.10 does not include the case where $l = m - 1$, i.e., the result of Theorem 2.9 is not contained in Theorem 2.10.

- t, m paramters in Theorems 2.6, 2.9, or 2.10.
- l parameter in Theorems 2.6 or 2.10.
- n, k length and dimension of codes, respectively, obtained from Theorems 2.6, 2.9, or 2.10 with given parameters t, m, l.
- d lower bounds on minimum distance of codes obtained from Theroems 2.6, 2.9, or 2.10 with given parameters t, m, l.
- d_B the lower bound on minimum distance of codes with given length n and dimension k quoted from Brouwer's table [1].

Remark 3.1: Besides codes directly coming from our construction, many new codes can be obtained from some codes in our tables in obvious ways. For example, in the table for $q = 7$, there is a 7-ary $[28, 6, 18]$ linear code, lengthening the code gives a new $[29, 6, 18]$ code.

ACKNOWLEDGMENT

The authors wish to thank two referees for their helpful comments on the earlier version of the correspondence. Special thanks go to one of the referees for very useful and detailed suggestions.

REFERENCES

[1] A. Brouwer. Bounds on the minimum distance of linear code. [Online]. Available: http://www.win.tue/nl/~aeb/voorlincod.html

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[3] M. A. Tsafasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.

Optimal Codes for Single-Error Correction, Double-Adjacent-Error Detection

Marina Biberstein and Tuvi Etzion, *Senior Member, IEEE*

***Abstract*—In certain memory systems the most common error is a single error and the next most common error is two errors in positions which are stored physically adjacent in the memory. In this correspondence we present optimal codes for recovering from such errors. We correct single errors and detect double adjacent errors. For detecting adjacent errors we consider codes which are byte-organized. In the binary case, it is clear that the length of the code is at most $2^r - r - 1$, where r is the redundancy of the code. We summarize the known results and some new ones in this case. For the nonbinary case we show an upper bound, called "the pairs bound," on the length of such code. Over GF (3) codes with bytes of size 2 which attain the bound exist if and only if perfect codes with minimum Hamming distance 5 over GF(3) exist. Over GF (4) codes which attain the bound with byte size 2 exist for all redundancies. For most other parameters we prove the nonexistence of codes which attain the bound.**

***Index Terms*—Byte-organized memory, double-adjacent errors, single-error correction, the pairs bound.**

I. INTRODUCTION

In certain memory systems, e.g., some spacecraft memories subject to soft upsets, the most common error is a single error and the next most common error is a *double-adjacent error*, i.e., two errors in bits which are stored physically adjacent in the memory [7]. This motivates the interest in codes which correct single errors and detect double-adjacent errors. An $[n, k, d]$ error-correcting code is a k-dimensional subspace of the n-dimensional space, in which it is possible to correct any $\lfloor \frac{d-1}{2} \rfloor$ or less errors which occur in any positions (bits) of the n positions of the codeword. Double-adjacent errors can occur in any of the $n-1$ pairs of consecutive bits. However, in most memory and storage devices, the information is stored in bytes of a given size b. Therefore, the words

Manuscript received January 27, 1999; revised March 28, 2000. This work was supported in part by the fund for the promotion of research at the Technion, in part by the Technion V.P.R. fund—fund for the promotion of sponsored research, and in part under Grant 88/99-1 from the Israeli Science Foundation. This research was performed while the first author was studying for the M.Sc. degree in the Computer Science Department of the Technion.

M. Biberstein is with IBM Research Laboratory in Haifa, Haifa 31905, Israel (e-mail: biberstein@il.ibm.com).

T. Etzion is with the Computer Science Department, Technion—Israel Institute of Technology, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

Communicated by A. Barg, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)07010-3.

of length n in the code are divided into $\frac{n}{b}$ consecutive nibbles, each one of size b. An error event can occur in a few positions of the same byte. Therefore, by double-adjacent errors we refer to any of the $b-1$ pairs of consecutive bits in any of the $\frac{n}{b}$ bytes. For more information on byte-oriented error-correcting codes, burst-correcting codes, and their applications the reader is referred to [3], [4], and [6].

Let $F_q = \mathrm{GF}(q)$ denote the Galois field with q elements and $F_q^* = \mathrm{GF}^*(q)$ the multiplicative group of the same field, i.e., $F_q^* = F_q \backslash \{0\}$. Let $(n,\ k)$ code denote a linear code of length n and dimension k, and let $SD_q(b)$ code denote a code over F_q which corrects single errors and detects double-adjacent errors in bytes of size b. The main purpose of this correspondence is to explore optimal $SD_q(b)$ codes for $q > 2$, i.e., nonbinary codes.

The remainder of this correspondence is organized as follows. In Section II, we consider $SD_q(b)$ codes. For $q > 2$, we show a bound which ties together the length of the code, its redundancy, the size of the bytes, and the field size. Codes which attain this bound with equality are constructed and it is shown that for most parameters there exist no codes which attain the bound. An interesting connection between $SD_3(2)$ codes and perfect codes over $\mathrm{GF}(3)$ is also given. In Section III, we summarize the known results for $q = 2$, the binary case, and present new results obtained in [1]. Conclusions and a list of open problems are given in Section IV.

II. Nonbinary Codes and the Pairs Bound

A. Preliminaries

In this section we consider codes over $\mathrm{GF}(q)$, $q > 2$, which correct single errors and detect double-adjacent errors. Let C be an $(n,\ n-r)$ $SD_q(b)$ code, whose parity-check matrix is $H = [h_1,\ \ldots,\ h_n]$. The vectors $\alpha h_i,\ \alpha \in \mathrm{GF}^*(q)$ are single-error syndromes which correspond to errors in the ith coordinate. The syndromes that correspond to a double error in the coordinates i and $i+1$ are all the vectors of the form $\alpha h_i + \beta h_{i+1}$, where $\alpha,\ \beta \in \mathrm{GF}^*(q)$. For a vector $v \in F_q^n$, the set $L(v) = \{\alpha v | \alpha \in F_q^*\}$ is called the *line* of v. If the line contains single-error syndromes, we say it is a *single-error syndromes line*; if the line contains double-error syndromes, we say it is a *double-error syndromes line*, where in this correspondence a double error is always an error in two adjacent coordinates. For two adjacent coordinates i and $i+1$, the set of all the syndromes that correspond to these coordinates is equal to $\mathrm{span}\,(h_i,\ h_{i+1})$, where $\mathrm{span}\,(V)$ denotes the linear space spanned by the elements of V. This set of syndromes will be denoted by $S(i,\ i+1)$ and called the $(i,\ i+1)$ *syndromes set*. Some of the properties of the syndromes sets are described in the following lemma.

Lemma 1:

2) A syndromes set contains $q+1$ syndromes lines, two of which are single-error syndromes lines and the remaining $q-1$ are double-error syndromes lines.
3) Any pair of representatives of different syndromes lines from a syndromes set spans the whole syndromes set.
4) Any single-error syndrome that corresponds to an error in the first/last coordinate of a byte belongs to a single syndromes set. Any single-error syndrome that corresponds to an error inside a byte belongs to two syndromes sets.

Proof:

2) By definition, $S(i,\ i+1)$ consists of all the vectors of the form

$$\alpha_i h_i + \alpha_{i+1} h_{i+1}, \alpha_i,\ \alpha_{i+1} \in \mathrm{GF}(q).$$

All the multiples of h_i and h_{i+1} form two single-error syndromes lines. All the vectors of the form

$$\alpha_i h_i + \alpha_{i+1} h_{i+1}, \alpha_i,\ \alpha_{i+1} \in \mathrm{GF}^*(q)$$

belong to $q-1$ double-errors syndromes lines.

3) The syndromes set $S(i,\ i+1)$ is equal to $\mathrm{span}\,(h_i,\ h_{i+1})$ and hence it has dimension 2 and any two linearly independent vectors from the set span it.
4) If i is the first coordinate in some byte, then h_i belongs to $S(i,\ i+1)$. If i is the last coordinate in some byte, then h_i belongs to $S(i-1,\ i)$. If i is in the middle of the byte, then h_i belongs both to $S(i-1,\ i)$ and to $S(i,\ i+1)$.

B. The Pairs Bound

We start with a bound which ties together the length of the code, its redundancy, the size of the bytes, and the size of the alphabet.

Theorem 1: If C is an $(n,\ n-r)$ $SD_q(b)$ code and $t = \frac{q^r-1}{q-1} - n$ then

$$(q^r - 1 - (q-1)t)(b-1)(q-2) \le bt(t-1), \qquad b|n \quad (1)$$

Proof: The proof is by enumeration of syndromes lines. Recall that a double-error syndrome line can occur in a few syndrome sets as it corresponds to a detected error. However, a pair of double-error syndromes lines can occur together only in one syndromes set since by Lemma 1 we can span the whole set, including the single-error syndromes, from this pair. Let C be an $(n,\ n-r)$ $SD_q(b)$ code. Since the code is organized in bytes of size b, it follows that b divides n. n is also the number of lines used as single-error syndromes lines. The number of lines in F_q^r is $\frac{q^r-1}{q-1}$. Hence, $t = \frac{q^r-1}{q-1} - n$ is the number of lines that are not single-error syndromes lines. Therefore, t is an upper bound on the number of double-error syndromes lines, and $\frac{t(t-1)}{2}$ is an upper bound on the number of pairs of double-error syndromes lines. On the other hand, the number of bytes of length b is $\frac{n}{b}$, and the number of syndromes sets induced by a byte is $b-1$. Therefore, there are $\frac{n}{b}(b-1)$ syndromes sets, each containing $q-1$ double-error syndromes lines, i.e., $\frac{(q-1)(q-2)}{2}$ pairs of double-error syndromes lines. Hence, the total number of pairs of double-error syndromes lines in the syndromes set of an $(n,\ n-r)$ $SD_q(b)$ code is $\frac{n}{b}(b-1)\frac{(q-1)(q-2)}{2}$. Thus we have the following inequality:

$$\frac{\frac{q^r-1}{q-1} - t}{b}(b-1)\frac{(q-1)(q-2)}{2} \le \frac{t(t-1)}{2},$$

which reduce to

$$(q^r - 1 - (q-1)t)(b-1)(q-2) \le bt(t-1). \qquad \square$$

The bound of (1) will be called the *pairs bound*. We are interested in codes that attain (1) with equality. We will say that such code attains (or meets) the bound.

We found two families of parameters that attain (1). The first family is for $q = 3$, $b = t = 3^{r/2} - 1$, r even. This family is discussed in Section II-C. We have been able to show that there exists no code with parameters given by the first nontrivial member of this family. However, the question of existence of codes for other parameters from this family remains open. The second family is for $q = 4$, $b = 2$, $t = 2^r - 1$, and $r \ge 2$. This family is discussed in Section II-D. It is shown that for each set of parameters from this family there exists a corresponding $SD_4(2)$ code.

In Section II-C we show that there exists no $SD_q(b)$ code with $q > 3$ and $b > 2$ that meets the pairs bound. A computer search which checked for other parameters attaining the pairs bound for $5 \le q \le 101$, $b = 2$, and $3 \le r \le 1000$ found no such parameters. In another

computer search for parameters that attain the pairs bound with $q = 3$, $3 \leq r \leq 1000$, and $2 \leq b \leq 1000$, the following parameters were found:

Byte length	Code redundancy	Code length	No. of double error syndromes
2	5	110	11
3	3	9	4
106	5	106	15

The codes with $q = 3$ and $b = 2$ are discussed in Section II-D. The parity-check matrix of the $(9, 6)$ $SD_3(3)$ code is shown in Section II-D. The last set of parameters with $b = n = 106$, $r = 5$, and $t = 15$ is discussed in Section II-C, where we show that there exist no $(n, n - r)$ $SD_3(n)$ codes.

C. Nonexistence Results

In this subsection, we will show that codes which attain the pairs bound with equality do not exist.

Theorem 2: If $q > 3$ and $b > 2$ then there is no $SD_q(b)$ code that attains the pairs bound.

Proof: Let $H = [h_1 h_2 h_3 \dots h_n]$ be the parity-check matrix of an $SD_q(b)$ code C which meets the pairs bound for $q > 3$, $b > 2$. Since C is single-error correcting double-adjacent error detecting, any three consecutive columns of H are linearly independent. Therefore, without loss of generality (w.l.o.g.) we can assume that h_i, $1 \leq i \leq 3$, is the unit vector with a ONE in the ith entry. Clearly, the double-error syndromes in $S(1, 2)$ are exactly the vectors of the form $a_x = (1x00\cdots0)^T$, $x \in \mathrm{GF}^*(q)$, and their multiples, while the double-error syndromes in $S(2, 3)$ are exactly the vectors of the form $b_y = (0y10\cdots0)^T$, $y \in \mathrm{GF}^*(q)$, and their multiples. Since C attains the pairs bound, each pair of double-error syndromes $\{a_x, b_y\}$, $x, y \in \mathrm{GF}^*(q)$ should span exactly one syndromes set.

Let $V = \mathrm{span}\,(h_1, h_2, h_3)$, i.e. V contains exactly the lines of the form $c_{\alpha,\beta} = (\alpha\beta10\cdots0)^T$. For a line $c_{\alpha,\beta} = (\alpha\beta10\cdots0)^T$, where $\alpha \neq 0$, we calculate the number of pairs $\{a_x, b_y\}$ which span it. Such a vector $c_{\alpha,\beta}$ can only be obtained from linear combinations of the form $\alpha a_x + b_y$, where the variables x, y and the parameters α, β should satisfy

$$\alpha x + y = \beta. \tag{2}$$

If $\beta = 0$, there is a nonzero solution x to (2) for every nonzero value of y, i.e., $c_{\alpha,0}$ is spanned by $q - 1$ pairs. For $\beta \neq 0$, there is a nonzero solution x to (2) for every $y \neq 0$, $y \neq \beta$, i.e., there are $q - 2$ pairs that span $c_{\alpha,\beta}$.

Two distinct pairs $\{a_x, b_y\}$, $\{a_{x'}, b_{y'}\}$ cannot belong to a common syndromes set, since both a_x and $a_{x'}$ belong to $S(1, 2)$, and both b_y and $b_{y'}$ belong to $S(2, 3)$. Therefore, since C meets the pairs bound, a vector u is spanned by N pairs $\{a_x, b_y\}$ only if it belongs to at least N syndromes sets. For $q > 4$ this implies that each $c_{\alpha,\beta}$ belongs to at least three syndromes sets. On the other hand, by Lemma 1, any single-error syndrome belongs to at most two syndromes sets. This produces a contradiction for $q > 4$, since every pair $\{a_x, b_y\}$ spans some single-error syndrome which is different from h_1, h_2, h_3.

For $q = 4$, each of the three vectors of the form $c_{\alpha,0}$ belongs to three syndromes sets. Therefore, each $c_{\alpha,0}$ is a double-error syndrome. Also, each a_x and each b_y is a double-error syndrome and hence there are nine double-error syndromes lines in V. Therefore, there are $\binom{9}{2} = 36$ pairs of double-error syndromes lines in V. Each syndromes set spanned by such a pair contains three double-error syndromes lines and, therefore, three pairs of double-error syndromes lines. Hence, there are at least $\frac{36}{3} = 12$ syndromes sets spanned by the a_x's, b_y's, and $c_{\alpha,0}$'s. Twelve syndromes sets include at least 13 single-error syndromes lines, all of them also in V. Hence, in V there are $\frac{4^3-1}{4-1} = 21$ syndromes lines, nine single-error syndromes lines, and 13 double-error syndromes lines, a contradiction.

Thus there is no $SD_q(b)$ code which attains the pairs bound if $q > 3$ and $b > 2$. □

Next, we further characterize double-error syndromes for $SD_3(b)$ codes.

Lemma 2: Let C be an $SD_3(b)$ code which attains the pairs bound and let s_1, s_2, s_3, and s_4, be four distinct double-error syndromes of C. If $\{s_1, s_2\}$ and $\{s_3, s_4\}$ belong to adjacent syndromes sets of the same byte, then whenever two of these syndromes belong to a syndromes set, the other two belong to an adjacent syndromes set in the same byte.

Proof: Let H be the parity-check matrix of C. If s_1 and s_2 belong to $S(i, i+1)$ and s_3 and s_4 belong to $S(i+1, i+2)$, where positions i, $i+1$, and $i+2$ belong to the same byte, then the $(i+1)$th column of H is spanned by both $\{s_1, s_2\}$ and $\{s_3, s_4\}$. Therefore,

$$\alpha_1 s_1 + \alpha_2 s_2 = \alpha_3 s_3 + \alpha_4 s_4, \qquad \alpha_i \neq 0.$$

Hence,

$$\alpha_1 s_1 + 2\alpha_3 s_3 = 2\alpha_2 s_2 + \alpha_4 s_4$$

and

$$\alpha_1 s_1 + 2\alpha_4 s_4 = 2\alpha_2 s_2 + \alpha_3 s_3.$$

Since C attains the pairs bound and the pairs $\{s_1, s_3\}$ and $\{s_2, s_4\}$ generate the same single-error syndrome, it follows that the pairs $\{s_1, s_3\}$ and $\{s_2, s_4\}$ are contained in adjacent syndromes sets of the same byte. The same is true for the pairs $\{s_1, s_4\}$ and $\{s_2, s_3\}$. □

Four double-error syndromes which appear in adjacent syndromes sets as described in Lemma 2 are said to belong to the same *syndromes company*.

Theorem 3: An $(n, n-r)$ $SD_3(n)$ code that meets the pairs bound cannot exist.

Proof: Let C be an $(n, n - r)$ $SD_3(n)$ code which attains the pairs bound, let H be its parity-check matrix, and t the number of its double-error syndromes lines. Let $\{s_1, s_2\}$ be the double-error syndromes in $S(1, 2)$ and $\{s_3, s_4\}$ be the double-error syndromes in $S(n - 1, n)$. W.l.o.g., we can assume that $s_1 \neq s_3$ and $s_1 \neq s_4$. Let N_1 be the number of syndromes companies that contain s_1. With each company, s_1 appears three times. If s_1 belongs to $S(i, i + 1)$ then it belongs to two syndromes companies, the one which corresponds to $S(i - 1, i)$ and $S(i, i + 1)$ and the one which corresponds to $S(i, i + 1)$ and $S(i + 1, i + 2)$, unless $i = 1$ or $i + 1 = n$. Since C meets the pairs bound, s_1 appears in $t - 1$ syndromes sets. Hence we have $2(t - 1) - 1 = 3N_1$.

Now, let s be a double-error syndrome different from s_1, s_2, s_3, and s_4. Let N_2 be the number of syndromes companies that include s. Clearly, we have $2(t - 1) = 3N_2$. Therefore, $3N_1 + 1 = 3N_2$, a contradiction. Therefore, there is no $(n, n - r)$ $SD_3(n)$ code which meets the pairs bound. □

As described in Section II-B, one family of parameters that attain the pairs bound is $q = 3$, r even, $b = t = 3^{r/2} - 1$. In this case the length of the code

$$n = \frac{3^r - 1}{2} - t = \frac{(3^{r/2} - 1)(3^{r/2} + 1)}{2} - (3^{r/2}1) = \frac{b^2}{2}$$

and hence b divides n. The only known code from this family is the trivial $SD_3(2)$ code with the parity-check matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

which has the parameters $q = 3$, $r = 2$, $b = t = 2$, and $n = 2$. We show that there is no code with parameters $q = 3$, $r = 4$, $b = t = 8$, and $n = 32$.

Theorem 4: There is no $(32, 28)$ $SD_3(8)$ code.

Proof: Assume a $(32, 28)$ $SD_3(8)$ code exists. Let S be the set of double-error syndromes lines of the code and let s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, be eight representatives of S. Since S spans F_3^4, we can assume that s_1, s_2, s_3, and s_4, are vectors of weight one. All the vectors of weight two are linear combinations of two vectors from S and hence they are single-error syndromes. Therefore, the other vectors of S should be of weights 3 and 4.

First, assume that at least three of the vectors s_5, s_6, s_7, and s_8, have weight 4. There are eight syndromes lines of weight 4 in F_3^4, and hence there will be at most five single-error syndromes lines of weight 4. For each double-error syndromes line s, the four syndromes lines of weight 4, which are obtained from s in combination with a double-error syndrome of weight one, are single-error syndromes lines. Three double-error syndromes of weight 4 produce $3 \cdot 4 = 12$ single-error syndromes lines of weight 4, each one obtained at most twice, i.e., at least six distinct single-error syndromes lines of weight 4, a contradiction. Therefore, there are at least two double-error syndromes lines of weight 3, say s_5 and s_6, and w.l.o.g. we can assume that $s_5 = s_1 + \alpha_2 s_2 + \alpha_3 s_3$, $\alpha_i \neq 0$.

If $s_6 = s_1 + 2\alpha_2 s_2 + \alpha_3 s_3$ (or $s_6 = s_1 + \alpha_2 s_2 + 2\alpha_3 s_3$), then we would have $s_6 = s_5 + \alpha_2 s_2$ ($s_6 = s_5 + \alpha_3 s_3$), a contradiction since s_6 is a double-error syndrome and $s_5 + \alpha_2 s_2$ ($s_5 + \alpha_3 s_3$) is a single-error syndrome. If $s_6 = s_1 + 2\alpha_2 s_2 + 2\alpha_3 s_3$ then $s_5 + s_6 = 2s_1$, which is a similar contradiction. Thus w.l.o.g. we can assume that $s_6 = s_1 + \beta_2 s_2 + \beta_4 s_4$, $\beta_i \neq 0$. If $\beta_2 = \alpha_2$ then $s_5 + 2\alpha_3 s_3 = s_1 + \alpha_2 s_2 = s_6 + 2\beta_4 s_4$, i.e., a single error syndrome which belongs to three syndromes sets, a contradiction. Thus $s_6 = s_1 + 2\alpha_2 s_2 + \beta_4 s_4$. We distinguish now between two cases.

Case 1: s_7 is a vector of weight 3. Since s_5, s_6, and s_7, have weight 3, they have at least one common nonzero coordinate. W.l.o.g. we can assume it is the first coordinate. Hence, from the analysis for s_6 we have that $s_7 = s_1 + 2\alpha_3 s_3 + \gamma_4 s_4$. If $s_7 = s_1 + 2\alpha_3 s_3 + \gamma_4 s_4$ then $\gamma_4 = 2\beta_4$ since $s_7 \neq s_6$, and hence $2s_5 + 2s_6 = s_7$, a contradiction.

Case 2: s_7 is a vector of weight 4, i.e., $s_7 = s_1 + \gamma_2 s_2 + \gamma_3 s_3 + \gamma_4 s_4$, $\gamma_i \neq 0$. We consider all the possible values for γ_2, γ_3, and γ_4.

- If $\gamma_2 = \alpha_2$ and $\gamma_3 = \alpha_3$ then $s_7 = s_5 + \gamma_4 s_4$, a contradiction.
- If $\gamma_2 = \alpha_2$, $\gamma_3 = 2\alpha_3$, and $\gamma_4 = \beta_4$ then $s_7 + 2s_6 = 2\alpha_2 s_2 + 2\alpha_3 s_3 = 2s_5 + s_1$, a contradiction.
- If $\gamma_2 = \alpha_2$, $\gamma_3 = 2\alpha_3$, and $\gamma_4 = 2\beta_4$ then $s_7 + s_6 = 2s_1 + 2\alpha_3 s_3 = 2s_5 + \alpha_2 s_2$, a contradiction.
- If $\gamma_2 = 2\alpha_2$ and $\gamma_4 = \beta_4$ then $s_7 = s_6 + \gamma_3 s_3$, a contradiction.
- If $\gamma_2 = 2\alpha_2$, $\gamma_3 = \alpha_3$, and $\gamma_4 = 2\beta_4$ then $s_7 + 2s_5 = \alpha_2 s_2 + 2\beta_4 s_4 = 2s_6 + s_1$, a contradiction.
- If $\gamma_2 = 2\alpha_2$, $\gamma_3 = 2\alpha_3$, and $\gamma_4 = 2\beta_4$ then $s_7 + s_5 = 2s_1 + 2\beta_4 s_4 = 2s_6 + 2\alpha_2 s_2$, a contradiction.

Thus there is no $(32, 28) SD_3(8)$ code. □

We conjecture that also for $r > 4$, no $SD_q(b)$ code with these parameters exist, but we were not able to prove this conjecture.

D. Codes Which Attain the Pairs Bound

1) Codes over GF(3): In this subsection, we consider codes over GF(3) which attain the pairs bound. First, we show a tight connection between $(n, n-r)$ $SD_3(2)$ codes that attain the pairs bound and 2-perfect codes over GF(3). An $(n, n-r)$ code C over F_q with minimum Hamming distance $2e+1$ is called *e-perfect* if for every vector v in F_q^n, the Hamming distance between v and the nearest codeword of C is at most e. If H is the parity-check matrix of C then C is e-perfect code if and only if each syndrome $u \in F_q^r$ can be represented in exactly one way as a linear combination of at most e columns from H.

Lemma 3: Let $H = [h_1, \ldots, h_n]$ be the $r \times n$ parity-check matrix of a 2-perfect code C over GF(3) and let $H_{i,j} = [h_i + h_j \; h_i + 2h_j]$, $1 \leq i < j \leq n$. Then the code $\tilde{C}$ whose parity-check matrix is

$$\tilde{H} = [H_{1,2} \;\; H_{1,3} \;\; \ldots \;\; H_{1,n} \;\; H_{2,3} \;\; \ldots \;\; H_{2,n} \;\; \ldots \;\; H_{n-1,n}] \quad (3)$$

is an $SD_3(2)$ code that meets the pairs bound.

Proof: Since C is a 2-perfect code over GF(3), it follows that

$$\{h_i | 1 \leq i \leq n\} \cup \{h_i + h_j | 1 \leq i < j \leq n\} \cup \{h_i + 2h_j | 1 \leq i < j \leq n\}$$

is a set of all $\frac{3^r-1}{2}$ nonzero syndromes lines representatives. Therefore, it is easy to verify that $\tilde{H}$ is the parity-check matrix of an $SD_3(2)$ code, where $\{h_i | 1 \leq i \leq n\}$ is a set of the double-error syndromes lines representatives. Since each pair $\{h_i, h_j\}$ of double-error syndromes appears in exactly one syndromes set which corresponds to $H_{i,j}$, it follows that $\tilde{C}$ attains the pairs bound. □

Lemma 4: Let

$$H = [H_{1,2} \;\; H_{1,3} \;\; \ldots \;\; H_{1,t} \;\; H_{2,3} \;\; \ldots \;\; H_{2,t} \;\; \ldots \;\; H_{t-1,t}],$$
$$H_{i,j} = [h_i + h_j \; h_i + 2h_j]$$

be the $r \times (t-1)t$ parity-check matrix of an $SD_3(2)$ code C, which meets the pairs bound, where $\{h_i | 1 \leq i \leq t\}$ are the double-error syndromes lines representatives. Then the code $\tilde{C}$ whose parity-check matrix is $\tilde{H} = [h_1 h_2 \ldots h_t]$ is a 2-perfect code over GF(3).

Proof: Since H is the parity-check matrix of an $SD_3(2)$ code which corrects single errors and $\{h_i | 1 \leq i \leq t\}$ are the double-error syndromes, we have that all the columns of H and $\tilde{H}$ are distinct. Since C attains the pairs bound, the elements of

$$\{h_i | 1 \leq i \leq n\} \cup \{h_i + h_j | 1 \leq i < j \leq n\} \cup \{h_i + 2h_j | 1 \leq i < j \leq n\}$$

are distinct representatives of all the $\frac{3^r-1}{2}$ nonzero lines of F_3^r. Thus $\tilde{C}$ is a 2-perfect code over GF(3). □

Corollary 1: There exists an (n, k) 2-perfect code over GF(3) if and only if there exists an $(n(n-1), n(n-2)+k)$ $SD_3(2)$ code which meets the pairs bound.

It is well known [9] that the only 2-perfect code over GF(3) is the $(11, 6)$ Golay code. Thus the only $SD_3(2)$ code that attains the pairs bound is a $(110, 105)$ $SD_3(2)$ code that can obtained from the Golay code.

Another code over GF(3) which meets the pairs bound is the following $(9, 6)$ $SD_3(3)$ code:

$$\left[\begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 & 1 & 2 & 1 & 2 \end{array}\right].$$

2) Codes over GF(4): For $q = 4$ and $b = 2$ the pairs bound is reduced to

$$4^r \leq t^2 + 2t + 1 = (t+1)^2$$

which is equivalent to $t + 1 \geq 2^r$. For each $r \geq 2$ there exists a code which attains this bound with equality. Let GF(4) $= \{0, 1, \alpha, \beta\}$, where $\beta = \alpha^2$. For each $r \geq 2$ and $t = 2^r - 1$, we construct an $n \times r$ parity-check matrix H of a code C, where $n = \frac{2^r(2^r-3)+2}{3}$. The columns of H contain a vector from each line of F_4^r in which each vector has at least two nonzero entries with different values. Of all the

vectors in such a line, the vector with ONE in the first nonzero entry is chosen to be a column in H. The $t = 2^r - 1$ double-error syndromes lines are the lines defined by the $2^r - 1$ nonzero binary vectors of length r. Every column vector v in H can be written as $v = v_1 + \alpha v_\alpha + \beta v_\beta$, where v_x is a binary vector with ONEs exactly in positions in which v has x's. Let $\tilde{v} = v_1 + \beta v_\alpha + \alpha v_\beta$ and define $v\tilde{v}$ to be two adjacent columns of H which corresponds to the same byte. This is well defined since $\tilde{\tilde{v}} = v$ and also in $\tilde{v}$ the first nonzero entry is a ONE. We also have to show that the double-error syndromes of C are multiples of binary vectors. For the adjacent columns v and $\tilde{v}$ in a byte of H we have.

$$\begin{aligned} v+\tilde{v} &= 2v_1+(\alpha+\beta)v_\alpha+(\beta+\alpha)v_\beta &&= v_\alpha+v_\beta \\ v+\alpha\tilde{v} &= (1+\alpha)v_1+(\alpha+\alpha\beta)v_\alpha+(\beta+\alpha^2)v_\beta &&= (1+\alpha)(v_1+v_\alpha) \\ v+\beta\tilde{v} &= (1+\beta)v_1+(\alpha+\beta^2)v_\alpha+(\beta+\alpha\beta)v_\beta &&= (1+\beta)(v_1+v_\beta). \end{aligned}$$

Thus we have proved

Theorem 5: For every $t = 2^r - 1$, $r \geq 2$, and $n = \frac{4^r-1}{3} - t$ there exists an $(n,\ n-r)\ SD_4(2)$ code which meets the pairs bound.

III. Binary Codes

The best known binary single-error correcting, double-errors detecting codes are the $[2^m,\ 2^m - m - 1,\ 4]$ extended Hamming codes, which correct single errors and detect arbitrary double errors. However, for adjacent double errors significantly better code length can be achieved. Blaum, Bruck, and Tolhuizen [2] have constructed a $(12,\ 8)$ $SD_2(4)$ code. Etzion [5] has proved that for a given $r > 3$, the largest n such that an $(n,\ n-r)\ SD_2(n)$ exists satisfies $n \leq 2^r - r - 2$. He also gave a construction of a $(2^r - r - 2,\ 2^r - 2r - 2)\ SD_2(2^r - r - 2)$ code for each $r > 3$. The code can be easily made cyclic, i.e., an error corresponding to the first and the last positions can be also detected. He has constructed $(2^r - 2^\beta,\ 2^r - 2^\beta - r)\ SD_2(2^\beta)$ codes which detect all double errors within bytes of size 2^β, which are clearly the codes with the largest length for codes with bytes of size 2^β. It was also proved that for b which is not a power of 2, a $(2^r - r - i,\ 2^r - 2r - i)\ SD_2(b)$ code exists for every $r > 3$ and $i \geq 2$ if and only if b divides $2^r - r - i$. An $(n,\ n-r)\ SD_2(b)$ code can exist only if $n \leq 2^r - r - 1$ and b divides n. If b divides $2^r - r - 1$ then $(2^r - r - 1,\ 2^r - 2r - 1)\ SD_2(b)$ code may exists only if b is odd and

$$\frac{2^r - r - 1}{b} \geq r - 1.$$

Etzion [5] has shown a (57, 51) $SD_2(3)$ code, a $(120,\ 113)\ SD_2(3)$ code and a $(120,\ 113)\ SD_2(15)$ code. Tolhuizen [8] has proved that if b, s, and r are integers such that s is a multiple of b and there exist both a $(2^s - s - 1,\ 2^s - 2s - 1)\ SD_2(b)$ code and a $(2^r - r - 1,\ 2^r - 2r - 1)$ $SD_2(b)$ code, then there exists a

$$(2^{s+r} - (s+r) - 1,\ 2^{s+r} - 2(s+r) - 1)SD_2(b).$$

An immediate consequence from this result and the $(57,\ 51)\ SD_2(3)$ code and the $(120,\ 113)\ SD_2(3)$ code is the existence of a

$$(2^r - r - 1,\ 2^r - 2r - 1)SD_2(3)$$

code for each $r \equiv 0$ or $1 \pmod 6$ (the only values for which $2^r - r - 1$ is a multiple of 3).

As discussed in the previous paragraph, Etzion [5] has constructed $(n,\ n-r)\ SD_2(n)$ codes for $n = 2^r - r - 2$. The parity-check matrix of such a code consists of all binary column vectors of length r and weight at least 2, except for one vector of weight 2. An $(n,\ n-r)$ $SD_2(b)$ code of length $n \leq 2^r - r - 2$, $b|n$ is constructed from a

$$(2^r - r - 2,\ 2^r - 2r - 2)SD_2(2^r - r - 2)$$

code C with parity matrix H by dividing the consecutive columns of H into bytes of size b and dropping the remaining columns. By [5]

$$(2^r - r - 1,\ 2^r - 2r - 1)SD_2(b)$$

codes can exist only if b is an odd integer, b divides $2^r - r - 1$ and

$$\frac{2^r - r - 1}{b} \geq r - 1.$$

If such code exists then its parity-check matrix can be constructed from all the binary column vectors whose weight is at least 2. Each two consecutive columns in a byte should differ in exactly one position. Using these observations the following theorem is proved in [1].

Theorem 6: If b is an odd integer which divides $2^r - r - 1$ and $b < 2^{\lfloor r/2 \rfloor} - 2$ then there exists a

$$(2^r - r - 1,\ 2^r - 2r - 1)SD_2(b)$$

code.

The idea behind the construction in [1], which proves Theorem 6, is to take a Gray code of length 2^{r-2}, which has column vectors of length $r - 2$ and to append the tails $00,\ 01,\ 11,\ 10$, in an appropriate way to all column vectors (except the vectors of weight one for which the tail 00 is not appended, and the all-zero vector for which only the tail 11 is appended). These tails are appended in such a way that they form "Gray lists" of length divisible by b. These lists form the parity-check matrix of the code.

IV. Conclusion and Open Problems

In this correspondence we have considered optimal single-error-correcting double-adjacent error-detecting codes. We have considered codes which are organized in bytes of size b.

For the nonbinary case, we have given a bound (called the pairs bound) which ties together the length of the code, its redundancy, the size of the bytes, and the alphabet size. Codes which attain this bound were produced and it was shown that for most parameter sets, codes which meet the bound do not exist. Furthermore, we have summarized known and improved results in the binary case.

Several interesting questions remain open in this context.

2) Prove that there are no other codes meeting the pairs bound except for the codes discussed in Section II-D.

3) It seems that the pairs bound is especially good either for codes over GF (3) or for codes with bytes of size 2. A better bound for codes over GF (q), $q \geq 4$, and $b > 2$, would be very interesting.

4) Prove that if b is an odd integer, which divides $2^r - r - 1$ and

$$\frac{2^r - r - 1}{b} \geq r - 1$$

then there exists a $(2^r - r - 1,\ 2^r - 2r - 1)\ SD_2(b)$ code.

References

[1] M. Biberstein, "Constructions and bounds for blot-correcting codes," M.Sc. thesis, Comput. Sci. Dept., Technion–Israel Institute of Technology, Haifa, Israel, May 1999.

[2] M. Blaum, J. Bruck, and L. Tolhuizen, "A note on 'A systematic (12,8) code for correcting single errors and detecting double adjacent errors'," *IEEE Trans. Comput.*, vol. 43, p. 125, 1994.

[3] C. L. Chen, "Error-correcting codes with byte error detection capability," *IEEE Trans. Comput.*, vol. C-32, pp. 615–621, 1983.

[4] ——, "Byte oriented error-correcting code for semiconductor memory systems," *IEEE Trans. Comput.*, vol. C-35, pp. 646–648, 1986.

[5] T. Etzion, "Optimal codes for correcting single errors and detecting adjacent errors," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1357–1360, July 1992.

[6] T. R. N. Rao and E. Fujiwara, *Error-Control Coding for Computer System*. Englewood Cliffs, NJ: Prentice-Hall, 1989.
[7] J. W. Schwartz and J. K. Wolf, "A systematic (12,8) code for correcting single errors and detecting double adjacent errors," *IEEE Trans. Comput.*, vol. 39, pp. 1403–1404, 1990.
[8] L. Tolhuizen, private communication.
[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

On Algebraic Decoding of the $\boldsymbol{Z}_4$-Linear Goethals-Like Codes

Kalle Ranto

***Abstract*—The $\boldsymbol{Z}_4$-linear Goethals-like code of length 2^m has $2^{2^{m+1}-3m-2}$ codewords and minimum Lee distance 8 for any odd integer $m \geq 3$. We present an algebraic decoding algorithm for all $\boldsymbol{Z}_4$-linear Goethals-like codes $\mathcal{C}_k$ introduced by Helleseth *et al.*. We use Dickson polynomials and their properties to solve the syndrome equations.**

***Index Terms*—Decoding, Dickson polynomials, Goethals code, quaternary codes.**

I. Introduction

Let m be an odd integer and let $\boldsymbol{Z}_l$ denote the ring of integers modulo l. Let $R = \mathrm{GR}(4, m)$ be a Galois ring of characteristic 4 with 4^m elements. The multiplicative group of units R^* contains a unique cyclic subgroup $\langle\beta\rangle$ of order $2^m - 1$. Every element of R can be expressed uniquely as $A + 2B$ where $A, B \in \mathcal{T}$ and

$$\mathcal{T} = \{0, 1, \beta, \ldots, \beta^{2^m-2}\}.$$

Let $\mu: \boldsymbol{Z}_4 \to \boldsymbol{Z}_2$ denote the modulo 2 reduction map. We extend μ to R in a natural way and thus $\mu(\mathcal{T}) = \boldsymbol{F}$ where $\boldsymbol{F}$ is a finite field of order 2^m.

A $\boldsymbol{Z}_4$-linear code of length 2^m is a subgroup of $\boldsymbol{Z}_4^{2^m}$ with componentwise addition. The Lee weights of the elements $0, 1, 2, 3$ in $\boldsymbol{Z}_4$ are $0, 1, 2, 1$, respectively, and the weight of a vector is the sum of weights of the components. Hammons *et al.* [4] showed that the $\boldsymbol{Z}_4$-linear code $\mathcal{C}_1$ defined by the parity-check matrix

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \beta & \beta^2 & \ldots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^3 & 2\beta^6 & \ldots & 2\beta^{3(2^m-2)} \end{bmatrix}$$

has minimum Lee distance 8. They also showed that the $\boldsymbol{Z}_4$-linear code $\mathcal{P}$ with the parity-check matrix consisting of the two first rows of H_1 has minimum Lee distance equal to 6 and presented a decoding algorithm for $\mathcal{P}$.

Let ϕ be the Gray map which maps $\boldsymbol{Z}_4$-codewords componentwise to binary words by the rules: $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, and $\phi(3) = 10$. The binary nonlinear codes $\phi(\mathcal{C}_1)$ and $\phi(\mathcal{P})$ have parameters $(2^{m+1}, 2^{2^{m+1}-3m-2}, 8)$ and $(2^{m+1}, 2^{2^{m+1}-2m-2}, 6)$, that is, those of the Goethals and Preparata codes. The Preparata code is known to be optimal and the Goethals code has four times as many codewords as the comparable extended three-error-correcting primitive Bose–Chaudhuri–Hocquenghem (BCH) code.

TABLE I
Different Choices for k with Different Codelengths

m	length	k	$2^k + 1$
3	8	1	3
5	32	1,2	3,5
7	128	1,2,3	3,5,9
9	512	1,2, ,4	3,5, ,17
11	2048	1,2,3,4,5	3,5,9,17,33
13	8192	1,2,3,4,5,6	3,5,9,17,33,65
15	32768	1,2, ,4, , ,7	3,5, ,17, , ,129
17	131072	1,2,3,4,5,6,7,8	3,5,9,17,33,65,129,257

Helleseth, Kumar, and Shanbhag [6] observed that the $\boldsymbol{Z}_4$-linear codes $\mathcal{C}_k$ with parity-check matrices

$$H_k = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \beta & \beta^2 & \ldots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^{2^k+1} & 2\beta^{(2^k+1)2} & \ldots & 2\beta^{(2^k+1)(2^m-2)} \end{bmatrix}$$

have the same Lee weight distribution as the code $\mathcal{C}_1$ whenever $\gcd(k, m) = 1$. Helleseth and Kumar [5] presented a complete decoding algorithm for the code $\mathcal{C}_1$. In this correspondence we give an algebraic decoding algorithm for all codes $\mathcal{C}_k$ with $\gcd(k, m) = 1$ up to the error-correcting capability.

A question arises: Are some codes $\mathcal{C}_k$ equivalent? If so, it is unnecessary to develop the decoding algorithm for all of them. Two binary codes are equivalent if one code is obtained from the other by some permutation of coordinates. In the $\boldsymbol{Z}_4$-domain it is natural to also allow the multiplication of codewords by -1 in some fixed coordinates.

If two codes $\mathcal{C}_k$ and $\mathcal{C}_{k'}$ are equivalent, then so are the binary codes $\mu(\mathcal{C}_k)$ and $\mu(\mathcal{C}_{k'})$. If we restrict the values of k to an interval $1 \leq k \leq (m-1)/2$, the numbers $2^k + 1$ belong to different cyclotomic cosets modulo $2^m - 1$ and therefore the binary codes are different. They are also affine-invariant and by [1] nonequivalent. Hence for the values of k in Table I the codes $\mathcal{C}_k$ are nonequivalent.

In Section II we present two useful lemmas which are used frequently. In Section III we introduce Dickson polynomials and some basic facts about them. In Section IV we give the algebraic decoding algorithm for the codes $\mathcal{C}_k$.

II. Preliminaries

Let $\mathrm{Tr}(x)$ denote the trace function from $\boldsymbol{F}$ to the binary field $\boldsymbol{F}_2$. The following lemma is well known.

Lemma 1: The quadratic equation $x^2 + x + \delta = 0$ with $\delta \in \boldsymbol{F}$ has two roots $\theta = \sum_{j=0}^{(m-1)/2} \delta^{4^j}$ and $\theta + 1$ in $\boldsymbol{F}$, if $\mathrm{Tr}(\delta) = 0$, and no roots in $\boldsymbol{F}$, if $\mathrm{Tr}(\delta) = 1$. In the latter case, the two roots $\theta + \alpha$ and $\theta + \alpha + 1$ are in the quadratic extension of $\boldsymbol{F}$ where $\alpha^2 + \alpha + 1 = 0$.

Equation $x^2 + \gamma x + \delta = 0$ where $\gamma \neq 0$ can be transformed to $(x/\gamma)^2 + x/\gamma + \delta/\gamma^2 = 0$ and the condition in the previous lemma changes to $\mathrm{Tr}(\delta/\gamma^2) = 0$

The next lemma from [5] is useful when transforming the syndrome equations over the Galois ring to equations over the finite field.

Lemma 2: Let $(e_X)_{X \in \mathcal{T}} \in \boldsymbol{Z}_4^{2^m}$ and $E_j = \{\mu(X) | e_X = j\}$ for $j = 0, 1, 2, 3$. The equation

$$\sum_{X \in \mathcal{T}} e_X X = A + 2B, \qquad A, B \in \mathcal{T}$$

Manuscript received August 31, 1999.
The author is with Turku Centre for Computer Science TUCS, FIN-20520 Turku, Finland.
Communicated by P. Solé, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(00)07004-8.