Then

$$f_0(x)f_2(x) = (x-8)(x+8)(x-1) = x^3 + -1x^2 + x - 1$$
$$f_0(x)f_1(x) = (x-8)(x+1) = x^2 - 7x - 8.$$

Let C be the code such that $C = \langle\{f_0(x)f_2(x);\, 13f_0(x)f_1(x)\}\rangle$. We note that the code is also nonfree. Then $\text{rank}\,(C) = 4 - \deg(f_0(x)) = 3$ and $d(C) = 2 = 4 - 3 + 1$. So the code is also MDR.

A. Chinese Remainder Theorem of RS Codes

We shall show how the CRT construction applies to RS codes. Let n be a divisor of $\gcd\,(\phi_1(p_1^{m_1}), \cdots, \phi_1(p_s^{m_s}))$, with $k = \prod_{i=1}^{s} p_i^{m_i}$, where α_i is an element of $\mathbb{Z}_{p_i^{m_i}}$ satisfying the conditions given above. Namely, α_i is a unit, $\alpha_i^{n=1}$, $\alpha_i^j \neq 1$ for $j < n$, and $1 - \alpha_i^j$ is a unit for $j = 1, 2, \cdots, n-1$.

Lemma 3.4: $\alpha = \Phi_k^{-1}(\alpha_1, \cdots, \alpha_s)$ has the desired properties in $\mathbb{Z}_k$.

Proof: It is clear that α is a unit. If α^j were 1 for $j < n$ then that would imply that α_i^j was 1 in $\mathbb{Z}_{p_i^m}$ giving a contradiction. Moreover,

$$(\Phi_k^{-1}(\alpha_1, \cdots, \alpha_s))^n = \Phi_k^{-1}(\alpha_1^n, \cdots, \alpha_s^n) = 1$$

since Φ_k^{-1} is a ring isomorphism.

Then it is clear that $1 - \alpha^j$ is a unit for $j = 1, \cdots, n-1$. □

Let $\{C^{(p_i)}\}$ be the cyclic codes given in Theorem 2.6, respectively.

Theorem 3.5: If $\{C^{(p_i)}\}$ are Reed–Solomon codes of designed distance δ, then CRT $(C^{(p_1)}, \cdots\cdots, C^{(p_s)})$ is also a Reed–Solomon code of designed distance δ.

Proof: From Proposition 2.4 and Theorem 2.6, we can take a proper generator polynomial $f_0'(x)$ of CRT $(C^{(p_1)}, \cdots, C^{(p_s)})$ as

$$f_0'(x) = \Phi_k^{-1}\left(f_0^{(1)}(x), \cdots, f_0^{(s)}(x)\right).$$

Since $f_0^{(i)}(x) = (x - \alpha_i)(x - \alpha_i^2)\cdots(x - \alpha_i^{\delta-1})$, for all i and by the above lemma

$$\begin{aligned} f_0'(x) &= \Phi_k^{-1}(x - \alpha_1, \cdots, x - \alpha_s)\cdots\Phi_k^{-1} \\ &\quad \cdot \left(x - \alpha_1^{\delta-1}, \cdots, x - \alpha_s^{\delta-1}\right) \\ &= (x-\alpha)(x-\alpha^2)\cdots\left(x - \alpha^{\delta-1}\right). \end{aligned}$$

The theorem follows. □

Acknowledgment

The authors wish to thank the referee for a careful reading.

References

[1] A. A. Bruen and R. Silverman, "On the nonexistence of certain MDS codes and projective planes," *Mathematische Z.*, vol. 183, pp. 171–175, 1983.

[2] A. A. Bruen, J. A. Thas, and A. Blokhuis, "On MDS codes, arcs in $PG(n, q)$ with q even, and a solution of three fundamental problems of B. Segre," *Indagationes Math.*, vol. 92, pp. 441–459, 1988.

[3] J. Denes and A. D. Keedwell, *Latin Squares and Their Applications*. New York, NY: Academic, 1974.

[4] S. T. Dougherty, M. Harada, and P. Solé, "Self-dual codes over rings and the Chinese remainder theorem," *Hokkaido Math. J.*, vol. 28, pp. 253–283, 1999.

[5] W. Heise, "Optimal codes, n-arcs and Laguerre geometry," *Acta Inform.*, vol. 6, pp. 403–406, 1976.

[6] W. Heise and P. Quattrocchi, *Informations und Codierungstheorie*, 3rd ed. Berlin, Germany: Springer-Verlag, 1995.

[7] D. D. Joshi, "A note on the upper bounds for minimum distance codes," *Inform. Contr.*, vol. 1, pp. 289–295, 1958.

[8] P. Kanwar and S. R. López-Permouth, "Cyclic codes over the integers modulo p^m," *Finite Fields and Their Applications*, vol. 3, pp. 334–352, 1997.

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

[10] B. R. McDonald, *Finite Rings with Identity*. New York, NY: Dekker, 1974.

[11] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 480–483, Juky 1979.

[12] K. Shiromoto and T. Yoshida, "A Singleton bound for linear codes over $\mathbb{Z}/l\mathbb{Z}$," preprint.

[13] K. Shiromoto, "Note on MDS Codes over the integers modulo p^m," *Hokkaido Math. J.*, to be published.

A Single Asymmetric Error-Correcting Code with 2^{13} Codewords of Dimension 17

Sulaiman A. Al-Bassam and Sultan Al-Muhammadi

***Abstract*—A new single asymmetric error-correcting code is proposed. This code is constructed using a product of two codes of smaller dimensions. The proposed code is of dimension 17 and of size 8192, i.e., with 2^{13} codewords. The best known code of dimension 17 has size 7968 and capable of handling 12 information bits only. The only other three known cases of single asymmeteric codes accommodating one more extra information bit than the symmetric case are for code dimensions $2,\ 4,$ and 16.**

***Index Terms*—Asymmetric errors, Cartesian product, error correction, lower bounds, partitions.**

I. Introduction

In this work, a new code capable of correcting a single asymmetric error is proposed. Before describing the code construction we recall few definitions. The asymmetric distance of two binary vectors x and y of the same length is defined as

$$d_a(x, y) = \max\{N(x, y),\, N(y, x)\}$$

where

$$N(x, y) = |\{i\colon x_i = 1 \text{ and } y_i = 0\}|$$

i.e., the number of positions where x has a 1 and y has a 0.

Manuscript received January 26, 1999.

S. A. Al-Bassam is with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia (e-mail: albassam@ccse.kfupm.edu.sa).

S. Al-Muhammadi is with the Computer Science Department, University of California, San Diego, La Jolla, CA 92093-0407 USA (e-mail: muhamadi@ccse.kfupm.edu.sa).

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

Publisher Item Identifier S 0018-9448(00)00358-8.

0018–9448/00$10.00 © 2000 IEEE

The minimum asymmetric distance of a code C is defined as follows:

$$D_a(C) = \min\{d_a(x, y) : x, y \in C \text{ and } x \neq y\}$$

In general, a code C can correct d asymmetric errors or fewer if $D_a(C) > d$. In the proposed code the asymmetric distance d is 2.

The construction of the proposed code (C) is similar to that given in [1]. The method is based on the Cartesian product of two sets of partitioned codes, say $\{A_1, A_2, \cdots\}$ and $\{B_1, B_2, \cdots\}$, where

$$C = A_1 \times B_1 \cup A_2 \times B_2 \cup A_3 \times B_3 \cup \cdots.$$

These two sets are defined as follows.

Let A be the set of all the 2^p binary vectors of length p and let $A_1, A_2, \cdots, A_{p'}$ be a partition of A, i.e.,

$$A_i \bigcap A_j = \phi$$

and

$$\bigcup A_i = A$$

such that $D_a(A_i) \geq 2$ for all i.

Also, let B be the set of the 2^{q-1} even-weight binary vectors of length q and $B_1, B_2, \cdots, B_{q'}$ be a partition of B such that $D_a(B_i) \geq 2$ for all i.

It was shown in [1] that the code constructed using this method is of asymmetric distance 2. The cardinality of the code is clearly

$$|C| = |A_1| * |B_1| + |A_2| * |B_2| + |A_3| * |B_3| + \cdots$$

and the dimension of the constructed code is $p + q$.

II. The New Code

The code of dimension 17, given in [7], had 7968 codewords. In [1], a code with 7688 codewords was constructed using the Cartesian product of two partitions, A and B. The A partition contains all binary vectors of length $p = 7$ and it is obtained from the Abelian group Z_8; yielding eight partitions each of size 16 codewords, i.e., $A = \{A_1, A_2, \cdots, A_8\}$ with $|A_i| = 16$ for all i. From [2], one may obtain a B partition containing all the even binary vectors of length $q = 10$ having nine partitions $B = \{B_1, B_2, \cdots B_9\}$ with the following nine sizes: $72, 70, 70, 70, 62, 60, 54, 40,$ and 14, respectively. Using the Cartesian product method with these A and B partitions, the code of dimension 17 and of size

$$16 * (72 + 70 + 70 + 70 + 62 + 60 + 54 + 40) + 0 * 14 = 7688$$

codewords can be obtained.

Here, a new A partition of length 7 bits is given. The new A partition has eight partitions with the following sizes: $18, 18, 18, 18, 17, 16, 13,$ and 10. The actual partition is shown in Fig. 1. Applying the Cartesian product method using this A partition with the above B partition gives a new code of dimension 17 and of size:

$$18 * (72+70+70+70)+17*62+16*60+13*54+10*40+0*14 = 8192$$

codewords which is exactly equal to 2^{13}. This code improves the best known code by 224 codewords.

The new A partition is obtained using graph-coloring method. In this method, a graph $G = (N, E)$ is constructed with the set of nodes, N, being all 2^7 binary vectors, and the set of edges E is defined as follows:

$$E = \{(x, y) \colon x, y \in N;\ D_a(x, y) = 1\}.$$

The nodes of the graph are colored using eight colors. From the setup of the graph, we see that if $(x, y) \in E$ then x and y have different colors, $\forall\ x, y \in N$. Clearly, the subset of nodes having color k, say A_k, satisfies the condition $D_a(A_k) \geq 2$ and hence constitutes a single asymmetric error-correcting code.

A_1	A_2	A_3	A_4
0 0 1 0 0 0 0	0 1 0 0 0 0 0	0 0 0 0 1 0 0	0 0 0 0 0 0 0
0 0 0 0 0 1 1	0 0 0 1 0 1 0	0 0 0 1 0 0 1	0 0 1 1 0 0 0
0 0 0 1 1 0 0	0 0 1 0 0 0 1	0 1 0 0 0 1 0	0 1 0 0 1 0 0
1 1 0 0 0 0 0	1 0 0 0 1 0 0	1 0 1 0 0 0 0	1 0 0 0 0 0 1
0 0 1 1 0 0 1	0 0 1 0 1 1 0	0 0 0 1 1 1 0	0 0 0 0 1 1 1
0 1 0 0 1 0 1	0 1 0 0 0 1 1	0 0 1 0 1 0 1	0 1 0 1 0 1 0
0 1 1 0 0 1 0	0 1 0 1 1 0 0	0 1 1 1 0 0 0	0 1 1 0 0 0 1
1 0 0 1 0 1 0	1 0 0 1 0 0 1	1 0 0 0 0 1 1	1 0 0 1 1 0 0
1 0 1 0 1 0 0	1 1 1 0 0 0 0	1 1 0 0 1 0 0	1 0 1 0 0 1 0
0 0 1 0 1 1 1	0 0 1 1 1 0 1	0 1 0 1 1 0 1	0 0 1 1 0 1 1
0 1 0 1 1 1 0	0 1 1 1 0 1 0	0 1 1 0 0 1 1	0 1 1 1 1 0 0
1 0 0 1 1 0 1	1 0 0 1 1 1 0	1 0 1 0 1 1 0	1 0 1 0 1 0 1
1 1 0 0 0 1 1	1 0 1 0 0 1 1	1 0 1 1 0 0 1	1 1 0 0 1 1 0
1 1 1 1 0 0 0	1 1 0 0 1 0 1	1 1 0 1 0 1 0	1 1 0 1 0 0 1
0 1 1 1 1 0 1	0 1 1 0 1 1 1	0 1 1 1 1 1 0	0 1 0 1 1 1 1
1 0 1 1 0 1 1	1 1 0 1 0 1 1	1 0 0 1 1 1 1	1 0 1 1 1 1 0
1 1 1 0 1 1 0	1 1 1 1 1 0 0	1 1 1 0 1 0 1	1 1 1 0 0 1 1
1 1 0 1 1 1 1	1 0 1 1 1 1 1	1 1 1 1 0 1 1	1 1 1 1 1 0 1

A_5	A_6	A_7	A_8
0 0 0 0 0 1 0	0 0 0 1 0 0 0	0 0 0 0 0 0 1	1 0 0 0 0 0 0
0 0 1 0 1 0 0	1 0 0 0 0 1 0	0 0 0 0 1 1 0	0 0 0 0 1 0 1
0 1 0 0 0 0 1	0 1 1 0 0 0 0	1 0 0 1 0 0 0	0 0 1 0 0 1 0
0 0 0 1 1 0 1	0 0 1 0 0 1 1	1 1 0 0 0 1 0	0 1 0 1 0 0 0
0 0 1 1 0 1 0	0 0 1 1 1 0 0	0 0 0 1 0 1 1	1 0 0 0 1 1 0
0 1 0 0 1 1 0	0 1 0 1 0 0 1	0 1 1 0 1 0 0	1 0 1 1 0 0 0
1 0 1 0 0 0 1	1 0 0 0 1 0 1	0 0 1 1 1 1 0	1 1 0 0 0 0 1
1 1 0 1 0 0 0	0 0 0 1 1 1 1	0 1 0 0 1 1 1	1 0 0 1 0 1 1
0 1 0 1 0 1 1	0 1 1 0 1 1 0	0 1 1 1 0 0 1	1 1 1 0 1 0 0
0 1 1 0 1 0 1	1 0 1 1 0 1 0	1 0 1 0 1 1 1	1 1 1 1 1 1 1
1 0 0 0 1 1 1	1 1 0 1 1 0 0	1 1 0 1 1 0 1	
1 0 1 1 1 0 0	1 1 1 0 0 0 1	1 1 1 1 0 1 0	
1 1 1 0 0 1 0	0 1 1 1 0 1 1	0 1 1 1 1 1 1	
0 0 1 1 1 1 1	1 0 1 1 1 0 1		
1 1 0 1 1 1 0	1 1 0 0 1 1 1		
1 1 1 1 0 0 1	1 1 1 1 1 1 0		
1 1 1 0 1 1 1			

Fig. 1. The new A-partition of the 2^7 binary vectors, with cardinalities $18, 18, 18, 18, 17, 16, 13,$ and 10, respectively.

It should be noted that, using this new A partition, one can also improve two other codes given in [1], namely, the code of dimension 15 from 2188 to 2214 codewords and the code of dimension 19 from 28032 to 28548.

III. Conclusion

A single asymmetric error-correcting code with 17 bits now can accommodate 13 information bits. Previously, only 12 information bits were possible which was similar to the *symmetric* case. The maximum symmetric single error-correcting code of dimension 17 is at most $2^{17}/18$, by the Hamming bound, which is only 7281 codewords. Therefore, the maximum number of information bits in any single symmetric error of dimension 17 is at most 12.

The only three other known cases of single asymmeteric codes accomodating one more extra information bit than the symmetric case are of dimensions 2, 4, and 16.

Acknowledgment

The authors wish to thank King Fahad University of Petroleum and Minerals for their continued support.

References

[1] S. Al-Bassam, R. Venkatesan, and S. Al-Muhammadi, “New single asymmetric error correcting codes,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 1619–1623, Sept. 1997.

[2] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, “A new table of constant weight codes,” *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, Nov. 1990.

[3] S. Constantin and T. R. N. Rao, “On the theory of binary asymmetric error-correcting codes,” *Inform. Contr.*, vol. 40, pp. 20–36, 1979.

[4] N. Darwish, “New bounds and constructions for error control codes,” Ph.D. dissertation, Oregon State University, Corvallis, 1989.

[5] R. R. Varshamov, “A class of codes for asymmetric channels and a problem from the additive theory of numbers,” *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 92–95, Jan. 1973.

[6] J. Weber, C. DeVroedt, and D. Boekee, “Bounds and construction for binary codes of length less than 24 and asymmetric distance less than 6,” *IEEE Trans. Inform. Theory*, vol. 34, pp. 1321–1331, Sept. 1988.

[7] Z. Zhang and X. Xia, “New lower bounds for binary codes of asymmetric distance two,” *IEEE Trans. Inform. Theory*, vol. 38, pp. 1592–1597, Sept. 1992.

Optimal Double Circulant Self-Dual Codes Over $\mathbb{F}_4$

T. Aaron Gulliver, *Senior Member, IEEE*

***Abstract*—Optimal double circulant self-dual codes over $\mathbb{F}_4$ have been found for each length $n \le 40$. For lengths $n \le 14, 20, 22, 24, 28$, and 30, these codes are optimal self-dual codes. For length 26, the code attains the highest known minimum weight. For $n \ge 32$, the codes presented provide the highest known minimum weights. The $[36, 18, 12]$ self-dual code improves the lower bound on the highest minimum weight for a $[36, 18]$ linear code**

***Index Terms*—Double circulant codes, self-dual codes.**

I. Introduction

A linear $[n, k]$ code C over $\mathbb{F}_4$ is a k-dimensional vector subspace of $\mathbb{F}_4^n$, where $\mathbb{F}_4$ is the Galois field with four elements. In this correspondence, the elements of $\mathbb{F}_4$ are taken to be $\{0, 1, 2, 3\}$, where $2 = \alpha$ and $3 = \alpha^2$, and $\alpha^2 + \alpha + 1 = 0$. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. The (Hermitian) inner product is defined as

$$x \cdot y = x_1\overline{y_1} + \cdots + x_n\overline{y_n}$$

for two vectors $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$ where $\overline{0} = 0$, $\overline{1} = 1$, $\overline{\alpha} = \alpha^2$ and $\overline{\alpha^2} = \alpha$. The dual code $C^\perp$ of C is defined as

$$C^\perp = \{x \in (\mathbb{F}_2 \times \mathbb{F}_2)^n | x \cdot y = 0 \text{ for all } y \in C\}.$$

C is (Hermitian) *self-dual* if $C = C^\perp$. For a self-dual code over $\mathbb{F}_4$, the following upper bound is known [9]:

$$d \le 2\left\lfloor \frac{n}{6} \right\rfloor + 2.$$

A self-dual $[n, n/2, 2\lfloor \frac{n}{6} \rfloor + 2]$ code is called *extremal*.

TABLE I
DC-Optimal Self-Dual Codes

code	first row of R or R'	d	α	β	γ	WD
$C_{24,1}$	110111101000	8				$W_{24,1}$
$C_{24,2}$	232312222110	8				$W_{24,2}$
$C_{24,3}$	212322132110	8				$W_{24,3}$
$C_{24,4}$	12112100000	8	0	1	1	$W_{24,4}$
$C_{26,1}$	1012321010000	8				$W_{26,1}$
$C_{26,2}$	2122120013100	8				$W_{26,2}$
$C_{26,3}$	2212230333110	8				$W_{26,3}$
$C_{26,4}$	1223232121100	8				$W_{26,4}$
$C_{26,5}$	2211212111111	8				$W_{26,5}$
$C_{26,6}$	210201200100	8	2	1	1	$W_{26,6}$
$C_{26,7}$	332330011100	8	2	1	1	$W_{26,7}$
$C_{26,8}$	113013321310	8	2	1	1	$W_{26,8}$
C_{28}	22113323210100	10				W_{28}
C_{30}	111202320211100	12				Q_{30} [7]
C_{32}	1231111220201000	10				W_{32}
C_{34}	13102230120100000	10				W_{34}
C_{36}	200311211212001000	12				W_{36}
C_{38}	1001112121110010000	12				W_{38}
C_{40}	12313030313210000000	12				W_{40}

Let A_i is the number of codewords of weight i in C. Then the numbers $A_0, \cdots, A_n$ form the weight distribution of C.

A *pure double circulant* code has a generator matrix of the form $[I,\ R]$ where I is the identity matrix of order n and R is an n by n circulant matrix. A $[2n, n]$ code over $\mathbb{F}_4$ with generator matrix of the form

$$\left[\begin{array}{ccc} & \alpha & \beta \ \cdots \ \beta \\ & \gamma & \\ I & \vdots & R' \\ & \gamma & \end{array}\right] \tag{1}$$

where R' is an $n-1$ by $n-1$ circulant matrix, and α, β and $\gamma \in \mathbb{F}_4$ is called a *bordered double circulant* code. These two families of codes are collectively called *double circulant* (DC) codes [6]. Both pure and bordered DC self-dual codes exist for all even lengths.

All self-dual codes over $\mathbb{F}_4$ are classified for lengths $n \le 16$ [2], [7] and the extremal codes are classified for lengths 18 and 20 [5]. The highest possible minimum weight is also known for lengths $n \le 24$ and $n = 28, 30$. For length 26, the highest minimum weight is 8 or 10.

By exhaustive search, the highest minimum weight has been determined for double circulant self-dual codes over $\mathbb{F}_4$ with length $n \le 40$. For all lengths $n \le 30$, $n \ne 18$, these codes attain the highest possible minimum weight (except length 26, where the code attains the highest known minimum weight). For $n \ge 32$, the codes presented have the highest minimum weights for self-dual codes. In fact, the $[36, 18, 12]$ self-dual code improves the lower bound on the highest minimum weight for a linear code over $\mathbb{F}_4$. The notation and terminology for coding theory follow that in [6].

II. Optimal Self-Dual Double Circulant Codes

A self-dual DC code is called *DC-optimal* if it attains the highest possible minimum distance for a self-dual DC code of that length. For lengths $n \le 20$, the DC-optimal codes are equivalent to known

Manuscript received February 4, 1999; revised March 29, 1999.

The author was with the Department of Electrical and Electronic Engineering, University of Canterbury, Christchurch, New Zealand. He is now with the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6 (e-mail: agullive@ece.uvic.ca).

Communicated by P. Solé, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(00)00079-1.

0018–9448/00$10.00 © 2000 IEEE