BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 16, Number 4, December 1988

SOME RESULTS ON CYCLIC UEP CODES*

BY

MAO-CHAO LIN (林茂昭)

Abstract. The minimum distance structures of cyclic codes are determined by the distribution of their zeros or equivalently their nonzeros. In this paper, we consider each cyclic code as the direct sum of cyclic subcodes. From the relations on the distribution of the nonzeros of subcodes, we are able to derive extra error protection capabilities for some message bits. Hence, we construct some cyclic UEP codes

1. Introduction. In a coding system, each message is encoded into a unique codeword. Conventionally, an error-correcting code is designed so that either the whole transmitted message is correctly recovered from the received vector or the whole transmitted message is incorrectly decoded. If we consider each message as a k-tuple, the conventional coding technique gives all the k message bits of a message the same level of error protection. However, in some applications, some message bits of a message are more significant than other message bits of the same message. Therefore, it is desired to give the more significant message bits greater level of error protection. A code which provides multiple levels of error protection for its message bits is called an unequal error protection (*UEP*) code. The notion of *UEP* codes was first introduced by Masnick and Wolf [1]. Then, *UEP* codes have been studied by many coding theorists [2–9]. An important subclass of *UEP* codes is the class of cyclic *UEP* codes. Many cyclic codes for which the code lengths are equal to products of relatively prime integers have been proved to have good *UEP* capabilities [8, 9], since such

Received by the editors December 10, 1987 and in revised form April 21, 1988.
AMS classification numbers: 94B15.
Key words: UEP codes, Separation vector.
* This research was supported by the National Science Council of the Republic of China under grant NSC 77-0404-E002-13.

codes are equivalent to direct sums of concatenated codes. In this paper, we study the UEP capabilities of some cyclic codes which are not necessary to be equivalent to direct sums of concatenated codes.

2. **Preliminaries.** The error protection capability of a UEP code can be represented by its separation vector. For simplicity, we only consider UEP codes with two different levels of error protection. Let C be an $(n, k_1 + k_2)$ code for the message space $\{0, 1\}^{k_1} \times \{0, 1\}^{k_2}$. Each message $\bar{x}$ for C, which is a $(k_1 + k_2)$-tuple, is composed of two parts, $\bar{x}_1$ and $\bar{x}_2$, such that $\bar{x} = (\bar{x}_1, \bar{x}_2)$, where $\bar{x}_i$ is a k_i-tuple from the component message space $\{0, 1\}^{k_i}$ for $i = 1, 2$. We denote each codeword in C encoded from $\bar{x}$ by $\bar{v}(\bar{x})$. Denote the Hamming distance between two codewords, $\bar{v}(\bar{x})$ and $\bar{v}(\bar{x}')$, by $d(\bar{v}(\bar{x}), \bar{v}(\bar{x}'))$. The separation vector $\bar{s} = (s_1, s_2)$ of C is defined by

$$
(1)\quad
\begin{aligned}
s_1 = \min \{d[\bar{v}(\bar{x}_1, \bar{x}_2), \bar{v}(\bar{x}_1', \bar{x}_2')] : \bar{v}(\bar{x}_1, \bar{x}_2) \text{ and } \bar{v}(\bar{x}_1', \bar{x}_2') \in C,\\
\bar{x}_i \text{ and } \bar{x}_i' \in \{0, 1\}^{k_i} \text{ for } i = 1, 2, \text{ and } \bar{x}_1 \neq \bar{x}_1'\},\\
s_2 = \min \{d[\bar{v}(\bar{x}_1, \bar{x}_2), \bar{v}(\bar{x}_1', \bar{x}_2')] : \bar{v}(\bar{x}_1, \bar{x}_2) \text{ and } \bar{v}(\bar{x}_1', \bar{x}_2') \in C,\\
\bar{x}_i \text{ and } \bar{x}_i' \in \{0, 1\}^{k_i} \text{ for } i = 1, 2, \text{ and } \bar{x}_2 \neq \bar{x}_2'\}.
\end{aligned}
$$

Let $\bar{v}(\bar{x}_1, \bar{x}_2)$ be a transmitted codeword of C and let $\bar{r}$ be the received vector. It [3] has been shown that $\bar{x}_i$ for $i = 1, 2$ can be correctly decoded from $\bar{r}$ if

$$(2)\qquad d[\bar{v}(\bar{x}_1, \bar{x}_2), \bar{r}] \leq \lfloor (s_i - 1)/2 \rfloor.$$

Equation (1) can be simplified if C is a linear code. Let $w(\bar{v}(\bar{x}))$ denote the Hamming weight of each codeword $\bar{v}(\bar{x})$ in C. The separation vector $\bar{s} = (s_1, s_2)$ for C is

$$(3)\qquad s_i = \min \{w[\bar{v}(\bar{x}_1, \bar{x}_2)] : \bar{x} \neq 0\},$$

where $i = 1, 2$. The linear $(n, k_1 + k_2)$ code C is the direct sum of an (n, k_1) linear code C_1 and an (n, k_2) linear code C_2. Each codeword $\bar{v}(\bar{x}_1, \bar{x}_2)$ can be uniquely expressed as the sum of a codeword $\bar{v}(\bar{x}_1)$ in C_1 and a codeword $\bar{v}(\bar{x}_2)$ in C_2. The following Theorem shows an easy method of investigating the UEP capability of a linear code.

THEOREM 1. *Let $d_1 > d_2$. If the minimum distance of C is d_2 and the minimum weight of any codeword in $C - C_2$ is at least d_1. Then, C is a code with separation vector (s_1, s_2) for the message space $\{0, 1\}^{k_1} X \{0, 1\}^{k_2}$, where $s_1 \geq d_1$ and $s_2 = d_2$.*

Proof. See [3].

3. **Cyclic *UEP* Codes.** A cyclic code can be easily decomposed into the direct sum of cyclic subcodes. Some classes of cyclic *UEP* codes have been discovered [2, 4, 7, 8, 9]. In an earlier work [9], we show that many cyclic codes of composite length are *UEP* codes by considering these codes as direct sums of concatenated codes. We now turn our attention to cyclic *UEP* codes which are not necessarily equivalent to direct sums of concatenated codes. Hartmann, *et. al.* [10] studied the minimum distance structures of cyclic codes by investigating the relations on the distribution of the zeros for each code. In this paper, we modify Hartmann's work by considering cyclic codes as direct sums of cyclic subcodes and studying the relations on the nonzeros of the subcodes.

Let C be the direct-sum code of an (n, k_1) binary cyclic code C_1 and an (n, k_2) binary cyclic code C_2. Let β be a primitive n-th root of unity. Define the location polynomial $\sigma(X)$ associated with a code polynomial $v(X)$ in C, which has weight r,

$$(4) \qquad \sigma(X) = \prod_{i=1}^{r} (X + \beta^{b_i}) = X^r \sigma_1 X^{r-1} + \cdots + \sigma_{r-1} X + \sigma_r.$$

The Generalized Newton's identity [10, 11]

$$(5) \qquad S_j + \sigma_1 S_{j-1} + \sigma_2 S_{j-2} + \cdots + \sigma_r S_{j-r} = 0$$

must be satisfied for any integer j, where $S_j = v(\beta^j)$. Since S_j are related to the distribution of zeros and nonzeros of C, we can apply equation (5) to the study the error-correcting capability of C.

THEOREM 2. *Let C be a binary cyclic code with minimum distance d_2. Let C_1 contain $\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_l}$ and their conjugates as nonzeros. Consider equation* (5) *with $r = d_2, d_2 + 1, \cdots, d_1 - 1$, where $d_1 > d_2$. Suppose that equation* (5) *either can not be satisfied* *or yields* $S_j = 0$ for $j \in \{i_1, i_2, \cdots, i_l\}$. *Then, C is a UEP code for the message space* $\{0, 1\}^{k_1} \times \{0, 1\}^{k_2}$ *with separation vector at least* (d_1, d_2).

Proof. The code C_2 contains $\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_l}$ and their conjugates as zeros. Any code polynomial in C but not in C_2 does not contain all the $\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_l}$ as roots. Consider a code polynomial $v(X)$ in which $w(v(X)) = r$. Suppose equation (5) with r is not satisfied. Then, $w(v(X))$ can not be r. Suppose that equation (5) is satisfied only for $S_j = 0$, where $j = i_1, i_2, \cdots, i_l$. Then, $v(X)$ must be in C_2. Hence, the condition given in this theorem implies that a code polynomial in C but not in C_2 has weight at least d_1. The proof then follows from Theorem 1.

EXAMPLE 1. Consider the (27, 7) binary cyclic code C which contains β^0, β^3 and their conjugates as nonzeros. Let C_1 be the (27, 1) cyclic code with β^0 as nonzero and C_2 be the (27, 6) cyclic code with β^3 and its conjugates as nonzeros. Clearly, C is the direct sum of C_1 and C_2. Note that C has $\beta^7, \beta^8, \beta^9, \beta^{10}, \beta^{11}$ as zeros. Hence, the minimum distance of C is at least $d_2 = 6$. Consider $v(X) \in C$. For $w(v(X)) = 6$, apparently, $S_0 = 0$. Suppose $w(v(X)) = 7$. Consider equation (5) with $r = 7$. Clearly, $S_{15} = (S_{21})^2 = (S_{24})^4 = (S_{12})^8 = (S_6)^{16} = (S_3)^{32} \neq 0$. From Lemma 4 of [10], we have $\sigma_1 = \sigma_6 = S_1 = 0$. For $j = 11$ in equation (5), we have $S_6\,\sigma_5 = 0$. Hence, $\sigma_5 = 0$. For $j = 14$, we have $S_{12}\,\sigma_2 = 0$. Hence, $\sigma_2 = 0$. Similarly, for $j = 16$, 18, and 19, we have $\sigma_4 = 0$, $\sigma_3 = 0$ and $\sigma_7 = 0$ respectively. The fact of $\sigma_1 = \sigma_2 = \sigma_3 = \sigma_4 = \sigma_5 = \sigma_6 = \sigma_7 = 0$ implies that $S_j = 0$ for all j. Clearly, equation (5) can not be satisfied for $r = 7$. Suppose $w(v(X)) = 8$. This implies $S_0 = 0$. It follows from Theorem 2 that C is a code for the message space $\{0, 1\} \times \{0, 1\}^6$ with separation vector at least (9, 6).

EXAMPLE 2. Consider the (27, 20) cyclic code C containing β, β^9, and their conjugates as nonzeros. Let C_1 be the (27, 2) cyclic code containing β^9 and β^{18} as nonzeros and C_2 be the (27, 18) cyclic code containing β and its conjugates as nonzeros. The minimum distance d_2 of C is at least 2. Let $v(X) \in C$ and assume

$w(v(X))=2$. Consider equation (5) with $r=2$. For $j=2$, we have $S_2+\sigma_1 S_1=0$. Note that $S_2=S_1^2$. Hence, $\sigma_1=S_1$. For $j=3$, we have $\sigma_1 S_2+\sigma_2 S_1=0$. Thus, $\sigma_2=\sigma_1 S_1$. For $j=5$, we have $S_5+\sigma_1 S_4=0$, which implies $S_1^{32}+S_1^5=0$. Thus, $S_1^{27}=1$. For $j=18$, we have $\sigma_1 S_{17}+\sigma_2 S_{16}=S_{18}$. Note that $S_{17}=S_{27\cdot 1213+17}=S_{2^{15}}=(S_1)^{2^{15}}=(S_1)^{27\cdot 1213+17}=(S_1)^{17}$ and $S_{16}=(S_1)^{16}$. Then $S_{18}=0$. It follows from Theorem 2 that C is a code for the message space $\{0,1\}^2\times\{0,1\}^{18}$ with separation vector at least $(3, 2)$.

The results in Example 1 and 2 coincide with those achieved by van Gils [7] using computer search.

By modifying Hartmann's [10] Theorem, we have the following result.

THEOREM 3. *Let C be a binary cyclic code of length n. Suppose β^j is a zero of C for $1\le j\le 4t+1$, $j\ne 2t+1$, where $2t+1$ does not divide n. Let C_1 be an (n, k_1) binary cyclic subcode of C which contains $\beta^{i_1},\cdots,\beta^{i_l}$ and their conjugates as nonzeros. Suppose that $\{i_1,\cdots,i_l\}\subset\{j2^s:(2t+2)i\le j\le(2t+1)(i+1)-1,\ 0\le i\le 2t$ and s is any integer$\}$. Then, the separation vector for C is at least $(2t+3, 2t+2)$ and the message space for C is $\{0,1\}^{k_1}\times\{0,1\}^{k_2}$.*

Proof. Since C contains $2t$ consecutive zeros, its minimum distance d_2 is at least $2t+1$. Let $v(X)$ be a code polynomial in C. Consider equation (5) with $r=2t+1$. Clearly, S_{2t+1} and S_{4t+2} are not zero. For $j=4t+1, 4t,\cdots, 2t+2$, we have $\sigma_{2t}=\sigma_{2t-1}\cdots=\sigma_1=0$ respectively. Thus, equation (5) reduces to

(6) $$S_j+\sigma_{2t+1}S_{j-2t-1}=0.$$

Since n is not a multiple of $2t+1$, then $n=q(2t+1)+r$ for some integers q and r, where $0<r<2t+1$. Then, $S_{(q+1)(2t+1)}=S_{n+(2t+1)-r}=S_{2t+1-r}=0$. From (6), we see that $S_{(q+1)(2t+1)}=[\sigma_{2t+1}]^q\cdot S_{2t+1}$. Since $S_{2t+1}\ne 0$, we have $\sigma_{2t+1}=0$. Thus, $S_j=0$ for all j, which contradicts the previous assumption. Hence, $w(v(X))\ne 2t+1$ and d_2 is at least $2t+2$. Now, suppose $w(v(X))=2t+2$ and apply equation (5) with $r=2t+2$. Clearly, $S_0=0$. For $j=4t+1, 4t,\cdots, 2t+2$, we have $\sigma_{2t}=\sigma_{2t-1}=\cdots=\sigma_1=0$. Thus, equation (5) reduces to

$$S_j + \sigma_{2t+1} S_{j-2t-1} + \sigma_{2t+2} S_{j-2t-2} = 0. \tag{7}$$

For $4t + 4 \leq j \leq 6t + 2$, we see that $S_{j-2t-1} = S_{j-2t-2} = 0$. From (7), we have $S_j = 0$ for $4t + 4 \leq j \leq 6t + 2$. Recursively, we found that $S_j = 0$ for $(2t + 2)i \leq j \leq (2t + 1)(i + 1) - 1$, where $0 \leq i \leq 2t$. Since $\{i_1, \cdots, i_l\} \subset \{j2^s : (2t + 2)i \leq j \leq (2t + 1)(i + 1) - 1,\ 0 \leq i \leq 2t$ and s is any integer$\}$, then, $S_j = 0$ for $j = i_1, \cdots, i_l$. From Theorem 2, C is a code for the message space $\{0, 1\}^{k_1} \times \{0, 1\}^{k_2}$ with separation vector at least $(2t + 3, 2t + 2)$.

Example 3. Let C be the (63, 42) binary cyclic code which contains β, β^3, β^7, β^9 and their conjugates a zeros. Let C_1 be the (63, 7) binary cyclic code with β^0, β^{13} and their conjugates as nonzeros and let C_2 be the (63, 35) binary cyclic code with β^5, β^{11}, β^{15}, β^{21}, β^{23}, β^{27}, β^{31} and their conjugates as nonzeros. Then, C is the direct sum of C_1 and C_2. Note that C contains β^j for $1 \leq j \leq 9$, $j \neq 5$ as zeros. Also note that $\{0, 13\} \subset \{j2^s : 6i \leq j \leq 5(i + 1) - 1,\ 0 \leq i \leq 4,\ s$ is any integer$\}$. Hence, C is a code for the message space $\{0, 1\}^7 \times \{0, 1\}^{35}$ with separation vector at least (7, 6). Note that the true minimum distance of C is 6 [12].

References

1. B. Masnick and J. Wolf, *On linear unequal error protection codes*, IEEE Trans. on Information Theory, IT-13, no. 4, pp. 600–507, July, 1967.
2. W. C. Gore and C. C. Kilgus, *Cyclic codes with unequal error protection*, IEEE Trans. on Information Theory, IT-17, no. 2, pp. 214–215, March, 1971.
3. L. A. Dunning and W. E. Robbins, *Optimal encoding of linear block codes for unequal error protection*, Information and Control, 37, pp. 150–177, 1978.
4. V. N. Dynkin and V. A. Togonidze, *Cyclic codes with unequal symbol protection*, Problemy Peredachi Informatsii, vol. 12, no. 1, pp. 24–28, January-March, 1976.
5. I. M. Boyarinov and G. L. Katsman, *Linear unequal error protection codes*, IEEE Trans. on Information Theory, IT-27, no. 2, pp. 168–175, March 1981.
6. I. M. Boyarinov, *Combined decoding methods for linear codes with unequal protection of information symbols*, Problemy Peredachi Informatsii, vol. 19, no. 1, pp. 17–25, January-March, 1983.
7. W. J. van Gils, *Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes*, IEEE Trans. on Information Theory, IT-29, no. 6, pp. 866–876, November, 1983.
8. M. C. Lin, *Coding for unequal error protection*, Ph. D. dissertation, University of Hawaii, Department of Electrical Engineering, 1986.
9. M. C. Lin and S. Lin, *Cyclic unequal error protection codes constructed from cyclic codes of composite length*, to appear on IEEE Trans. on Information Theory.

10. C. R. P. Hartmann, K. K. Tzeng and R. T. Chien, *Some results on the minimum distance structure of cyclic codes,* IEEE Trans. on Information Theory, IT-18, no. 3, pp. 402–409, May 1972.

11. F. J. MacWilliams and N. J. Sloane, *The theory of Error-Correcting Codes,* New York: North-Holland, 1983.

12. W. W. Peterson and E. J. Weldon Jr, *Error Correcting Codes,* Appendix D, The MIT Press, Cambridge, Massachussetts, 1972.

Deparment of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R. O. C.