The 7th International Telecommunications Symposium (ITS 2010)

Nonlinear Binary Codes Derived from Constacyclic Codes

V. C. da Rocha Jr. and J. S. de Lemos Neto
Communications Research Group - CODEC
Department of Electronics and Systems
Federal University of Pernambuco
Recife, PE, BRAZIL, 50711-970, PO Box 7800
e-mail: vcr@ufpe.br, jose.lemosnt@ufpe.br

***Abstract*— This paper presents theorems showing how to obtain a binary nonlinear code from a p-ary linear constacyclic maximum distance separable code, where p is a prime number, by using a representation of GF(p) as binary p-tuples. Two asymptotically optimum classes of binary constant-weight codes are constructed. Binary cyclic codes are derived for a representation of GF(p) as (p-1)-tuples. It is shown for Mersenne primes p greater than 3 that all p-ary codewords of these codes have full constacyclic order. An application of some of the cyclically permutable codes constructed is given as an example of the construction of protocol sequences for the M-active-out-of-T users collision channel without feedback introduced by Massey.**

Keywords*— *Constacyclic codes, constant-weight codes, cyclically permutable codes, maximum-distance-separable codes, collision channel, protocol sequences.

I. Introduction

This paper presents theorems showing how to obtain a binary nonlinear code from a p-ary linear constacyclic [1] maximum distance separable code, where p is a prime number, by using a representation of GF(p) as binary p-tuples. Two asymptotically optimum classes of binary constant-weight codes are constructed, one of them is optimum with respect to the Johnson bound while the other is optimum with respect to the Plotkin low-rate bound [2]. Binary nonlinear cyclic codes are constructed from p-ary constacyclic codes by using a representation of GF(p) as binary $(p-1)$-tuples. For a positive odd integer m, such that $p = 2^m - 1 > 3$ is a Mersenne prime, we show that all p-ary codewords of these codes have full cyclic order. A cyclically permutable code is a binary code the codewords of which are cyclically distinct and have full cyclic order. An application of some of the cyclically permutable codes constructed is given as an example of the construction of protocol sequences for the M-active-out-of-T users collision channel without feedback introduced by Massey [3].

II. p-ary Code construction

Let p denote a prime number, $p > 3$. It is a known fact [4], [5] that the roots of $x^{p+1} - a$ belong to GF(p^2) and have the form $\alpha^{1+(p-1)i}$, for $0 \le i \le p$, where a denotes a primitive element in the multiplicative group of GF(p) and α denotes an element of order $p^2 - 1$ in GF(p^2) such that $\alpha^{p+1} = a$. However, since the roots of $x^{p+1} - a$ belong to conjugate classes of cardinality 2, i.e., their exponents appear in pairs as $[1-(p-1)i, p+(p-1)i]$, $0 \le i \le (p-1)/2$, it will be convenient to denote these roots as $\alpha^{p+(p-1)i}$, for $-(p-1)/2 \le i \le (p+1)/2$, remembering that both $p-1$ and $p+1$ are always even numbers because p is an odd prime.

A. Constacyclic order of codewords

Definition 1: We define the constacyclic order of a codeword $c(x)$ belonging to a (n,k,d) constacyclic code over GF(p), modulo $x^n - a$, where $a \neq 0, a \in$ GF(p), as the minimum number t of constacyclic shifts such that $c(x) = x^t c(x) \bmod x^n - a$.

Example 1: The constacyclic order of the GF(5) vectors $(2,0,1,0,3,0)$ and $(3,2,1,0,0,0)$ modulo $x^6 - 3$ are, respectively, 8 and 24.

It is known in general that the cyclic order of a root in a $(p+1, k, p-k+2)$ constacyclic code must divide $p^2 - 1$. We consider next a special case where all the roots of the resulting codes are guaranteed to have full cyclic order, i.e., order $p^2 - 1$.

Lemma 1: For a given Mersenne prime $p = 2^m - 1$, where m denotes an odd positive integer, the numbers $p^2 - 1$ and $i(p-1) - 1$ are relatively prime, i.e., $\gcd[p^2 - 1, i(p-1) - 1] = 1$, for $0 \le i \le p^2 - 2$.

Proof: Suppose that $p = 2^m - 1$ is a Mersenne prime. It follows that $\gcd[p^2 - 1, i(p-1) - 1] = \gcd[2^{2m} - 2^{m+1}, i(2^m - 2) - 1] = \gcd[2^m(2^m - 2), i(2^m - 2) - 1] = 1$ since $i(2^m - 2) - 1$ has no common factor with either 2^m or $2^m - 2$. ■

Theorem 1: For a given Mersenne prime $p = 2^m - 1 > 3$, the nonzero codewords of the MDS code $(p+1, k, p+1-k)$, where k is even, have full constacyclic order, i.e. order $p^2 - 1$.

Proof: As mentioned earlier, the roots of the generator polynomial are in the set $\{\alpha^{1+(p-1)i}, 0 \le i \le p\}$, and when $p = 2^m - 1$ is a Mersenne prime, by Lemma 1 all roots of $x^{p+1} - a$ have full cyclic order. Equivalently, all the roots of $x^{2^m} - a$ are primitive roots of GF($2^m - 1$) and thus $x^{2^m} - a$ belongs to the exponent $p^2 - 1 = (2^m - 1)^2 - 1$ [7, page 161].

Suppose that $\mathbf{c} = S^t(\mathbf{c})$, $t \neq 0$, or equivalently that

$$c(x) = x^t c(x) \bmod (x^{p+1} - a), \tag{1}$$

for some positive integer t. It follows from (1) that

$$(x^t - 1)c(x) = 0 \bmod (x^{p+1} - a). \tag{2}$$

Equation (2) implies that all the roots of $x^{p+1}-a$ are present in $(x^t-1)c(x)$. Since $c(x)$ has degree at most p it follows that x^t-1 has at least one root in common with $x^{p+1}-a$, which implies that t must be at least p^2-1 and therefore we conclude that $t=p^2-1$.

In summary, $p>3$ being a Mersenne prime is a sufficient condition for the nonzero codewords to have full constacyclic order. ■

III. Constructions of binary nonlinear codes

We consider now the binary mapping of p-ary (n,k,d) constacyclic MDS codes from Section II, where $n=p+1,k$, and d are the blocklength, dimension and minimum Hamming distance, respectively, of these codes with code digits in GF(p). The codes produced are asymptotically optimum with respect to the Johnson bound and the Plotkin bound, respectively. In principle we can arbitrarily map to binary each element of GF(p) in the codewords of a p-ary MDS code and produce a binary nonlinear code. However, some particular choices for the binary mapping of the elements of GF(p) produce good codes as we show in the sequel. Let $\mathbf{U}$ be a set of cardinality p the elements of which are binary p-tuples $\mathbf{u}$ with Hamming weight $w(\mathbf{u})$, where $0\le w(\mathbf{u})\le p$, and associate one-to-one the elements of $\mathbf{U}$ with the elements of GF(p).

Definition 2: We define the $\mathbf{U}$-representation of GF(p) to be the representation in which the element i of GF(p) is represented by the binary p-tuple $\mathbf{u}_i\in\mathbf{U}$, for $1\le i\le p$, and denote by $d(\mathbf{u})$ the minimum Hamming distance in the set $\mathbf{U}$.

We note that if the p-tuples in the $\mathbf{U}$-representation of GF(p) have the same Hamming weight then they form a binary constant-weight code. Let $d(\mathbf{u})$ denote the minimum distance, or Hamming distance, of this code. We will call the $\mathbf{U}$-representation equidistant if the Hamming distance between every pair of distinct codewords in this code is equal to $d(\mathbf{u})$. In the sequel we will make use of the following three lemmas stated and proved in [2].

Lemma 2: For every prime number p, the p-tuple $\mathbf{u}=[1,0,\ldots,0]$ and its cyclic shifts yields an equidistant $\mathbf{U}$-representation of GF(p) with $d(\mathbf{u})=2$.

Lemma 3: If p is a Mersenne prime and $\mathbf{U}$ consists of a binary m-sequence of length p and its cyclic shifts, then the $\mathbf{U}$-representation of GF(p) is equidistant with $d(\mathbf{u})=(p+1)/2$.

Lemma 4: For every prime number p such that $(p-1)/2$ is odd, a Legendre sequence $\mathbf{u}$ of length p and its cyclic shifts yields an equidistant $\mathbf{U}$-representation of GF(p) with $d(\mathbf{u})=(p+1)/2$.

Furthermore the constant-weight codes produced in Lemmas 2, 3 and 4 are cyclic codes.

Theorem 2: Let p be a prime number, $p>3$, and let C be a p-ary linear constacyclic (n,k,d) code. Let each codeword $\mathbf{c}=[c_0,c_1,\ldots,c_{n-1}]$ in C determine a binary N-tuple $\mathbf{b}$, $N=pn$, by the $\mathbf{U}$-representation of GF(p), assuming all $\mathbf{u}_i$ have the same Hamming weight, for $1\le i\le p$. Then the set of p^k N-tuples $\mathbf{b}$, corresponding in this way to the p^k codewords $\mathbf{c}$ of C, form a binary code the codewords of which have constant weight $w=nw(\mathbf{u})$ and the minimum distance $d_{\min}$ of which satisfies

$$d_{\min}\ge d\ d(\mathbf{u}) \tag{3}$$

with equality when the representation of the elements of GF(p) is equidistant.

Proof: Because all vectors in the $\mathbf{U}$-representation of GF(p) have Hamming weight $w(\mathbf{u})$, it follows that every binary N-tuple $\mathbf{b}$ in the set has Hamming weight $nw(\mathbf{u})$ so that the set is a constant weight code. Two distinct codewords $\mathbf{c}$ and $\mathbf{c}'$ in $\mathbf{C}$ will differ in at least d positions, i.e., their Hamming distance satisfies $d(\mathbf{c},\mathbf{c}')\ge d$, causing the corresponding binary N-tuples $\mathbf{b}$ and $\mathbf{b}'$ to differ in at least $d\ d(\mathbf{u})$ positions, with equality if the $\mathbf{U}$-representation of GF(p) is equidistant. Because $d(\mathbf{c},\mathbf{c}')\ge d$ with equality for some codewords $\mathbf{c}$ and $\mathbf{c}'$ in C, the theorem follows. ■

Construction I: Let p be an odd prime and let k be an even integer satisfying $1<k<p+1$. Choosing a p-ary linear constacyclic $(n,k,d)=(p+1,k,p+2-k)$ MDS code and choosing the $\mathbf{U}$-representation consisting of the binary p-tuple $[1,0,\ldots,0]$ and its distinct cyclic shifts yields by Theorem 2 and Lemma 2 a binary constant-weight code with p^k codewords of length $N=(p+1)p$ and weight $w=p+1$ that has minimum distance $d_{\min}=2(p+2-k)$.

Construction II: Let p be a Mersenne prime and let k be an even number. Then Construction I altered only in that $\mathbf{U}$ is chosen to be an m-sequence of length p yields a binary constant-weight code with p^k codewords of length $N=(p+1)p$ and weight $w=(p+1)^2/2$ that has minimum distance $d_{\min}=(p+2-k)(p+1)/2$.

Construction III: Let p be a Mersenne prime number such that $(p-1)/2$ is odd and let k be an even number. Then Construction I altered only in that $\mathbf{U}$ is chosen to be a Legendre sequence of length p yields a binary constant-weight code with p^k codewords of length $N=(p+1)p$ and weight $w=(p+1)^2/2$ that has minimum distance $d_{\min}=(p+2-k)(p+1)/2$.

The function $A(n,d,w)$ is defined as the maximum number of codewords in a binary code of blocklength n, constant weight w, and minimum distance at least d, and has proved to be of considerable interest in coding theory [6, pp. 524-534]. The codes of Construction I, by an entirely similar argument to that used in [2], are also asymptotically optimum with respect to the Johnson bound [6, Corollary 5, p. 528]. Analogously, the codes in Construction II and Construction III are also asymptotically optimum with respect to the Plotkin low-rate bound [2].

IV. A cyclic representation of GF(p)

Our code constructions so far have produced codes which are asymptotically good however they are not cyclic, which is an interesting property of a code for practical applications.

In order to derive a binary cyclic code from a p-ary constacylic code we need to develop an appropriate representation of GF(p). We recall that the *cyclic order* of an N-tuple $\mathbf{b}$ is the smallest positive integer i such that $\mathbf{S}^i(\mathbf{b}) = \mathbf{b}$, where the operator $\mathbf{S}^i(*)$ denotes i cyclic shifts to the right. It follows that the cyclic order of an N-tuple must be a divisor of N. Let $\mathbf{v}$ be a binary $(p-1)$-tuple of cyclic order $p-1$. Since $p-1$ is even it follows that there will always exist a binary $(p-1)$-tuple of cyclic order 2 and at least one $(p-1)$-tuple of cyclic order $p-1$.

Example 2: For $p = 7$ it follows that $\mathbf{v} = (1,0,1,0,1,0)$ is a binary 6-tuple of cyclic order 2 and that $\mathbf{v}_1 = (1,1,1,0,0,0)$ and $\mathbf{v}_2 = (1,1,0,1,0,0)$ are binary 6-tuples of cyclic order $p-1 = 6$.

Definition 3: We define the $\mathbf{V}$-representation of GF(p) to be the representation such that the non-zero element a^i, $i = 0,1,\ldots,p-2$ is represented by the binary $(p-1)$-tuple $\mathbf{S}^i(\mathbf{v})$, the i-th cyclic shift of $\mathbf{v}$ to the right, where a denotes a primitive element in the multiplicative group of GF(p), and 0 is represented by a binary $(p-1)$-tuple $\mathbf{v}'$ and its distinct cyclic shifts, and is such that $\mathbf{v}' \neq \mathbf{S}^i(\mathbf{v})$ for $0 \leq i \leq p-2$. In particular, $\mathbf{v}'$ can be chosen as the allzero $(p-1)$-tuple.

Example 3: Let $p = 7$, $a = 3$, $\mathbf{v}' = (1,0,1,0,1,0)$ and $\mathbf{v} = (1,1,1,0,0,0)$. The following $\mathbf{v}$-representation of GF(7) results.

$$\begin{array}{cc} 0 & (1,0,1,0,1,0) \\ 0 & (0,1,0,1,0,1) \\ 3^0 & (1,1,1,0,0,0) \\ 3^1 & (0,1,1,1,0,0) \\ 3^2 & (0,0,1,1,1,0) \\ 3^3 & (0,0,0,1,1,1) \\ 3^4 & (1,0,0,0,1,1) \\ 3^5 & (1,1,0,0,0,1) \end{array}$$

V. Two-dimensional arrays and N-tuples

We develop now a correspondence between $m \times n$ two-dimensional arrays and N-tuples which is quite general in the sense that it does not require the usual assumption that m and n must be relatively prime, a condition that is denoted as gcd(m,n) = 1. We prove also some properties of this correspondence which will be useful in the next section. We shall consider $m \times n$ arrays A, denoted as

$$A = \begin{bmatrix} a(0,0) & a(0,1) & \ldots & a(0,n-1) \\ a(1,0) & a(1,1) & \ldots & a(1,n-1) \\ \cdot & \cdot & \ldots & \cdot \\ a(m-1,0) & a(m-1,1) & \ldots & a(m-1,n-1) \end{bmatrix}$$

the entries of which are in an arbitrary alphabet. For positive integers m and n the following simple relationship specifies a one-to-one correspondence between such arrays A and mn-tuples $\mathbf{b} = [b_0, b_1, \ldots, b_{mn-1}]$ over the same alphabet in the manner that

$$b_{in+j} = a(i,j),\ 0 \leq i \leq m-1,\ 0 \leq j \leq n-1. \qquad (4)$$

Example 4: The 3×3 array A

$$A = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$$

corresponds by relation (4) to the 9-tuple $\mathbf{b} = [a_1,a_2,a_3,b_1,b_2,b_3,c_1,c_2,c_3]$.

Definition 4: The column constacyclic shift operator $\mathbf{R}$ shifts the columns of an $m \times n$ array A as follows.

1) The operator $\mathbf{R}$ cyclically shifts the columns of A one position to the right producing a matrix A' and then
2) cyclically shifts downwards by one position the furthest left column of A'.

Example 5: By applying $\mathbf{R}$ to matrix A from Example 1 it follows that

$$\mathbf{R}(A) = \begin{bmatrix} c_3 & a_1 & a_2 \\ a_3 & b_1 & b_2 \\ b_3 & c_1 & c_2 \end{bmatrix}.$$

We notice that $\mathbf{R}(A)$ corresponds to the 9-tuple $\mathbf{S}(b) = [c_3,a_1,a_2,a_3,b_1,b_2,b_3,c_1,c_2]$ where $\mathbf{S}$ denotes the cyclic shift to the right operator on N-tuples and $N = mn$.

Theorem 3: A set of $m \times n$ arrays over an arbitrary alphabet is closed under the constacyclic shift to the right operator $\mathbf{R}$ if and only if the corresponding set of mn-tuples is closed under the cyclic shift to the right operator $\mathbf{S}$.

Proof: Let the $m \times n$ array A correspond to the mn-tuple $\mathbf{b}$. The entry $a(i,j)$ in A is replaced in $\mathbf{R}(A)$ by $a(i \bmod m, j-1 \bmod n)$, if $1 \leq j \leq n-1, 0 \leq i \leq m-1$, and if $j = 0$ the entry $a(i,0)$ in A is replaced in $\mathbf{R}(A)$ by $a(i-1 \bmod m, n-1),\ 0 \leq i \leq m-1$, where "$i \bmod m$" denotes the remainder when i is divided by m. In $\mathbf{S}(\mathbf{b})$, the entry $b_{in+j \bmod mn}$ of $\mathbf{b}$ is replaced by $b_{in+j-1 \bmod mn}$, for $0 \leq j \leq n-1$ and $0 \leq i \leq m-1$. It follows from (1) and from the above considerations that for $0 \leq i \leq m-1$

$$\begin{aligned} b_{in+j-1 \bmod mn} &= a(i,j-1),\ 1 \leq j \leq n-1, \text{ and that} \\ b_{in-1 \bmod mn} &= a(i-1 \bmod m, n-1),\ j = 0 \end{aligned}$$

and hence that $\mathbf{S}(\mathbf{b})$ corresponds to $\mathbf{R}(A)$. Therefore, the set of $m \times n$ arrays is closed under $\mathbf{R}$ when the set of mn-tuples is closed under $\mathbf{S}$. Conversely, $\mathbf{R}(A)$ is the $m \times n$ array corresponding to the mn-tuple $\mathbf{S}(\mathbf{b})$, which guarantees that the set of mn-tuples is closed under $\mathbf{S}$ when the set of $m \times n$ arrays is closed under $\mathbf{R}$. ■

VI. Some linear binary cyclic codes

Theorem 4: Let p be a prime number, $p > 3$, and let C be a p-ary linear constacyclic (n,k,d) code. Let each codeword $c = [c_0, c_1, \ldots, c_{n-1}]$ in C determine a $(p-1) \times n$ array A in the manner that the i-th column of A is the transpose of the $(p-1)$-tuple that is the $\mathbf{v}$-representation of the i-th component of $\mathbf{c}$, and let $\mathbf{b}$ be the binary N-tuple, where $N = (p-1) \times n$, that corresponds to the array A by the relation in (4). Then the set of p^k binary N-tuples $\mathbf{b}$ corresponding in this way to the p^k codewords $\mathbf{c}$ of C

form a binary cyclic code the codewords of which have constant weight $w = nw(\mathbf{v})$ and the minimum distance $d_{\min}$ of which satisfies $d_{\min} \geq d\ d(\mathbf{v})$ with equality when the **v**-representation of GF(p) is equidistant.

Proof: We first show that the set of p^k binary N-tuples **b** is closed under cyclic shifting. Let **c** and A be the codeword in C and the corresponding $(p-1)\times n$ array, respectively. Because C is a linear constacyclic code, the constacyclic shift to the right of **c** is also in C and hence, the corresponding array, denoted as $R(A)$, is another array in the set. Thus, the set of p^k arrays A is closed under the R operator. It now follows from Theorem 3 that the corresponding set of p^k binary N-tuples **b** is closed under cyclic shifting, i.e., it is a binary cyclic code.

We shall omit the rest of the proof because it is identical to the corresponding proof in Theorem 3 when we consider here the **v**-representation instead of the **u**-representation. ■

By combining the results of Theorem 1 and Theorem 4 we obtain the following corollary.

Corollary 1: Let $n = p = 2^m - 1$, where $p > 3$ is a Mersenne prime. The $p^k - 1$ nonzero binary codewords produced by Theorem 4 have full cyclic order $N = p^2 - 1$.

VII. Protocol sequences

The binary cyclic codes produced from MDS constacyclic codes in the previous section may be used to construct cyclically permutable codes (CPC) [2] and thus have their codewords considered as protocol sequences for the users of a collision channel without feedback [2]. Following [2], the set $\{s_1, s_2, \ldots, s_T\}$ of binary sequences of length N is said to be a (T, M, N, σ) *protocol sequence set* if, when these sequences are used as protocol sequences for the T users and provided that at most M of the users are active in each received frame, each frame-active user can be identified by the receiver and at least σ of the packets transmitted by each frame-active user are sent without collision. The following theorem was proved in [2] and shows how constant-weight cyclically permutable codes can be used as (T, M, N, σ) protocol sequence sets.

Theorem 4 in Reference [2]: For any integer σ with $1 \leq \sigma \leq w$, a binary constant-weight w cyclically permutable code CPC $(N, M_c = T, d_c)$ is a (T, M, N, σ) protocol sequence set for

$$M = \min\{T, \lfloor (w-1)/(w-d_c/2) \rfloor, \lfloor (w-\sigma)/(w-d_c/2) \rfloor + 1\}. \quad (5)$$

The strictly binary constant-weight codes that we derived from constacyclic codes did not produce efficient protocol sequences, therefore we have resorted to subsets of binary codewords having a constant weight. Since the constacyclic codes considered in this paper are MDS codes, their weight distribution is well known [8, p.189]. In particular, the number of weight-j codewords of a p-ary $(p+1, k, d)$ MDS code is is given by

$$A_j = \binom{p+1}{j} (p-1) \sum_{i=0}^{j-d} (-1)^i \binom{j-1}{i} p^{j-i-d}. \quad (6)$$

Example 6: Let **v** be a binary 30-tuple of weight 1 in the **V**-representation of the nonzero elements of GF(31). By Theorem 4 the binary mapping of the $A_{32} = 297600$ distinct non-zero codewords of weight 32 of the 31-ary $(32, 4, 29)$ constacyclic code produces the binary $(N, M_c, d_c) = (960, 310, 58)$ CPC code for which $w = 32$. Considering $\sigma = 5$ in (5) it follows that.

$$\begin{aligned} \lfloor (w-1)/(w-d_c/2) \rfloor &= \lfloor (32-1)/(32-58/2) \rfloor \\ &= \lfloor 31/3 \rfloor = 10 \\ \lfloor (w-\sigma)/(w-d_c/2) \rfloor + 1 &= \lfloor (32-5)/(32-58/2) \rfloor + 1 \\ &= \lfloor 27/3 \rfloor + 1 = 10. \end{aligned}$$

In other words, provided that at most $M = 10$ out of the $T = 310$ users are active in each received frame of $N = 960$ slots, each frame-active user will be guaranteed at least $\sigma = 5$ collision-free packet transmissions among the $w = 32$ packets that he sends in a frame.

VIII. Comments

We have presented some nonlinear binary code constructions derived from linear p-ary constacyclic codes, enlarging the range of available choices [2]. Some of our constructions were expressed in terms of a general blocklength n, which can be chosen as a divisor of $p+1$ and still produce MDS codes [2], [4], [9]. The use of MDS constacyclic codes does not require the presence of the all-ones codewords in their respective codebooks when mapping their codewords to binary. Further investigations are being carried out by the authors concerning possible construction of families of protocol sequences for the collision channel without feedback.

IX. Acknowledgement

This work received partial support from the Brazilian National Council for Scientific and Technological Development - CNPq, Project 306612/2007-0.

References

[1] E.R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[2] Q.N. A, L. Györfi and J.L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes", *IEEE Trans. Inform. Theory*, vol.38, no.3, pp. 940-949, May 1992.

[3] J. L. Massey, "The capacity of the collision channel without feedback" Abstracts of Papers, *IEEE Int. Symp. Inform. Theory*, p.101, 1982.

[4] V. C. da Rocha, Jr., "Maximum distance separable multilevel codes", *IEEE Trans. Inform. Theory*, vol.30, no.3, pp. 547-548, May 1984.

[5] V. C. da Rocha, Jr., "Algebraic decoding of a class of multilevel pseudocyclic codes", *IEE Electronics Letters*, vol.25, no.5, pp.341-342, March 1989.

[6] F.J. MacWilliams, and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. New-York: North-Holland, 1978.

[7] W. W. Peterson and E. J. Weldon Jr., *Error-Correcting Codes*, MIT Press, 2nd Edition, 1972.

[8] S. B. Wicker, *Error Control Systems*, Prentice Hall, 1995.

[9] A. Krishna and D. Sarwate, "Pseudocyclic maximum-distance-separable codes", *IEEE Trans. Inform. Theory*, vol.36, no.4, pp. 880-884, May 1990.