International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:5, 2010

Squaring Construction for Repeated-Root Cyclic Codes

O. P. Vinocha , J. S. Bhullar , Manish Gupta

***Abstract*—**We considered repeated-root cyclic codes whose block length is divisible by the characteristic of the underlying field. Cyclic self dual codes are also the repeated root cyclic codes. It is known about the one-level squaring construction for binary repeated root cyclic codes. In this correspondence, we introduced of two level squaring construction for binary repeated root cyclic codes of length $2^a b$, a > 0, b is odd.

***Keywords*—**Squaring Construction, generator matrix, self dual codes, cyclic codes, coset codes, repeated root cyclic codes.

I. INTRODUCTION

TWO interesting codes in terms of pure mathematics are Cyclic and Self-Dual ones. As described Rains and Sloane [1], self-dual codes are an important class of linear codes for both theoretical and practical reasons. Many of best algebraic codes are self dual codes e.g. extended Hamming codes, extended Golay codes and the extended binary Q.R. Codes when $p = -1 \left(\bmod 8\right)$. Their interesting properties have been investigated widely in [2], [3] and [4]. However, research on their combination of cyclic and self dual codes is rather limited. Nonetheless, an interesting result were proved by Carmen-Simona Nedeloaia[5] in his paper containing 1 – level squaring construction and the minimal distances of all binary Cyclic Self-Dual (hence CSD for convenience) codes up to lengths of 120 digits. Then Brandenburg [12] in his Bachelor's thesis gave some definition and showed that the minimal distance of a CSD with length $2^a b$ has an upper bound of twice the minimal distance of a certain code with length b. Sloane and Thompson [6] introduced the class of self-dual repeated-root cyclic codes. On the other hand, Van Lint proved that repeated-root cyclic codes can be obtained via the well-known |u|u + v| construction [7]. Even though Castagnoli et al. proved in [8] that they cannot be asymptotically better than simple-root cyclic codes, repeated-root cyclic codes remain interesting objects. In general cyclic codes assume that *gcd (n,p)* = 1 where p is the characteristic of GF(q). This is equivalent to assuming that g(x) has no repeated irreducible factors, as follows from the fact that g(x) divides x^n-1 but not its formal derivative nx^{n-1} unless and only unless the latter is *0,* which is equivalent to the condition that p divides n or, equivalently, that *gcd (n,p)* = ***p*** > 1. The codes having these types of properties are called repeated root cyclic codes.

Nedeloaia [3] derived the one - level squaring construction for all binary repeated root cyclic codes by using VanLint's [7] result. In this paper we will use the result proved by Nadeloaia [3] and give the two – level squaring construction for all binary repeated root cyclic codes. Manuscript is arranged in following manner. In Section II we presented the notation and definition. In Section III we had given the previous results and some definition of theorems which will be help in our study and we derived the generator matrix for 2 – level squaring construction,

Dr. O.P. Vinocha is with Ferozpur College of Engineering and Technology, Ferozpur, Punjab, India.

Dr. Jaskaran S. Bhullar is with the Malout Institute of Management and Information Technology(MIMIT), Malot, Punjab, India. Ph. +919356737037 (e-mail: bhullarjaskarn@ yahoo.co.in).

Manish Gupta is with the D.A.V. College, Bathinda, Punjab, India. Ph. +919815138274. (e-mail: manish_guptabti@yahoo.com).

II. NOTATION AND DEFINATION

In this section we are giving the notation and definition which we will use through out the paper. The reference for this work is done from [3], [9], [10] and [11].

An [n, k, d] -code (or [n,k] -code) is as usual in coding theory as k-dimensional linear subspace of F^n. Here F is a finite field and d is the minimal distance of the code.

Definition 1: We begin by examining partitions of codes into *cosets* by subcodes. Let C_0 be a binary linear $[n, k_0]$ block with generator G_0 and let $C_1 \subset C_0$ be a $[n, k_1]$ -sub code of C_0 . A coset of C_1 is a set of the form $c_l + C_1 = \{c_l + c : c \in C_1\}$. where $c_l \in C_0$ is a coset leader. We will take that non zero coset leaders in $C_0 \setminus C_1$. $C_0 \setminus C_1$ forms a factor group, partitioning C_0 into $2^{k_0 - k_1}$ disjoint subsets each containing 2^{k_1} code words. Each of these subsets can be represented by a coset leader. The set of coset leaders is called the coset representative space. We denote this coset representative space by $[C_0 / C_1]$. The code C_1 and the set $[C_0 / C_1]$ share only the zero vector in common $C_1 \cap [C_0 / C_1] = 0$.

Every codeword in C_0 can be expressed as the sum of a codeword in C_1 and a vector in $[C_0 / C_1]$. We denote this as

$$C_0 = C_1 \oplus [C_0 / C_1] = \{u + v : u \in C_1, v \in [C_0 / C_1]\}$$

The set operand sum $\oplus$ is called the direct sum.

Definition 2: The |u | u + v| *construction:-*

Let C_1 *and* C_2 be a linear binary $[n, k_1]$ and $[n, k_2]$ block codes with the generator matrix G_1 *and* G_2 and minimum distance d_1 and d_2. Then code C is defined by

$$C = | C_1 | C_1 + C_2 | = \{[u \mid u + v]; u \in C_1, v \in C_2\}.$$

If G is generator of C then $G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$

❖ *Kronecker product :-*

$A \otimes B$ of an $m \times n$ matrix A with $p \times q$ matrix B is the $mp \times nq$. The k product is associative and distributive but not commutative

❖ *Direct sum:-* Let G_1 be generator matrix of $[n_1, k_1, d_1]$ – code and let G_2 be generator matrix of $[n_2, k_2, d_2]$ - code C_2. Then the direct sum of C_1 and C_2 written $C_1 \oplus C_2$ is $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ - code

Definition 3 : One particular group of block codes are the cyclic codes. A *cyclic codes* is an [n, k] code C with the property that if

$$(c_0, ...c_{n-1}) \in C$$

then we also have

$$(c_{n-1}, c_0.........c_{n-2}) \in C.$$

Usually n and q should be relatively prime. Where q is the number of elements in the field. In the context of this paper this last criteria will be waived. These codes are sometimes called *repeated root of cyclic codes*. It is possible to write a codeword $(c_0.........c_{n-1}) \in C$ in the form:

$$c_0 + c_1X + ...c_{n-1}X^{n-1} \in F[X]/(X^n - 1)$$

If we have a cyclic code then

$$X.(c_0 + c_1X + ...c_{n-1}X^{n-1})$$
$$= c_1 + c_2X + ...c_{n-1}X^{n-2} + c_0X^n - 1$$

is also a codeword. This means that if $c(X) \in C$ then also $Xc(X) \in C$. Here the code C is an ideal in $F[X]/(X^n - 1)$. Since $F[X]/(X^n - 1)$ is a principal ideals domain all ideals have a single generator. So we can write $C = < g(X) > where\ g(X) \mid X^n - 1.$

Definition 5 : If C is a code, then its dual is defined as

$$C^{\perp} = \{u \ : \ < u.v >= 0 \ \forall \ v \in C\}$$

❖ If $f = \alpha_0 + \alpha_1 x + ...\alpha_m x^m, \alpha_m \neq 0,$ then define its *reciprocal polynomial* by

$$f^* = \alpha_0 x^m + \alpha_1 x^{m-1} + ... + \alpha_m = x^{\deg(f)} f\left(\frac{1}{x}\right)$$

❖ *Cyclic Self Dual Codes :* C is called cyclic self dual (CSD) if it is both cyclic and self dual. i.e. we can say that

$$C = C^{\perp} \ \Rightarrow \ f^* = \frac{x^n - 1}{f}$$

So if f is the generator of a CSD then $f.f^* = x^n - 1$. Also, we have $2 \mid n \ and \ 2 \mid d(C)$.

Cyclic Self Dual Codes are also called Repeated Root Cyclic Codes.

A binary self dual code C is called doubly even if $A_i = 0$ unless i is divisible by 4.

A double even $\left(n, \frac{n}{2}\right)$ code exists if n is divisible by 8.

Definition 6: - One level squaring [9]:- Let C_0 and C_1 be two codes then

$$|C_0 / C_1|^2 = \{(a + x, \ b + x) : a, b \in C_1 \ and \ x \in [C_0 / C_1]\}$$

Where C_1 is sub code of C_0.

Since $\left(C^{\perp}\right)^{\perp} = C$, it follows that a generator matrix for the primal code serves as a parity check matrix for the dual code. Thus we have the following table.

Code	Generator Matrix	Parity Check Matrix
C $C^{\perp}$	G H	H G

III. Generator Matrix for Squaring Construction

In this section we will derive the two level squaring construction for any repeated root cyclic code

The one level square construction for all binary repeated root cyclic codes.

Theorem 2 [5]*:* The generator matrix for any binary repeated-root cyclic code $C_{A/B}$ can be written as

$$G_{A/B} = \begin{bmatrix} G_A & 0 \\ 0 & G_A \\ G_B & G_B \end{bmatrix}.$$

Therefore $C_{A/B} \cong |A/B|^2$ where G_A and G_B are the generator matrix of codes A and B of length n/2 respectively.

Lemma 1 [5]: - For any i which ranges form $[1, 2^{a-1}]$ the generator polynomial for a code C is

$$\frac{(x^b + 1)g_1.....g_i}{g_1.......g_{2^{a-1}+i}}$$

Generator Matrix for any two level squaring constriction

Proof: It being by forming the two one – level squaring construction codes $C_{A/B} \cong |A/B|^2$ and $C_{B/C} \cong |B/C|^2$, where A, B and C are codes of length $\frac{n}{2}$ and generator G_A, G_B and G_C. Also B is sub code of A and C is sub code of B.

Where as the generator matrix for binary repeated root cyclic codes $C_{A/B}$ and $C_{B/C}$ are $G_{A/B}$ and $G_{B/C}$ respectively which are given by

$$G_{A/B} = \begin{bmatrix} G_A & 0 \\ 0 & G_A \\ G_B & G_B \end{bmatrix}$$

and

$$G_{B/C} = \begin{bmatrix} G_B & 0 \\ 0 & G_B \\ G_C & G_C \end{bmatrix}$$

Here $C_{B/C}$ is a sub – code of $C_{A/B}$ The coset representative for $C_{A/B}$ / $C_{B/C}$ is denoted by $C_{A/B}$ / $C_{B/C}$ for a binary repeated -

root code. Then form a code $C_{A/B/C} = |A/B/C|^4$ by

$$C_{A/B/C} = |A/B/C|^4 = \{a+x, b+x;\ a,b \in C_2 \text{ and } x \in [C_1/C_2]\}$$

Which we can say that is obtained by the squaring construction of $C_{A/B}$ and $C_{A/B}$ / $C_{B/C}$. Let $G_{A/B/C}$ is the generator matrix for $C_{A/B/C}$ So the generator matrix for C is

$$G_{A/B/C} = \begin{bmatrix} G_{A/B} & 0 \\ 0 & G_{A/B} \\ G_{B\backslash C} & G_{B\backslash C} \end{bmatrix}$$

Writing $G_{A/B}$ and $G_{B/C}$ and new defined $G_{B\backslash C}$ as is defined 2.1 and 2.2 we will get the following generator matrix for $C_{A/B/C}$

$$G_{A/B/C} = \begin{bmatrix} G_A & 0 & 0 & 0 \\ 0 & G_A & 0 & 0 \\ G_B & G_B & 0 & 0 \\ 0 & 0 & G_A & 0 \\ 0 & 0 & 0 & G_A \\ 0 & 0 & G_B & G_B \\ G_C & G_C & G_C & G_C \\ 0 & G_B & 0 & G_B \end{bmatrix}$$

Now to represent the above generator matrix in simple form we will apply some row transformations and we will get the following generator matrix for binary repeated-root cyclic code $C_{A/B/C}$

$$G_{A/B/C} = \begin{bmatrix} G_A & 0 & 0 & 0 \\ 0 & G_A & 0 & 0 \\ 0 & 0 & G_A & 0 \\ 0 & 0 & 0 & G_A \\ G_C & G_C & G_C & G_C \\ G_B & G_B & G_B & G_B \\ 0 & 0 & G_B & G_B \\ 0 & G_B & 0 & G_B \end{bmatrix}$$

Now applying the fundamental rules which are also defined in Section II we can write the generator matrix of a code as $C_{A/B/C}$

$$G = I_4 \otimes [1\,1\,1\,1] \otimes G_C \oplus \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \otimes G_B,$$

Where $[1\,1\,1\,1]$ *and* $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$

are generator matrices for the zeroth and first order Reed – Muller codes of length 4.

REFERENCES

[1] E. Rains and N.J.A. Sloane, "Self-dual codes," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam, pp. 177-294, 1998.

[2] J. H. Conway and V. Pless, "On the enumeration of self-dual codes," J. Combinatorial Theory, 28A, 26-53, 1980.

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

[4] V. Pless and N. J. A. Sloane, "On the classi_cation and enumeration of self-dual codes," J. Combinational Theory,18A 313-335, 1975.

[5] Carmen-Simona Nedeloaia, "Weight Distribution of Cyclic Self-Dual Codes," IEEE Transactions on Information Theory, vol. 49, no.6 pp 1582-1591, June 2003.

[6] N. J. A. Sloane and J. G. Thompson, "Cyclic self-dual codes," IEEE Trans. Inform. Theory, vol. IT-29, no. 3, pp. 364–366, May 1983.

[7] J. H. van Lint, "Repeated-root cyclic codes," IEEE Trans. Inform. Theory, vol. 37, no. 2, pp. 343–345, Mar. 1991.

[8] G. Castagnoli, J. L. Massey, Ph. A. Shoeller, and N. von Seemann, "On repeated-root cyclic codes," IEEE Trans. Inform. Theory, vol. 37, no. 2, pp. 337–342, Mar. 1991.

[9] W.Cary Huffman and Vera Pless, Fundamentals of Error-Corrrecting Codes, Cambridge university press, 2003.

[10] V. Pless, Introduction to the Theory of Error Correcting Codes, 3rd ed. New York: Wiley, 1998.

[11] Bas Heijne, "Cyclic Self-Dual Codes", Master's Thesis Rijksuniversiteit Groningen, 7 MAY 2007, http://scripties.fwn.eldoc.ub.rug.nl/FILES/scripties/Wiskunde/Masters/2007/Heijne.B./Bas Heijne doctoraal WM 2007.pdf

[12] E.J.H. Brandenburg , "Finding the Minimal Distance of Cyclic Self-Dual Codes", Bachelor's Thesis Rijksuniversiteit Groningen, March 2009,