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 $p = -1 \mod 8$. 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. 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 $x^p - 1$ but not its formal derivative $x^{p-1}$ 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 Nedeloaia [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,

II. NOTATION AND DEFINITION

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 $C_1 \subseteq C_2 \subseteq \cdots \subseteq C_k$ be a $[n, k_0]$-sub code of $C_k$. A coset of $C_i$ is a set of the form $c_i + C_i = \{c_i + c : c \in C_i\}$, where $c_i \in C_i$ is a coset leader. We will take that non zero coset leaders in $C_i \cap C_0$ forms a factor group, partitioning $C_0$ into $2^{k_0-k_i}$ disjoint subsets each containing $2^h$ 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 $[C_0/C_i]$. The code $C_i$ and the set $[C_0/C_i]$ share only the zero vector in common $c_i \cap [C_0/C_i] = \{0\}$.

Every codeword in $C_0$ can be expressed as the sum of a codeword in $C_i$ and a vector in $[C_0/C_i]$. We denote this as $C_0 = C_i \oplus [C_0/C_i] = \{u + v : u \in C_i, v \in [C_0/C_i]\}$

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 $C = C_1 \cup C_2 = \{u | u + v : u \in C_1, v \in C_2\}$. If $G$ is generator of $C$ then $G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}$.
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
\[
(c_0, \ldots, c_{n-1}) \in C
\]
then we also have
\[
(c_{n}, c_{n+1}, \ldots, c_{2n-1}) \in C.
\]

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 cyclic codes. It is possible to write a codeword \((c_{-n}, \ldots, c_{n-1})\) in \(C\) in the form:
\[
c_x = c_0 X^n + \cdots + c_{n-1} X^{n-1} \in \mathbb{F}[X]/(X^n - 1)
\]

If we have a cyclic code then
\[
X(c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}) = c_0 X^n + c_1 X^{n-1} + \cdots + c_{n-1} X^1 + c_0 X^0
\]
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 \(\mathbb{F}[X]/(X^n - 1)\).

Since \(\mathbb{F}[X]/(X^n - 1)\) is a principal ideals domain all ideals have a single generator. So we can write
\[
C = \langle g(X) \rangle = \{ g(X) X^n \mid g(X) \in \mathbb{F}[X]/(X^n - 1) \}
\]

Definition 5: If \(C\) is a code, then its dual is defined as
\[
C^\perp = \{ u : \langle u, v \rangle = 0 \ \forall v \in C \}
\]

If \(f = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m \neq 0\), then define its reciprocal polynomial by
\[
f^* = \alpha_0 x^{-m} + \alpha_1 x^{-m-1} + \cdots + \alpha_m = x^{\deg(f)} f\left(\frac{1}{x}\right)
\]

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
\[
C = C^\perp \Rightarrow f^* = x^n f^{-1}
\]

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 \(A\) is 0 unless \(i\) is divisible by 4.

A double even \(\left(\frac{n}{2}\right)\) code exists if \(n\) is divisible by 8.
root code. Then form a code $C_{A/B:C} = \{ a/c, b/c \}$ for\ $a, b \in C, c \in \mathbb{C}$ which we can say that is obtained by the squaring construction of $C_{A/B}$ and $C_{A/B} / C_{B/C}$. Let $G_{A/B:C}$ be the generator matrix for $C_{A/B:C}$ so the generator matrix for $C$ is

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

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

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

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 $C_{A/B:C}$

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

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

$$G = I_{s} \oplus [1111] \oplus G_{C} \oplus \begin{bmatrix}
1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
\end{bmatrix} \oplus G_{s},$$

Where $[1111]$ and $0011, 0101$ are generator matrices for the zeroth and first order Reed–Muller codes of length 4.