DOI : 10.15613/sijrs/2018/v5i2/207624
ISSN (Print): 2349-8919
ISSN (Online): 2350-0999
ScieXplore: International Journal of Research in Science, *Vol 5(2), 27-33, July-December 2018*

Z_{27}-Quadratic Residue Codes

P. Shakila Banu* and M. Madhubala

Department of Mathematics, Vellalar College for Women (Autonomous), Erode – 638012, Tamil Nadu, India; shakimeeran10@gmail.com, madhubalamani6@gmail.com

Abstract

In this paper, we consider a certain types of cyclic codes over Z_{27}, called quadratic residue codes over Z_{27}. We find the Z_{27}-quadratic residue codes using their idempotent generators and show exhibit that these codes also have excellent properties which are similar in much respect to the properties of quadratic residue codes.

Keywords: Check Polynomial, Cyclic Codes, Generator Polynomial, Idempotent Generator, Orthogonal Codes, Quadratic Residues

1. Introduction

Codes are used to transmit the data across the noisy channel and recovering the message. The issue of an accurate communication is extremely important. The Error-correcting codes are used in CDs to correct scratches, dusts and to spread the data out over the disk. Coding theory is developed in the late 1940 in respect to the practical problem in communication. The article "A Mathematical theory of communication" is published by Claude Shannon in 1948[9], focused on how to encode the given information and gives some ideas to establish Error-correcting codes. An important type of Error-correcting codes is cyclic codes and is significant by means of their shift registers. The cyclic codes are linear codes.

In 1964, Andrew Gleason found quadratic residue codes which are the another type of cyclic codes. Qian and Pless[7] explained the role of idempotent generators in generating the quadratic residue codes and verified the conditions for the self dual of these codes. Latterly, Chiu, Yau and Yu[3] found quadratic residue codes over Z_8 using idempotent generators and exhibited the conditions for self dual codes. Taeri[2] defined the quadratic residue codes over Z_9 and also verified the conditions for self dual. In this paper, we define the quadratic residue codes over Z_{27} and provide the same interesting results over Z_{27}. Z_{27} is a ring with the zero divisors 3,6,9,12,15,18,21 and 24. A Z_{27} code is a set of n-tuple Z_{27} module.

2. Preliminaries

2.1 Definition 2.1[1]

If the congruence $x^2 \equiv n \pmod p$, where p is an odd prime and $n \not\equiv 0 (mod\ p)$, has a solution, then n is a quadratic residue mod p. Suppose the congruence has no solution, then n is called a quadratic non-residue mod p.

Example 2.1: Consider that p = 5. Then {1, 4} are the quadratic residues mod 5 and {2, 3} are quadratic non residues mod 5.

2.2 Definition 2.2 [4]

A (n,k) linear code C is cyclic if whenever $(c_0, c_1, \ldots, c_{n-1})$ is a codeword in C, $(c_{n-1}, c_0, c_1 \ldots, c_{n-2})$ is also a codeword in C.

Example 2.2: $C = \{000,101,011,110,111\}$ is a cyclic code.

**Author for correspondence*

2.3 Definition 2.3 [10]

If $g(x)$ is the monic polynomial of less degree in the factorization of $x^n - 1$ in $F^q[x]$ and if $C = g(x)$, $g(x)$ is the generator polynomial of C.

2.4 Definition 2.4 [6]

Let C be a cyclic $[n,k]$ code with generator polynomial $g(x)$. Then the polynomial $h(x) = (x^n - 1)/g(x)$ is called the check polynomial of C.

2.5 Definition 2.5 [10]

If C is an $[n,k]$ linear code over F, its dual or orthogonal code $C^{\perp}$ is the set of vectors which are orthogonal to all the code words of C :

$$C^{\perp} = \{u | u.v = 0 \text{ for all } v \in C\}.$$

2.6 Definition 2.6 [2]

A generator $e(x)$ of an ideal in R^n, is called an idempotent generator if it is an idempotent, that is , if $e^2(x) = e(x)$.

Theorem 2.1:[3] Suppose C is a Z_{p^m} cyclic code of odd length n. If $C = e$, where $ef = x^n - 1$ forsome f such that e and f are coprimes, C has an idempotent generator in $Z_{p^m}\frac{[x]}{x^n - 1}$ and also the idempotent generator of a cyclic code is unique.

Theorem 2.2 [2]: If $w(x)$ is an idempotent generator of a Z_{p^m}-cyclic code C, $C^{\perp}$ has the idempotent generator $(1 - w(x^{-1}))$.

Theorem 2.3 [2]: If and e_2 are the idempotent generators of $R[x]/(x^p - 1)$ and if the codes C_1 and C_2 are defined by $C_1 = \langle e_1 \rangle$ and $C_2 = \langle e_2 \rangle$ then $C_1 \cap C_2$ and $C_1 + C_2$ have idempotent generators $e_1 e_2$ and $e_1 + e_2 - e_1 e_2$, respectively.

Theorem 2.4 [2]: Suppose A and B are finite commutative rings with characteristic q^m and q^{m+1}, respectively, where q is a prime. Let $f : B \to A$ be an epimorphism, with kernel $f = q^m B$.

- $f(e)$If $= e$ is an idempotent of A, then e^q is an idempotent of B.
- e_i, i I$= 1,2,\ldots,r$ are primitive idempotents of A, and $f(\theta_i) = e_i$, $i = 1,2,\ldots,r$, then θ_i^q, $i = 1,2,\ldots,r$, are primitive idempotents of B.

Suppose N denotes the set of non-residues and Q denotes the set of quadratic residues for a prime p. So, e_1 and e_2 can be defined by, $e_1 = \sum_{j \in Q} x^j$ and $e_2 = \sum_{j \in N} x^j$. By [5], 3 is a quadratic residue $\bmod (p)$ if and only if $p = 12r \pm 1$. For the prime $p = 12r \pm 1$, $2e_i, 1 + e_i, i = 1,2$ are idempotents of $Z_3[x]/(x^p - 1)$ i.e., a Z_3 quadratic residue code is generated by any one of the above idempotents. For a prime $p = 12r + 1$, put $Q_1 = \langle 2e_1 \rangle, Q_2 = \langle 2e_2 \rangle, Q_1' = \langle 1 + e_2 \rangle$ and $Q_2' = \langle 1 + e_1 \rangle$. For a prime $p = 12r - 1$, put $Q_1 = \langle 1 + e_2 \rangle, Q_2 = \langle 1 + e_1 \rangle, Q_1' = \langle 2e_1 \rangle$ and $Q_2' = \langle 2e_2 \rangle$.

Theorem 2.5 [2]:

- Suppose that $p = 4k - 1$ and a is a number prime to p. Then in the set $a + (Q \cup \{0\})$, there are k elements in $Q \cup \{0\}$ and k elements in N. In the set $a + N$, there are k elements in $Q \cup \{0\}$ and $k - 1$ elements in N.
- Suppose that $p = 4k + 1$ and a is a number prime to p. Then in the set $a + (Q \cup \{0\})$, if $a \in Q$, there are $k + 1$ elements in $Q \cup \{0\}$ and k elements in N and also if $a \in N$, there are k elements in Q and $k + 1$ elements in N. In the set $a + N$, if $a \in Q$, there are k elements in Q and k elements in N and also if $a \in N$, there are $k + 1$ elements in $Q \cup \{0\}$ and $k - 1$ elements in N.

Theorem 2.6: If $p = 4l - 1$, then

$$e_1^2 = (l-1)e_1 + le, e_1^2 = le_1 + (l-1)e_2,$$
$$e_1 e_2 = (2l-1) + (l-1)e_1 + (l-1)e_2,$$
$$e_1^3 = (3l^2 - 3l + 1)e_1 + 2l(l-1)e_2 + 2l^2 - l,$$

If $p = 4l + 1$, then $e_1^2 = (l-1)e_1 + le_2 + 2l$,

$$e_2^2 = le_1 + (l-1)e_2 + 2l, e_1 e_2 = le_1 + le_2,$$
$$e_1^3 = (2l^2 + 1)e_1 + (2l^2 - l)e_2 + 2l^2 - l,$$
$$e_2^3 = (2l^2 - 1)e_1 + (2l^2 + l)e_2 + 2l^2 - l.$$

3. Quadratic Residue Codes Over Z_{27}

For defining quadratic residue codes over Z_{27}, consider $p = 12m \pm 1$, because 3 is a quadratic residue *mod* p. Denote the vector h by $h = 1 + e_1 + e_2$ and the idempotents for $Z_{27}[x]/(x^p - 1)$ are obtained below.

Theorem 3.1: Let $p = \pm 1 (mod\ 12)$.

I. Let $p = 12m - 1$.
   a. If $m = 9a$, then $26e_i, 1 + e_i, 26h, 1 + 2h$ are idempotents over $Z_{27}[x]/(x^p - 1)$, where $i = 1,2$.
   b. If $m = 9a + 1$, then $6e_i + 26e_j + 3, e_i + 21e_j + 25, 5h, 1 + 22h$ are idempotents over $Z_{27}[x]/(x^p - 1)$, where $1 \le i \ne j \le 2$.

c. If $m=9a+2$, then $3e_i+17e_j+24$, $10e_i+24e_j+4$, $20h$, $1+7h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

d. If $m=9a+3$, then $18e_i+26e_j+9$, e_i+9e_j+19, $17h$, $1+10h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

e. If $m=9a+4$, then $24e_i+26e_j+12$, e_i+3e_j+16, $23h$, $1+4h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

f. If $m=9a+5$, then $17e_i+21e_j+6$, $6e_i+10e_j+22$, $11h$, $1+16h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

g. If $m=9a+6$, then $26e_i+9e_j+18$, $18e_i+e_j+10$, $8h$, $1+19h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

h. If $m=9a+7$, then $26e_i+15e_j+21$, $12e_i+e_j+7$, $14h$, $1+13h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

i. If $m=9a+8$, then $17e_i+12e_j+15$, $15e_i+10e_j+13$, $2h$, $1+25h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

II. Let $p=12m+1$.

a. If $m=9a$, then $1+e_i$, $26e_i$, h, $1+26h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $i=1,2$.

b. If $m=9a+1$, then $10e_i+15e_j+13$, $12e_i+17e_j+15$, $25h$, $1+2h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

c. If $m=9a+2$, then e_i+12e_j+7, $15e_i+26e_j+21$, $13h$, $1+14h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

d. If $m=9a+3$, then $18e_i+e_j+10$, $26e_i+9e_j+18$, $19h$, $1+8h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

e. If $m=9a+4$, then $10e_i+6e_j+22$, $21e_i+17e_j+6$, $16h$, $1+11h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

f. If $m=9a+5$, then e_i+3e_j+16, $24e_i+26e_j+12$, $4h$, $1+23h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

g. If $m=9a+6$, then e_i+9e_j+19, $18e_i+26e_j+9$, $10h$, $1+17h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

h. If $m=9a+7$, then $10e_i+24e_j+4$, $3e_i+17e_j+24$, $7h$, $1+20h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

i. If $m=9a+8$, then e_i+21e_j+25, $6e_i+26e_j+3$, $22h$, $1+5h$ are idempotents over $Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

Proof. Part (I).

We prove this theorem for the case (a) and the remaining cases proved in the same way. For $p=12m-1$ and $m=9a+1$,

(i)

$$(6e_1+26e_2+3)^3 = 216e_1^3+17576e_2^3+27+2808e_1^2e_2$$
$$+324e_1^2+12168e_1e_2^2+6084e_2^2+162e_1+702e_2+2808e_1e_2$$
$$=26e_2^3+18e_1e_2^2+9e_2^2$$
$$=26(12e_1+10e_2+15)+18e_1(3e_1+2e_2)+9(3e_1+2e_2)$$
$$=312e_1+278e_2+390+54(2e_1+3e_2)+36(2e_1+2e_2+5)$$
$$=6e_1+26e_2+3.$$

(ii)

$$(e_1+21e_2+25)^3 = e_1^3+9261e_2^3+15625+63e_1^2e_2+75e_1^2$$
$$+1323e_1e_2^2+33075e_2^2+1875e_1+39375e_2+3150e_1e_2$$
$$=e_1^3+19+9e_1^2e_2+21e_1^2+12e_1+9e_2+18e_1e_2$$
$$=(10e_1+12e_2+15)+19+9(2e_1+3e_2)e_2+21(2e_1+3e_2)$$
$$+12e_1+9e_2+18(5+2e_1+2e_2)$$
$$=100e_1+120e_2+124+18e_1e_2+27e_2^2$$
$$=e_1+21e_2+25$$

(iii)

$$(5h)^3=(5(1+e_1+e_2))^3 = 125e_1^3+125e_2^3+125+375e_1^2e_2$$
$$+375e_1^2+375e_1e_2^2+375e_2^2+375e_1+375e_2+750e_1e_2$$
$$=17+17e_1^3+17e_2^3+24e_1^2e_2+24e_1^2+24e_2^2e_1+24e_2^2+24e_1$$
$$+24e_2+21e_1e_2$$
$$=17+17(10e_1+12e_2+15)+17(12e_1+10e_2+15)$$
$$+24(2e_1+3e_2)e_2+24(2e_1+3e_2)+24(3e_1+2e_2)e_1+24e_1$$
$$+24(3e_1+2e_2)+24e_2+21(5+2e_1+2e_2)$$
$$65+101e_1+101e_2+15(2e_1+2e_2+5)+18(3e_1+2e_2)+18(2e_1+3e_2)$$
$$=5+5e_1+5e_2$$

(iv)

$$(1+22h)^3=(22e_1+22e_2+23)^3 = 10648e_1^3+10648e_2^3$$
$$+12167 ++33396e_2^2+34914e_1 31944e_1^2e_2+33396e_1^2$$
$$+31944e_1e_2^2+34014e_2+66792e_1e_2$$
$$=10e_1^3+10e_2^3+17+3e_1^2e_2+24e_1^2+3e_2^2e_1+24e_2^2+3e_1$$
$$+3e_2+21e_1e_2$$
$$=10(10e_1+12e_2+15)+10(12e_1+10e_2+15)+17+3e_2(2e_1+3e_2)$$
$$+24(2e_1+3e_2)+3e_1(3e_1+2e_2)+24(3e_1+2e_2)+3e_1+3e_2$$
$$+21(5+2e_1+2e_2)$$
$$=22e_1+22e_2+23$$

Similarly, the other cases are proved.

Part (II).

Consider $p=12m+1$ and $m=9a+1$,

(i)

$$(10e_1+15e_2+13)^3 = 1000e_1^3+3375e_2^3+2197 +4500e_1^2e_2$$

$+3900e_1^2+6750e_1e_2^2+8775e_2^2+5070e_1+7605e_2+11700e_1e_2$
$=e_2^3+10+18e_1^2e_2+12e_1^2+21e_1+18e_2+9e_1e_2$
$=(19e_1+15e_2+12)+10+18(2e_1+3e_2+6)e_2+12(2e_1+3e_2+6)$
$e_2+12(2e_1+3e_2+6)+18e_2+9(3e_1+3e_2)$
$=10e_1+15e_2+13$

(ii)
$(12e_1+17e_2+15)^3=1728e_1^3+4913e_2^3+3375+7344e_1^2e_2$
$+6480e_1^2+10404e_1e_2^2+13005e_2^2+8100e_1+11475e_2+18360$
$=26e_2^3+9e_1e_2^2+18e_2^2$
$=26(15e_1+19e_2+12)+9e_1(3e_1+2e_2+6)+18(3e_1+2e_2+6)$
$=12e_1+17e_2+15$

(iii)
$(25h)^3=(25(1+e_1+e_2))^3=15625e_1^3+15625e_2^3+15625$
$+46875e_1^2e_2+46875e_1^2+46875e_1e_2^2+46875e_2^2+46875e_1$
$+46875e_2+93750e_1e_2$
$=19e_1^3+19e_2^3+19+3e_1^2e_2+3e_1^2+3e_1e_2^2+3e_2^2+3e_1+3e_2$
$+6e_1e_2$
$=19(19e_1+15e_2+12)+19(15e_1+19e_2+12)+19+3e_2(2e_1$
$+3e_2+6)+3(2e_1+3e_2+6)+3e_1(3e_1+2e_2+6)+3e_1+3e_2$
$+3(3e_1+2e_2+6)$
$=79e_1+79e_2+79+12(3e_1+3e_2)+9(2e_1+3e_2+6)$
$+9(3e_1+2e_2+6)$
$=25e_1+25e_2+25$

(iv)
$(2h+1)^3=(2e_1+2e_2+3)^3=8e_1^3+8e_2^3+27+24e_1^2e_2+36e_1^2$
$+24e_1e_2^2+36e_2^2+54e_1+54e_2+72e_1e_2$
$=8(19e_1+15e_2+12)+8(15e_1+19e_2+12)+24e_2(2e_1+3e_2+6)$
$+36(2e_1+3e_2+6)+24e_1(3e_1+2e_2+6)+36(3e_1+2e_2+6)$
$+72(3e_1+3e_2)$
$=2e_1+2e_2+3+15e_1e_2+18e_1^2+8e_2^2$
$=2e_1+2e_2+3+15(3e_1+3e_2)+18(2e_1+3e_2+6)+18$
$(3e_1+2e_2+6)$
$=2e_1+2e_2+3$

Definition 3.1: A Z_{27}-cyclic code is a Z_{27}-quadratic residue code if it is generated by any one of the idempotents in theorem 3.1.

Suppose d denotes a non zero element of Z_{27} and $d\in N$. Consider the map μ_d is defined by, $\mu_d: i\to d\ i \pmod p$ such that $\mu_d(i)=di \pmod p$. The following theorems investigate the properties of quadratic residue codes over Z_{27}.

Theorem 3.2: Suppose $p=12m-1$. If $m=9a$, let $Q_1=\langle 26e_1\rangle$, $Q_2=\langle 26e_2\rangle$, $Q_1'=\langle 1+e_1\rangle$, $Q_2'=\langle 1+e_2\rangle$. If $m=9a+1$, let $Q_1=\langle 6e_1+26e_2+3\rangle$, $Q_1'=\langle e_1+21e_2+25\rangle$, $Q_2'=\langle 21e_1+e_2+25\rangle$. If $m=9a+2$, let $Q_1=\langle 3e_1+176e_2+24\rangle$, $Q_2=\langle 17e_1+3e_2+24\rangle$, $Q_1'=\langle 10e_1+24e_2+4\rangle$, $Q_2'=\langle 24e_1+10e_2+4\rangle$. If $m=9a+3$, let $Q_1=\langle 18e_1+26e_2+9\rangle$, $Q_2=\langle 26e_1+18e_2+9\rangle$, $Q_1'=\langle e_1+9e_2+19\rangle$, $Q_2'=\langle 9e_1+e_2+19\rangle$. If $m=9a+4$, let $Q_1=\langle 24e_1+26e_2+12\rangle$, $Q_2=\langle 26e_1+24e_2+12\rangle$, $Q_1'=\langle e_1+3e_2+16\rangle$, $Q_2'=\langle 3e_1+e_2+16\rangle$. If $m=9a+5$, let $Q_1=\langle 17e_1+21e_2+6\rangle$, $Q_2=\langle 21e_1+17e_2+6\rangle$, $Q_1'=\langle 6e_1+10e_2+22\rangle$, $Q_2'=\langle 10e_1+6e_2+22\rangle$. If $m=9a+6$, let $Q_1=\langle 26e_1+9e_2+18\rangle$, $Q_2=\langle 9e_1+26e_2+18\rangle$, $Q_1'=\langle 18e_1+e_2+10\rangle$, $Q_2'=\langle e_1+18e_2+10\rangle$. If $m=9a+7$, let $Q_1=\langle 26e_1+15e_2+21\rangle$, $Q_2=\langle 15e_1+26e_2+21\rangle$, $Q_1'=\langle 12e_1+e_2+7\rangle$, $Q_2'=\langle e_1+12e_2+7\rangle$. If $m=9a+8$, let $Q_1=\langle 17e_1+12e_2+15\rangle$, $Q_2=\langle 12e_1+17e_2+15\rangle$, $Q_1'=\langle 15e_1+10e_2+13\rangle$, $Q_2'=\langle 10e_1+15e_2+13\rangle$. Then

- Q_1 and Q_2 are equivalent and also Q_1' and Q_2' are equivalent.
- $Q_1\cap Q_2=\langle\hat{h}\rangle$ and $Q_1+Q_2=Z_{27}[x]/(x^p-1)$, where $\hat{h}$ is a suitable element in $\{26h, 5h, 20h, 17h, 23h, 11h, 8h, 14h, 2h\}$ listed in theorem 3.1.
- $|Q_1|=27^{(p+1)/2}=|Q_2|$.
- $Q_1=Q_1'+\langle\hat{h}\rangle$, $Q_2=Q_2'+\langle\hat{h}\rangle$.
- $|Q_1'|=27^{(p-1)/2}=|Q_2'|$
- Q_1' and Q_2' are self orthogonal i.e., $Q_1^{\perp}=Q_1'$, $Q_2^{\perp}=Q_2'$.
- $Q_1'\cap Q_2'=\{0\}$ and $Q_1'+Q_2'=\langle 1-\hat{h}\rangle$. Also $Q_i'\cap Q_j'=\{0\}$ and $Q_i'+Q_j'=Z_{27}[x]/(x^p-1)$, where $1\le i\ne j\le 2$.

Proof: For $m=9a+4$, since, $Q_1=\langle 24e_1+26e_2+12\rangle$, $Q_2=\langle 26e_1+24e_2+12\rangle$ and $Q_1'=\langle e_1+3e_2+16\rangle$, $Q_2'=\langle 3e_1+e_2+16\rangle$ and $p=12m-1$, $-1\in N$.

- Consider that d is an element of N, $\mu_d e_1=e_2$, $\mu_d e_2=e_1$. Therefore, $\mu_d\langle 24e_1+26e_2+12\rangle=\langle 26e_1+24e_2+12\rangle$, $\mu_d\langle 26e_1+24e_2+12\rangle=\langle 24e_1+26e_2+12\rangle$.
  So, Q_1 and Q_2 are equivalent. Similarly, Q_1' and Q_2' are equivalent.
- (ii) $Q_1\cap Q_2=$
  $\langle 24e_1+26e_2+12\rangle\cap\langle 26e_1+24e_2+12\rangle$
  Then $Q_1\cap Q_2$ has an idempotent generator
  $(24e_1+26e_2+12)(26e_1+24e_2+12)$
  $24e_1+26e_2+12+26e_1+24e_2+12=23h+1$
  $(24e_1+26e_2+12)(23h)$
  $=(24e_1+26e_2+12)(26+(24e_1+26e_2+12)$
  $+(26e_1+24e_2+12))$

$=26(24e_1+26e_2+12)+(24e_1+26e_2+12)^2$
$+(24e_1+26e_2+12)\ (26e_1+24e_2+12)$
$=(24e_1+26e_2+12)(26e_1+24e_2+12)$.

Since, $p=12(9a+4)-1=108a+47$ and $\frac{(p-1)}{2}\equiv 23 \bmod 27$.

$(24e_1+26e_2+12)(23h)=24\frac{p-1}{2}(23h)+26\frac{p-1}{2}(23h)$
$+12(23h)=23h$

Therefore, $(24e_1+26e_2+12)(26e_1+24e_2+12)=23h$.

$23h$ is an idempotent generator of $Q_1 \cap Q_2$ and $|Q_1 \cap Q_2| = 27 = |<23h>|$.

Q_1+Q_2 has an idempotent generator
$(24e_1+26e_2+12)+(26e_1+24e_2+12)$
$-(24e_1+26e_2+12)(26e_1+24e_2+12)$
$=(23e_1+23e_2+24)-(23e_1+23e_2+23)=1$

Therefore, $Q_1+Q_2 = Z_{27}[x]/(x^p-1)$.

- $27^p = |Q_1+Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{27}$

  $|Q_1| = 27^{\frac{(p+1)}{2}} = |Q_2|$.

  Since, Q_1 and Q_2 are equivalent.
- $Q_1' \cap <23h>$ has an idempotent generator

  $(e_1+3e_2+16)(23h)=\frac{(p-1)}{2}(23h)+3\frac{(p-1)}{2}(23h)$
  $+16(23h)=(4(23)+16)(23h)=0$

  Therefore, $Q_1' \cap <23h> = \{0\}$. Also, $Q_1' + <23h>$ has an idempotent generator
  $(e_1+3e_2+16)+(23h)-(e_1+3e_2+16)(23h)=24e_1+26e_2+12$

  Hence, $Q_1' + <23h> = <24e_1+26e_2+12> = Q_1$. Similarly, $Q_2' + <23h> = Q_2$.
- $27^{\frac{(p+1)}{2}} = |Q_1| = |Q_1' + <23h>| = |Q_1'||<23h>| = |Q_1'|\,27$

  $|Q_1'| = 27^{(p-1)/2} = |Q_2'|$.

  Since, Q_1 and Q_2 are equivalent.
- Since, $-1 \in N$, $Q_1^{\perp}$ has an idempotent generator
  $1-(24e_1(x^{-1})+26e_2(x^{-1})+12)=3e_1(x^{-1})+e_2(x^{-1})+16$
  $=e_1+3e_2+16$

  Hence, $Q_1^{\perp} = Q_1'$ implies $Q_1 = Q_1'^{\perp}$. Similarly, $Q_2^{\perp} = Q_2'$. By (iv), $Q_1' \subseteq Q_1 = Q_1'^{\perp}$ and $Q_2' \subseteq Q_2 = Q_2'^{\perp}$. Hence, Q_1' and Q_2' are self orthogonal.
- Since, $e_1+3e_2+16+3e_1+e_2+16=4h+1$. $Q_1' \cap Q_2'$ has an idempotent generator $(e_1+3e_2+16)(3e_1+e_2+16)$.

  $(e_1+3e_2+16)(4h)$
  $=(e_1+3e_2+16)(26+(e_1+3e_2+16)+(3e_1+e_2+16))$
  $=26(e_1+3e_2+16)+(e_1+3e_2+16)^2+(e_1+3e_2+16)$
  $(3e_1+e_2+16)$
  $=(e_1+3e_2+16)(3e_1+e_2+16)$
  $(e_1+3e_2+16)(4h)=\frac{p-1}{2}(4h)+3\frac{p-1}{2}(4h)+16(4h)$
  $=(4\frac{p-1}{2}+16)(4h)=0$

  Therefore, $(e_1+3e_2+16)(3e_1+e_2+16)=0$.

  Hence, $Q_1' \cap Q_2' = \{0\}$.

  $Q_1'+Q_2'$ has an idempotent generator
  $(e_1+3e_2+16)+(3e_1+e_2+16)-(e_1+3e_2+16)(3e_1+e_2+16)$
  $=1+4h$.

  Therefore, $Q_1'+Q_2' = <1+4h> = <1-23h>$ and here $\hat{h}=23h$.

  Similarly, the other cases are proved.

Theorem 3.3: Suppose $p=12m+1$ is a prime. If $m=9a$, let $Q_1=<1+e_1>$, $Q_2=<1+e_2>$ and $Q_1'=<26e_1>$, $Q_2'=<26e_2>$. If $m=9a+1$, let $Q_1=<10e_1+15e_2+13>$, $Q_2=<15e_1+10e_2+13>$ and $Q_1'=<12e_1+17e_2+15>$, $Q_2'=<17e_1+12e_2+15>$. If $m=9a+2$, let $Q_1=<e_1+12e_2+7>$, $Q_2=<12e_1+e_2+7>$, and $Q_1'=<15e_1+26e_2+21>$, $Q_2'=<26e_1+15e_2+21>$. If $m=9a+3$, let $Q_1=<18e_1+e_2+10>$, $Q_2=<e_1+18e_2+10>$ and $Q_1'=<26e_1+9e_2+18>$, $Q_2'=<9e_1+26e_2+18>$. If $m=9a+4$, let $Q_1=<10e_1+6e_2+22>$, $Q_2=<6e_1+10e_2+22>$ and $Q_1'=<21e_1+17e_2+6>$, $Q_2'=<17e_1+21e_2+6>$. If $m=9a+5$, let $Q_1=<e_1+3e_2+16>$, $Q_2=<3e_1+e_2+16>$ and $Q_1'=<24e_1+26e_2+12>$, $Q_2'=<26e_1+24e_2+12>$. If $m=9a+6$, let $Q_1=<e_1+9e_2+19>$, $Q_2=<9e_1+e_2+19>$ and $Q_1'=<18e_1+26e_2+9>$, $Q_2'=<26e_1+18e_2+9>$. If $m=9a+7$, let $Q_1=<10e_1+124e_2+4>$, $Q_2=<24e_1+10e_2+4>$ and $Q_1'=<3e_1+17e_2+24>$, $Q_2'=<17e_1+3e_2+24>$. If $m=9a+8$, let $Q_1=<e_1+21e_2+25>$, $Q_2=<21e_1+e_2+25>$ and $Q_1'=<6e_1+26e_2+3>$, $Q_2'=<26e_1+6e_2+3>$. Then

- Q_1 and Q_2 are equivalent and also Q_1' and Q_2' are equivalent.
- $Q_1 \cap Q_2 = <\hat{h}>$ and $Q_1+Q_2 = Z_{27}[x]/(x^p-1)$, where $\hat{h}$ is a suitable element in $\{h, 25h, 13h, 19h, 16h, 4h, 10h, 7h, 22h\}$ listed in theorem 3.1.
- $|Q_1| = 27^{(p+1)/2} = |Q_2|$.
- $Q_1 = Q_1' + <\hat{h}>$, $Q_2 = Q_2' + <\hat{h}>$.
- $|Q_1'| = 27^{(p-1)/2} = |Q_2'|$.
- $Q_1^{\perp} = Q_2'$ and $Q_2^{\perp} = Q_1'$.
- $Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = <1-\hat{h}>$ and also $Q_i' \cap Q_j' = \{0\}$ and $Q_i' + Q_j' = <u>$, where $1 \le i \ne j \le 2$, u is a suitable element from $\{1+26h, 1+2h, 1+14h, 1+8h, 1+11h, 1+23h, 1+17h, 1+20h, 1+5h\}$ are listed in theorem 3.1.

Proof. For $m=9a+8$, since, $p=12m+1$, $Q_1 = <e_1+21e_2+25>$, $Q_2 =<21e_1+e_2+25>$ and $Q_1' =<6e_1+26e_2+3>$, $Q_2' =<26e_1+6e_2+3>$.

- By μ_d, d is an element of N, $\mu_d e_1 = e_2$, $\mu_d e_2 = e_1$
  Therefore, $\mu_d <e_1+21e_2+25> = <21e_1+e_2+25>$,
  $\mu_d <21e_1+e_2+25> = <e_1+21e_2+25>$.
  So, Q_1 and Q_2 are equivalent. Similarly, Q_1' and Q' are equivalent.
- $Q_1 \cap Q_2 = <e_1+21e_2+25> \cap <21e_1+e_2+25>$
  $Q_1 \cap Q_2$ has an idempotent generator $(e_1+21e_2+25)(21e_1+e_2+25)$.
  $e_1+21e_2+25+21e_1+e_2+25=22h+1$
  $(e_1+21e_2+25)(22h)$
  $=(e_1+21e_2+25)(26+(e_1+21e_2+25)+(21e_1+e_2+25))$
  $=26(e_1+21e_2+25)+(e_1+21e_2+25)^2+(e_1+21e_2+25)(21e_1+e_2+25) = (e_1+21e_2+25)(21e_1+e_2+25)$.
  Since, $p=12(9k+8)+1=108k+97$ and $\frac{(p-1)}{2} \equiv 21 \mod 27$
  $(e_1+21e_2+25)(22h)=(22\frac{p-1}{2}+25)(22h) = 22h.$
  Therefore, $(e_1+21e_2+25)(21e_1+e_2+25)=22h$.
  $Q_1 \cap Q_2$ has an idempotent generator $22h$. Hence, $|Q_1 \cap Q_2| = |<22h>| = 27$.
  $Q_1 + Q_2$ has an idempotent generator
  $(e_1+21e_2+25)+(21e_1+e_2+25)-(e_1+21e_2+25)(21e_1+e_2+25)$
  $=(22e_1+22e_2+23)-(22e_1+22e_2+22)=1$
  Therefore, $Q_1+Q_2 = Z_{27}[x]/(x^p-1)$.
- $$27^p = |Q_1+Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{27}$$
  $$|Q_1| = 27^{\frac{(p+1)}{2}} = |Q_2|.$$
- $Q_1' \cap <22h>$ has an idempotent generator
  $$(6e_1+26e_2+3)(22h) = 6\frac{(p-1)}{2}(22h)+26\frac{(p-1)}{2}(22h)$$
  $+3(22h)=(5(23)+3)(22h)=0$
  Therefore, $Q_1' \cap <22h> = \{0\}$. Also, $Q_1' + <22h>$ has an idempotent generator
  $(6e_1+26e_2+3)+(22h)-(6e_1+26e_2+3)(22h) = e_1+21e_2+25$.
  Hence, $Q_1' + <22h> = <e_1+21e_2+25> = Q_1$.
  Similarly, $Q_2' + <22h> = Q_2$.
- $$27^{\frac{(p+1)}{2}} = |Q_1| = |Q_1' + 22h| = |Q_1'||22h| = 27$$
  $$|Q_1'| = 27^{(p-1)/2} = |Q_2'|.$$
  Since, Q_1 and Q_2 are equivalent.
- Since, $-1 \in N$. $Q_1^{\perp}$ has an idempotent generator
  $1-(e_1(x^{-1})+21e_2(x^{-1})+25) = 26e_1(x^{-1})+6e_2(x^{-1})+3$
  $=26e_1+6e_2+3$.
  Hence, $Q_1^{\perp} = Q_2'$. Similarly, $Q_2^{\perp} = Q_1'$.
- Since, $6e_1+26e_2+3+26e_1+6e_2+3=5h+1$
  $(6e_1+26e_2+3)(5h)$
  $=(6e_1+26e_2+3)(26+(6e_1+26e_2+3)+(26e_1+6e_2+3)$
  $=26(6e_1+26e_2+3)+(6e_1+26e_2+3)^2$
  $+(6e_1+26e_2+3)(26e_1+6e_2+3)$
  $=(6e_1+26e_2+3)(26e_1+6e_2+3)$.
  $$(6e_1+26e_2+3)(5h) = 6\frac{p-1}{2}(5h)+26\frac{p-1}{2}(5h)+3(5h)$$
  $$=(5\frac{p-1}{2}+3)(5h)$$
  $(6e_1+26e_2+3)(5h)=0$
  Therefore, $(6e_1+26e_2+3)(26e_1+6e_2+3)=0$.
  Hence, $Q_1' \cap Q_2' = \{0\}$.
  $Q_1' + Q_2'$ has an idempotent generator
  $(6e_1+26e_2+3)+(26e_1+6e_2+3)-(6e_1+26e_2+3)(26e_1+6e_2+3) = 5h+1$.
  Therefore, $Q_1' + Q_2' = <1+5h>$ and here $u=1+5h$.
  Similarly, the other cases are proved.

4. Conclusion

Quadratic residue codes belong to the collection of BCH codes. In this paper, we exhibited the properties of Quadratic residue codes over Z_{27} and verified that these codes also have excellent error correction capabilities. With the help of these codes, we can find a class of constacyclic codes over F_{p^m}, a finite field, where $p=3$, which plays a significant role in the theory of error correcting codes.

5. References

1. Apostol TM. Introduction to analytic number theory. Springer International Student Edition. New Delhi: Narosa Publishing House; 1995.
2. Taeri B. Quadratic residue codes over Z_9. J Korean Math Soc. 2009; 46:13–30. https://doi.org/10.4134/JKMS.2009.46.1.013
3. Chiu MH, Yau SS-T, Yu Y. Z_8 Cyclic codes and quadratic residue codes. Advances in Applied Mathematics. 2000; 25:12–33. https://doi.org/10.1006/aama.2000.0687
4. Gallian JA. Contemporary abstract algebra. 4th Ed. New Delhi: Narosa Publishing House; 1999.
5. Mac Williams FJ, Sloane NJA. The Theory of Error-Correcting Codes. North-Holland Publishing Company; 1977.
6. Pless V. Introduction to the theory of Error-Correcting Codes. 3rd Ed. New York: Wiley- Intersciences; 1998. https://doi.org/10.1002/9781118032749

7. Pless V, Qian. Cyclic codes and quadratic residue codes over Z4. IEEE Trans Inform Theory. 1996; 42(5):1594-600. https://doi.org/10.1109/18.532906
8. Shakila Banu P, Madhubala M. Properties of Quadratic Residue Codes over Z27. Proceedings of the 2nd International Conference on Collaborative Research in Mathematical Sciences; 2018.
9. Shannon CE. A mathematical theory of communication. The Bell System Technical Journal. 1948; 3:379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x
10. Spence SA. Introduction to Algebraic Coding Theory. Supplementary material for Math 336. Cornell University; 2002.