5.1. Introduction

Let F_l be a field of odd prime order l and $k \geq 1$ be an integer such that gcd(l, k) = 1. It is well known that a cyclic code of a given length k over F_l is an ideal of the semisimple ring $R_k = \frac{F_l[x]}{<x^k-1>}$. As mentioned in Chapters 2, in R_k, $k = 2^n, p^n, 2p^n, p^n q, p^n q^m, 2p^n q^m$, the minimal cyclic codes over F_l has been discussed by many authors. Analogously, cyclic codes over finite rings may be useful in certain applications like communication in computers to computers. Let $(Z_m, +, .)$ be the ring of integers modulo m, where $m \geq 1$, is an integer. Since, a cyclic code of length n over a finite field F_l is an ideal in the ring $\frac{F_l[x]}{<x^n-1>}$. Similarly, a cyclic code of length n over Z_m is an ideal in the ring $\frac{Z_m[x]}{<x^n-1>}$. Spiegel [104] investigated codes which are ideals in the ring $Z_m G$, where G is a cyclic group of prime power order. Blake [19] defined analogs of Hamming, Reed-Solomon and BCH-codes over Z_m. Wasan [110] discussed codes over Z_m. Calderbank *et al* .[21, 28, 29] computed quarternary and binary quadratic residue codes.

A set of $n-$ tuples over Z_4 is called a code over Z_4. Let $R_m = \frac{Z_4[x]}{<x^m-1>}$. If C is a cyclic code of length m over Z_4, an element $c = (a_0, a_1, \ldots, a_{m-1}) \in C$ is identified with a polynomial $a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}$ in R_m. Under this mapping, C is isomorphic to an ideal in R_m. A particular interesting family of Z_4 $-$ cyclic codes is quadratic residue codes (QR$-$Codes).These codes have many good properties which are analogous in many respects to the properties of quadratic residues codes over a field. For prime $p = 8k \pm 1$(k is even or odd), Pless and Qian [84] obtained the QR$-$ Codes of length p over Z_4.

In this chapter, we obtain the quadratic residues codes of length p^n, $p = 8k \pm 1$(k is even or odd, $n \geq 1$) by extending the above results. In Section 5.3, (Theorems 5.3.2-5.3.5) some properties of QR-codes of prime power length are obtained. In Section 5.4, the properties of quadratic residue codes of length 49 are discussed.

5.2. Some Idempotents in $R_m(m = p^n, n \geq 1)$ over Z_4

Notations 5.2.1.

$R =$ set of all quadratic residues modulo p

$S =$ set of all quadratic non residue modulo p

$$e_1^1 = \sum_{\alpha \in R} x^\alpha = e_1, \quad e_2^1 = \sum_{\alpha \in S} x^\alpha = e_2,$$

$$e_1^{(n)} = \sum_{\alpha \in Q} x^\alpha, \qquad e_2^{(n)} = \sum_{\alpha \in N} x^\alpha,$$

$$h^{(n)} = \sum_{\alpha \in M} x^\alpha,$$

where $Q = \{r + kp \mid r \in R, 0 \leq k \leq p^{n-1} - 1\}$ is the set of all quadratic residues modulo $p^n,\ n \geq 1$.

$N = \{t + kp \mid t \in S, 0 \leq k \leq p^{n-1} - 1\}$ is the set of all quadratic non residues modulo $p^n,\ n \geq 1$ and $M = \{kp \mid 0 \leq k \leq p^{n-1} - 1\}$.

Note 5.2.2.(i) If $p \equiv -1$ modulo 8, then $e_1$and e_2 are idempotents of binary $[p, \frac{p+1}{2}]$ QR-codes.

(ii) If $p \equiv 1$ modulo 8, then $e_1$and e_2 are idempotents of binary $[p, \frac{p-1}{2}]$ QR-codes..

Lemma 5.2.3. For $n \geq 1,\ e_1^{(n)} = e_1 h^{(n)}$ and $e_2^{(n)} = e_2 h^{(n)}$.

Proof. Trivial

Lemma 5.2.4. For $h^{(n)}$ defined above and $n \geq 1$, then $(h^{(n)})^2 = p^{n-1} h^{(n)}$.

Proof. By Notation 5.2.1, $M = \{kp \mid 0 \leq k \leq p^{n-1} - 1\}$.

Therefore, for $0 \leq j \leq p^{n-1} - 1$,

$$M + jp = M.$$

and

$$\left(h^{(n)}\right)^2 = \sum_{j=0}^{p^{n-1}-1} \sum_{r \in M} x^r x^{jp}$$

$$= \sum_{j=0}^{p^{n-1}-1} h^{(n)} = p^{n-1}h^{(n)}.$$

The Theorems 5.2.5 and 5.2.6 are from McWilliams and Sloane [79, p 487].

Theorem 5.2.5. If $p = 4k - 1$, then

(i) $e_1^2 = \left(\frac{p-3}{4}\right)e_1 + \left(\frac{p+1}{4}\right)e_2$,

(ii) $e_2^2 = \left(\frac{p-3}{4}\right)e_2 + \left(\frac{p+1}{4}\right)e_1$,

(iii) $e_1e_2 = \left(\frac{p-1}{2}\right) + \left(\frac{p-3}{4}\right)(e_1 + e_2)$.

Theorem 5.2.6. If $p = 4k + 1$, then

(i) $e_1^2 = \left(\frac{p-1}{2}\right) + \left(\frac{p-5}{4}\right)e_1 + \left(\frac{p-1}{4}\right)e_2$,

(ii) $e_2^2 = \left(\frac{p-1}{2}\right) + \left(\frac{p-1}{4}\right)e_1 + \left(\frac{p-5}{4}\right)e_2$,

(iii) $e_1e_2 = \left(\frac{p-1}{4}\right)(e_1 + e_2)$.

The following Theorem 5.2.7 and Theorem 5.2.10 are the generalization of above theorems.

Theorem 5.2.7. If $p = 4k - 1$, then

(i) $(e_1^{(n)})^2 = p^{n-1}\left(\left(\frac{p-3}{4}\right)e_1^{(n)} + \left(\frac{p+1}{4}\right)e_2^{(n)}\right)$,

(ii) $(e_2^{(n)})^2 = p^{n-1}\left(\left(\frac{p-3}{4}\right)e_2^{(n)} + \left(\frac{p+1}{4}\right)e_1^{(n)}\right)$,

(iii) $e_1^{(n)}e_2^{(n)} = p^{n-1}\left(\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-3}{4}\right)(e_1^{(n)} + e_2^{(n)})\right)$.

Proof. By Lemma 5.2.3, we have

$$(e_1^{(n)})^2 = (e_1h^{(n)})^2.$$

By Theorem 5.2.5 and Lemma 5.2.4, we have

$$e_1^2 = \left(\frac{p-3}{4}\right)e_1 + \left(\frac{p+1}{4}\right)e_2$$

and

$$(h^{(n)})^2 = p^{n-1}h^{(n)}.$$

Therefore,

$$(e_1^{(n)})^2 = p^{n-1}\left\{\left(\frac{p-3}{4}\right)e_1 + \left(\frac{p+1}{4}\right)e_2\right\}h^{(n)}$$

$$= p^{n-1}\left\{\left(\frac{p-3}{4}\right)e_1h^{(n)} + \left(\frac{p+1}{4}\right)e_2h^{(n)}\right\}.$$

Again by Lemma 5.2.3, we get

$$(e_1^{(n)})^2 = p^{n-1}\left\{\left(\frac{p-3}{4}\right)e_1^{(n)} + \left(\frac{p+1}{4}\right)e_2^{(n)}\right\}.$$

(ii) By Lemma 5.2.3, we have

$$(e_2^{(n)})^2 = (e_2h^{(n)})^2.$$

By Theorem 5.2.5 and Lemma 5.2.4, we have

$$e_2^2 = \left(\frac{p-3}{4}\right)e_2 + \left(\frac{p+1}{4}\right)e_1$$

and

$$(h^{(n)})^2 = p^{n-1}h^{(n)}.$$

Therefore,

$$(e_2^{(n)})^2 = p^{n-1}\left\{\left(\frac{p-3}{4}\right)e_2 + \left(\frac{p+1}{4}\right)e_1\right\}h^{(n)}$$

$$= p^{n-1}\left\{\left(\frac{p-3}{4}\right)e_2h^{(n)} + \left(\frac{p+1}{4}\right)e_1h^{(n)}\right\}.$$

Again by Lemma 5.2.3, we get

$$(e_2^{(n)})^2 = p^{n-1}\left\{\left(\frac{p-3}{4}\right)e_2^{(n)} + \left(\frac{p+1}{4}\right)e_1^{(n)}\right\}.$$

(iii) By Lemma 5.2.3, we have

$$e_1^{(n)}e_2^{(n)} = e_1e_2\left(h^{(n)}\right)^2.$$

By Theorem 5.2.5, we get

$$= \left\{\left(\frac{p-1}{2}\right) + \left(\frac{p-3}{4}\right)(e_1+e_2)\right\}(h^{(n)})^2$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right) + \left(\frac{p-3}{4}\right)(e_1 + e_2)\right\}h^{(n)}$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-3}{4}\right)(e_1 h^{(n)} + e_2 h^{(n)})\right\}$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-3}{4}\right)(e_1^{(n)} + e_2^{(n)})\right\}.$$

Corollary 5.2.8. If $p = 8k - 1$, k is odd integer, then

(i) $(e_1^{(n)})^2 = 3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right)$,

(ii) $(e_2^{(n)})^2 = 3^{n-1}\left(e_2^{(n)} + 2e_1^{(n)}\right)$,

(iii) $e_1^{(n)}e_2^{(n)} = 3^{n-1}\left(3h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)$.

Proof. (i) Let $p = 8k - 1$, k is odd integer, then $\frac{p-3}{4} \equiv 1(\text{mod } 4)$, $\frac{p+1}{4} \equiv 2(\text{mod } 4)$ and $p \equiv 3(\text{mod } 4)$.

By using Theorem 5.2.7(i), we have

$$(e_1^{(n)})^2 = 3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right).$$

(ii) Again using above values in Theorem 5.2.7(ii), we get

$$(e_2^{(n)})^2 = 3^{n-1}\left(e_2^{(n)} + 2e_1^{(n)}\right).$$

(iii) For $p = 8k - 1$, we have $\frac{p-1}{2} \equiv 3(\text{mod } 4)$.

Then by Theorem 5.2.7(iii), we get

$$e_1^{(n)}e_2^{(n)} = 3^{n-1}\left(3h^{(n)} + e_1^{(n)} + e_2^{(n)}\right).$$

Corollary 5.2.9. If $p = 8k - 1$, k is even integer, then

(i) $(e_1^{(n)})^2 = 3^n e_1^{(n)}$,

(ii) $(e_2^{(n)})^2 = 3^n e_2^{(n)}$,

(iii) $e_1^{(n)}e_2^{(n)} = 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)$.

Proof. Let $p = 8k - 1$, k is even integer, then

$\frac{p-3}{4} \equiv 3(\text{mod } 4)$, $\frac{p+1}{4} \equiv 0(\text{mod } 4)$ and $p \equiv 3(\text{mod } 4)$.

Using Theorem 5.2.7(i), we have

$$\left(e_1^{(n)}\right)^2 = 3^{n-1}\left(3e_1^{(n)}\right)$$

$$= 3^n e_1^{(n)}.$$

(ii) Again using above values in Theorem 5.2.7(ii), we get

$$\left(e_2^{(n)}\right)^2 = 3^{n-1}\left(3e_2^{(n)}\right)$$

$$= 3^n e_2^{(n)}.$$

(iii) For $p = 8k - 1$, we have $\frac{p-1}{2} \equiv 3(\text{mod } 4)$.

Then by Theorem 5.2.7(iii), we get

$$e_1^{(n)} e_2^{(n)} = 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right).$$

Theorem 5.2.10. If $p = 4k + 1$, then

(i) $(e_1^{(n)})^2 = p^{n-1}\left(\frac{p-1}{2} + \left(\frac{p-5}{4}\right)e_1^{(n)} + \left(\frac{p-1}{4}\right)e_2^{(n)}\right)$,

(ii) $(e_2^{(n)})^2 = p^{n-1}\left(\frac{p-1}{2} + \left(\frac{p-1}{4}\right)e_1^{(n)} + \left(\frac{p-5}{4}\right)e_2^{(n)}\right)$,

(iii) $e_1^{(n)} e_2^{(n)} = p^{n-1}\left(\frac{p-1}{4}\right)(e_1^{(n)} + e_2^{(n)})$.

Proof. (i) By Lemma 5.2.3, we have

$(e_1^{(n)})^2 = (e_1 h^{(n)})^2$.

By Theorem 5.2.6 and Lemma 5.2.4, we have

$$e_1^2 = \frac{p-1}{2} + \left(\frac{p-5}{4}\right)e_1 + \left(\frac{p-1}{4}\right)e_2$$

and

$$(h^{(n)})^2 = p^{n-1}h^{(n)}.$$

Therefore,

$$(e_1^{(n)})^2 = p^{n-1}\left\{\frac{p-1}{2} + \left(\frac{p-5}{4}\right)e_1 + \left(\frac{p-1}{4}\right)e_2\right\}h^{(n)}$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-5}{4}\right)e_1h^{(n)} + \left(\frac{p-1}{4}\right)e_2h^{(n)}\right\}.$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-5}{4}\right)e_1^{(n)} + \left(\frac{p-1}{4}\right)e_2^{(n)}\right\}.$$

(ii) By Lemma 5.2.3, we have

$(e_2^{(n)})^2 = (e_2h^{(n)})^2$.

By Theorem 5.2.6 and Lemma 5.2.4, we have

$$e_2^2 = \frac{p-1}{2} + \left(\frac{p-1}{4}\right)e_1 + \left(\frac{p-5}{4}\right)e_2$$

and

$$(h^{(n)})^2 = p^{n-1}h^{(n)}.$$

Therefore,

$$(e_2^{(n)})^2 = p^{n-1}\left\{\frac{p-1}{2} + \left(\frac{p-1}{4}\right)e_1 + \left(\frac{p-5}{4}\right)e_2\right\}h^{(n)}$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-1}{4}\right)e_1h^{(n)} + \left(\frac{p-5}{4}\right)e_2h^{(n)}\right\}$$

$$= p^{n-1}\left\{\left(\frac{p-1}{2}\right)h^{(n)} + \left(\frac{p-1}{4}\right)e_1^{(n)} + \left(\frac{p-5}{4}\right)e_2^{(n)}\right\}.$$

(iii) By Lemma 5.2.3, we have

$$e_1^{(n)}e_2^{(n)} = e_1e_2\left(h^{(n)}\right)^2.$$

By Theorem 5.2.6, we get

$$e_1e_2 = \left(\tfrac{p-1}{4}\right)(e_1 + e_2).$$

Therefore,

$$e_1^{(n)}e_2^{(n)} = \left\{\left(\frac{p-1}{4}\right)(e_1 + e_2)\right\}(h^{(n)})^2$$

$$= p^{n-1}\left(\frac{p-1}{4}\right)(e_1+e_2)h^{(n)}$$

$$= p^{n-1}\left(\frac{p-1}{4}\right)(e_1h^{(n)}+e_2h^{(n)})$$

$$= p^{n-1}\left(\frac{p-1}{4}\right)\left(e_1^{(n)}+e_2^{(n)}\right).$$

Corollary 5.2.11. If $p = 8k+1$, k is odd integer, then

(i) $(e_1^{(n)})^2 = e_1^{(n)} + 2e_2^{(n)}$,

(ii) $(e_2^{(n)})^2 = 2e_2^{(n)} + e_1^{(n)}$,

(iii) $e_1^{(n)}e_2^{(n)} = 2\left(e_1^{(n)}+e_2^{(n)}\right)$.

Proof. Let $p = 8k+1$, k is odd integer, then

$\frac{p-5}{4} \equiv 1(\text{mod } 4)$, $\frac{p-1}{4} \equiv 2(\text{mod } 4)$, $\frac{p-1}{2} \equiv 0(\text{mod } 4)$ and $p \equiv 1(\text{mod } 4)$.

By Theorem 5.2.10 (i), we have

$$\left(e_1^{(n)}\right)^2 = e_1^{(n)} + 2e_2^{(n)}.$$

Again using above values in Theorem 5.2.10 (ii) and (iii), we get

$$\left(e_2^{(n)}\right)^2 = 2e_2^{(n)} + e_1^{(n)}$$

and

$$e_1^{(n)}e_2^{(n)} = 2\left(e_1^{(n)}+e_2^{(n)}\right).$$

Corollary 5.2.12. If $p = 8k+1$, k is even integer, then

(i) $(e_1^{(n)})^2 = 3e_1^{(n)}$,

(ii) $(e_2^{(n)})^2 = 3e_2^{(n)}$,

(iii) $e_1^{(n)}e_2^{(n)} = 0$.

Proof. Let $p = 8k+1$, k is even integer, then

$\frac{p-5}{4} \equiv 3(\text{mod } 4)$, $\frac{p-1}{4} \equiv 0(\text{mod } 4)$, $\frac{p-1}{2} \equiv 0(\text{mod } 4)$ and $p \equiv 1(\text{mod } 4)$.

By Theorem 5.2.10 (i), we have

$$\left(e_1^{(n)}\right)^2 = 3e_1^{(n)}.$$

Again using above values in Theorem 5.2.10 (ii) and (iii), we get

$$\left(e_2^{(n)}\right)^2 = 3e_2^{(n)}$$

and

$$e_1^{(n)} e_2^{(n)} = 0.$$

Theorem 5.2.13. If $p = 8k - 1$, k is odd integer,

(i) $\theta_1^{(n)} = 3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right)$,

(ii) $\theta_2^{(n)} = 3^{n-1}\left(e_2^{(n)} + 2e_1^{(n)}\right)$,

(iii) $\theta_3^{(n)} = 3^{n-1}\left(h^n + 3e_2^{(n)} + 2e_1^{(n)}\right)$,

(iv) $\theta_4^{(n)} = 3^{n-1}\left(h^n + 3e_1^{(n)} + 2e_2^{(n)}\right)$,

then $\theta_1^{(n)}, \theta_2^{(n)}, \theta_3^{(n)}$ and $\theta_4^{(n)}$ are idempotents over Z_4.

Proof. (i) It is given that, $\theta_1^{(n)} = 3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right)$.

Therefore, $\left(\theta_1^{(n)}\right)^2 = \left[3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right)\right]^2$.

Since, $3^{n-1} \equiv (-1)^{n-1} (\text{mod } 4)$, therefore $(3^{n-1})^2 \equiv 1 (\text{mod } 4)$.

This gives that, $\left(\theta_1^{(n)}\right)^2 = \left(e_1^{(n)} + 2e_2^{(n)}\right)^2$

$$= (e_1^{(n)})^2$$

By corollary 5.2.8, we have

$$(e_1^{(n)})^2 = 3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right).$$

Hence, $\left(\theta_1^{(n)}\right)^2 = \theta_1^{(n)}$.

(ii) As, $\theta_2^{(n)} = 3^{n-1}\left(e_2^{(n)} + 2e_1^{(n)}\right)$, therefore

$$\left(\theta_2^{(n)}\right)^2 = \left[3^{n-1}\left(e_2^{(n)} + 2e_1^{(n)}\right)\right]^2.$$

This gives that,

$$\left(\theta_2^{(n)}\right)^2 = \left(e_2^{(n)}\right)^2.$$

By Cor. 5.2.8, we have

$$(e_2^{(n)})^2 = 3^{n-1}\left(e_2^{(n)} + 2e_1^{(n)}\right).$$

Thus,

$$\left(\theta_2^{(n)}\right)^2 = \theta_2^{(n)}.$$

(iii) It is given that, $\theta_3^{(n)} = 3^{n-1}\left(h^n + 3e_2^{(n)} + 2e_1^{(n)}\right)$.

Therefore, $$\left(\theta_3^{(n)}\right)^2 = \left[3^{n-1}\left(h^n + 3e_2^{(n)} + 2e_1^{(n)}\right)\right]^2$$

$$= \left(h^n + 3e_2^{(n)}\right)^2.$$

By Lemma 5.2.3, we have $e_2^{(n)} = e_2 h^n$, therefore

$$\left(\theta_3^{(n)}\right)^2 = (1 + 3e_2)^2 (h^n)^2.$$

By Lemma 5.2.4 and Cor. 5.2.8, we get

$$(h^n)^2 = p^{n-1}h^n$$

$$= 3^{n-1}h^n.$$

So,

$$\left(\theta_3^{(n)}\right)^2 = 3^{n-1}(1 + {e_2}^2 + 2e_2)h^n.$$

Using Theorem 5.2.5 and Cor. 5.2.8, we can solve $(e_2)^2 = e_2 + 2e_1$.

Thus,

$$\left(\theta_3^{(n)}\right)^2 = 3^{n-1}(1 + e_2 + 2e_1 + 2e_2)h^n$$

$$= 3^{n-1}(1 + 2e_1 + 3e_2)h^n$$

$$= 3^{n-1}(h^n + 2e_1h^n + 3e_2h^n)$$

$$= 3^{n-1}(h^n + 2e_1^{(n)} + 3e_2^{(n)})$$

$$= \theta_3^{(n)}.$$

(iv) It is given that, $\theta_4^{(n)} = 3^{n-1}\left(h^n + 3e_1^{(n)} + 2e_2^{(n)}\right)$.

Therefore, $$\left(\theta_4^{(n)}\right)^2 = \left[3^{n-1}\left(h^n + 3e_1^{(n)} + 2e_2^{(n)}\right)\right]^2$$

$$= \left(h^n + 3e_1^{(n)} + 2e_2^{(n)}\right)^2.$$

By Lemma 5.2.3, we have $e_1^{(n)} = e_1 h^n$ and $e_2^{(n)} = e_2 h^n$, therefore

$$\left(\theta_4^{(n)}\right)^2 = (1 + 3e_1 + 2e_2)^2 (h^n)^2.$$

By Lemma 5.2.4 and Cor. 5.2.8, we get

$$(h^n)^2 = p^{n-1}h^n,$$

$$(h^n)^2 = 3^{n-1}h^n.$$

So,

$$\left(\theta_4^{(n)}\right)^2 = 3^{n-1}(1 + 3e_1 + 2e_2)^2 h^n$$

$$= 3^{n-1}(1 + 3e_1)^2 h^n$$

$$= 3^{n-1}(1 + e_1^2 + 2e_1)h^n.$$

Using Theorem 5.2.5 and Cor. 5.2.8, we can solve $(e_1)^2 = e_2 + 2e_1$.

Thus,

$$\left(\theta_4^{(n)}\right)^2 = 3^{n-1}(1 + e_1 + 2e_2 + 2e_1)h^n$$

$$= 3^{n-1}(1 + 3e_1 + 2e_2)h^n$$

$$= 3^{n-1}(h^n + 3e_1 h^n + 2e_2 h^n)$$

$$= 3^{n-1}(h^n + 3e_1^{(n)} + 2e_2^{(n)})$$

$$= \theta_4^{(n)}.$$

Theorem 5.2.14. If $p = 8k - 1$, k is even integer,

(i) $\theta_1^{(n)} = 3^n e_1^{(n)}$,

(ii) $\theta_2^{(n)} = 3^n e_2^{(n)}$,

(iii) $\theta_3^{(n)} = 3^{n-1}\left(h^n + e_2^{(n)}\right)$,

(iv) $\theta_4^{(n)} = 3^{n-1}\left(h^n + e_1^{(n)}\right)$,

then $\theta_1^{(n)}, \theta_2^{(n)}, \theta_3^{(n)}$ and $\theta_4^{(n)}$ are idempotents over Z_4.

Proof. (i) It is given that, $\theta_1^{(n)} = 3^n e_1^{(n)}$.

Therefore, $\left(\theta_1^{(n)}\right)^2 = \left[3^n e_1^{(n)}\right]^2$.

Since, $3^n \equiv (-1)^n \pmod 4$, therefore $(3^n)^2 \equiv 1 \pmod 4$.

This gives that, $\left(\theta_1^{(n)}\right)^2 = (e_1^{(n)})^2$.

By Corollary 5.2.9, we have

$$(e_1^{(n)})^2 = 3^n e_1^{(n)}.$$

Hence, $\left(\theta_1^{(n)}\right)^2 = \theta_1^{(n)}$.

(ii) As, $\theta_2^{(n)} = 3^n e_2^{(n)}$, therefore

$$\left(\theta_2^{(n)}\right)^2 = \left[3^n e_2^{(n)}\right]^2$$

$$= \left(e_2^{(n)}\right)^2.$$

By Corollary 5.2.9, we have

$$(e_2^{(n)})^2 = 3^n e_2^{(n)}.$$

Thus,

$$\left(\theta_2^{(n)}\right)^2 = \theta_2^{(n)}.$$

(iii) It is given that, $\theta_3^{(n)} = 3^{n-1}\left(h^n + e_2^{(n)}\right)$.

Therefore, $\left(\theta_3^{(n)}\right)^2 = \left[3^{n-1}\left(h^n + e_2^{(n)}\right)\right]^2$

$$= \left(h^n + e_2^{(n)}\right)^2.$$

By Lemma 5.2.3, we have $e_2^{(n)} = e_2 h^n$, therefore

$$\left(\theta_3^{(n)}\right)^2 = (1 + e_2)^2 (h^n)^2.$$

By Lemma 5.2.4 and Cor. 5.2.9, we get

$$(h^n)^2 = p^{n-1} h^n,$$

$$(h^n)^2 = 3^{n-1} h^n.$$

So,

$$\left(\theta_3^{(n)}\right)^2 = 3^{n-1}(1 + {e_2}^2 + 2e_2)h^n.$$

Using Theorem 5.2.5 and Cor. 5.2.9, we can solve $(e_2)^2 = 3e_2$.

Thus,

$$\left(\theta_3^{(n)}\right)^2 = 3^{n-1}(1 + 3e_2 + 2e_2)h^n$$

$$= 3^{n-1}(1 + e_2)h^n$$

$$= 3^{n-1}(h^n + e_2 h^n)$$

$$= 3^{n-1}(h^n + e_2^{(n)})$$

$$= \theta_3^{(n)}.$$

(iv) It is given that, $\theta_4^{(n)} = 3^{n-1}\left(h^n + e_1^{(n)}\right)$.

Therefore, $\left(\theta_4^{(n)}\right)^2 = \left[3^{n-1}\left(h^n + e_1^{(n)}\right)\right]^2$

$$= \left(h^n + e_1^{(n)}\right)^2.$$

By Lemma 5.2.3, we have $e_1^{(n)} = e_1 h^n$, therefore

$$\left(\theta_4^{(n)}\right)^2 = (1 + e_1)^2 (h^n)^2.$$

By Lemma 5.2.4 and Cor. 5.2.9, we get

$$(h^n)^2 = p^{n-1}h^n$$

$$(h^n)^2 = 3^{n-1}h^n.$$

So,

$$\left(\theta_4^{(n)}\right)^2 = 3^{n-1}(1+e_1)^2h^n$$

$$= 3^{n-1}(1+e_1^2+2e_1)h^n.$$

Using Theorem 5.2.5 and Cor. 5.2.9, we can solve

$$(e_1)^2 = 3e_1.$$

Thus,

$$\left(\theta_4^{(n)}\right)^2 = 3^{n-1}(1+3e_1+2e_1)h^n$$

$$= 3^{n-1}(1+e_1)h^n$$

$$= 3^{n-1}(h^n+e_1h^n)$$

$$= 3^{n-1}(h^n+e_1^{(n)})$$

$$= \theta_4^{(n)}.$$

Theorem 5.2.15. If $p = 8k+1$, k is odd integer,

(i) $\theta_1^{(n)} = e_1^{(n)} + 2e_2^{(n)}$,

(ii) $\theta_2^{(n)} = 2e_1^{(n)} + e_2^{(n)}$,

(iii) $\theta_3^{(n)} = h^n + 2e_1^{(n)} + 3e_2^{(n)}$,

(iv) $\theta_4^{(n)} = h^n + 3e_1^{(n)} + 2e_2^{(n)}$,

then $\theta_1^{(n)}, \theta_2^{(n)}, \theta_3^{(n)}$ and $\theta_4^{(n)}$ are idempotents over Z_4.

Proof. (i) It is given that, $\theta_1^{(n)} = e_1^{(n)} + 2e_2^{(n)}$.

Therefore, $$\left(\theta_1^{(n)}\right)^2 = \left(e_1^{(n)} + 2e_2^{(n)}\right)^2$$

$$= (e_1^{(n)})^2$$

By Corollary 5.2.11, we have

$$(e_1^{(n)})^2 = e_1^{(n)} + 2e_2^{(n)}.$$

Hence, $$\left(\theta_1^{(n)}\right)^2 = \theta_1^{(n)}.$$

(ii) As, $\theta_2^{(n)} = 2e_1^{(n)} + e_2^{(n)}$, therefore

$$\left(\theta_2^{(n)}\right)^2 = \left[2e_1^{(n)} + e_2^{(n)}\right]^2$$

$$= \left(e_2^{(n)}\right)^2.$$

By Corollary 5.2.11, we have

$$(e_2^{(n)})^2 = 2e_1^{(n)} + e_2^{(n)}.$$

Thus,

$$\left(\theta_2^{(n)}\right)^2 = \theta_2^{(n)}.$$

(iii) It is given that, $\theta_3^{(n)} = h^n + 2e_1^{(n)} + 3e_2^{(n)}$.

Therefore, $$\left(\theta_3^{(n)}\right)^2 = \left[h^n + 2e_1^{(n)} + 3e_2^{(n)}\right]^2$$

$$= \left(h^n + 3e_2^{(n)}\right)^2.$$

By Lemma 5.2.3, we have $e_2^{(n)} = e_2 h^n$, therefore

$$\left(\theta_3^{(n)}\right)^2 = (1 + 3e_2)^2 (h^n)^2.$$

By Lemma 5.2.4 and Cor. 5.2.11, we get

$$(h^n)^2 = p^{n-1}h^n,$$

$$(h^n)^2 = h^n.$$

So,

$$\left(\theta_3^{(n)}\right)^2 = (1 + {e_2}^2 + 2e_2)h^n.$$

Using Theorem 5.2.6 and Cor. 5.2.11, we can solve $(e_2)^2 = 2e_1 + e_2$.

Thus,

$$\left(\theta_3^{(n)}\right)^2 = (1 + e_2 + 2e_1 + 2e_2)h^n$$

$$= (1 + 2e_1 + 3e_2)h^n$$

$$= (h^n + 2e_1h^n + 3e_2h^n)$$

$$= (h^n + 2e_1^{(n)} + 3e_2^{(n)})$$

$$= \theta_3^{(n)}.$$

(iv) It is given that, $\theta_4^{(n)} = h^n + 3e_1^{(n)} + 2e_2^{(n)}$.

Therefore, $\left(\theta_4^{(n)}\right)^2 = \left[h^n + 3e_1^{(n)} + 2e_2^{(n)}\right]^2$.

By Lemma 5.2.3, we have $e_1^{(n)} = e_1h^n$ and $e_2^{(n)} = e_2h^n$, therefore

$$\left(\theta_4^{(n)}\right)^2 = (1 + 3e_1 + 2e_2)^2(h^n)^2.$$

By Lemma 5.2.4 and Cor. 5.2.11, we get

$$(h^n)^2 = p^{n-1}h^n$$

$$= h^n.$$

So,

$$\left(\theta_4^{(n)}\right)^2 = (1 + 3e_1 + 2e_2)^2h^n$$

$$= (1 + 3e_1)^2h^n$$

$$= (1 + e_1^2 + 2e_1)h^n.$$

Using Theorem 5.2.6 and Cor. 5.2.11, we can solve $(e_1)^2 = 2e_2 + e_1$.

Thus,

$$\left(\theta_4^{(n)}\right)^2 = (1 + e_1 + 2e_2 + 2e_1)h^n$$

$$= (1 + 3e_1 + 2e_2)h^n$$

$$= h^n + 3e_1h^n + 2e_2h^n$$

$$= h^n + 3e_1^{(n)} + 2e_2^{(n)}$$

$$= \theta_4^{(n)}.$$

Theorem 5.2.16. If $p = 8k + 1$, k is even integer,

(i) $\theta_1^{(n)} = 3e_1^{(n)}$,

(ii) $\theta_2^{(n)} = 3e_2^{(n)}$,

(iii) $\theta_3^{(n)} = h^n + e_2^{(n)}$,

(iv) $\theta_4^{(n)} = h^n + e_1^{(n)}$,

then $\theta_1^{(n)}, \theta_2^{(n)}, \theta_3^{(n)}$ and $\theta_4^{(n)}$ are idempotents over Z_4.

Proof. (i) It is given that, $\theta_1^{(n)} = 3e_1^{(n)}$.

Therefore, $$\left(\theta_1^{(n)}\right)^2 = \left(3e_1^{(n)}\right)^2$$

$$= (e_1^{(n)})^2$$

By Corollary 5.2.12, we have

$$(e_1^{(n)})^2 = 3e_1^{(n)}.$$

Hence, $$\left(\theta_1^{(n)}\right)^2 = \theta_1^{(n)}.$$

(ii) As, $\theta_2^{(n)} = 3e_2^{(n)}$, therefore

$$\left(\theta_2^{(n)}\right)^2 = \left[3e_2^{(n)}\right]^2$$

$$= \left(e_2^{(n)}\right)^2.$$

By Corollary 5.2.12, we have

$$(e_2^{(n)})^2 = 3e_2^{(n)}.$$

Thus,

$$\left(\theta_2^{(n)}\right)^2 = \theta_2^{(n)}.$$

(iii) It is given that, $\theta_3^{(n)} = h^{(n)} + e_2^{(n)}$.

Therefore, $\left(\theta_3^{(n)}\right)^2 = (h^{(n)} + e_2^{(n)})^2$.

By Lemma 5.2.3, we have $e_2^{(n)} = e_2 h^{(n)}$, therefore

$$\left(\theta_3^{(n)}\right)^2 = (1 + e_2)^2 \left(h^{(n)}\right)^2.$$

By Lemma 5.2.4 and Cor. 5.2.12, we get

$$\left(h^{(n)}\right)^2 = p^{n-1} h^{(n)}$$

$$= h^{(n)}.$$

So,

$$\left(\theta_3^{(n)}\right)^2 = (1 + {e_2}^2 + 2e_2) h^{(n)}.$$

Using Theorem 5.2.6 and Cor. 5.2.12, we can solve $(e_2)^2 = 3e_2$.

Thus,

$$\left(\theta_3^{(n)}\right)^2 = (1 + 3e_2 + 2e_2) h^{(n)}$$

$$= (1 + e_2) h^{(n)}$$

$$= \left(h^{(n)} + e_2 h^{(n)}\right)$$

$$= (h^{(n)} + e_2^{(n)})$$

$$= \theta_3^{(n)}.$$

(iv) It is given that, $\theta_4^{(n)} = h^{(n)} + e_1^{(n)}$.

Therefore, $\left(\theta_4^{(n)}\right)^2 = \left[h^{(n)} + e_1^{(n)}\right]^2$.

By Lemma 5.2.3, we have $e_1^{(n)} = e_1 h^n$, therefore

$$\left(\theta_4^{(n)}\right)^2 = (1 + e_1)^2 \left(h^{(n)}\right)^2.$$

By Lemma 5.2.4 and Cor. 5.2.12, we get

$$\left(h^{(n)}\right)^2 = p^{n-1}h^{(n)},$$

$$= h^{(n)}.$$

So,

$$\left(\theta_4^{(n)}\right)^2 = (1 + e_1^2 + 2e_1)h^{(n)}.$$

Using Theorem 5.2.6 and Cor. 5.2.12, we can solve $(e_1)^2 = 3e_1$.

Thus,

$$\left(\theta_4^{(n)}\right)^2 = (1 + 3e_1 + 2e_1)h^{(n)}$$

$$= (1 + e_1)h^{(n)}$$

$$= h^{(n)} + e_1h^{(n)}$$

$$= h^{(n)} + e_1^{(n)}$$

$$= \theta_4^{(n)}.$$

5.3. Some Properties of Quadratic Residue Codes of Length $p^n(n \geq 1, p$ is odd prime)

Definition 5.3.1. The codes C_1, C_2, C_3 and C_4 generated by $\theta_1^{(n)}, \theta_2^{(n)}, \theta_3^{(n)}$and $\theta_4^{(n)}$ respectively, are called QR−Codes.

Theorem 5.3.2. If $p = 8k - 1$, k is odd, let

$$C_1 = \left(3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right)\right),$$

$$C_2 = \left(3^{n-1}\left(2e_1^{(n)} + e_2^{(n)}\right)\right),$$

$$C_3 = \left(3^{n-1}\left(h^{(n)} + 3e_2^{(n)} + 2e_1^{(n)}\right)\right),$$

$$C_4 = \left(3^{n-1}\left(h^{(n)} + 3e_1^{(n)} + 2e_2^{(n)}\right)\right),$$

then the following hold for Z_4 quadratic residue codes C_1, C_2, C_3 and C_4:

(i) C_1, C_2 and C_3, C_4 are equivalent.

(ii) $C_1 \cap C_2 = \left(3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$ and $C_1 + C_2 = (3^n h^{(n)})$.

(iii) $|C_1| = |C_2| = 4^{\frac{p+1}{2}}$.

(iv) $C_1 = C_3 + C_1 \cap C_2, C_2 = C_4 + C_1 \cap C_2$.

(v) $|C_3| = |C_4| = 4^{\frac{p-1}{2}}$.

Proof. (i) Let $s \in N$, then the mapping μ_s interchanges $e_1^{(n)}$and $e_2^{(n)}$. Hence

$$\mu_s\left(3^{n-1}\left(e_1^{(n)} + 2e_2^{(n)}\right)\right) = 3^{n-1}\left(2e_1^{(n)} + e_2^{(n)}\right),$$

$$\mu_s\left(3^{n-1}\left(h^{(n)} + 3e_2^{(n)} + 2e_1^{(n)}\right)\right) = 3^{n-1}\left(h^{(n)} + 3e_1^{(n)} + 2e_2^{(n)}\right)$$

and

$$\mu_s\left(h^{(n)}\right) = h^{(n)}.$$

Thus, C_1, C_2 and C_3, C_4 are equivalent.

(ii) By Pless and Qian [84], $C_1 \cap C_2$ has idempotent generator $\theta_1^{(n)}\theta_2^{(n)}$ and $C_1 + C_2$ has idempotent generator $\theta_1^{(n)} + \theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}$.

Thus,

$$C_1 \cap C_2 = (\theta_1^{(n)}\theta_2^{(n)})$$

$$= \left(\left(e_1^{(n)} + 2e_2^{(n)}\right)\left(2e_1^{(n)} + e_2^{(n)}\right)\right)$$

$$= \left(e_1^{(n)}e_2^{(n)} + 2\left(e_1^{(n)}\right)^2 + 2\left(e_2^{(n)}\right)^2\right)$$

By Cor.5.2.8, we have

$$= \left(3^{n-1}\left(3h^{(n)} + e_1^{(n)} + e_2^{(n)} + 2e_1^{(n)} + 2e_2^{(n)}\right)\right)$$

$$= \left(3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right).$$

Also from above discussion, we have

$$C_1 + C_2 = \left(\theta_1^{(n)} + \theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}\right)$$

As, $$\theta_1^{(n)}\theta_2^{(n)} = 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right).$$

So,

$$= \left(3^{n-1}\left(e_1^{(n)} + 2e_1^{(n)}\right) + 3^{n-1}\left(2e_1^{(n)} + e_2^{(n)}\right) - 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$$

$$= \left(3^{n-1}\left(3e_1^{(n)} + 3e_2^{(n)}\right) - 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$$

$$= \left(3^n h^{(n)}\right).$$

(iii) By part (ii) we have

$$C_1 \cap C_2 = \left(3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$$

$$= \left\{a\ 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\middle|\ a \in Z_4\right\}.$$

This gives that

$$|C_1 \cap C_2| = 4.$$

Similarly,

$$C_1 + C_2 = \left(3^n h^{(n)}\right)$$

$$= \left\{\left(a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1}x^{p-1}\right)h^{(n)}\middle|\ a_i \in Z_4, 0 \le i \le p-1\right\}.$$

This implies that

$$|C_1 + C_2| = 4^p.$$

As,

$$|C_1 + C_2| = \frac{|C_1||C_2|}{|C_1 \cap C_2|}.$$

So

$$|C_1||C_2| = 4^{p+1}.$$

Hence,

$$|C_1| = |C_2| = 4^{\frac{p+1}{2}}.$$

(iv) By part (iii) we have

$$C_1 + C_1 \cap C_2 = (\theta_3^{(n)} + \theta_1^{(n)}\theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)}).$$

First we solve,

$$\theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)} = 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)3^{n-1}\left(h^{(n)} + 3e_2^{(n)} + 2e_1^{(n)}\right)$$

$$= 3\{\left(h^{(n)}\right)^2 + 3e_1^{(n)}h^{(n)} + 2(e_1^{(n)})^2 + e_1^{(n)}e_2^{(n)} + 3(e_2^{(n)})^2\}$$

$$= 3\left\{\left(h^{(n)}\right)^2 + 3e_1\left(h^{(n)}\right)^2 + 2e_1^2\left(h^{(n)}\right)^2 + e_1e_2\left(h^{(n)}\right)^2\right.$$

$$\left. + 3e_2^2\left(h^{(n)}\right)^2\right\} \ = 3\left(h^{(n)}\right)^2\{1 + 3e_1 + 2e_1^2 + e_1e_2 + 3e_2^2\}.$$

By Corollary 5.2.8, we have

$$= 3\left(h^{(n)}\right)^2\{1 + 3e_1 + 2e_1 + 3 + e_1 + e_2 + 3e_2 + 2e_1\}$$

$$= 3\left(h^{(n)}\right)^2\{0\}$$

$$= 0.$$

Thus,

$$C_1 + C_1 \cap C_2 = (\theta_3^{(n)} + \theta_1^{(n)}\theta_2^{(n)})$$

$$= \left(3^{n-1}\left(h^{(n)} + 3e_2^{(n)} + 2e_1^{(n)}\right) + 3^n\left(h^{(n)} + e_2^{(n)} + e_1^{(n)}\right)\right)$$

$$= \left(3^{n-1}\{e_1^{(n)} + 2e_2^{(n)}\}\right)$$

$$= (\theta_1^{(n)})$$

$$= C_1.$$

Similarly, we can prove, $C_2 = C_4 + C_1 \cap C_2$.

(v) We know that,

$$|C_3 + C_1 \cap C_2| = \frac{|C_3||C_1 \cap C_2|}{|C_1 \cap C_2 \cap C_3|}.$$

By part (iv), we get

$$|C_1| = \frac{|C_3||C_1 \cap C_2|}{|C_1 \cap C_2 \cap C_3|}.$$

As, $$C_1 \cap C_2 \cap C_3 = \left(\theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)}\right) = (0).$$

Thus,

$$|C_1 \cap C_2 \cap C_3| = 1.$$

Hence,

$$|C_1| = |C_3||C_1 \cap C_2|$$

From part (iii), $|C_1 \cap C_2| = 4$ and $|C_1| = 4^{\frac{p+1}{2}}$.

Thus,

$$|C_3| = 4^{\frac{p-1}{2}}.$$

Similarly,

$$|C_4| = 4^{\frac{p-1}{2}}.$$

Theorem 5.3.3. If $p = 8k - 1$, k is even, let

$$C_1 = \left(3^n e_1^{(n)}\right),$$

$$C_2 = \left(3^n e_2^{(n)}\right),$$

$$C_3 = \left(3^{n-1}\left(h^{(n)} + e_2^{(n)}\right)\right),$$

$$C_4 = \left(3^{n-1}\left(h^{(n)} + e_1^{(n)}\right)\right),$$

then the following hold for Z_4 quadratic residue codes C_1, C_2, C_3 and C_4:

(i) C_1, C_2 and C_3, C_4 are equivalent.

(ii) $C_1 \cap C_2 = \left(3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$ and $C_1 + C_2 = (3^n h^{(n)})$.

(iii) $|C_1| = |C_2| = 4^{\frac{p+1}{2}}$.

(iv) $C_1 = C_3 + C_1 \cap C_2, C_2 = C_4 + C_1 \cap C_2$.

(v) $|C_3| = |C_4| = 4^{\frac{p-1}{2}}$.

Proof. (i). Let $s \in N$, then the mapping μ_s interchanges $e_1^{(n)}$and $e_2^{(n)}$. Hence

$$\mu_s\left(3^n e_1^{(n)}\right) = 3^n e_2^{(n)},$$

$$\mu_s\left(3^n e_2^{(n)}\right) = 3^n e_1^{(n)}$$

and

$$\mu_s\left(h^{(n)}\right) = h^{(n)}$$

Thus, C_1, C_2 and C_3, C_4 are equivalent.

(ii) Here

$$C_1 \cap C_2 = (\theta_1^{(n)}\theta_2^{(n)})$$

$$= \left(3^n e_1^{(n)} 3^n e_2^{(n)}\right)$$

$$= \left(e_1^{(n)} e_2^{(n)}\right).$$

By Cor. 5.2.9, we have $$= \left(3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right).$$

Also,

$$C_1 + C_2 = \left(\theta_1^{(n)} + \theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}\right)$$

As, $$\theta_1^{(n)}\theta_2^{(n)} = 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right).$$

So,

$$C_1 + C_2 = \left(3^n e_1^{(n)} + 3^n e_2^{(n)} - 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$$

$$= \left(-3^n\left(h^{(n)}\right)\right)$$

$$= \left(3^n h^{(n)}\right).$$

(iii) By part (ii) we get

$$C_1 \cap C_2 = \left(3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right).$$

Therefore,

$$|C_1 \cap C_2| = 4.$$

Similarly,

$$C_1 + C_2 = \left(3^n h^{(n)}\right)$$

Hence,

$$|C_1| = |C_2| = 4^{\frac{p+1}{2}}.$$

(iv) By part (iii),

$$C_1 + C_1 \cap C_2 = (\theta_3^{(n)} + \theta_1^{(n)}\theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)}).$$

Using value of $(\theta_1^{(n)}\theta_2^{(n)})$ from part (ii), we have

$$\theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)} = 3^n\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)3^{n-1}\left(h^{(n)} + e_2^{(n)}\right)$$

$$= 3\{\left(h^{(n)}\right)^2 + e_1^{(n)}h^{(n)} + 2e_2^{(n)}h^{(n)} + e_1^{(n)}e_2^{(n)} + (e_2^{(n)})^2\}$$

$$= 3\left\{\left(h^{(n)}\right)^2 + e_1\left(h^{(n)}\right)^2 + 2e_2\left(h^{(n)}\right)^2 + e_1e_2\left(h^{(n)}\right)^2 + e_2^2\left(h^{(n)}\right)^2\right\}$$

$$= 3\left(h^{(n)}\right)^2\{1 + e_1 + 2e_2 + e_1e_2 + e_2^2\}$$

By Corollary 5.2.9, we have

$$= 3\left(h^{(n)}\right)^2\{1 + e_1 + 2e_2 + 3 + 3e_1 + 3e_2 + 3e_2\}$$

$$= 3\left(h^{(n)}\right)^2\{0\}$$

$$= 0.$$

Thus,

$$C_1 + C_1 \cap C_2 = (\theta_3^{(n)} + \theta_1^{(n)}\theta_2^{(n)})$$

$$= \left(3^{n-1}\left(h^{(n)} + e_2^{(n)}\right) + 3^n\left(h^{(n)} + e_2^{(n)} + e_1^{(n)}\right)\right)$$

$$= \left(3^{n-1}\{3e_1^{(n)}\}\right)$$

$$= (\theta_1^{(n)})$$

$$= C_1.$$

Similarly, we can prove, $C_2 = C_4 + C_1 \cap C_2$.

(v) This part is on similar line of Theorem 5.3.2 (v).

Theorem 5.3.4. If $p = 8k + 1$, k is odd, let

$$C_1 = \left(h^{(n)} + 3e_1^{(n)} + 2e_2^{(n)}\right),$$

$$C_2 = \left(h^{(n)} + 2e_1^{(n)} + 3e_2^{(n)}\right),$$

$$C_3 = \left(2e_1^{(n)} + e_2^{(n)}\right),$$

$$C_4 = \left(e_1^{(n)} + 2e_2^{(n)}\right),$$

then the following hold for Z_4 quadratic residue codes C_1, C_2, C_3 and C_4:

(i) C_1, C_2 and C_3, C_4 are equivalent.

(ii) $C_1 \cap C_2 = \left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)$ and $C_1 + C_2 = (h^{(n)})$.

(iii) $|C_1| = |C_2| = 4^{\frac{p+1}{2}}$.

(iv) $C_1 = C_3 + C_1 \cap C_2, C_2 = C_4 + C_1 \cap C_2$.

(v) $|C_3| = |C_4| = 4^{\frac{p-1}{2}}$.

Proof. (i). Similar to Theorem 5.3.2 (i).

(ii) As we know,

$$C_1 \cap C_2 = (\theta_1^{(n)}\theta_2^{(n)})$$

$$= \left(\left(h^{(n)} + 3e_1^{(n)} + 2e_2^{(n)}\right)(h^{(n)} + 2e_1^{(n)} + 3e_2^{(n)})\right)$$

$$= \left(\left(h^{(n)}\right)^2 + e_1^{(n)}h^{(n)} + e_2^{(n)}h^{(n)} + 2\left(e_1^{(n)}\right)^2 + e_1^{(n)}e_2^{(n)} + 2\left(e_2^{(n)}\right)^2\right)$$

Using the Cor. 5.2.11, we get

$$= \left(\left(h^{(n)}\right)^2\{1 + e_1 + e_2\} + 2e_1^{(n)} + 2e_1^{(n)} + 2e_2^{(n)} + 2e_2^{(n)}\right)$$

$$= \left(h^{(n)}\{1 + e_1 + e_2\}\right)$$

$$= \left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right).$$

Also,

$$C_1 + C_2 = \left(\theta_1^{(n)} + \theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}\right).$$

As, $\theta_1^{(n)}\theta_2^{(n)} = h^{(n)} + e_1^{(n)} + e_2^{(n)}$.

So,

$$C_1 + C_2 = \left(h^{(n)} + 3e_1^{(n)} + 2e_2^{(n)} + h^{(n)} + 2e_1^{(n)} + 3e_2^{(n)} - \left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\right)$$

$$= \left(h^{(n)}\right).$$

(iii) By part (ii) we get

$$C_1 \cap C_2 = (h^{(n)} + e_1^{(n)} + e_2^{(n)})$$

$$= \left\{a\left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right) \middle| \, a \in Z_4\right\}.$$

This gives that

$$|C_1 \cap C_2| = 4.$$

Similarly,

$$C_1 + C_2 = \left(h^{(n)}\right)$$

$$= \left\{\left(a_0 + a_1x + a_2x^2 + \cdots + a_{p-1}x^{p-1}\right)h^{(n)} \middle| \, a_i \in Z_4, 0 \leq i \leq p-1\right\}.$$

This implies that

$$|C_1 + C_2| = 4^p.$$

As,

$$|C_1 + C_2| = \frac{|C_1||C_2|}{|C_1 \cap C_2|}.$$

So,

$$|C_1||C_2| = 4^{p+1}.$$

Hence,

$$|C_1| = |C_2| = 4^{\frac{p+1}{2}}.$$

(iv) By part (iii)

$$C_1 + C_1 \cap C_2 = (\theta_3^{(n)} + \theta_1^{(n)}\theta_2^{(n)} - \theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)}).$$

First we solve,

$$\theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)} = \left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)\left(2e_1^{(n)} + e_2^{(n)}\right)$$

$$= 2e_1^{(n)}h^{(n)} + 2(e_1^{(n)})^2 + 3e_1^{(n)}e_2^{(n)} + e_2^{(n)}h^{(n)} + (e_2^{(n)})^2$$

$$= 2e_1^{(n)}h^{(n)} + 2e_1^{(n)} + 2e_1^{(n)} + 2e_2^{(n)} + e_2^{(n)}h^{(n)} + e_2^{(n)} + 2e_1^{(n)}$$

$$= 2e_1^{(n)}h^{(n)} + e_2^{(n)}h^{(n)} + 2e_1^{(n)} + 3e_2^{(n)}$$

$$= \left(h^{(n)}\right)^2\{2e_1 + e_2\} + 2e_1^{(n)} + 3e_2^{(n)}.$$

Using Lemma 5.2.4, we get

$$= \left(h^{(n)}\{2e_1 + e_2\} + 2e_1^{(n)} + 3e_2^{(n)}\right)$$

$$= (2e_1^{(n)} + e_2^{(n)} + 2e_1^{(n)} + 3e_2^{(n)})$$

$$= 0.$$

Thus,

$$C_1 + C_1 \cap C_2 = (\theta_3^{(n)} + \theta_1^{(n)}\theta_2^{(n)})$$

$$= \left(2e_1^{(n)} + e_2^{(n)} + h^{(n)} + e_2^{(n)} + e_1^{(n)}\right)$$

$$= \left(h^{(n)} + 3e_1^{(n)} + 2e_2^{(n)}\right)$$

$$= (\theta_1^{(n)})$$

$$= C_1.$$

Similarly, we can prove, $C_2 = C_4 + C_1 \cap C_2$.

(v) We know that,

$$|C_3 + C_1 \cap C_2| = \frac{|C_3||C_1 \cap C_2|}{|C_1 \cap C_2 \cap C_3|}.$$

By part (iv), we get

$$|C_1| = \frac{|C_3||C_1 \cap C_2|}{|C_1 \cap C_2 \cap C_3|}.$$

As, $C_1 \cap C_2 \cap C_3 = \left(\theta_1^{(n)}\theta_2^{(n)}\theta_3^{(n)}\right) = (0)$.

Thus,

$$|C_1 \cap C_2 \cap C_3| = 1.$$

Hence,

$$|C_1| = |C_3||C_1 \cap C_2|$$

From part (iii), $|C_1 \cap C_2| = 4$ and $|C_1| = 4^{\frac{p+1}{2}}$.

Thus,

$$|C_3| = 4^{\frac{p-1}{2}}.$$

Similarly,

$$|C_4| = 4^{\frac{p-1}{2}}.$$

Theorem 5.3.5. If $p = 8k + 1$, k is even, let

$$C_1 = \left(h^{(n)} + e_1^{(n)}\right),$$

$$C_2 = \left(h^{(n)} + e_2^{(n)}\right),$$

$$C_3 = \left(3e_2^{(n)}\right),$$

$$C_4 = \left(3e_1^{(n)}\right),$$

then the following hold for Z_4 quadratic residue codes C_1, C_2, C_3 and C_4:

(i) C_1, C_2 and C_3, C_4 are equivalent.

(ii) $C_1 \cap C_2 = \left(h^{(n)} + e_1^{(n)} + e_2^{(n)}\right)$ and $C_1 + C_2 = (h^{(n)})$.

(iii) $|C_1| = |C_2| = 4^{\frac{p+1}{2}}$.

(iv) $C_1 = C_3 + C_1 \cap C_2, C_2 = C_4 + C_1 \cap C_2$.

(v) $|C_3| = |C_4| = 4^{\frac{p-1}{2}}$.

Proof. Similar to Theorem 5.3.4.

5.4. Example.

Example 5.4.1. To construct quadratic residue codes of length 49, let $p = 7$ and $n = 2$.

Then, by Notation 5.2.1, we get

$$R = \{1,2,4\},$$

$$S = \{3,5,6\},$$

$$e_1 = x^1 + x^2 + x^4,$$

$$e_2 = x^3 + x^5 + x^6.$$

Also,

$$Q = \{1,2,4,8,9,11,15,16,18,22,23,25,29,30,32,36,37,39,43,44,46\},$$

$$N = \{3,5,6,10,12,13,17,19,20,24,26,27,31,33,34,38,40,41,45,47,48\},$$

$$M = \{0,7,14,21,28,35,42\}.$$

Then,

$$e_1^{(2)} = x^1 + x^2 + x^4 + x^8 + x^9 + x^{11} + x^{15} + x^{16} + x^{18} + x^{22} + x^{23} + x^{25}$$
$$+x^{29} + x^{30} + x^{32} + x^{36} + x^{37} + x^{39} + x^{43} + x^{44} + x^{46},$$

$$e_2^{(2)} = x^3 + x^5 + x^6 + x^{10} + x^{12} + x^{13} + x^{17} + x^{19} + x^{20} + x^{24} + x^{26}$$
$$+x^{27} + x^{31} + x^{33} + x^{34} + x^{38} + x^{40} + x^{41} + x^{45} + x^{47} + x^{48},$$

$$h^{(2)} = 1 + x^7 + x^{14} + x^{21} + x^{28} + x^{35} + x^{42}.$$

By Theorem 5.2.13, we have

$$\theta_1^{(2)} = 3(x^1 + x^2 + 2x^3 + x^4 + 2x^5 + 2x^6 + x^8 + x^9 + 2x^{10} + x^{11}$$
$$+2x^{12} + 2x^{13} + x^{15} + x^{16} + 2x^{17} + x^{18} + 2x^{19} + 2x^{20} + x^{22} + x^{23}$$
$$+2x^{24} + x^{25} + 2x^{26} + 2x^{27} + x^{29} + x^{30} + 2x^{31} + x^{32} + 2x^{33} + 2x^{34}$$
$$+x^{36} + x^{37} + 2x^{38} + x^{39} + 2x^{40} + 2x^{41} + x^{43} + x^{44} + 2x^{45} + x^{46}$$

$$+2x^{47}+2x^{48}),$$

$$\theta_2^{(2)} = 3(2x^1+2x^2+x^3+2x^4+x^5+x^6+2x^8+2x^9+x^{10}+2x^{11}$$
$$+x^{12}+x^{13}+2x^{15}+2x^{16}+x^{17}+2x^{18}+x^{19}+x^{20}+2x^{22}+2x^{23}$$
$$+x^{24}+2x^{25}+x^{26}+x^{27}+2x^{29}+2x^{30}+x^{31}+2x^{32}+x^{33}+x^{34}$$
$$+2x^{36}+2x^{37}+x^{38}+2x^{39}+x^{40}+x^{41}+2x^{43}+2x^{44}+x^{45}+2x^{46}$$
$$+x^{47}+x^{48}),$$

$$\theta_3^{(2)} = 3(1+2x^1+2x^2+3x^3+2x^4+3x^5+3x^6+x^7+2x^8+2x^9$$
$$+3x^{10}+2x^{11}+3x^{12}+3x^{13}+x^{14}+2x^{15}+2x^{16}+3x^{17}+2x^{18}$$
$$+3x^{19}+3x^{20}+x^{21}+2x^{22}+2x^{23}+3x^{24}+2x^{25}+3x^{26}+3x^{27}$$
$$+x^{28}+2x^{29}+2x^{30}+3x^{31}+2x^{32}+3x^{33}+3x^{34}+x^{35}+2x^{36}$$
$$+2x^{37}+3x^{38}+2x^{39}+3x^{40}+3x^{41}+x^{42}+2x^{43}+2x^{44}+3x^{45}$$
$$+2x^{46}+3x^{47}+3x^{48}),$$

$$\theta_4^{(2)} = 3(1+3x^1+3x^2+2x^3+3x^4+2x^5+2x^6+x^7+3x^8+3x^9$$
$$+2x^{10}+3x^{11}+2x^{12}+2x^{13}+x^{14}+3x^{15}+3x^{16}+2x^{17}+3x^{18}$$
$$+2x^{19}+2x^{20}+x^{21}+3x^{22}+3x^{23}+2x^{24}+3x^{25}+2x^{26}+2x^{27}$$
$$+x^{28}+3x^{29}+3x^{30}+2x^{31}+3x^{32}+2x^{33}+2x^{34}+x^{35}+3x^{36}$$
$$+3x^{37}+2x^{38}+3x^{39}+2x^{40}+2x^{41}+x^{42}+3x^{43}+3x^{44}+2x^{45}$$
$$+3x^{46}+2x^{47}+2x^{48}).$$

Then quadratic residue codes are given below:

$$C_1 = \left(\theta_1^{(2)}\right),$$

$$C_2 = \left(\theta_2^{(2)}\right),$$

$$C_3 = \left(\theta_3^{(2)}\right),$$

$$C_4 = \left(\theta_4^{(2)}\right).$$

Then,

$$C_1 \cap C_2 = \left(\theta_1^{(2)}\theta_2^{(2)}\right) = (1 + x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + x^{26} + x^{27} + x^{28} + x^{29} + x^{30} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{36} + x^{37} + x^{38} + x^{39} + x^{40} + x^{41} + x^{42} + x^{43} + x^{44} + x^{45} + x^{46} + x^{47} + x^{48})$$

and

$$C_1 + C_2 = (1 + x^7 + x^{14} + x^{21} + x^{28} + x^{35} + x^{42})$$

$$= \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 | a_i \in Z_4, 0 \leq i \leq 6\}.$$

Here

$$|C_1 \cap C_2| = 4,$$

and

$$|C_1 + C_2| = 4^7.$$

Therefore, $|C_1| = |C_2| = 256$.

Similarly, we can solve $C_1 = C_3 + C_1 \cap C_2$ and $C_2 = C_4 + C_1 \cap C_2$.