Idempotent generators of cyclic and quadratic residue codes over $\mathbb{F}_3 + v\mathbb{F}_3$

Mohammed M. AL-Ashker
Mathematics Department
Islamic University of Gaza P.O.Box 108, Gaza, Palestine
E.mail:mashker@iugaza.edu.ps

Abstract: In this paper we study idempotent generators of cyclic codes and quadratic residue codes over $R = \mathbb{F}_3 + v\mathbb{F}_3$, where $v^2 = 1$ and $\mathbb{F}_3 = \{0, 1, 2\}$. The forms of some idempotents over this ring are given, the quadratic residue codes are defined in forms of the idempotent generators, and the relation between them and their extended codes is discussed as well as their duality. The specific forms of idempotent generators of quadratic residue codes of lengths 11 and 13 over the ring R are ascertained.

AMS: Subject Classification 2010: Primary 94B05, Secondary 11H71
Key words: Cyclic codes, Quadratic residue codes, Idempotent generators, dual codes.

1 Introduction

Let R be a finite commutative ring with identity. A subset $\mathcal{C}$ of $n-$tuples of elements of R is called an-R code (code over R) if it is an R-module. Recall that a code $\mathcal{C}$ over R is called cyclic if a cyclic shift of every element of $\mathcal{C}$ is an element of $\mathcal{C}$, or equivalently $\mathcal{C}$ is an ideal of $R_n = R[x]/\langle x^n - 1\rangle$. Hammons, Kumar, Calderbank, Sloane and Sole in a seminal paper [1], discuss the $\mathbb{Z}_4-$linearity of Kerdock, Perparta, Goethals and other codes. the structure of cyclic codes is considered by Pless and Qian [2] and Pless, Sole and Qian [3]. They found generator polynomials as well as idempotent generators for cyclic $\mathbb{Z}_4-$codes. They have also outlined the necessary and sufficient family of cyclic codes to be self-dual. An interesting family of cyclic codes is the family of quadratic residue codes. Quadratic residue codes were first defined and investigated by Andrew Gleason. Pless and Qian [3] defined quadratic residue codes over $\mathbb{Z}_4$ in terms of their idempotent generators. They showed that these codes have many good properties which are analogous in many respects to properties of quadratic residue codes over finite fields. The same results were obtained for quadratic residue codes over $\mathbb{Z}_8$ and over $\mathbb{Z}_9$; see [5] and [7]. Shixin Zhu, Tae Zhang [6] defined the quadratic residue codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$, $\mathbb{F}_2 = \{0, 1\}$, in terms of their idempotent generators.
In this paper, we consider the ring $R = \mathbb{F}_3 + v\mathbb{F}_3$, where $v^2 = 1$, $\mathbb{F}_3 = \{0, 1, 2\}$, and we define quadratic residue codes over $\mathbb{F}_3 + v\mathbb{F}_3$. We prove that the results of [6] remain valid over $\mathbb{F}_3 + v\mathbb{F}_3$. Our method suggests that if one has the idempotent generators of quadratic residue codes over $\mathbb{F}_3$, one can obtain idempotent generators over $\mathbb{F}_3 + v\mathbb{F}_3$, and define quadratic residue codes over $\mathbb{F}_3 + v\mathbb{F}_3$.

2 Preliminaries

The alphabet $R = F_3 + vF_3 = \{0, 1, 2, v, 2v, a = 1 + v, b = 2 + v, c = 1 + 2v, d = 2 + 2v\}$, where $v^2 = 1$, $F_3 = \{0, 1, 2\}$, is a commutative ring with nine elements. The elements $1, 2, v, 2v$ are units. Addition and multiplication over R are given in the following tables,

+	0	1	2	v	2v	a	b	c	d
0	0	1	2	v	2v	a	b	c	d
1	1	2	0	a	c	b	v	d	2v
2	2	0	1	b	d	v	a	2v	c
v	v	a	b	2v	0	c	d	1	2
2v	2v	c	d	0	v	1	2	a	b
a	a	b	v	c	1	d	2v	2	0
b	b	v	a	d	2	2v	c	0	1
c	c	d	2v	1	a	2	0	b	v
d	d	2v	c	2	b	0	1	v	a

·	0	1	2	v	2v	a	b	c	d
0	0	0	0	0	0	0	0	0	0
1	0	1	2	v	2v	a	b	c	d
2	0	2	1	2v	v	d	c	b	a
v	0	v	2v	1	2	a	c	b	d
2v	0	2v	v	2	1	d	b	c	a
a	0	a	d	a	d	d	0	0	a
b	0	b	c	c	b	0	b	c	0
c	0	c	b	b	c	0	c	b	0
d	0	d	a	d	a	a	0	0	d

This ring is a semi-local ring. It has two maximal ideals $(v-1) = (b)$ and $(1+v) = (a)$. It can be shown that $R/(v-1)$ and $R/(v+1)$ are isomorphic to F_3. From the Chinese Remainder Theorem,

$$R = (v-1) \oplus (v+1) = (b) \oplus (a),$$

where $(v-1) = \{0, v+2, 1+2v\}$ and $(1+v) = \{0, 1+v, 2+2v\}$.

In [8], it was shown that,

$$a + vb = (a-b)(v-1) - (a+b)(v+1)$$

for all $a, b \in \mathbb{F}_3$.

A linear code $\mathcal{C}$ of length n over R is an R-submodule of R^n. An element of $\mathcal{C}$ is called a codeword of $\mathcal{C}$. There are three different known weights over R. These are the Hamming, Lee and Bachoc weights.

The Hamming weight $wt_H(x)$ of a codeword $x = (x_1, x_2, \ldots, x_n) \in R^n$ is the number of nonzero components. The minimum weight $wt_H(\mathcal{C})$ of a code $\mathcal{C}$ is the smallest weight among all its nonzero codewords.

In [8], the Lee weight for the codeword $x = (x_1, x_2, \ldots, x_n) \in R^n$ is defined by $wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$, where

$$wt_L(x_i) = \begin{cases} 0 & \text{if} \quad x_i = 0 \\ 1 & \text{if} \quad x_i = 1, 2, v \quad \text{or} \quad 2v \\ 2 & \text{if} \quad x_i = 1+v, 2+v, 1+2v \quad \text{or} \quad 2+2v \end{cases}$$

The Bachoc weight for the codeword $x = (x_1, x_2, \ldots, x_n) \in R^n$ is defined by $wt_B(x) = \sum_{i=1}^{n} wt_B(x_i)$, where

$$wt_B(x_i) = \begin{cases} 0 & \text{if} \quad x_i = 0 \\ 1 & \text{if} \quad x_i = 1+v, 2+v, 1+2v \quad \text{or} \quad 2+2v \\ 3 & \text{if} \quad x_i = 1, 2, v \quad \text{or} \quad 2v \end{cases}$$

The minimum Lee weight $wt_L(\mathcal{C})$ and the minimum Bachoc weight $wt_B(\mathcal{C})$ of code $\mathcal{C}$ are defined analogously.

For $x = (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in R^n$, $d_H(x, y) = |\{i | x_i \neq y_i\}|$ is called the Hamming distance between x and $y \in R^n$ and is denoted by

$$d_H(x, y) = wt_H(x - y).$$

The minimum Hamming distance between distinct pairs of codewords of a code $\mathcal{C}$ is called the minimum distance of $\mathcal{C}$ and denoted by $d_H(\mathcal{C})$ or shortly d_H.

The Lee distance and Bachoc distance between x and $y \in R^n$ is defined by

$$d_L(x, y) = wt_L(x - y) = \sum_{i=1}^{n} wt_L(x_i - y_i),$$

$$d_B(x,y) = wt_B(x-y) = \sum_{i=1}^{n} wt_B(x_i - y_i),$$

respectively.

The minimum Lee and Bachoc distance between distinct pairs of codewords of a code $\mathcal{C}$ are called the minimum distance of $\mathcal{C}$ and denoted by $d_L(\mathcal{C})$ and $d_B(\mathcal{C})$ or shortly d_L and d_B, respectively.

If $\mathcal{C}$ is a linear code, $d_H(\mathcal{C}) = wt_H(\mathcal{C})$, $d_L(\mathcal{C}) = wt_L(\mathcal{C})$, $d_B(\mathcal{C}) = wt_B(\mathcal{C})$.

A generator matrix of $\mathcal{C}$ is a matrix whose rows generate $\mathcal{C}$.

Two codes are equivalent if one can be obtained from the other by permuting the coordinates.

The Gray map ϕ from R^n to $\mathbb{F}_3^{2n}$ is defined by

$$\phi : R^n \to \mathbb{F}_3^{2n}$$

$\mathbf{x} + \mathbf{v}\mathbf{y} \mapsto (\mathbf{x}, \mathbf{y})$ where $\mathbf{x}, \mathbf{y} \in \mathbb{F}_3^n$. The Lee weight of $x + vy$ is the Hamming weight of its Gray image. Note that ϕ is linear.

By the of Chinese Remainder Theorem, any code over R is permutation equivalent to a code generated by the following matrix

$$\begin{pmatrix} I_{k_1} & (1-v)B_1 & (v+1)A_1 & (1+v)A_2 + (1-v)B_2 & (1+v)A_3 + (1-v)B_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)B_4 \end{pmatrix},$$

where A_i and B_j are ternary matrices. Such a code is said to have rank $\{9^{k_1}, 3^{k_2}, 3^{k_3}\}$. If H is a code over R, let H^+ (resp. H^-) be the ternary code such that $(1+v)H^+$ (resp. $(1-v)H^-$) is read H mod $(1-v)$ (resp. H mod $(1+v)$).

In [8], it was proved that,

$$H = (1+v)H^+ \oplus (1-v)H^-$$

with

$$H^+ = \{s | \exists t \in F_3^n | (1+v)s + (1-v)t \in H\}$$
$$H^- = \{t | \exists s \in F_3^n | (1+v)s + (1-v)t \in H\}$$

The code H^+ is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix},$$

where A_i are ternary matrices for $i = 1, 2, 3, 4$ and the ternary code H^- is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix},$$

where B_i are ternary matrices for $i = 1, 2, 3, 4$.
The Euclidean inner product for $x = (x_1, x_2, \cdots, x_n),\ y = (y_1, y_2, \cdots, y_n) \in R^n$ is defined by

$$xy = \sum_{i=1}^{n} x_i y_i.$$

The dual of the code $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \{x \in R^n : xy = 0,\ \forall\ y \in \mathcal{C}\}.$$

If $\mathcal{C} = \mathcal{C}^\perp$, we say that the code $\mathcal{C}$ is self dual and if $\mathcal{C} \subseteq \mathcal{C}^\perp$ it is called self-orthogonal.
In [9], Y. Cengellenmis studied cyclic codes over the ring $\mathbb{F}_3 + v\mathbb{F}_3$ and found the generator polynomials for these codes. Not much works has been done on the structure of idempotent generators of cyclic codes over the ring $\mathbb{F}_3 + v\mathbb{F}_3$. In this paper, we investigate the structure of idempotent generators of cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$.

Theorem 2.1. *[9] Let H be a linear code of length n over R. Then $\Phi(H) = H^+ \bigotimes H^-$ and $|H| = |H^+||H^-|$.*

Lemma 2.2. *[9] If $\Phi(H) = H^+ \bigotimes H^-$, then $H = (1+v)H^+ \bigoplus (1-v)H^-$.*

Lemma 2.3. *[9] If $\Phi(H) = H^+ \bigotimes H^-$, then $H^\perp = (1+v)(H^+)^\perp \bigoplus (1-v)(H^-)^\perp$.*

Corollary 2.4. *[9] Every ideal of $R_n = R[x]/ < x^n - 1 >$ is principal.*

Corollary 2.5. *[9] $\mathcal{C} = (1+v)H^+ \bigoplus (1-v)H^-$ is a cyclic code of length n over R if and only if H^+, H^- are ternary cyclic codes.*

Corollary 2.6. *[9] If H is a cyclic code over R then the dual code $H^\perp$ of H is also cyclic.*

Theorem 2.7. *[9] H is a cyclic self dual code over R if and only if H^+, H^- are ternary cyclic self dual codes.*

Theorem 2.8. *[9] If $H = (1+v)H^+ \bigoplus (1-v)H^-$ is a cyclic code of length n over R, then $H = ((1+v)g_1(x), (1-v)g_2(x))$ and $|H| = 3^{2n} - deg\ (g_1(x)) - deg\ (g_2(x)$, where $g_1(x)$, $g_2(x)$ are the generator polynomials of H^+ and H^- respectively.*

Theorem 2.9. *[9] For any cyclic code H of length n over R there is a unique polynomial $g(x)$ such that $H =< g(x) >$ and $g(x)|x^n - 1$, where $g(x) = (g_1(x) + g_2(x)) + v(g_1(x) - g_2(x)))$. Moreover if $g_1(x) = g_2(x)$, then $g(x) = 2g_1(x)$.*

Theorem 2.10. *Let $x^n - 1 \in \mathbb{F}_3[x]$ be uniquely expressed as $x^n - 1 = \prod_{i=1}^{r} P_i^{s_i}(x)$ where $P_i(x)$ are pairwise relatively prime nonzero polynomials over $\mathbb{F}_3$. Then the number of cyclic codes of length n over R is $\prod_{i=1}^{r}(s_i+1)^2$.*

Proof. The result directly follows from the fact that the number of ternary cyclic codes of length n over R is $\prod_{i=1}^{r}(s_i+1)^2$. □

Theorem 2.11. *If n is odd, then every cyclic codes $\mathcal{C}$ of length n over R contains a unique idempotent $e(x) \in \mathcal{C}$, such that $\mathcal{C} =< e(x) >$.*

Proof. If n is odd, then there exist two unique idempotent polynomials $e_1, e_2 \in \mathbb{F}_3[x]/ < x^n - 1 >$ such that $\mathcal{C}_1 =< e_1(x) >$, $\mathcal{C}_2 =< e_2(x) >$ according to Theorems 2.9 and 2.10. We have $\mathcal{C} =< de_1 + be_2 >$, where $b = 2(1 - v) = 2 - 2v = 2 + v$, $d = 2(1 + v) = 2 + 2v$.
Let $e(x) =< de_1 + be_2 >$. Then $\mathcal{C} =< e(x) >$ and $(e(x))^2 = d^2e_1^2 + b^2e_2^2 = de_1 + be_2$.
If there is another $d(x) \in \mathcal{C}$ such that $\mathcal{C} =< d(x) >$ and $(d(x))^2 = d(x)$, since $d(x) \in \mathcal{C} =< e(x) >$, we have $d(x) = e(x)a(x)$ for some $a(x) \in R_n$, thus $d(x)e(x) = a(x)e^2(x) = a(x)e(x) = d(x)$. Similarly we can prove that $d(x)e(x) = e(x)$, namely $d(x) = e(x)$. □

Lemma 2.12. *If e_1, e_2 are idempotent generators in R, and if $\mathcal{C}_1$, $\mathcal{C}_2$ are cyclic codes of length n over R and $\mathcal{C}_1 =< e_1 >$, $e_2 =< e_2 >$, then (1) e_1e_2 and $e_1 + e_2 - e_1e_2$ are idempotent generators of $\mathcal{C}_1 \cap \mathcal{C}_2$ and $\mathcal{C}_1 \cup \mathcal{C}_2$ respectively.*
(2) the idempotent generators of the dual of $\mathcal{C}_i$, i.e., $\mathcal{C}_i^{\perp}$ are $1 - e_i(x^{-1})$, $i = 1, 2$.

Theorem 2.13. *Let n be odd. If $\mathcal{C} = \langle e(x) \rangle$ is a cyclic code of length n over R, where $e(x)$ is an idempotent polynomial. Then $\mathcal{C}^{\perp}$ has the idempotent polynomial $1 - e(x^{-1})$.*

Proof. Let $e_1(x)$, $e_2(x)$ be the idempotent polynomials of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Then $e(x) = de_1 + be_2 = 2(1 + v)e_1 + 2(1 - v)e_2 = 2(e_1 + e_2) + 2v(e_1 - e_2)$, and the idempotent polynomials of cyclic codes $\mathcal{C}_1^{\perp}$, $\mathcal{C}_2^{\perp}$ are $1-e_1(x^{-1})$ and $1-e_2(x^{-1})$. In the light of Theorem 2.11, $\mathcal{C}^{\perp} = 2(1 + v)\mathcal{C}_1^{\perp} + 2(1 - v)\mathcal{C}_2^{\perp}$ has idempotent generator $2(1 + v)(1-e_1(x^{-1}))+2(1-v)(1-e_2(x^{-1})) = 2(1+v)-2(1+v)e_1(x^{-1})+2(1-v)-2(1-v)e_2(x^{-1}) = 1-(2(1+v)e_1(x^{-1})+2(1-v)e_2(x^{-1}) = 1-(2(1+v)e_1(x^{-1}) + 2(1-v)e_2(x^{-1})) = 1-d(e_1(x^{-1}) + be_2(x^{-1})) = 1-e(x^{-1})$. So the idempotent generator of $\mathcal{C}^{\perp}$ is $1 - e(x^{-1})$. □

Example 2.1. *Example of cyclic codes over R. If $n = 2$, then $x^2-1 = (2+x)(1+x)$ in $\mathbb{F}_3[x]$. There are 15 non zero cyclic codes of length 2 over R. Table I gives the list of all such codes.*

code	generator matrices	order	generator polynomial	generator idempotent	d_L
1	$2 \quad 1$	9	2+x	2+x	2
2	$2(1+v) \quad (1+v)$	3	(1+v)(2+x)	(2+2v)(2+x)	4
3	$2(1-v) \quad (1-v)$	3	(1-v)(2+x)	(2+v)(2+x)	4
4	$1 \quad 1$	9	1+x	2+2x	2
5	$1+v \quad 1+v$	3	(1+v)(1+x)	(1+v)(1+x)	4
6	$1-v \quad 1-v$	3	(1-v)(1+x)	(1-v)(1+x)	4
7	$\begin{matrix}1 & 0\\ 0 & 1\end{matrix}$	81	1	1	1
8	$\begin{matrix}1+v & 0\\ 0 & 1+v\end{matrix}$	9	1+v	2+2v	2
9	$\begin{matrix}1-v & 0\\ 0 & 1-v\end{matrix}$	9	1-v	2+v	2
10	$v \quad 2$	9	2x+v	2+vx	2
11	$2v \quad 2$	9	2x+2v	2+2vx	2
12	$v \quad v+1$	9	v(1+x)+x	2v(x+1)+2x	3
13	$2 \quad 1+v$	9	vx+(2+x)	v(2+x)+x	3
14	$2v \quad 2v+1$	3	v(2v+2)+c	v(x+1)+2x	3
15	$2 \quad 2v+1$	9	v(2x)+x+2	2v(x+2)+x	3

3 Quadratic residue codes over $R = \mathbb{F}_3 + v\mathbb{F}_3$

Throughout the paper, we assume that p is prime. For considering quadratic residue codes over $\mathbb{F}_3$ we must assume that $p = 12r \pm 1$. First of all we find idempotents of $R_p = (\mathbb{F}_3 + v\mathbb{F}_3)/\langle x^p - 1\rangle$ from idempotent generators of $\mathbb{F}_3/\langle x^p - 1\rangle$.

Definition 3.1. Let p be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod p$ has a solution, then a is said to be a quadratic residue of p. Otherwise a is called a quadratic non-residue of p.

Let Q be the set of quadratic residues and N be the set of non-residues for p. let $e_1 = \sum_{i\in Q} x^i$ and $e_2 = \sum_{i\in N} x^i$. In [4] it was shown that 3 is quadratic residue (mod p) if and only if $p = 12r \pm 1$. Therefore for considering quadratic residue codes over $\mathbb{F}_3$ and hence over $\mathbb{F}_3 + v\mathbb{F}_3$ we must assume that $p = 12r \pm 1$. It is well known that $2e_i,\ 1 + e_i,\ i = 1, 2$, are idempotents over $\mathbb{F}_3/\langle x^p - 1\rangle$. An $\mathbb{F}_3$-cyclic codes is An $\mathbb{F}_3$-quadratic residue (QR) code if it is generated by one of the idempotents $2e_i,\ 1 + e_i,\ i = 1, 2$. If $p = 12r - 1$ put $Q_1 = \langle 2e_1\rangle,\ Q_2 = \langle 2e_2\rangle,\ Q_1' = \langle 1 + e_2\rangle,\ Q_2' = \langle 1 + e_1\rangle$. If $p = 12r + 1$ put $Q_1 = \langle 1+e_2\rangle,\ Q_2 = \langle 1+e_1\rangle,\ Q_1' = \langle 2e_1\rangle,\ Q_2' = \langle 2e_2\rangle$. In order to

define quadratic residue codes over $\mathbb{F}_3 + v\mathbb{F}_3$ in terms of idempotent generators, the following theorem is needed for such computations

Theorem 3.1. *[10]*

(i) Suppose that $p = 4k-1$, and a is a number relatively 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.

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

By a routine application of theorem 3.1, we obtain the following result.

Theorem 3.2. *[7] If $p = 4k-1$, then*

$$e_1^2 = (k-1)e_1 + ke_2,$$
$$e_2^2 = ke_1 + (k-1)e_2,$$
$$e_1e_2 = (2k-1) + (k-1)e_2 + (k-1)e_2.$$

If $k = 4k+1$, then

$$e_1^2 = (k-1)e_1 + ke_2 + 2k,$$
$$e_2^2 = ke_1 + (k-1)e_2 + 2k,$$
$$e_1e_2 = ke_1 + ke_2.$$

Theorem 3.3. *Let $p \equiv \pm 1(mod\ 12)$. If $2e_i,\ 1+e_i$ are idempotent generators of quadratic residue codes over $\mathbb{F}_3$, then $ce_i + ae_j$, $b(1+e_i)+d(1+e_j) = 1+be_i+de_j$ where $a = 1+v,\ b = 2+v,\ c = 1+2v,\ d = 2+2v,\ v^2 = 1$ are idempotent generators over $R[x]/\langle x^p - 1\rangle$, where $i,j = 1,2$.*

Proof. If $p \equiv \pm 1 (\text{mod } 12)$ and $2e_i, 1+e_i$ are idempotents over $\mathbb{F}_3/\langle x^p - 1\rangle$, then by Theorem 3.2 we have, $(ce_i+de_j)^2 = c^2e_i^2+2cae_ie_j+a^2e_j^2 = c^2e_i^2 + a^2e_j^2 = ce_i + ae_j$. Similarly $(b(1+e_i)+d(1+e_j))^2 = b(1+e_i) + d(1+e_j) = (b+d) + be_i + de_j = 1 + be_i + de_j$ and all other cases are idempotent over $R[x]/\langle x^p - 1\rangle$, where $i, j = 1, 2$. □

Let $h = 1 + e_1 + e_2$ be the all one vector. Let a be any nonzero element of $\mathbb{F}_3$. The map μ_a is defined as $\mu_a(i) = ai$ (mod p). It is easy to see that $\mu_a(fg) = \mu_a(f)\mu_a(g)$ for polynomials f and $g \in R[x]/\langle x^p - 1\rangle$. In the following theorem we investigate some properties of QR-codes over $R = \mathbb{F}_3 + v\mathbb{F}_3$.

Theorem 3.4. *Let p be a prime with $p = 12r - 1$, $Q_1 = \langle ce_1 + ae_2\rangle$, $Q_2 = \langle ce_2+ae_1\rangle$, $Q_1' = \langle 1+be_1+de_2\rangle$, $Q_2' = \langle 1+be_2+de_1\rangle$, then the following holds for Q_1, Q_2, Q_1' and Q_2' :*

(a) Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent;

(b) $Q_1 \cap Q_2 = \langle 2h\rangle$ and $Q_1 + Q_2 = R[x]/\langle x^p - 1\rangle$

(c) $Q_1 = Q_1' + \langle 2h\rangle$, $Q_2 = Q_2' + \langle 2h\rangle$;

(d) $|Q_1| = |Q_2| = 9^{\frac{p+1}{2}}$, $|Q_1'| = |Q_2'| = 9^{\frac{p-1}{2}}$;

(e) $Q_1^{\perp} = Q_2'$, $Q_2^{\perp} = Q_1'$;

(f) $Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = \langle 1 + h\rangle$.

Proof. (a) Since $p = 12r - 1 = 4(3r) - 1$, $-1 \in N$, for $a \in N$, then $\mu_a e_1 = e_2$ and $\mu_a e_2 = e_1$. Thus $\mu_a(ce_1 + ae_2) = ce_2 + ae_1$ and $\mu_a(ce_2 + ae_1) = ce_1 + ae_2$. So Q_1 and Q_2 are equivalent. The proof of the other case is similar.

(b) Since by lemma 2.12, $Q_1 \cap Q_2$ has an idempotent generator, $(ce_1 + ae_2)(ce_2 + ae_1) = c^2e_1e_2 + a^2e_1e_2 = (c^2 + a^2)(e_1e_2) = (b + d)(-1 - e_1 - e_2) = 2 + 2e_1 + 2e_2 = 2h$. So $Q_1 \cap Q_2 = \langle 2h\rangle$ and $Q_1 + Q_2$ has an idempotent generator, $ce_1 + ae_2 + ce_2 + ae_1 - 2h = c(e_1 + e_2) + a(e_1 + e_2) - 2h = (c + a)(e_1 + e_2) - 2h = 2e_1 + 2e_2 - 2 - 2e_1 - 2e_2 = 1$. So $Q_1 + Q_2 = R[x]/\langle x^p - 1\rangle$

(c) By lemma 2.12 $Q_1' \cap \langle 2h \rangle$ has an idempotent generator $(1+be_1+de_2)(2+2e_1+2e_2) = 0$. Thus $Q_1' \cap \langle 2h \rangle = \{0\}$, by Lemma 2.12 $Q_1' + \langle 2h \rangle$ has an idempotent generator $(1+be_1+de_2)+2h-(1+be_1+de_2)(2h) = ae_1+ce_2$, So $Q_1' + \langle 2h \rangle = Q_1$. Similarly $Q_2' + \langle 2h \rangle = Q_2$

(d) By parts (a) and (b) we have, $9^p = |Q_1+Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{9}$, so $|Q_1| = |Q_2| = 9^{\frac{p+1}{2}}$ and $9^{\frac{p+1}{2}} = |Q_1| = |Q_1' + \langle 2h \rangle| = |Q_1'||\langle 2h \rangle| = 9|Q_1'|$. Thus $|Q_1'| = 9^{\frac{p-1}{2}}$.

(e) By Theorem 2.13 and the fact that $-1 \in N$, $Q_1^{\perp}$ has an idempotent generator $1 - [(ce_1(x^{-1}) + ae_2(x^{-1})] = 1 + be_1(x^{-1}) + de_2(x^{-1}) = 1 + be_2 + de_1$. So $Q_1^{\perp} = Q_2'$. Similarly $Q_2^{\perp} = Q_1'$.

(f) Since $1+be_1+de_2+1+be_2+de_1 = 2+e_1+e_2 = 1+h$ and $(1+be_1+de_2)(1+be_2+de_1) = 0$. So by Lemma 2.12 we have $Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = \langle 1+h \rangle$.

□

Theorem 3.5. *Let p be a prime with $p = 12r+1$, $Q_1 = \langle 1+be_1+de_2 \rangle$, $Q_2 = \langle 1+be_2+de_1 \rangle$, $Q_1' = \langle ce_1+ae_2 \rangle$, $Q_2' = \langle ce_2+ae_1 \rangle$. Then the following hold for Q_1, Q_2, Q_1' and Q_2' :*

(a) Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent;

(b) $Q_1 \cap Q_2 = \langle h \rangle$ and $Q_1 + Q_2 = R[x]/\langle x^p - 1 \rangle$

(c) $Q_1 = Q_2' + \langle h \rangle$, $Q_2 = Q_1' + \langle h \rangle$;

(d) $|Q_1| = |Q_2| = 9^{\frac{p+1}{2}}$, $|Q_1'| = |Q_2'| = 9^{\frac{p-1}{2}}$;

(e) $Q_1^{\perp} = Q_1'$, $Q_2^{\perp} = Q_2'$;

(f) $Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = \langle 1-h \rangle$.

Proof. (a) Let a be an element of N. Then $\mu_a e_1 = e_2$ and $\mu_a e_2 = e_1$. Thus $\mu_a(1+be_1+de_2) = 1+be_2+de_1$ and $\mu_a(1+be_2+de_1) = 1+be_1+de_2$. So Q_1 and Q_2 are equivalent. Similarly for the other case.

(b) Since $(1+be_1+de_2)(1+be_2+de_1) = 1+(d+b)(e_1+e_2) = 1+e_1+e_2 = h$. It follows by Lemma 2.12 $Q_1 \cap Q_2$ has an idempotent generator h, hence $Q_1 \cap Q_2 = \langle h \rangle$. Also by Lemma 2.12 $(1+be_1+de_2)+(1+be_2+de_1)-(1+be_1+de_2)(1+be_2+de_1) = (1+be_1+de_2)+(1+be_2+de_1)-h = 2+(b+d)(e_1+e_2)-1-e_1-e_2 = 1$. Thus Q_1+Q_2 has an idempotent generator 1, so $Q_1+Q_2 = \mathbb{R}[x]/\langle x^p-1\rangle$.

(c) By Lemma 2.12 $Q_1' \cap \langle h \rangle$ has an idempotent generator $(ce_1+ae_2)(1+e_1+e_2) = ce_1+ce_1^2+ce_1e_2+ae_2+ae_2e_1+ae_2^2 = ce_1+c(-e_1)+c(0)+ae_2+a(0)+a(-e_2) = 0$. Thus $Q_1' \cap \langle h \rangle = \{0\}$. By lemma 2.12, $Q_1'+\langle h \rangle$ has an idempotent generator $ce_1+ae_2+h-(ce_1+ae_2)(h) = 1+e_1(c+1)+e_2(a+1) = 1+de_1+be_2$, so $Q_1'+\langle h \rangle = Q_2$. Similarly $Q_2'+\langle h \rangle = Q_1$.

(d) By parts (a) and (b) we have, $9^p = |Q_1+Q_2| = \frac{|Q_1||Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{9}$, so $|Q_1| = |Q_2| = 9^{\frac{p+1}{2}}$ and $9^{\frac{p+1}{2}} = |Q_1| = |Q_2'+\langle h \rangle| = |Q_2'||\langle h \rangle| = 9|Q_2'|$. Thus $|Q_2'| = 9^{\frac{p-1}{2}}$. Similarly $|Q_1'| = 9^{\frac{p-1}{2}}$.

(e) By Theorem 2.13 and the fact $-1 \in Q$, $Q_1^\perp$ has an idempotent generator $1-[1+be_1(x^{-1})+de_2(x^{-1})] = -be_1(x^{-1})+de_2(x^{-1}) = ce_1(x^{-1})+ae_2(x^{-1}) = ce_1+ae_2$ hence $Q_1^\perp = Q_1'$. Similarly $Q_2^\perp = Q_2'$.

(f) Since $(ce_1+ae_2)(ce_2+ae_1) = c^2e_1e_2cae_1^2+ace_2^2+a^2e_1e_2 = 2c(0)+0+0+2a(0) = 0$ and $ce_1+ae_2+ce_2+ae_1 = (a+c)(e_1+e_2)2e_1+2e_2 = 1-h$ So by Lemma 2.12, $Q_1' \cap Q_2' = \{0\}$ and $Q_1'+Q_2'$ has an idempotent generator $\langle 1-h \rangle$.

□

Definition 3.2. The extended code of $\mathcal{C}$ over R denoted by $\overline{\mathcal{C}}$, is the code obtained by adding an over all parity check to each codeword of $\mathcal{C}$

When $p \equiv -1 (\text{mod } 12)$, we define $\overline{Q_1}$ to be the $\mathbb{R}$-code generated

by the matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \cdots & p-1 \\ 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix},$$

where each row of G_1' is ia a cyclic shift of the vector $1+be_1+de_2$. We define $\overline{Q_2}$ similarly. Note that these are extended codes of Q_1, and Q_2, since the sum of components of all one vector is 0 (mod 3).

Theorem 3.6. *Let Q_1, Q_2, Q_1', Q_2' be the quadratic residue codes over $\mathbb{R}$ in theorems 3.4. Let $\overline{Q_1}$, $\overline{Q_2}$ denote their extended codes. When $p \equiv -1(mod\ 12)$, then the dual of $\overline{Q_1}$, is $\overline{Q_2}$ and the dual of $\overline{Q_1}$ is $\overline{Q_2}$.*

Proof. By Theorem 3.4 $Q_1 = Q_1' + \langle 2h \rangle$ and $\overline{Q_1}$ has the $\frac{p+1}{2} \times p+1$ generator matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \cdots & p-1 \\ 0 & & & & & \\ 0 & & & G_1' & & \\ \vdots & & & & & \\ 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix},$$

where each row of G_1' ia a cyclic shift of the vector $1 + be_1 + de_2$. We know that G_1' generates Q_1' and $Q_2^{\perp} = Q_1'$, by Theorem 3.4(e), any row in the above matrix is orthogonal to any row in the matrix which defines $\overline{Q_2}$ and the vector $(2, 2h)$ is orthogonal to itself. By comparing the order of the dual of $\overline{Q_1}$ and the order of $\overline{Q_2}$, we find $\overline{Q_1}^{\perp} = \overline{Q_2}$ and $\overline{Q_2}^{\perp} = \overline{Q_1}$ □

When $p \equiv 1(\text{mod } 12)$, we define $\widetilde{Q_1}$ to be the $\mathbb{R}$-code generated by the matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \cdots & p-1 \\ 0 & & & & & \\ 0 & & & G_2' & & \\ \vdots & & & & & \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

where each row of G_2' is a cyclic shift of the vector ce_2+ae_1. We define $\widetilde{Q_2}$ similarly. Note that these are not extended codes of Q_1 and Q_2, since the sum of components of all one vector is not 0 (mod 3).

Theorem 3.7. *Let Q_1, Q_2 Q_1', Q_2' be the quadratic residue codes over $\mathbb{R}$ in Theorem 3.5. When $p \equiv 1(mod\ 12)$, then the dual of $\overline{Q_1}$ is $\widetilde{Q_1}$ and the dual of $\overline{Q_2}$ is $\widetilde{Q_2}$.*

Proof. By Theorem 3.5, $Q_1 = Q_2' + \langle h \rangle$ and $\overline{Q_1}$ has the $\frac{p+1}{2} \times p+1$ generator matrix

$$\begin{pmatrix} \infty & 0 & 1 & 2 & \cdots & p-1 \\ 0 & & & & & \\ 0 & & & G_2' & & \\ \vdots & & & & & \\ 2 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

where each row of G_2' ia a cyclic shift of the vector ce_2+ae_1. We know that G_2' generates Q_2'. Since $Q_2^{\perp} = Q_2'$, it follows that by (Theorem 3.5(e)), any row of the above matrix is orthogonal to any row in the matrix which defines $\widetilde{Q_1}$. By comparing the order of $\overline{Q_1}$ and $\widetilde{Q_1}^{\perp}$, we find $\overline{Q_1}^{\perp} = \widetilde{Q_1}$. Similarly $\overline{Q_2}^{\perp} = \widetilde{Q_2}$. □

Definition 3.3. A vector $\mathbf{x} = \{x_1, x_2, \cdots, x_2\} \in \mathbb{F}_3^n$ is called even-like if $\sum_{i=1}^{n} x_i = 0$ and is called odd-like otherwise. We say that a code $\mathcal{C}$ over $\mathbb{F}_3$ is even-like if it has only even-like codewords, and it is odd-like if it is not even-like

By direct computation we have the following example:

Example 3.1. *The $\mathbb{R}-$ quadratic residue code of length $p = 11 \equiv -1(mod\ 12)$.*
We first find the generating idempotents of quadratic residue codes of length 11 over $\mathbb{F}_3$.
Here
$Q_{11} = \{1, 3, 4, 5, 9\}$ *and* $N_{11} = \{2, 6, 7, 8, 10\}$.
The generating idempotents of odd-like quadratic codes over $\mathbb{F}_3$ are
$2e_1 = 2\sum_{j \in Q_{11}} x^j = 2(x + x^3 + x^4 + x^5 + x^9)$

and $2e_2 = 2\sum_{j\in N_{11}} x^j = 2(x^2+x^6+x^7+x^8+x^{10})$
and the generating idempotents of even-like quadratic residue codes over $\mathbb{F}_3$ *are*
$1+e_1 = 1+\sum_{j\in Q_{11}} x^j = 1+(x+x^3+x^4+x^5+x^9)$
and $1+e_2 = 1+\sum_{j\in N_{11}} x^j = 1+(x^2+x^6+x^7+x^8+x^{10})$
Then the generating idempotent of even-like quadratic residue codes over $\mathbb{R}$ *are*
$1+b((x+x^3+x^4+x^5+x^9))+d((x^2+x^6+x^7+x^8+x^{10}))$
and $1+b((x^2+x^6+x^7+x^8+x^{10}))+d((x+x^3+x^4+x^5+x^9))$
and the generating idempotents of odd-like quadratic residue codes over $\mathbb{R}$ *are*
$c((x+x^3+x^4+x^5+x^9))+a((x^2+x^6+x^7+x^8+x^{10}))$
and $c(x^2+x^6+x^7+x^8+x^{10})+a(x+x^3+x^4+x^5+x^9)$
as an example, since $c = 1+2v,\ a = 1+v$, *then the idempotent generator of odd-like (QR) codes over* $\mathbb{R}$ *is* $ce_1+ae_2 = c((x+x^3+x^4+x^5+x^9)+a((x^2+x^6+x^7+x^8+x^{10})) = cx+ax^2+cx^3+cx^4+cx^5+ax^6+ax^7+ax^8+cx^9+ax^{10}$.

Example 3.2. *Consider the case of the prime* $p = 13 \equiv 1(mod\ 12)$.
We first find the generating idempotents of quadratic residue codes of length 13 *over* $\mathbb{F}_3$.
Here
$Q_{13} = \{1,3,4,9,10,12\}$ *and* $N_{13} = \{2,5,6,7,8,11\}$.
The generating idempotents of odd-like quadratic codes over $\mathbb{F}_3$ *are*
$1+e_1 = 1+\sum_{j\in Q_{13}} x^j = 1+(x+x^3+x^4+x^9+x^{10}+x^{12})$
and $1+e_2 = 1+\sum_{j\in N_{13}} x^j = 1+(x^2+x^5+x^6+x^7+x^8+x^{11})$
and the generating idempotents of even-like quadratic residue codes over $\mathbb{F}_3$ *are*
$2e_1 = 2\sum_{j\in Q_{13}} x^j = 2(x+x^3+x^4+x^9+x^{10}+x^{12})$
and $2e_2 = 2\sum_{j\in N_{13}} x^j = 2(x^2+x^5+x^6+x^7+x^8+x^{11})$
Then the generating idempotents of odd-like quadratic residue codes

over $\mathbb{R}$ *are*
$1 + be_1 + de_2 = 1 + b(x + x^3 + x^4 + x^9 + x^{10} + x^{12}) + d(x^2 + x^5 + x^6 + x^7 + x^8 + x^{11})$
and $1 + be_2 + de_1 = 1 + b(x^2 + x^5 + x^6 + x^7 + x^8 + x^{11}) + d(x + x^3 + x^4 + x^9 + x^{10} + x^{12})$
and the generating idempotents of even-like quadratic residue codes over $\mathbb{R}$ *are*
$c2e_1 + a2e_2 = c((x + x^3 + x^4 + x^9 + x^{10} + x^{12})) + a((x^2 + x^5 + x^6 + x^7 + x^8 + x^{11}))$
and $c2e_2 + a2e_1 = c((x^2 + x^5 + x^6 + x^7 + x^8 + x^{11})) + a((x + x^3 + x^4 + x^9 + x^{10} + x^{12}))$

References

[1] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The Z_4-linearty of Kerdock, Preparata, Goethals, and related codes, IEEE Trans Inform. Theory, vol.40,no.2,pp.301-319.1994.

[2] V.Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. Inform. theory 42 (1996), no. 5, 1594-1600.

[3] V. Pless, P. Sole and Z. Qian, Cyclic self-dual Z_4 codes. Finite fields and their applications 3 . 48-69 , 1997.

[4] V. Pless and W. Gary Huffman, Fundamentals of error corecting codes, Cambridge (2003). codes. Finite fields and their applications 3 . 48-69 , 1997.

[5] M. H. chin, s. s. T. You and Y. Yu, $\mathbb{Z}_8$-cyclic codes and quadratic residue codes, Adv. in appl. math. 25(2000), no. 1, 12-33.

[6] Shixin Zhu, Tao Zhang, Quadratic residue codes over $\mathbb{Z}_2 + v\mathbb{Z}_2$, Journal of Hefei University of Technology 34(8) 1268-1271 (2011).

[7] Bijan Teari, Quadratic residue codes over $\mathbb{Z}_9$, J. Korean Math. Soc. 64(2009), no. 1, 13-30.

[8] R. Chapman, S. T. Dougherty, P. Gaborit, P. Sole, 2− modular Lattices from ternary codes, Journal de theoric des nombers de bordeanx, 14, 73-85 (2002).

[9] Yasemin Cengellenmis, On the cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$, international Journal of algebra, vol. 4,2010, no. 6, 253-259.

[10] O. Perron, Bemerkungen uber die verteilung der quadratischen reste, Math. Z. 56 (1952), 122-130.