J. Appl. Math. & Informatics Vol. **36***(2018), No. 5 - 6, pp. 359 - 368*
https://doi.org/10.14317/jami.2018.359

ONE GENERATOR QUASI-CYCLIC CODES OVER $\mathbb{F}_2 + v\mathbb{F}_2$

MEHMET ÖZEN, N. TUĞBA ÖZZAİM*, NUH AYDIN

Abstract. In this paper, we investigate quasi-cyclic codes over the ring $R = \mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$. We investigate the structure of generators for one-generator quasi-cyclic codes over R and their minimal spanning sets. Moreover, we find the rank and a lower bound on minimum distances of free quasi-cyclic codes over R. Further, we find a relationship between cyclic codes over a different ring and quasi-cyclic codes of index 2 over R.

AMS Mathematics Subject Classification : 94B05, 94B15.
Key words and phrases : Gray map, quasi-cyclic codes.

1. Introduction

Codes are studied by various scientific disciplines such as information theory, electrical engineering, mathematics, and computer science. Quasi-cyclic codes are generalization of cyclic codes. These codes give a very good performance on the codes of great lengths. Hence quasi-cyclic codes are one of the most important and most intensively studied classes of linear codes. Many researchers exploit the structure of quasi-cyclic (QC) codes to construct such codes over fields (some examples among many such works are[14]-[2]).

In the last few decades, codes over finite rings received considerable attention. Among the finite rings of interest, $\mathbb{Z}_4$ and other rings of order 4 have a special place. The important class of QC codes have been studied over the rings of order 4 as well. For example, in [2] and [12], optimal codes and new binary linear codes are found from the Gray images of QC codes over $\mathbb{Z}_4$ and over $\mathbb{F}_2 + u\mathbb{F}_2$, respectively. In [6], one generator QC codes of length mn over $\mathbb{Z}_4$ are studied with the conditions that n is odd and $\gcd(|2|_n, m) = 1$. We refer the reader to the papers [10], [11], [5] for more on the algebraic structure of QC codes. There are 4 commutative rings of order 4: $GF(4)$, $\mathbb{Z}_4$, $\mathbb{F}_2 + u\mathbb{F}_2$ where $u^2 = 0$, and $\mathbb{F}_2 + v\mathbb{F}_2$ where $v^2 = v$. We will focus on the ring $\mathbb{F}_2 + v\mathbb{F}_2$ in this paper.

Received June 20, 2017. Revised April 23, 2018. Accepted April 27, 2018. *Corresponding author.

This work has been organised in the following way. In section II, we investigate the structure of the ring $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$. Some basic definitions and theorems which are preliminary for the next sections are given. In section III, we study one generator quasi-cyclic codes over R and determine their minimal spanning sets. We find the rank and lower bounds on minimum distances of free QC codes over R. In the last section we give a relationship between cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ where $u^2 = u$, $v^2 = v$ and $uv = vu$ and 2-QC codes over $\mathbb{F}_2 + v\mathbb{F}_2$.

2. Preliminaries

Let R denote the ring $\mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1+v\}$ where $v^2 = v$. It is clear that we can consider the ring R as the quotient ring $\mathbb{F}_2[v]/\langle v^2 + v\rangle$. Let C be a non-empty subset of R^n. If C is an R-submodule of R^n, then C is called a linear code of length n over R. A linear code C of length n is called cyclic if $(r_{n-1}, r_0, \ldots, r_{n-2}) \in C$ whenever $(r_0, r_1, ..., r_{n-1}) \in C$. Let R_n denote the quotient ring $R[x]/\langle x^n - 1\rangle$. Then we consider the following correspondence:

$$\delta : R^n \longrightarrow R_n$$
$$r = (r_0, r_1, ..., r_{n-1}) \longrightarrow r(x) = r_0 + r_1 x + ... + r_{n-1}x^{n-1}$$

It is well known that C is a cyclic code if and only if $\delta(C)$ is an ideal of R_n. Let $r = (r_0, r_1, ..., r_{n-1})$ be a codeword in C. The Hamming weight of $r = (r_0, r_1, ..., r_{n-1})$ is the number of nonzero coordinates in r and is denoted by $w_H(r)$. The Lee weights of $0, 1, v, 1+v \in R$ are $0, 2, 1, 1$ respectively and Lee weight of a codeword
$r = (r_0, r_1, ..., r_{n-1})$, which is the sum of the Lee weights of its components, is denoted by $w_L(c)$.

Any element of R can be written as $z = x + vy$,where $x, y \in \mathbb{F}_2$. The Gray map from R to $\mathbb{F}_2^2$ is defined as follows:

$$\varphi : R \longrightarrow \mathbb{F}_2^2$$
$$x + vy \longrightarrow (x, x+y)$$

This map is naturally extended from R^n to $\mathbb{F}_2^{2n}$. It can be easily seen that the Gray map is an isometry from ($\mathbb{F}_2 + v\mathbb{F}_2^n$, Lee distance) to ($\mathbb{F}_2^{2n}$, Hamming distance). We need the following definition and theorems before studying QC codes over $\mathbb{F}_2 + v\mathbb{F}_2$.

Theorem 2.1 ([15]). *Let C be a linear code over $\mathbb{F}_2 + v\mathbb{F}_2$ with length n. Define $C_1 = \{a \in \mathbb{F}_2^n | a + vb \in C$, for some $b \in \mathbb{F}_2^n\}$ and $C_2 = \{a + b \in \mathbb{F}_2^n | a + vb \in C\}$. Then C can be expressed as $C = (1+v)\ C_1 + vC_2$. Obviously, C_1 and C_2 are binary linear codes.*

Theorem 2.2 ([15]). *Let $C = (1 + v)\ C_1 + vC_2$ be a linear code over $\mathbb{F}_2 + v\mathbb{F}_2$. Then C is a cyclic code over $\mathbb{F}_2 + v\mathbb{F}_2$ if and only if C_1 and C_2 are binary cyclic codes.*

Theorem 2.3 ([15]). *Let $C = (1+v)\ C_1+vC_2$ be a cyclic code of length n over R and $g_1(x), g_2(x)$ be generator polynomials of C_1 and C_2 respectively. Then, there exists a unique polynomial $g(x)$ such that $C = \langle g(x)\rangle = \langle (1 + v)g_1(x) + vg_2(x)\rangle$ and $g(x)|x^n - 1$. Moreover, if $g_1(x) = g_2(x)$, then $g(x) = g_1(x)$.*

Following lemma states a well-known result about cyclic codes for the ring R. The usual proof works for the ring R as well. We call two polynomials $p_1(x), p_2(x) \in R[x]$ co-prime if there exist polynomials $r_1(x), r_2(x) \in R[x]$ such that $p_1(x)r_1(x) + p_2(x)r_2(x) = 1$.

Lemma 2.4. *Let C be a cyclic code with generator $g(x)$ such that $x^n - 1 = g(x)h(x)$. Then any generator of C is of the form $\langle f(x)g(x)\rangle$ where $f(x)$ and $h(x)$ are co-prime.*

3. Structure of QC Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

Motivations for studying cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ as opposed to the other rings of order 4 (that is, $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$) include the following facts [15]:

- For a given n, the number of cyclic codes of length n over $\mathbb{F}_2 + v\mathbb{F}_2$ is much greater than the number of cyclic codes of length n over $\mathbb{Z}_4$ or $\mathbb{F}_2 + u\mathbb{F}_2$.
- Most of the binary codes which are Gray images of cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ cannot be obtained from Gray images of linear codes over $\mathbb{Z}_4$ or $\mathbb{F}_2 + u\mathbb{F}_2$.

These facts also motivate the investigation of QC codes over R. We can see, for example, that the number of QC codes of a given length and index over R will be greater than the number of QC codes of the same length and index over $\mathbb{Z}_4$ or $\mathbb{F}_2 + u\mathbb{F}_2$. One disadvantage of cyclic codes over R is their minimum distances tend to be smaller compared to cyclic codes over $\mathbb{Z}_4$ or $\mathbb{F}_2 + u\mathbb{F}_2$ [15].

Definition 3.1. If for every codeword $c \in C$ there exists a number ℓ such that the codeword obtained by ℓ cyclic shifts is also a codeword in C, then C is called an ℓ-quasi-cyclic (QC) code. The number ℓ is defined as the smallest number of cyclic shifts under which the code is invariant and is called the index of C.

Let $R_s = R[x]/\langle x^s - 1\rangle$ be. Then the map

$$\Psi : R^{s\ell} \longrightarrow R_s^{\ell}$$
$$(u_{11}, u_{12}, ..., u_{1\ell}; ...; u_{s1}, u_{s2}, ..., u_{s\ell}) \longrightarrow (u_1(x), u_2(x), ..., u_\ell(x)) = u(x)$$

where $u_i(x) = \sum_{j=1}^{s} u_{ji}x^{j-1}$ for $i = 1, .., \ell$ defines a one-to-one correspondence. It can be seen that an $\ell-$QC code C of length $n = \ell s$ over R is an R_s-submodule of R_s^ℓ. If C is generated by a single element $u(x)$ then C is defined as a one generator quasi-cyclic code. We also write $C = \langle u_1(x), u_2(x), ..., u_\ell(x)\rangle$ to mean

$$C = \{(g(x)u_1(x), g(x)u_2(x), \dots, g(x)u_\ell(x))\,|g(x) \in R_m\}$$

Theorem 3.2. *Let C be a one generator quasi-cyclic code of length $n = s\ell$ over $\mathbb{F}_2 + v\mathbb{F}_2$ generated by $G(x) = (G_1(x), G_2(x), ..., G_\ell(x))$ where $G_i(x) \in R_s$ for $1 \leq i \leq \ell$. Then $G_i(x) \in C_i$ where C_i is a cyclic code of length s in R_s, and there exist polynomials $f_i(x) \in R[x]$ and $r_i(x), s_i(x) \in \mathbb{F}_2[x]$ such that $G_i(x) = f_i(x)[(1 + v)r_i(x) + vs_i(x)]$.*

Proof. For each $i = 1, ..., \ell$ define the map

$$\begin{gathered}\Psi_i : R_s^\ell \longrightarrow R_s \\ (G_1(x), G_2(x), ..., G_\ell(x)) \longrightarrow G_i(x)\end{gathered}$$

Assume that $C = (G_1(x), G_2(x), \dots, G_\ell(x))$ is one generator QC code over R with length $n = s\ell$. Then $\Psi_i(C)$ is a cyclic code over R_s. By Theorem 2.3 and Lemma 2.4, a generator G_i of $\Psi_i(C)$ is of the form $G_i(x) = f_i(x)[(1 + v)r_i(x) + vs_i(x)]$. □

Theorem 3.3. *Let C be one generator quasi-cyclic code of length $n = s\ell$ over $\mathbb{F}_2 + v\mathbb{F}_2$ generated by $G(x) = (f_1r_1 + vp_1, f_2r_2 + vp_2, \dots, f_\ell r_\ell + vp_\ell)$ and there exists an index i such that $f_ir_i + vp_i$ is not a zero divisor in R_s. Suppose that*

$g = gcd(f_1r_1, f_2r_2, ..., f_\ell r_\ell, x^s - 1)$ *;* $hg = x^s - 1$ *and* $\deg h = k$

$p = gcd(hp_1, hp_2, ..., hp_\ell, x^s - 1)$ *;* $pq = x^s - 1$ *and* $\deg q = t$

and let $F(x) = \{vhp_1, vhp_2, ..., vhp_\ell\}$. Then C has the minimal generating set $S_1 \cup S_2$, where

$S_1 = \{G(x), xG(x), ..., x^{k-1}G(x)\}$ *and* $S_2 = \{F(x), xF(x), \dots, x^{t-1}F(x)\}$.

Proof. Let $k(x) = f(x)G$ be a codeword of C. By the Euclidean algorithm, there are two polynomials $Q_1(x), R_1(x) \in R[x]$ such that

$$f(x) = hQ_1(x) + R_1(x) \quad \text{ and } \quad 0 \leq \deg R_1(x) < k.$$

Hence,

$$\begin{aligned} k(x) &= (hQ_1(x) + R_1(x)\ )G \\ &= Q_1(x)(hf_1r_1 + vhp_1, hf_2r_2 + vhp_2, ..., hf_\ell r_\ell + vhp_\ell) \\ &+ R_1(x)\ (f_1r_1 + vp_1, f_2r_2 + vp_2, ..., f_\ell r_\ell + vp_\ell). \end{aligned}$$

Since there exist polynomials $g_i(x) \in \mathbb{F}_2[x]$ such that $f_ir_i = gg_i$ for all $i = 1, 2, ..., \ell$, we obtain $hf_ir_i = 0$. Hence, we have

$$k(x) = Q_1(x)(vhp_1, vhp_2, ..., vhp_\ell) + R_1(x)\ (f_1r_1 + vp_1, f_2r_2 + vp_2, \cdots, f_\ell r_\ell + vp_\ell).$$

Note that $R_1(x)(f_1r_1+vp_1, f_2r_2+vp_2, ..., f_\ell r_\ell+vp_\ell) \in Span(S_1)$. Again by the Euclidean algorithm, we get polynomials $Q_2(x), R_2(x) \in R[x]$ such that

$$Q_1(x) = qQ_2(x) + R_2(x) \quad \text{and} \qquad 0 \leq \deg R_2(x) < t$$
$$Q_1(x)(vhp_1, ..., vhp_\ell) = Q_2(vqhp_1, ..., vqhp_\ell) + R_2(x)(vhp_1, ..., vhp_\ell).$$

Since there exist polynomials $q_i(x) \in \mathbb{F}_2[x]$ such that $hp_i = pq_i$ for all $i = 1, 2, ...\ell$, we get $qhp_i = 0$. We have

$$Q_1(x)(vhp_1, vhp_2, ..., vhp_\ell) = R_2(vhp_1, vhp_2, ..., vhp_\ell) \in Span(S_2)$$

which implies that $k(x) \in Span(S_1) \cup Span(S_2)$, i.e $S_1 \cup S_2$ generates C.

Next we will show $Span(S_1) \cap Span(S_2) = \{0\}$. Suppose that $e(x) = (e_1(x), e_2(x), ..., e_\ell(x)) \in Span(S_1) \cap Span(S_2)$. Since $e(x) \in Span(S_1)$, it follows that

$$e_i(x) = (f_ir_i + vp_i)(\alpha_0 + \alpha_1 x + ... + \alpha_{k-1}x^{k-1}).$$

We can assume that $\deg(x^{k-1}f_ir_i) < s$ since computations are in R_s. On the other hand, since $e(x) \in Span(S_2)$, we have

$$e_i(x) = (vhp_i)(\beta_0 + \beta_1 x + ... + \beta_{t-1}x^{t-1}).$$

From last equality, we have $(1+v)e_i(x) = 0$ for all $i = 1, 2, ..., \ell$, which implies that

$$(1+v)e_i(x) = (1+v)(\alpha_0 + \alpha_1 x + ... + \alpha_{k-1}x^{k-1})f_ir_i = 0.$$

Since $\deg(x^{k-1}f_ir_i) < s$, this means $\alpha_i = 0$ or $\alpha_i = v$. Let $M_1(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{k-1}x^{k-1}$ and $M_2(x) = \beta_0 + \beta_1 x + \cdots + \beta_{t-1}x^{t-1}$. Then $(f_ir_i + vp_i)M_1 = vhp_iM_2$. Considering the facts $hf_ir_i = hgg_i = 0$, we get $(f_ir_i+vp_i)(M_1+hM_2) = (f_ir_i + vp_i)M_1 + hf_ir_iM_2 + vhp_iM_2 = 2vhp_iM_2 = 0$. Since $f_ir_i + vp_i$ is not a zero divisor, we have $M_1 + hM_2 = 0$ which means $\alpha_i = 0$ and $\beta_j = 0$ for all $i = 1, 2, ..., k-1$ and $j = 1, 2, ..., t-1$. Consequently, $Span(S_1) \cap Span(S_2) = \{0\}$. □

Corollary 3.4. *Let C be a quasi-cyclic code of the form given in Theorem 3.3. If for each $i = 1, 2, .., \ell$ the polynomial $f_ir_i + vp_i$ is a factor of $x^s - 1$, then C is a free ℓ-QC code with rank $= k$ and $|C| = 4^k$.*

Proof. Since $f_ir_i + vp_i | x^s - 1$ over R, it follows that $f_ir_i | x^s - 1$ over $\mathbb{F}_2$. Let $h_i = \frac{x^s-1}{f_ir_i}$ and $h = lcm(h_1, h_2, ..., h_\ell)$ over $\mathbb{F}_2$. Then there exists a polynomial $s_i \in \mathbb{F}_2[x]$ such that $\frac{x^s-1}{f_ir_i+vp_i} = h_i + vs_i$. So there is a polynomial $c \in \mathbb{F}_2[x]$ such that $(h + vc) = lcm(h_1 + vs_1, h_2 + vs_2, ..., h_\ell + vs_\ell)$. Thus, $(f_ir_i + vp_i)(h + vc) = 0$ in R_s which implies that $hf_ir_i + vhp_i + vcp_i + vcf_ir_i = 0$. Since $gh = x^s - 1$, $hf_ir_i = 0$. Therefore, $v(h_ip_i + cp_i + cf_ir_i) = 0$ or $cp_i + cf_ir_i = hp_i$. So $(vhp_1, vhp_2, ..., vhp_\ell) = vc(f_1r_1 + vp_1, f_2r_2 + vp_2, ..., f_\ell r_\ell + vp_\ell)$ i.e., $S_2 \in$

$Span(S_1)$. Therefore C is free with rank k and the number of codewords of C is 4^k. □

Theorem 3.5. *Let C be an ℓ-quasi-cyclic code of length n over $\mathbb{F}_2 + v\mathbb{F}_2$. Then its Gray image $\varphi(C)$ is a 2ℓ-quasi-cyclic code of length $2n$ over $\mathbb{F}_2$, i.e $\tau^{2\ell}(\varphi(C)) = \varphi(C)$, where τ is the cyclic shift operator on R^n.*

Proof. Let $r = (r_1, r_2, ..., r_n) \in C$ where $r_i = p_i + vq_i$, $p_i, q_i \in R$ for all $i = 1, 2, ..., n$. Then $\tau^{\ell}(r) = \tau^{\ell}(r_1, r_2, ..., r_n) = (r_{n-(\ell-1)}, r_{n-(\ell-2)}, ..., r_{n-\ell})$ and

$$\varphi(\tau^{\ell}(r)) = (p_{n-(\ell-1)}, p_{n-(\ell-1)} + q_{n-(\ell-1)}, ..., p_{n-\ell}, p_{n-\ell} + q_{n-\ell}) \quad (1)$$

On the other hand, $\varphi(r) = (p_1,p_1 + q_1, ..., p_n, p_n + q_n)$ and

$$\tau^{2\ell}(\varphi(r)) = (p_{n-(\ell-1)}, p_{n-(\ell-1)} + q_{n-(\ell-1)}, ..., p_{n-\ell}, p_{n-\ell} + q_{n-\ell}) \quad (2)$$

Comparing equations 1 and 2 we obtain $\tau^{2\ell}(\varphi(c)) = \varphi(\tau^{\ell}(c)) = \varphi(c)$. The result follows from this equation. □

If we take $\ell = 1$ in Theorem 3.5 , then we get the following corollary.

Corollary 3.6 ([15]). *Let C be a cyclic code of length n over $\mathbb{F}_2 + v\mathbb{F}_2$. Then its Gray image $\varphi(C)$ is a 2-QC code of length $2n$ over $\mathbb{F}_2$.*

Theorem 3.7. *Let C be an ℓ-quasi-cyclic code of length $n = s\ell$ over $\mathbb{F}_2 + v\mathbb{F}_2$ generated by $G(x) = (g(x)f_1(x), g(x)f_2(x), ..., g(x)f_l(x))$ where $g(x)|x^m - 1$. Let $\deg g(x) = k$, $h(x) = x^s - 1/g(x)$ and $\gcd(f_i(x), h(x)) = 1$ for all $i = 1, 2, ..., l$. Then C is a free $R-$module with basis $\gamma = \{G(x), xG(x), ..., x^{s-k-1}G(x)\}$ Also, $d_L(C) \geq \ell \cdot d_L(\widetilde{C})$ where $d_L(\widetilde{C})$ is the minimum Lee weight of the cyclic code $\widetilde{C} = \langle g(x) \rangle$.*

Proof. Since $\gcd(f_i(x), h(x)) = 1$, there exist polynomials $\alpha_i(x), \beta_i(x) \in R[x]$ such that

$f_i(x)\alpha_i(x) + h(x)\beta_i(x) = 1$

$g(x)f_i(x)\alpha_i(x) + g(x)h(x)\beta_i(x) = g(x)$

$g(x)f_i(x)\alpha_i(x) = g(x)$

which means that $\Psi_i(C) = \widetilde{C}$. Since the cyclic code $\langle g(x)f_i(x) \rangle$ is the same as the free code $\langle g(x) \rangle$ with basis $\{g(x), xg(x), ..., x^{s-k-1}g(x)\}$, the set γ spans C. Now let's show γ is linearly independent. Suppose

$$c_0G(x) + c_1xG(x) + ... + c_{m-k-1}x^{m-k-1}G(x) = (0, 0, ..., 0).$$

This implies that for all $i = 1, 2, ..., \ell$, we get

$$g(x)f_i(x)(c_0 + c_1x + ... + c_{m-k-1}x^{m-k-1}) = 0.$$

Let $c(x) = c_0 + c_1x + ... + c_{m-k-1}x^{m-k-1}$. Then $g(x)f_i(x)c(x) = 0$.

Since $g(x)h(x) = x^s - 1$, we have $h(x)|f_i(x)c(x)$. Since $\gcd(f_i(x), h(x)) = 1$, we get $h(x)|c(x)$. But $\deg h(x) = s - k$ while $\deg c(x) = s - k - 1$, which is a contradiction. Hence γ is linearly independent, so it is a basis.

To prove the assertion on the minimum distance, let $k(x) = a(x) \cdot G(x) = (a(x)g(x)f_1(x), ..., a(x)g(x)f_\ell(x))$ be a codeword of C. Then

$$\begin{aligned} a(x)g(x)f_i(x) = 0 &\iff x^s - 1|a(x)g(x)f_i(x) \\ &\iff g(x)h(x)|a(x)g(x)f_i(x) \\ &\iff h(x)|a(x)f_i(x) \end{aligned}$$

Since $\gcd(f_i(x), h(x)) = 1$,we must have $h(x)|a(x)$. This means that $k(x) = 0$ if and only if $a(x)g(x)f_i(x) = 0$, and $h(x) \nmid a(x)$ if and only if $k(x) \neq 0$. Therefore for any nonzero codeword $k(x)$, $\Psi_i(k(x)) \neq 0$, which implies that $d_L(C) \geq \ell \cdot d_L(\widetilde{C})$. □

3.1. Examples.

Example 3.8. The cyclic code of length $s = 7$ over R with generator polynomial $g = x^4+vx^3+x^2+(v+1)x+1$ (and $g_1 = x^4+x^2+x+1$, $g_2 = x^4+x^3+x^2+1$) has size 64 and minimum Lee distance 4. Hence, its Gray image is a $[14, 6, 4]$ binary linear code. By Theorem 3.7 a 2-QC code with a generator of the form $\langle g, g \cdot f\rangle$ (with f satisfying the condition stated in the theorem) has parameters $[14, 3, \geq 8]$ over R, and binary parameters $[28, 6, \geq 8]$. We verified that for all such codes the binary parameters are always $[28, 6, 8]$. For example, the polynomial f can be taken to be $f = vx^5 + vx^4 + vx^3 + (1 + v)x^2 + x + (1 + v)$.

Example 3.9. The cyclic code of length $s = 8$ over R with generator polynomial $g = x+1$ (and $g_1 = g_2 = x+1$) has size $2^{14} = 16384$ and minimum Lee distance 2. Hence, its Gray image is a $[16, 14, 2]$ binary linear code, which is an optimal code. By Theorem 3.7 a 2-QC code with a generator of the form $\langle g, g\cdot f\rangle$ (with f satisfying the condition stated in the theorem) has parameters $[16, 14, \geq 4]$ over R, and binary parameters $[32, 14, \geq 4]$. For $f = vx^4 + x^3 + vx^2 + (v + 1)x + 1$, the resulting code has minimum distance 6. Therefore, we obtain a $[32, 14, 6]$ binary linear code which is 4-QC. The best known binary linear code of length 32 and dimension 14 has minimum weight 8.

4. A Special Class of 2-QC Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

We investigate the special case for $\ell = 2$. We give a relationship between cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ where $u^2 = u$, $v^2 = v$ and $uv = vu$, and 2-QC codes over $\mathbb{F}_2+v\mathbb{F}_2$. Let K denote the ring $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$. Structure of cyclic codes over the ring K were investigated in [8]. The Lee weight of an element of K is defined as $w_L(x+uy+vz+uvt) = w_H(x, x+y, x+z, x+y+z+t)$ where w_H denotes the Hamming weight for binary codes. Now we define a Gray map from K to R^2 by

$$\phi(x + uy + vz + uvt) = (x + vz, x + y + v(z + t))$$

where $x, y, z, t \in \mathbb{F}_2$. This map is naturally extended from K^n to R^{2n}. It can be easily seen that the Gray map is an isometry from (K, Lee distance) to (R, Lee distance).

Theorem 4.1. *Let ϕ be the Gray map as above and let τ be the cyclic shift operator. Then $\tau^2\phi = \phi\tau$.*

Proof. Let $c = (c_1, c_2, ..., c_n) \in C$ where $c_i = a_i + vb_i + uc_i + uvd_i$, $a_i, b_i, c_i, d_i \in \mathbb{F}_2$ for all $i = 1, 2, ..., n$. Then $\tau(c) = \tau(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$ and $\phi(\tau(c))$ is

$$(a_n+vc_n, a_n+b_n+v(c_n+d_n), \dots, a_{n-1}+vc_{n-1}, a_{n-1}+b_{n-1}+v(c_{n-1}+d_{n-1})) \quad (3)$$

On the other hand,
$\phi(c) = (a_1 + vc_1, a_1 + b_1 + v(c_1 + d_1), \dots, a_n + vc_n, a_n + b_n + v(c_n + d_n))$ and $\tau^2(\phi(c))$ is

$$(a_n+vc_n, a_n+b_n+v(c_n+d_n), \dots, a_{n-1}+vc_{n-1}, a_{n-1}+b_{n-1}+v(c_{n-1}+d_{n-1})) \quad (4)$$

Comparing equations 3 and 4, we get $\phi\tau = \tau^2\phi$ from which the result follows. □

Theorem 4.2. *If C is a cyclic code of length n over K then $\phi(C)$ is a 2-QC code over R with length $2n$.*

Proof. Let C be a cyclic code of length n over K i.e $\tau(C) = C$. By Theorem 4.1 we have $\tau^2(\phi(C)) = \phi(\tau(C)) = \phi(C)$. Hence $\phi(C)$ is a 2-QC code over $\mathbb{F}_2 + v\mathbb{F}_2$. □

This theorem shows that there is a special class of 2-quasi cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ as the Gray images of cyclic codes over K.

Example 4.3. Let C be a cyclic code of length 8 with generator $g(x) = uvx^2 + (1 + uv)x + 1$ over K. By the theorem above, its Gray image is a 2-QC code of length 16 and minimum Lee weight 2. Its binary Gray image is a linear code with parameters $[32, 27, 2]$ which has a best minimum distance among codes that have same n and k parameters.

Example 4.4. Let C be a cyclic code of length 9 with generator $g(x) = (1 + u + v + uv)x^2 + x + 1$ over K. By Theorem 4.2, its Gray image is a 2-QC code of length 18 and minimum Lee weight 2. Its binary Gray image is a linear code with parameters $[36, 31, 2]$ which has a best minimum distance among codes that have same n and k parameters.

We end with the observation that Theorem 4.2 can easily be generalized as follows.

Theorem 4.5. *Let C be a cyclic code of length n over K then $\phi(C)$ is a 2ℓ-QC code over $\mathbb{F}_2 + v\mathbb{F}_2$ with length $2n$. Moreover, $d_L(\phi(C)) = d_L(C)$.*

5. Conclusion

We investigate quasi-cyclic codes over the ring R, where $v^2 = v$. We give a map which defines one to one correspondence between quasi-cyclic codes of length $n = s\ell$ over R and linear codes of length ℓ over R_s. The fact that the number of quasi-cyclic codes of a given length and index over R will be greater than the number of quasi-cyclic codes of the same length and index over $\mathbb{Z}_4$ or $\mathbb{F}_2 + u\mathbb{F}_2$ is the motivation to study of quasi-cyclic codes over R. We investigate the structure of generators for one-generator quasi-cyclic codes over R and their minimal spanning sets. Moreover, for free quasi-cyclic codes over R we find the rank and a lower bound on minimum distances. In particular, we investigate the special case for $\ell = 2$. We give a relationship between cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ where $u^2 = u$, $v^2 = v$ and $uv = vu$, and 2-QC codes over $\mathbb{F}_2 + v\mathbb{F}_2$.

References

1. T. Abualrub, N. Aydin, and P. Seneviratne, *Theta-Cyclic Codes Over* $\mathbb{F}_2+v\mathbb{F}_2$, Australasian J. Combinatorics **54** (2012), 115-126.
2. N. Aydin and D. K. Ray-Chaudhuri, *Quasi cyclic codes over* $\mathbb{Z}_4$ *and some new binary codes*, IEEE Trans. Inf. Theory **48** (2002), 2065-2069.
3. N. Aydin, S. Karadeniz, and B. Yildiz, *Some new binary quasi-cyclic codes from codes over the ring* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, AAECC **24** (2013), 355-367.
4. M. Bhaintwal and S. Wasan, *On quasi cyclic codes over* $\mathbb{Z}_q$, Appl. Algebra Eng. Commun. Comput **20** (2009), 459-480.
5. Y. Cao, *1-generator quasi-cyclic codes over finite chain ring*s, AAECC **24** (2013), 53-72.
6. J. Cui and J. Pei, *Quaternary 1-generator quasi cyclic codes*, Des. Codes.and Cryptogr. **58** (2011), 23-33.
7. R. Daskalov and P. Hristov, *New binary one-generator quasi-cyclic codes*, IEEE Trans. Inf. Theory **49** (2003), 3001-3005.
8. A. Dertli, Y. Cengellenmis, S. Eren, *On Quantum Codes Obtained From Cyclic Codes Over* A_2, International Journal of Quantum Information **13** (2015).
9. J. Gao, L. Shen and F. Wei. Fu, *Generalized quasi cyclic codes over* $\mathbb{F}_q + u\mathbb{F}_q$, arXiv: 1307.1746v1 [cs.IT], 2013.
10. K. Lally and P. Fitzpatrick, *Algebraic structure of quasi-cyclic codes*, Discr. Appl. Math. **111** (2001), 157-175.
11. S. Ling and P. Sole, *On the algebraic structure of quasi-cyclic codes I: Finite Fields*, IEEE Trans. Inf. Theory **47** (2001), 2751-2760.
12. I. Siap, T. Abualrub and B. Yildiz, *One generator quasi-cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, J. Frank. Inst. **349** (2012), 284-291.
13. I. Siap and N. Kulhan, *The structure of generalized quasi-cyclic codes*, Appl. Math. E-Notes **5** (2005), 24-30.
14. I. Siap, N. Aydin and D. K. Ray-Chaudhuri, *New ternary quasi-cyclic codes with better minimum distances*, IEEE Trans. Inf. Theory **46** (2000), 1554-1558.
15. S. Zhu, Y. Wang, and M. Shi, *Some results on cyclic codes over* $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Trans. Inf. Theory **56** (2010), 1680-1684.

Mehmet ÖZEN received M.Sc. and Ph.D from Sakarya University. He is currently a professor at Sakarya University. His research interests include algebra, coding theory and cryptography.

Department of Mathematics, Faculty of Science and Arts, Sakarya University, Sakarya, Turkey.

e-mail: ozen@sakarya.edu.tr

N. Tuğba ÖZZAİM received M.Sc. and Ph.D. from Sakarya University. Her research interests are algebra and coding theory.

Department of Mathematics, Faculty of Science and Arts, Sakarya University, Sakarya, Turkey.
e-mail: tugbaozzaim@gmail.com

Nuh AYDIN received M.Sc. and Ph. D. from Ohio State University. He is currently a professor at Kenyon Collage since 2002. His research interests are algebraic coding theory, algebra, finite fields, cryptography and combinatorics.

Department of Mathematics and Statistics, Kenyon College, Ohio, United States.
e-mail: aydinn@kenyon.edu