Quaternary Quasi-Cyclic Codes with Even Length Components

Irfan Siap
Department of Mathematics, Yıldız Technical University,
Istanbul, TURKEY
isiap@hyildiz.edu.tr

Taher Abualrub
Department of Mathematics and Statistics
American University of Sharjah
Sharjah, UAE.
abualrub@aus.edu

Nuh Aydin
Department of Mathematics, Kenyon College
Gambier, Ohio, U.S.A.
aydinn@kenyon.edu

January 12, 2011

Abstract

In this paper, we study quaternary quasi-cyclic (QC) codes with even length components. We determine the structure of one generator quaternary QC codes whose cyclic components have even length. By making use of their structure, we establish the size of these codes and give a lower bound for minimum distance. We present some examples of codes from this family whose Gray images have the same Hamming distances as the Hamming distances of the best known binary linear codes with the given parameters. In addition, we obtain a quaternary QC code that leads to a new binary non-linear code that has parameters $(96, 2^{26}, 28)$.

Keywords: Quaternary codes, quasi cyclic codes, even length codes.

1 Introduction

There are many good reasons to investigate the structure and the design of quasi cyclic (QC) codes. Some of them are as follows: QC codes form an important

class of linear codes which includes cyclic codes as a subclass, meet a modified version of Gilbert Varshamov bound unlike many other classes of codes [15], and some well-known linear codes are equivalent to QC codes. Due to these facts and many more that are not listed here, the research on QC codes has been attractive. This family has proven to be a very good candidate for good linear codes since many record breaking and optimal QC codes over finite fields of various orders have been discovered (see [11], [13], [22], among many others). Tables of best-known linear codes over small finite fields published in [9] and also updated version available online [12]. The computer algebra system MAGMA [8] contains a similar database as well. Additionally, a table of best-known binary non-linear codes is available [20].

There have been many papers in the literature dealing with the design of 1-generator QC over fields. They are investigated via a polynomial approach introduced in [23], [21] and [10], and more recently, via Gröbner basis in [16] and [17], and by viewing them as modules over some special rings [18].

On the other hand, there has been intensive research on codes over Z_4, integers modulo 4, for over a decade. The term "quaternary code" has been used both for codes over $GF(4)$, the finite field of order 4, and for codes over Z_4, integers modulo 4. Throughout this paper, we shall use the term "quaternary code" exclusively for codes over the ring Z_4.

The structure and the design of quaternary QC codes of length $n = ml$ with the restriction that m is odd are studied in [6], where the authors found a new non-linear binary code and some other good binary codes from quaternary QC codes by applying the standard Gray map. Additional new codes over Z_4 are discovered in [7] and [5] in the class of cyclic codes and QC codes with cyclic components having odd length. Moreover, an online database of best known quaternary codes has been recently introduced [4]. In this paper, we investigate the design of quaternary QC codes of length $n = ml$ where m is even. This class of codes has been largely avoided in the literature. In [19], algebraic structure of QC codes over chain rings are considered. Although, Z_4 QC codes are in the class of QC codes over chain rings, our approach is different and we relax the condition on the length of QC codes over Z_4.

The paper is organized as follows: In the next section, we summarize some basic facts related to our work. In the third section, we study the structure of quaternary QC codes where components have even lengths. Section 4 gives the results of some of our searches which include several quaternary QC codes with even length components whose Gray images have the same Hamming distances as the Hamming distances of the best known binary codes with comparable parameters. Besides exploring the algebraic structure of these codes, in particular, our search results in the construction of a quaternary QC code whose Gray image is a new binary non-linear code with parameters $(96, 2^{26}, 28)$. Hence, we contribute several new codes to the database [4]. Finally, we conclude by summarizing our results and pointing out some directions for further work on the subject.

A remark on notation: as is common in the literature, sometimes we may write f for a polynomial $f(x)$.

2 Basics

A linear code C of length n over Z_4 is defined to be an additive submodule of the Z_4-module Z_4^n. A free module C is a module with a basis (a linearly independent spanning set for C). A cyclic code of length n over Z_4 is defined to be a submodule of Z_4^n that is invariant under the standard (right) shift operator τ that maps the element $(c_0,\ldots,c_{n-1})$ of Z_4^n to $(c_{n-1},c_0,\ldots,c_{n-2})$. As usual, for each vector $(c_0,\ldots,c_{n-1})$ in Z_4^n we associate the polynomial $c_0+c_1x+\ldots c_{n-1}x^{n-1}$ in the ring $R_n = Z_4[x]/(x^n-1)$. With this identification, cyclic codes are ideals in R_n. The Hamming weight of a codeword $u=(u_0,u_1,\cdots,u_{n-1})$, denoted by $w_H(u)$, is the number of nonzero entries in u. The (minimum) Hamming distance of a linear code C is given by

$$d_H(C) = \min\{w_H(u):\ u\in C \text{ and } u\neq 0\}.$$

The *Hamming weight enumerator*, $W_C(y)$, of a code C is defined by

$$W_C(y) = \sum_{c\in C} y^{w_H(c)} = \sum_i A_i y^i \tag{1}$$

where $A_i = |\{c\in C | w_H(c)=i\}|$, i.e. the number of codewords in C whose weights equal to i.

The smallest non-zero exponent of y with a nonzero coefficient in $W_C(y)$ is equal to the minimum distance of the code.

The Lee weights w_L of the elements $0,1,2$ and 3 of Z_4 are $0,1,2$ and 1 respectively. Further, the Lee weight of an n tuple in Z_4^n is the sum of Lee weights of its components.

The *Lee weight enumerator* of a quaternary code C is defined by

$$L_C(y) = \sum_{c\in C} y^{w_L(c)}. \tag{2}$$

An important connection between quaternary codes and binary codes is established by Hammons et. al in [14] where some well-known non-linear binary codes, such as Kerdock and Preperata codes, are obtained as images of quaternary linear codes via the Gray map. The Gray map maps $0,1,2,3$ to $(0,0)$, $(0,1)$, $(1,1)$ $(1,0)$ respectively. After this work, the interest in studying quaternary codes and codes over other finite rings has grown intensively. Further, the Gray map is an isometry from $(Z_4^n,$Lee distance$)$ to $(Z_2^{2n},$Hamming distance$)$. In [6], the structure of quaternary QC codes with odd component lengths are studied and a new non-linear binary code and some optimal binary codes are found by applying the Gray map to quaternary QC codes.

Recently, quaternary cyclic codes and their structures are investigated in [1], [2], and [3]. A recent result for the structure and the design of quaternary cyclic codes of arbitrary length is stated below.

Theorem 1 *[1] Let C be a cyclic code in $R_n = Z_4[x]/(x^n-1)$.*

1. *If n is odd, then R_n is a principal ideal ring and $C = (g(x), 2a(x)) = (g(x) + 2a(x))$ where $g(x)$, $a(x)$ are polynomials with $a(x) \mid g(x) \mid (x^n - 1) \mod 4$.*

2. *If n is even, then either*

   (a) *C is a free module with a generator of the form*

   $$C = (g(x) + 2p(x)),$$

   where $g(x) \mid (x^n - 1) \mod 2$ and $(g(x) + 2p(x)) \mid (x^n - 1) \mod 4$, or,

   (b) *$C = (g(x) + 2p(x),\ 2a(x))$ where $g(x)$, $a(x)$, and $p(x)$ are polynomials with $g(x) \mid (x^n - 1) \mod 4$, $a(x) \mid g(x) \mod 2$, $a(x) \mid p(x) \left(\frac{x^n - 1}{g(x)}\right) \mod 2$, and $\deg g(x) > \deg a(x)$.*

If n is odd then R_n is a principal ideal ring, and $x^n - 1$ has a unique factorization. Moreover, there is a one-to-one correspondence between factors of $x^n - 1$ over $\mathbb{Z}_2$ and factors of $x^n - 1$ over Z_4. More specifically, a factor f_2 of $x^n - 1$ in $\mathbb{Z}_2[x]$ can be " lifted" to a factor f of $x^n - 1$ in $Z_4[x]$, called Hensel lift. There are well known methods to compute the Hensel lift of a polynomial (e.g. [24]).

Definition 1 *[24] Two polynomials $f_1(x)$, $f_2(x) \in Z_4[x]$ are said to be relatively prime, denoted by $(f_1(x), f_2(x)) = 1$, in $Z_4[x]$ if there exist polynomials $p_1(x)$, $p_2(x) \in Z_4[x]$ such that*

$$p_1(x)f_1(x) + p_2(x)f_2(x) = 1.$$

Note that if $(f_1(x), f_2(x)) = 1$ in $Z_4[x]$ then $\left(\overline{f_1(x)}, \overline{f_2(x)}\right) = 1$ in $Z_2[x]$, where $\overline{f_i(x)} = f_i(x) \mod 2$.

3 Algebraic Structure of Quaternary Quasi Cyclic Codes

Definition 2 *A quaternary code is called an l-QC code if it is invariant under τ^l, the l-fold composition of the shift operator τ.*

It is well-known that, after a suitable permutation of the coordinates, an l-QC code of length $n = ml$ over Z_4 (or over any ring) can be regarded as an $R_m = Z_4[x]/(x^m - 1)$ submodule of R_m^l. This is because the quasi-cyclic shift operation corresponds to (after a permutation of the coordinates) multiplication by x in module R_m^l. An r generator QC code is a submodule with r generators. In this paper, we only study 1-generator quaternary QC codes. A 1-generator quaternary QC code C generated by $(a_1(x), a_2(x), \ldots a_l(x))$ is defined as

$$C = \left\{ \begin{array}{c} f(x)\,(a_1(x),\ a_2(x), \ldots, a_l(x)) = \\ (f(x)a_1(x),\ f(x)a_2(x), \ldots, f(x)a_l(x)) \mid f(x) \in R_m \end{array} \right\}.$$

In [6], quaternary QC codes with the restriction that m is odd are studied. In this paper, we study quaternary QC codes of length $n = ml$, where m is even.

By the remarks above, we shall always view quaternary QC codes as submodules of R_m^l. Our first theorem easily follows from the observations already made.

Theorem 2 *Let C be a quaternary 1-generator l-QC code of length $n = ml$ with even m and generator $\mathbf{F}(x) = (F_1(x), F_2(x), \ldots, F_l(x))$ where $F_i(x) \in R_m$ for $1 \leq i \leq l$. Then, $F_i(x) \in C_i$ where C_i is a cyclic code of length m in R_m. Therefore, F_i is of the form $F_i(x) = f_i(x)(g_i(x) + 2p_i(x)) + 2a_i(x)k_i(x)$ where $g_i(x)$ and $a_i(x)$ are as in Theorem 1, $f_i(x) \in Z_4[x]$ and $k_i(x) \in \mathbb{Z}_2[x]$.*

Proof: For all $1 \leq i \leq l$ define the following projection map $\Pi_i : R_m^l \to R_m$ such that $\Pi_i((f_1, f_2, \ldots, f_i, \ldots, f_l)) = f_i$. Let $C = (F_1, F_2, \ldots, F_l)$ be such a code. Then $\Pi_i(C)$ is a cyclic code in R_m. By Theorem 1, we get that $F_i \in C_i = (g_i(x) + 2p_i(x),\ 2a_i(x))$ for all $1 \leq i \leq l$ (where $a(x)$ is possibly 0). □

Corollary 3 *A 1-generator quaternary QC code is equivalent to a quaternary code generated by $(f_1g_1 + 2q_1, f_2g_2 + 2q_2, \ldots, f_lg_l + 2q_l)$ where $f_i, g_i, q_i \in \mathbb{Z}_2[x]$, $g_i|(x^m - 1)$ for all $1 \leq i \leq l$ and $\deg(q_1) < \deg(g_1)$.*

Proof: By Theorem 2, the generator should be in the form $(F_1, F_2, \ldots, F_l)$ where $F_i \in C_i$ for all $1 \leq i \leq l$. Next, each F_i can be written in the form $F_i = f_i(g_i + 2p_i) = f_ig_i + 2f_ip_i$, for some binary polynomials f_i, g_i and p_i. Let $q_i = f_ip_i$ then

$$C = (f_1g_1 + 2q_1, f_2g_2 + 2q_2, \ldots, f_lg_l + 2q_l).$$

Finally, since the ideals generated by (a, b) and $(a + rb, b)$ are equal for any ring element r, if $\deg(q_1) \geq \deg(g_1)$ we can replace the first generator by $g_1 + 2q_1 + 2x^k(f_2g_2 + 2q_2) \pmod{x^m - 1}$ for a suitable k to satisfy the degree requirement. □

For a code C with generator $G(x) = (g_1 + 2q_1, f_2g_2 + 2q_2, \ldots, f_lg_l + 2q_l)$, we will have $g(x)$ denote

$$g(x) = gcd(g_1, f_2g_2, \ldots, f_lg_l, x^m - 1) \text{ and } h_g = (x^m - 1)/g \text{ in } \mathbb{Z}_2[x]. \quad (3)$$

Theorem 4 *Suppose C is a quaternary, 1-generator, l- QC code of length $n = ml$ for even m with a generator $G(x) = (g_1 + 2q_1, f_2g_2 + 2q_2, \ldots, f_lg_l + 2q_l)$ where $f_i, g_i, q_i \in \mathbb{Z}_2[x]$, $g_i|(x^m - 1)$ for all $i \leq 1 \leq l$ and $\deg(q_1) < deg(g_1)$. Let $g(x)$, $h_g = (x^m - 1)/g$ be as in Equation (3), $h_gG(x) = 2H(x) = 2[H_1(x), \ldots, H_l(x)]$ where $H_i(x) \in \mathbb{Z}_2[x]$, $k = gcd(H_1(x), H_2(x), \ldots, H_l(x), x^m - 1)$ in $\mathbb{Z}_2[x]$, and $h_k = (x^m - 1)/k$. Take C_0 to be the $\mathbb{Z}_4$-submodule of C generated by $\alpha = \{G(x), xG(x), \ldots, x^{\deg(h_g)-1}G(x)\}$.*

1. *If $2H(x) \in C_0$, then $C = C_0$ and C is a free $\mathbb{Z}_4$-module generated by the set α and $|C| = 4^{\deg(h_g)-1}$.*

2. *If* $2H(x) \notin C_0$, *then there exists an* $0 \leq r \leq \deg h_k - 1$ *such that*

$$\beta = \Big\{ G(x), xG(x), \ldots, x^{\deg(h_g)-1}G(x), \\ 2H(x), 2xH(x), \ldots, 2x^r H(x) \Big\}.$$

generates C *and* $|C| = 4^{\deg(h_g)-1} \cdot 2^r$.

Proof: Let $G(x) = (g_1 + 2q_1, f_2 g_2 + 2q_2, \ldots, f_l g_l + 2q_l)$. Let $c(x) = f(x)G(x) \in C$. If $\deg f(x) < \deg h_g$ then $c(x) \in \text{Span}(\alpha)$. Otherwise by the division algorithm we have

$$f(x) = h_g q(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg r(x) < \deg h_g.$$

This implies that

$$\begin{aligned} c(x) &= (h_g q(x) + r(x))\, G(x) \\ &= q(x) h_g G(x) + r(x) G(x) \\ &= 2q(x) H(x) + r(x) G(x) \end{aligned}$$

Now, we consider two cases:

1. If $h_g G(x) = 2H(x) \in C_0$ then $q(x)2H(x) \in \text{Span}(\alpha)$ and $r(x)G(x) \in \text{Span}(\alpha)$ (because $\deg r(x) < \deg h_g$). Hence $c(x) \in \text{Span}(\alpha)$. It is also clear that α is linearly independent (over Z_4). So C is a free Z_4-module generated by the set α and $|C| = 4^{\deg(h_g)-1}$.

2. If $h_g G(x) = 2H(x) \notin C_0$, then

$$\begin{aligned} c(x) &= (h_g q(x) + r(x))\, G(x) \\ &= q(x) h_g G(x) + r(x) G(x) \\ &= 2q(x) H(x) + r(x) G(x). \end{aligned}$$

If $\deg q(x) \geq \deg h_k$, then $q(x) = \tilde{q}(x) h_k(x) + \tilde{r}(x)$ where $\tilde{q}, \tilde{r} \in \mathbb{Z}_2[x]$ and $0 \leq \deg \tilde{r} < \deg h_k$. Hence,

$$\begin{aligned} q(x) H_i(x) &= (\tilde{q}(x) h_k(x) + \tilde{r}(x)) H_i(x) = \tilde{q}(x) h_k(x) H_i(x) + \tilde{r}(x) H_i(x) \\ &= \tilde{r}(x) H_i(x) \end{aligned}$$

for all i. Thus, $2q(x)H_i(x) = 2\tilde{r}(x)H_i(x)$ and $\deg \tilde{r}(x) \leq \deg h_k - 1$ and hence β generates C. Therefore $|C| = 4^{\deg(h_g)-1} \cdot 2^r$ for some $r \leq \deg h_k - 1$. □

The following corollary presents a lower bound on minimum distance for a subclass of QC codes considered in this paper.

Corollary 5 *Let C be a 1-generator, l-QC quaternary code of length $n = ml$ for even m of the form $C = ((g+2p)f_1, (g+2p)f_2, \ldots, (g+2p)f_l)$ where $(g+2p)|(x^m-1) \mod 4$. Let $\deg g(x) = r$, $H_g(x) = \dfrac{x^m-1}{g+2p}$, $(f_i(x), H_g(x)) = 1$ in $Z_4[x]$ for all $i = 1, 2, \ldots, l$, and $\mathbf{G}(x) = ((g+2p)f_1, (g+2p)f_2, \ldots, (g+2p)f_l)$. Then, C is a free $\mathbb{Z}_4$-module with basis*

$$\beta = \left\{G(x), xG(x), \ldots, x^{m-r-1}G(x)\right\},$$

$$rank(C) = m - r, \quad |C| = 4^{m-r}, \quad \text{and } d_L(C) \geq l \cdot d,$$

where $d_L(C)$, and d are the minimum Lee weights of C and the $\mathbb{Z}_4$ cyclic code generated by $(g+2p)$ respectively.

Proof: $\Pi_i(C) = ((g+2p)f_i)$ is a cyclic code of length m, where $(g+2p)|(x^m-1) \mod 4$ and $g|x^m-1 \mod 2$. Let $K = g+2p$ and $H_g = h_g + 2s$ where $g, p, h_g, s \in \mathbb{Z}_2[x]$, $KH_g = 0 \mod 4$, $K = g$ and $H_g = h_g$ and $gh_g = 0 \mod 2$, $gh_g = x^m - 1 + 2\tilde{r} \mod 4$. Then, $0 = (g+2p)H_g = (g+2p)(h_g+2s) = gh_g + 2ph_g + 2sg \mod 4$. So $2ph_g = g(2s+h_g)$. Hence, $h_g(g+2p) = gh_g + 2ph_g = gh_g + g(2s+h_g) = 2sg$. Then, $2H_i = h_gG_i = h_g(g+2p)f_i = 2sgf_i$. So h_gG_i is a multiple of $2gf_i$. Thus, $2H \in C$. Therefore, by the previous theorem first three assertions in this corollary follow. To prove the assertion on the minimum distance, consider an arbitrary codeword

$$\begin{aligned}\mathbf{c}(x) &= k(x)G(x) \\ &= (k(x)(g+2p)f_1, k(x)(g+2p)f_2, \ldots, k(x)(g+2p_l)f) \in C\end{aligned}$$

for some $k(x) \in \mathbb{Z}_4[x]$. Since $\left(f_i, \dfrac{x^m-1}{g+2p}\right) = 1$ in Z_4 then we have

$$\alpha_i f_i + \beta_i \frac{x^m-1}{g+2p} = 1 \text{ for all } i = 1, \ldots, l.$$

Hence we have $(g+2p)\,\alpha_i f_i = (g+2p)$ for all $i = 1, \ldots, l$.

If $k(x)(g+2p)f_j = 0$ for some j, then

$$k(x)\alpha_j(g+2p)f_j = k(x)\,(g+2p) = 0.$$

This implies that $k(x)(g+2p)f_i = 0$ for all $i = 1, 2, .., l$. So, either $\mathbf{c}(x) = \mathbf{0}$ or $k(x)(g+2p)f_i \neq 0$ for all $i = 1, 2, ..., l$. Since $k(x)(g+2p)f_i \in (g+2p)$ then $w_L(k(x)(g+2p)f_i) \geq d$ for all i. Therefore $d_L(C) \geq l \cdot d$. □

4 Examples and a New Code

In these examples, we look at the parameters of the Gray images of these codes and compare them with the best known binary linear codes. If the Gray image of a Z_4 linear code has the same parameters as the best known binary linear

code, we call such a code a *decent code*, if the parameters are better than the best known binary linear code, we call it a *good code*. Finally, if the resulting parameters happen to be contained in the range of the table [20] and improve them, we call it an *exceptional code*. Our examples include some decent codes and an exceptional code.

Example 1 *(A decent, 2-QC code of length* 16*)*

Let $g(x) = x^6 + x^4 + x^2 + 1$, $p(x) = x^5 + x^4 + x + 1$ and $f(x) = x$. Then, $g(x) + 2p(x) = x^6 + 2x^5 - x^4 + x^2 + 2x - 1$, and $(g(x) + 2p(x))|(x^8 - 1) \mod 4$. Consider the quaternary QC code $C = ([g + 2p,\ (g + 2p)\, f])$. By Corollary 5, this is a free code. Indeed, $h_g = x^2 + 1$ and $hgG = 2[g, gx] = 2G = 2H \in C_0$. Hence, $2H(x) \in C_0$ and $C = C_0$. Thus, this code has length 16, and it is free with 4^2 codewords.

In order to use the space efficiently, we introduce the notation below for weight enumerators (1) and (2), where the base and the power represent the weight and the number of the codewords corresponding to that weight respectively. A computer computation shows that the Lee weight enumerator of C is given by $0^1 16^{14} 32^1$ and the Hamming weight enumerator of C is given by $0^1 8^2 12^8 16^5$. So, $w_L(C) = 16$ and $w_H(C) = 8$. Hence, the quaternary QC code C has length 16, rank 2, and minimum distance 16. The Gray image of this code is a binary code of length 32, minimum Hamming distance 16, and it has 16 codewords. It is known that there exits an optimal binary linear code with these parameters [12].

Example 2 *(A decent, 2-QC code of length* 28*):*

There are 796 distinct divisors of $x^{14} - 1$ over Z_4. One of those divisors is $g = x^4 + 3x^2 + 3x + 3$ which generates a cyclic code of length 14, dimension 10 and minimum Lee weight 4. Let $f = 2x^9 + 3x^8 + 2x^6 + 2x^5 + x^4 + x^3$. Then the 2-QC code C generated by (g, fg) is free of rank 10, and has minimum Lee weight 16. Therefore, the Gray image of C has parameters $(56, 2^{20}, 16)$. These parameters are the same as the parameters of the best-known binary linear code. We have found several other factors of $(x^{14} - 1)$ that yielded codes with the same parameters.

Example 3 *(An exceptional, 2-QC code of length* 48*):*

There are 37558 distinct factors of $x^{24} - 1$ over Z_4. One of those divisors is $g = 3x^{11} + x^{10} + 3x^9 + x^8 + x^7 + 3x^6 + 3x^5 + 3x^4 + 3x^3 + 3x^2 + 3x + 3$ which generates a cyclic code of length 24, dimension 13 and minimum Lee weight 4. Let $f = x^{12} + 3x^{10} + 3x^9 + 3x^8 + x^7 + 2x^6 + x^5 + x^4$. We found that the 2-QC code C generated by $[g, fg]$ is free of rank 13, and has minimum Lee weight 28. Therefore, the Gray image of C has parameters $(96, 2^{26}, 28)$ (and it is non-linear). This binary code not only has a larger minimum distance than a best-known comparable linear code with parameters $[96, 26, 26]$, but also it turns out to be better than the previously best-known comparable binary non-linear code [20]. In the notation of [20], $A(95, 27)$ is improved from 2^{25} to 2^{26}.

Therefore, we obtain a *new* binary code and we call this code an exceptional code. Out of the 37558 divisors of $x^{24}-1$ found, a number of them lead to good codes. The weight enumerator of this code is as follows:

$0^{1}28^{4368}32^{102135}36^{1078224}40^{5816832}44^{15616800}48^{21872144}52^{15616800}56^{5816832}60^{1078224}64^{102135}68^{4368}96^{1}$.

5 Conclusion

We have investigated the structure of quaternary quasi-cyclic codes of length ml, with m even. We proved some results related to the number of codewords of 1-generator quaternary QC codes and gave a lower bound on minimum distance for a special case. Our search results show that this class is a larger family (since number of factors of x^m-1 is much larger) compared to odd component length QC codes. We constructed a quaternary QC code that leads to a new binary non-linear code that has parameters $(96, 2^{26}, 28)$. Further research problems would be to study r which contributes to non-free part in Theorem 4 or compute it for a specific subclass of this family and study quasi cyclic codes over different finite rings with no restrictions on lengths.

Acknowledgements: The authors would like to thank the anonymous referees for their careful reading and useful comments which improved the writing and presentation of the paper.

References

[1] Abualrub T., Siap I., Reversible cyclic codes over $\boldsymbol{Z_4}$. Australas. J. Combin. **38**, 195-206 (2007).

[2] Abualrub T., Ghrayeb A., Oehmke R., A mass formula and rank of Z_4 cyclic codes of length 2e. IEEE Trans. Inform. Theory **50**, 3306-3312 (2004).

[3] Abualrub T., R. Oehmke R., On the generators of Z_4 cyclic codes. IEEE Trans. Inform. Theory **49**, 2126-2133 (2003).

[4] Asamov T., Aydin N., Database of Z_4-codes. Available at www.Z4codes.net.

[5] Aydin N., Asamov T., A database of Z_4 codes. Journal of Combinatorics, Information and System Sciences Vol. 34 No. 1-4 Comb, (2009), p: 1-12.

[6] Aydin N., Ray-Chaudhuri D. K., Quasi cyclic codes over $\mathbb{Z}_4$ and some new binary codes. IEEE Trans. Inform. Theory **48**, 2065-2069 (2002).

[7] Aydin N., Gulliver T. A., Some good cyclic and quasi-twisted $\mathbb{Z}_4$-linear codes. to appear in Ars Comb.

[8] Bosma W., Cannon J. J.,C. Playoust C., The magma algebra system I: The user language. J. Symbolic Computation. **24**, 235-266 (1997).

[9] A. E. Brouwer, Bounds on the size of linear codes, in Handbook of Coding Theory, V. S. Pless and W. Huffman, Eds. Amsterdam, The Netherlands:North-Holland, vol. 1,(1998).

[10] Conan J., Seguin G., Structural properties and enumeration of quasi cyclic codes. Appl Algebra. Engrg. Comm. Comput. **4**, 25-39 (1993).

[11] Daskalov R., Hristov P.: New binary one-generator quasi-cyclic codes. IEEE Trans. Inform. Theory, **49**, 301-305 (2003).

[12] Grassl M., Table of bounds on linear codes. Available at: http://www.codetables.de.

[13] Greenough P. P., Hill R., Optimal ternary quasi-cyclic codes. Des. Codes Cryptogr. **2**, 81-91 (1992).

[14] Hammons A. R., Kumar P. V.,Calderbank A. R., SloaneN. J. A., Sole P., The Z_4-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory **40**, 301-319 (1994).

[15] Kasami T., A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2. IEEE Trans. Inform. Theory **20**, 679 (1974).

[16] Lally K., Fitzpatrick P., Construction and classification of quasi-cyclic codes. WCC 99, Workshop on Coding and Cryptography January 11-14, PARIS (France), (1999).

[17] Lally K., Fitzpatrick P., Algebraic structure of quasi-cyclic codes. Discr. Appl. Math. **111**,157-175 (2001).

[18] Ling S., Sole P., On the algebraic structure of the quasi-cyclic codes I: finite fields. IEEE Trans. Inform. Theory **47**, 2751-2759 (2001).

[19] Ling S., Sole P., On the algebraic structure of the quasi-cyclic codes II: chain rings. Des. Codes Cryptogr. **30**, 113-130 (2003).

[20] Litsyn S., Table of non-linear binary codes. Available at: http://www.eng.tau.ac.il/~ litysn/tableand/index.html.

[21] Séguin G. E.,Drolet G., The theory of 1-generator quasi-cyclic codes, Technical Report, Royal Military College of Canada, Kingston, ON, (1991).

[22] Siap I., Aydin N., Ray-Chaudhuri D. K., New ternary quasi-cyclic codes with better minimum distances. IEEE Trans. Inform. Theory **46**, 1554-1558 (2000).

[23] Thomas K., Polynomial approach to quasi-cyclic codes. Bul. Cal. Math. Soc. **69**, 51-59 (1977).

[24] Wan Z. X., Quaternary codes. World Scientific, Singapore (1997).