Applied Mathematics E-Notes, 5(2005), 24-30 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

THE STRUCTURE OF GENERALIZED QUASI CYCLIC CODES *

Irfan Siap †, Nilgun Kulhan ‡

Received 21 March 2004

Abstract

We investigate the structure of generalized quasi cyclic (GQC) codes. We determine the generator of 1-generator GQC codes and prove a BCH type bound for this family of codes.

1 Introduction

There are many well-known reasons to investigate and work on quasi cyclic codes. Some of them are as follows: quasi-cyclic codes form an important class of linear codes which also include cyclic codes ($l = 1$). These codes meet a modified version of Gilbert Varshamov bound unlike many other classes of codes, [6]. Recently, there has been much research on quasi-cyclic codes. Many record breaking and optimal quasi-cyclic codes over finite fields of orders $2, 3, 4, 5, 7, 8$ and 9 have been discovered [4], [5], [16], [3], [1] and [15]. The structure of quasi cyclic codes is investigated in [9] via a polynomial approach. The structure of 1-generator quasi cyclic codes is investigated in [14] and [2]. Recently the structure of quasi cyclic codes is investigated in [10] and [11] via Gröbner basis and in [12] by viewing them as modules over some special rings.

The class of quasi cyclic codes is generalized to codes in which a permutation automorphism has orbits of varying lengths on the coordinate positions in [7] and [8]. In this paper we call such codes generalized quasi cyclic codes and focus on the 1 generator case of this family of codes which have better minimum distances than generalized quasi cyclic codes with more than generator.

Error correction capability and decoding of codes is the main problem of coding theory. Hence it is very important to know the dimension and the minimum distance of a linear code. A class of linear codes where this problem is achieved partially is the family of quasi cyclic codes, especially 1-generator quasi cyclic codes. The structure of a quasi cyclic code is well known. Further, the dimension and a lower BCH-type bound is also established for quasi cyclic codes. In this paper, we broaden the family of quasi cyclic codes in a way that still the dimension and a BCH-type bound can be

*Mathematics Subject Classifications: 9405, 94B60.
†Adıyaman Education Faculty, Gaziantep University, Adıyaman, Turkey
‡Department of Mathematics, Sakarya University, Sakarya, Turkey

determined. We also believe that new record breaking codes can be found within this family as in the case of quasi cyclic codes.

Let F_q (or $GF(q)$) be a finite field of order q. A linear code C of length n over F_q is a vector subspace of $V := F_q^n$. The elements of C are called codewords. The (Hamming) distance $d(\boldsymbol{u}, \boldsymbol{v})$ between two vectors $\boldsymbol{u} = (u_1, \dots, u_n) \in V$ and $\boldsymbol{v} = (v_1, \dots, v_n) \in V$ is defined by

$$d : V \times V \to \mathbb{N}_0$$

and $d(\boldsymbol{u}, \boldsymbol{v}) := |\{i : u_i \neq v_i\}|$, where $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and $\mathbb{N}$ is the set of positive integers. d is a metric on V. The minimum distance between distinct pairs of codewords of a code C is called the minimum distance of C and denoted by $d(C)$ or simply d.

DEFINITION 1. A vector subspace C of F_q^n of dimension k and $d(C) = d$ is denoted by $[n, k, d]_q$.

Another important notion is the (Hamming) weight of a codeword $\boldsymbol{u}$ which is defined by $w(\boldsymbol{u}) = |\{i | u_i \neq 0\}|$, i.e. the number of the nonzero entries of $\boldsymbol{u}$. The minimum weight $w(C)$ of a code C is the smallest possible weight among all its nonzero codewords. We observe that if C is a linear code then $d(C) = w(C)$.

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

$$W_C(y) = \sum_{\boldsymbol{u} \in C} y^{w(\boldsymbol{u})} = \sum_i A_i y^i \tag{1}$$

where $A_i = |\{\boldsymbol{u} \in C | w(\boldsymbol{u}) = i\}|$ i.e. the number of codewords in C with weights equal to i.

The smallest nonzero exponent of y in $W_C(y)$ is equal to the minimum distance of the code.

A linear code C is called a t-error correcting code if $t = \lfloor \frac{d-1}{2} \rfloor$, where $d = d(C)$. One of the important problems of coding theory is to construct a linear code over a finite field F_q that has the largest possible minimum distance for a fixed length n and dimension k.

DEFINITION 2. A linear code C over a field F is called an l-quasi-cyclic (l-QC) code if and only if any codeword in C after a cyclic right shift of l positions is still a codeword in C.

THEOREM 1. [13] Let C be a cyclic code of length n generated by $g(x)$. Let a denote the number of consecutive powers of the n-th root of unity that are the zeroes of $g(x)$. Then $d(C) \geq a + 1$.

2 The Structure of GQC Codes

Let $m_1, m_2, \dots, m_l$ be positive integers. Let $R_i = F_q[x]/(x_i^m - 1)$ and $(m_i, q) = 1$ where $1 \leq i \leq l$. The Cartesian product $R' = R_1 \times R_2 \times \cdots \times R_l$ is an $F_q[x]$ module under component wise addition and scalar multiplication.

DEFINITION 3. Let $n = m_1 + m_2 + \cdots + m_l$. An $F_q[x]$ submodule of R' is called a generalized quasi cyclic code or shortly a GQC code of length $(m_1, m_2, \dots, m_l)$.

Note that if C is a GQC code of length $(m_1, m_2, \ldots, m_l)$ with $m = m_1 = m_2 = \ldots = m_l$, then C is a quasi cyclic code with length ml. Further if $l = 1$, then C is a cyclic code of length m.

The following lemma gives some information regarding the structure of GQC codes:

LEMMA 1. Let C be an s generated GQC code of length $(m_1, m_2, \ldots, m_l)$ and generated by the set $\{g_1'(x), g_2'(x), \ldots, g_s'(x)\}$ where $g_j = (g_{j1}, g_{j2}, \ldots, g_{jl})$ for $1 \leq j \leq s$. Then, for all $1 \leq j \leq s$ and $1 \leq i \leq l$, $g_{ji}(x) = f_{ji}(x)g_i(x)$ there exist $f_{ji}(x) \in \mathbb{F}_q[x]/(x^{m_i} - 1)$ such that $g_{ji}(x) = f_{ji}(x)g_i(x)$ where $g_i(x) \in \mathbb{F}_q[x]/(x^{m_i} - 1)$ and $g_i(x)|(x^{m_i} - 1)$.

PROOF. For all $1 \leq i \leq l$, we define the following projection map:

$$\Pi_i : R' \to \mathbb{F}_q[x]/(x^{m_i} - 1)$$

such that $\Pi_i(f_1(x), f_2(x), \ldots, f_l(x)) = f_i(x)$. The set $\Pi_i(C)$ is an ideal of $\mathbb{F}_q[x]/(x^{m_i} - 1)$, i.e.e a cyclic code of length m_i over $\mathbb{F}_q[x]/(x^{m_i} - 1)$. Hence, there exists a $g_i(x) \in \mathbb{F}_q[x]/(x^{m_i} - 1)$ such that $C = \langle g_i(x) \rangle$. Since $g_{ji}(x) \in \Pi_i(C) = \langle g_i(x) \rangle$ there exists $f_{ji}(x) \in \mathbb{F}_q[x]/(x^{m_i} - 1)$ such that $g_{ji}(x) = f_{ji}(x)g_i(x)$ where $g_i(x) \in \mathbb{F}_q[x]/(x^{m_i} - 1)$ and $g_i(x)|(x^{m_i} - 1)$.

COROLLARY 1. Let C be a 1-generator GQC code. Then, C is generated by an element

$$\overline{f}(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$$

where $f_i(x), g_i(x) \in F_q[x]/(x^{m_i} - 1)$ and $g_i(x)|(x^{m_i} - 1)$ for all $1 \leq i \leq l$.

Now we give some theorems regarding the parameters of GQC codes.

THEOREM 2. Let C be a 1-generator GQC code. Then, C is generated by an element

$$\overline{f}(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$$

where $f_i(x), g_i(x) \in F_q[x]/(x^{m_i} - 1)$ and $g_i(x)|(x^{m_i} - 1)$ for all $1 \leq i \leq l$. Let $h_i(x) = \frac{x^{m_1} - 1}{g_i(x)}$ and $(f_i(x), g_i(x))$ for all $1 \leq i \leq l$. Then (i)

$$\dim(C) = \deg\left((h_1(x), h_2(x), \ldots, h_l(x), x^{m_1} - 1, x^{m_2} - 1, \ldots, x^{m_l} - 1)\right)$$

where $[h_1(x), h_2(x), \ldots, h_l(x), x^{m_1} - 1, x^{m_2} - 1, \ldots, x^{m_l} - 1]$ denotes the lowest common factor of the polynomials over $\mathbb{F}_q$, and (ii)

$$d(C) \geq \min_{i=1,\ldots,l}\{a_i + 1\}$$

where a_i denotes the number of consecutive powers of the m_i-th root of unity that are the zeroes of $g_i(x)$,

PROOF. (i). Let $h(x) = (h_1(x), h_2(x), \ldots, h_l(x))$. Then, for all $0 \neq p(x) \in F_q[x]$ with $\deg(p(x)) < \deg(h(x))$ $p(x)\,(f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x)) \neq 0$. Otherwise, $p_i(x)f_i(x)g_i(x) = 0$ for all $1 \leq i \leq l$. In $F_q[x]$, $x^{m_i} - 1|p(x)f_i(x)g_i(x) = 0$ for all

$1 \leq i \leq l$. Since $(f_i(x), h_i()x)\ h_i(x)|p(x)$ for all $1 \leq i \leq l$. Hence, $h(x)|p(x)$ which is a contradiction to the fact that $\deg(p(x)) < \deg(h(x))$. Let

$$B = \left\{ \overline{f}(x), x\overline{f}(x), \dots, ..., x^{\deg(h(x))-1}\overline{f}(x) \right\}.$$

Elements of B which also are elements of C are F_q linear independent.

(ii) For a given non zero codeword c of C there exist at least one i-th component of c different from zero. Assume that the i-th component of c is different from zero. Since $c \in \Pi_i(C) = \langle f_i(x)g_i(x) \rangle = \langle g_i(x) \rangle$, the non zero weights of the element of the cyclic code $c \in \Pi_i(C) = \langle g_i(x) \rangle$ are larger or equal to $a_i + 1$.

EXAMPLE 1. Let $C = \langle x^2 + x + 1, x^3 + x + 1 \rangle$ be a GQC code of length 10 where $q = 2, l = 2, m_1 = 3$ and $m_2 = 7$. By part 1 of Theorem 2, $\Pi_1(x) = \langle (x^2 + x + 1) \rangle)$ is a cyclic code over $F_2[x]/(x^3 - 1)$ and $\Pi_2(x) = \langle (x^3 + x + 1) \rangle)$ is a cyclic code over $F_2[x]/(x^7 - 1)$. $h_1(x) = x - 1$, $h_2(x) = x^4 + x^2 + x + 1$ and $h(x) = [h_1(x), h_2(x)] = x^4 + x^2 + x + 1$, $\dim(C) = deg(x^4 + x^2 + x + 1) = 4$. Further, by part 2 of Theorem 2 we determine a lower bound for $d(C)$. The degree of the splitting field of $x^3 - 1$ over $\mathbb{F}_2$ is 2 (that is the multiplicative order of 2 mod 3), and $g_1(x) = x^2 + x + 1$ is a primitive polynomial of degree 2 over $\mathbb{F}_2$. Let α be a root of $g_1(x)$ which is also a third primitive root of unity. The consecutive powers of primitive roots of unity α and α^2 are also the roots of $g_1(x)$ and hence $a_1 = 2$. Similarly, the degree of the splitting field of $x^7 - 1$ over $\mathbb{F}_2$ is 3 and $g_2(x) = x^3 + x + 1$ is a primitive polynomial of degree 3 over $\mathbb{F}_2$. Let β be a root of $g_2(x)$ which is also a 7-th primitive root of unity. The consecutive powers of primitive roots of unity are β, β^2 and β^4 are also the roots of $g_2(x)$ and hence $a_2 = 3$. Thus, by part 2 of Theorem 2 $d(C) \geq \min\{3, 4\} = 3$.

In fact, the Hamming weight enumerator of this code is

$$W(y) = 1 + y^3 + 7y^4 + 7y^7.$$

Hence, $d(C) = 3$. In this example we see that the minimum lower bound given for GQC codes is also attained by this family.

Though the bound given in Theorem 2 is attained by a general family of GQC codes there is a way to restrict the family and obtain a better bound as follows:

THEOREM 3. Let C be a 1-generator GQC code generated by an element

$$\overline{f}(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \dots, f_l(x)g_l(x))$$

where the notation is the same as in Theorem 2. Let $m = \min_{i=1,\dots,l}\{\deg(h_i(x))\}$. Let C' be a sub code of C generated by

$$\left\{ \overline{f}(x), x\overline{f}(x), x^2\overline{f}(x), , \dots, x^{m-1}\overline{f}(x) \right\}.$$

Let a_i denote the number of consecutive powers of the m_i-th root of unity that are the zeroes of $g_i(x)$. Hence,

$$d(C') \geq \min_{i=1,\dots,l}\{a_i + 1\}.$$

PROOF. Since $\Pi_i(C)$ is a cyclic code of length m_i by Theorem 1 for all $c_i \neq 0$, $w(c_i) \leq a_i + 1$. Due to hypothesis of the theorem for all $c \in C'$ if $c \neq 0$ then $c_i \neq 0$. Hence, for all $c \neq 0$ and $c \in C'$ $w(c) \geq \min_{i=1,\ldots,l}\{a_i + 1\}$.

EXAMPLE 2. Let $C = \langle(x^8 + x^7 + x^6 + x^4 + 1, x^8 + x^5 + x^4 + x^3 + 1)\rangle$ be a GQC binary code of length 32 with $m_1 = 15$ and $m_2 = 17$. Let us establish a lower bound for the minimum distance of C by applying Theorem 3. Let α be a root of $g_1(x) = x^8 + x^7 + x^6 + x^4 + 1$ which is also a fifteenth primitive root of unity. Since $\alpha, \alpha^2, \alpha^3$ and al^4 is e set of consecutive powers of α which are zeroes of $g_1(x)$ then $a_1 = 4$. Similarly, let β be a root of $g_2(x) = x^8 + x^5 + x^4 + x^3 + 1$ which is also a seventeenth primitive root of unity then $a_2 = 3$. Now let $C' \subset C$ be a linear code generated by $G(x) = (g_1(x), g_2(x))$. $\{G(x), xG(x), x^2G(x), \ldots, x^8G(x)\}$ is a basis for C' and by Theorem 3, $d(C') \geq 9$. Hence, C' is a linear code of length 32, dimension 9 and minimum distance at least 9.

The Hamming weight enumerator of C' is given below:

$$W_{C'}(y) = 1 + 9y^9 + 9y^{10} + 11y^{11} + 19y^{12} + 41y^{13} + 59y^{14} + 58y^{15} + 77y^{16} + 71y^{17} + 59y^{18} + 51y^{19} + 23y^{20} + 15y^{21} + 9y^{22}.$$

C' is a $[32, 9, 9]_2$ code. The minimum distance bound given in the Theorem 3 is attained. On the other hand C is a $[32, 16, 4]_2$ code.

By taking $g_1(x) = g_2(x) = \cdots = g_l(x)$ in the Theorem 3 we obtain the following corollary.

COROLLARY 2. Let C be a GQC code generated by

$$\overline{f}(x) = (f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x))$$

where $g(x) \in F_q[x]/(x^{m_i} - 1)$. Let $s = \max_{i=1,\ldots,l}\{m_i\}$, $t = \min_{i=1,\ldots,l}\{\deg(h_i(x))\}$ and a_i denote the largest possible consecutive powers of the primitive roots of unity of order m_i.

Then,

1. $\dim(C) = s - \deg(g(x))$,
2. $d(C) \geq \min_{i=1,\ldots,l}\{a_i + 1\}$,
3. If $C' \subset C$ is generated by $\{\overline{f}(x), x\overline{f}(x), x^2\overline{f}(x), \ldots, x^{t-1}\overline{f}(x)\}$, then the dimension of C' is t and

$$d(C') \geq \sum_{i=1}^{l}\{a_i + 1\}.$$

EXAMPLE 3. Let $C = \langle x^2 + x + 1, x^2 + x + 1\rangle$ be a GQC code of length 12 where $q = 2, l = 2, m_1 = 3$ and $m_2 = 9$. In Example 1 we found that $a_1 = 2$. However the zeroes of $g(x) = x^2 + x + 1$ in $x^9 - 1$ differ. $a_2 = 1$. In this case, since $s = \max\{3, 6\} = 6$, C is a GQC code of length 12, dimension 6 and minimum distance at least 2. In fact, the Hamming weight enumerator of this code is

$$W_C(y) = 1 + 7y^2 + 15y^4 + 27y^6 + 12y^8 + 2y^{10}.$$

Again the minimum distance bound is attained.

By part 3 of Corollary 2, C' is a linear code of length 12, dimension 1 and minimum distance at least 5.

In fact, the Hamming weight enumerator of C' is

$$W_{C'}(y) = 1 + y^6.$$

Hence, $d(C') = 6$.

3 Conclusion

We showed that we can determine the critical parameters of generalized quasi cyclic codes and give a BCH type bound. Similar to quasi cyclic codes by taking advantage of the structure of generalized quasi cyclic codes we believe that many new and optimum codes will be constructed. Further, 1 generator generalized quasi cyclic codes are discussed. Though the family of one generator generalized quasi cyclic codes give codes with better minimum distances, the structure of generalized quasi cyclic codes with generators more than one remain to be investigated.

Acknowledgment. We would like to thank the referees for their valuable remarks.

References

[1] Z. Chen, Six new binary quasi-cyclic codes, IEEE Trans. on Information Theory, 40(5)(1994), 1666–1667.

[2] J. Conan and G. Seguin, Structural properties and enumeration of quasi cyclic codes, AAECC, 4(1993), 25–39.

[3] P. P. Greenough and R. Hill, Optimal ternary quasi-cyclic codes, Designs Codes and Cryptography, 2(1992), 81–91.

[4] T. A. Gulliver and V. K. Bhargava, Nine good rate $(m-1)/pm$ quasi-cyclic codes, IEEE Trans. on Information Theory, 38(1992), 1366–1369.

[5] T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4), IEEE Trans. on Information Theory, 38(4)(1992), 1369–1374.

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

[7] J. Little, C. Heegard and K. Saints, Systematic encoding via Groebner bases for a class of algebraic geometric Goppa codes, IEEE Transactions on Information Theory, 41(6)(1995), 1752–1761.

[8] J. Little, C. Heegard and K. Saints, On the structure of Hermitian codes, J. Pure Appl. Algebra 121(1997), 293–314.

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

[10] K. Lally and P. Fitzpatrick, Construction and classification of quasi-cyclic codes, WCC 99, Workshop on Coding and Cryptography January 11-14, PARIS (France), 1999, 11-20.

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

[12] S. Ling and P. Sole, On the algebraic structure of the quasi-cyclic codes I: finite fields, IEEE Trans. Inform. Theory, 47(7)(2001), 2751–2759.

[13] F. J. MacWilliams and N. J. A Sloane, The Theory Of Error Correcting Codes, North-Holland Mathematical Library; 16, 1996.

[14] G.E. Séguin and G. Drolet, The theory of 1-generator quasi-cyclic codes, preprint, 1990.

[15] I. Siap, N. Aydin and D. K. Ray-Chaudhuri, New ternary quasi-cyclic codes with better minimum distances, IEEE Information Theory, 46(4)(2000), 1554–1558.

[16] S. E. Tavares, V. K. Bhargava and S. G. S. Shiva, Some rate $p/(p+1)$ quasi-cyclic codes, IEEE Trans. on Information Theory, 20(1)(1974), 133–135.

[17] C. P. Xing and S. Ling, A class of linear codes with good parameters, IEEE IT, 46(2000), 2184–2188.