New Quasi-Cyclic Codes over GF(8) with Improved Minimum Distances

Irfan Siap, isiap@gantep.edu.tr
Adıyaman Faculty of Education, Gaziantep University, Turkey

Abstract

One of the most important problems of coding theory is to construct codes with the best possible minimum distance. The class of quasi-cyclic codes has proved to be a good source for such codes. In this paper, we use the algebraic structure of quasi-cyclic codes and the BCH type bound introduced in [17] to search for quasi-cyclic codes which improve the minimum distances of the best-known linear codes. We construct 11 new linear codes over $GF(8)$ where 3 of these codes are one unit away from being optimal.

Keywords: Quasi-cyclic codes, new linear codes, new bounds.

1 Introduction

In this paper we apply similar methods introduced in [21] on quasi-cyclic codes over $GF(8)$. We begin with the basic definitions of linear codes and go over some well-known properties of quasi-cyclic codes. Then, we give an example that explains the search method applied for constructing new codes. We conclude by giving the parameters, generator matrices and Hamming weight enumerators of new linear 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 $d(u, v)$ between two vectors $u = (u_1, \ldots, u_n) \in V$ and $v = (v_1, \ldots, v_n) \in V$ is defined by

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

where $d(u, v) := |\{i : u_i \neq v_i\}|$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ 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 1.1 *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.

2 Quasi-Cyclic Codes

Definition 2.1 *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.*

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, [16]. Recently, there has been much research on quasi-cyclic codes. Many record breaking quasi-cyclic codes over finite fields of orders 2,3,4, 5,7,8, and 9 have been discovered. Most can be found in [9], [10], [11], [12], [15], [24], [1], [22], [14], [5], [6],[13], [7], [8], [3], and [21].

Let

$$G_0 = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ g_{m-1} & g_0 & g_1 & \cdots & g_{m-2} \\ g_{m-2} & g_{m-1} & g_0 & \cdots & g_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ g_1 & g_2 & g_3 & \cdots & g_0 \end{bmatrix}. \tag{2}$$

An $(m \times m)$ matrix of the type G_0 is called a circulant matrix of order m or simply a circulant matrix.

If a code C_2 can be obtained from another code C_1 by permuting the coordinate positions, then C_2 is said to be (permutation) equivalent to C_1. It is shown in [23] that the generator matrices of QC codes can be transformed into blocks of circulant matrices by suitable permutation of columns.

Since a code C is l-QC if and only if it is (l,n)-QC [7], ((l,n) denoting the greatest common divisor of n and l) we will assume, without loss of generality, that $l|n$, so that $n = ml$ for some integer m. Note that if $(l,n) = 1$, the code is cyclic.

Similar to the cyclic code case, an l-QC code over F_q of length $n = ml$ can be viewed as an $F_q[x]/(x^m - 1)$ submodule of $(F_q[x]/(x^m - 1))^l$. Then an r-generator QC code is spanned by r elements of $(F_q[x]/(x^m - 1))^l$. 1-generator QC codes have proven to be more suitable for constructing new codes, so, we restrict our search to 1-generator QC codes.

1-Generator QC codes and their structural properties have been studied in [20] and [4], respectively. Recently, in [17] the structure of r-generator QC codes has been investigated by use of Gröbner basis.

Let $1 \leq i \leq l$. For a fixed i consider the following **i^{th} restriction map** on an l-QC code C of length $n = ml$:

$$\Pi_i : (c(1), \ldots, c(ml)) \rightarrow (c(1 + (i-1)m), \ldots, c(m + (i-1)m)).$$

In view of the result in [23] cited above, $\Pi_i(C)$ is a cyclic code for all i.

A well-known result regarding the 1-generator QC codes is the following:

Theorem 2.1 *[20][17] Let C be a 1-generator l-QC code over F_q of length $n = ml$. Then, a generator $g(x) \in (F_q[x]/(x^m - 1))^l$ of C has the following form*

$$g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x)),$$

where $g_i(x)|(x^m - 1)$ and $(f_i(x), (x^m - 1)/g_i(x)) = 1$ for all $1 \leq i \leq l$.

The following theorem which plays an important role in our research has been introduced in [17] also an alternative proof to this theorem is given in [21].

Theorem 2.2 *[17] Let C be a 1-generating l-QC code of length $n = ml$ with the generator of the form:*

$$g(x) = (f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x)) \tag{3}$$

where $g(x)|(x^m - 1), g(x), f_i(x) \in F[x]/(x^m - 1)$, and $(f_i(x), \frac{x^m-1}{g(x)}) = 1$ for all $1 \leq i \leq l$. Let e denote the largest consecutivity among the exponents of the primitive mth root of unity that are roots of $g(x)$. Then,

$$l \cdot (e+1) \leq d(C), \tag{4}$$

and dimension of C is equal to $n - deg(g(x))$.

We have restricted our research to 1-generator QC codes with generators of the following form:

$$(g(x), f_2(x)g(x), \ldots, f_l(x)g(x)).$$

In most cases we have taken $l = 2$. For small dimensions our search for 2-quasi cyclic codes is almost exhaustive. In order to refine the search we have worked with good $g(x)$'s, i.e. $g(x)$'s which give reasonably high minimum distances due to the Theorem 2.2. When choosing $g(x)$ we have compared the BCH bound (Theorem 2.2) with the best-known codes (table of A.E. Brouwer). Having chosen m and $g(x)$, we search for $f_i(x)$, in case $l = 2$ it is only one $f(x)$ with $deg(f(x)) < m - deg(g(x))$ and in this case the search is exhaustive if dimension is not too large. Depending on the degree of $g(x)$, we obtain improvements on minimum distances for some dimensions. We wrote a program in C^{++} to search for $f_i(x)$'s.

Let α be a primitive element of $\mathbb{F}_8^* = \mathbb{F}_8 - \{0\}$ where we take α to be a root of $m_\alpha(x) = x^3 + x + 1$ over $\mathbb{F}_2$. In order to save space, we use the following notation for the elements of $\mathbb{F}_8$:

$$\mathbb{F}_8 = \{\beta = 2^{2a_2} + 2^{a_1} + a_0 | \beta = a_0 + a_1\alpha + a_2\alpha^2, a_i \in \mathbb{F}_2 \text{ and } m_\alpha(\alpha) = 0\}.$$

We explain the search method with the following example:

Example: We take $m = 9$. The degree of the splitting field of $x^9 - 1$ over $GF(8)$ is 2 (that is the multiplicative order of 8 mod 9), and $p(x) = x^6 + x^5 + 1$ is a primitive polynomial of degree 6 over $GF(2)$. Let β be a root of $p(x)$ which is a 63-rd primitive root of unity. Hence, β^7 is a 9^{th} primitive root of unity.

$$x^9 - 1 = \prod_{i=0}^{8}(x - (\beta^7)^i).$$

Let cl_a denote the cyclotomic coset of 8 mod 9 containing a. Then, the cyclotomic cosets of 8 modulo 9 are

$$cl_0 = \{0\}, cl_1 = \{1, 8\}, cl_2 = \{2, 7\}, cl_3 = \{3, 6\}, \text{ and } cl_4 = \{4, 5\}.$$

We pick cl_0 and cl_1 to form the polynomial $g(x) = x^3 + 5x^2 + 5x + 1 \in \mathbb{F}_8[x]$.

Thus, the 3-QC code generated by

$$(g(x), f_1(x)g(x), f_2(x)g(x))$$

where $f_1(x) = 4x + x^2 + 5x^4 + x^5$, and $f_2(x) = 2 + 7x + 3x^2 + 2x^3 + x^4 + x^5$, has minimum distance at least 9 and dimension 6 by Theorem 2.2. As it is apparent from the cyclotomic cosets, this choice is the best possible for forming a polynomial of degree 3 that has the largest consecutivity among the exponents of its roots. Actually, this code has minimum distance 18 and improves the minimum distance of the best-known linear codes for this particular length and dimension.

3 The generator matrices and weight enumerators of new codes

Since a generator matrix of a 1-generator QC code is determined by the first row alone, we give only the first rows of generator matrices, where the blocks will be separated by a comma.

In the representation of the Hamming weight enumerator, $W_C(y)$, the bases will correspond to the weights of codewords and the exponents will correspond to the number of codewords having that particular weight.

1. A $[26, 4, 20]_8$ 2-QC code:

$$(1327337231000, 024213031242).$$

The weight enumerator of this code is

$$0^1 20^{637} 21^{364} 22^{546} 23^{1092} 24^{728} 25^{728}.$$

2. A $[28, 4, 22]_8$ 4-QC code:

$$(7201000, 15464251, 0415156, 6740624).$$

The weight enumerator of this code is

$$0^1 22^{931} 24^{1372} 26^{1617} 28^{175}.$$

3. A $[27, 6, 18]_8$ 3 QC code:

$$(155100000, 264274001, 043747201).$$

The weight enumerator of this code is

$$0^1 18^{1155} 19^{2772} 20^{8253} 21^{17514} 22^{33327} 23^{51912} 24^{62370} 25^{50274} 26^{27342} 27^{7224}.$$

4. A $[30, 6, 20]_8$ 2-QC code:

$$(110011100100000, 342672011614371).$$

The weight enumerator of this code is

$$0^1 20^{2016} 21^{840} 22^{4620} 23^{12600} 24^{21105} 25^{37800} 26^{61740} 27^{51240} 28^{47670} 29^{18480} 30^{4032}.$$

5. A $[38, 6, 28]_8$ 2-QC code:

$$(0017561772745140621, 1776072221245327701).$$

The weight enumerator of this code is

$$0^1 28^{5586} 29^{7182} 30^{14364} 31^{19152} 32^{40698} 33^{50274} 34^{51737} 35^{38836} 36^{24339} 37^{7980} 38^{1995}.$$

6. A $[42, 6, 29]_8$ 2-QC code:

$$(032247041167114234361, 535527467201353475341).$$

The weight enumerator of this code is

$$0^{1}29^{1176}30^{1323}31^{882}32^{4704}33^{8820}34^{19698}35^{36582}36^{36603}37^{49392}38^{49098}39^{32340}40^{14700}41^{5880}42^{945}.$$

7. A $[90, 6, 67]_8$ 2-QC code:

$$(13335517234540167411675131227327347320210000 0,$$
$$340652561712300776144451504742445362764561 21).$$

The weight enumerator of this code is

$$0^{1}67^{133}68^{245}69^{448}70^{868}71^{2184}72^{3451}73^{6440}74^{10101}75^{15729}76^{20993}77^{27013}78^{30933}79^{33089}80^{32921}81^{27265}82^{20986}83^{14210}84^{8701}85^{3969}86^{1736}87^{539}88^{168}89^{21}.$$

8. A $[30, 7, 19]_8$ code:

$$(100010111000000, 742170421325551).$$

The weight enumerator of this code is

$$0^{1}19^{2100}20^{4830}21^{13860}22^{37800}23^{85890}24^{193935}25^{329658}26^{448350}27^{443730}28^{332850}29^{162330}30^{41818}.$$

9. A $[38, 7, 26]_8$ 2-QC code:

$$(1667136317661000000, 17612406373723426 51).$$

The weight enumerator of this code is

$$0^{1}26^{2394}27^{9576}28^{25935}29^{41496}30^{126882}31^{208278}32^{278103}33^{390222}34^{405384}35^{359898}36^{177289}37^{46018}38^{25676}.$$

10. A $[42, 7, 28]_8$ 2-QC code:

$$(207716511207511000 00, 045017276237104324 0561).$$

The weight enumerator of this code is

$$0^{1}28^{1827}29^{588}30^{8085}31^{11613}32^{47481}33^{75411}34^{176106}35^{212562}36^{391167}37^{351330}38^{399105}39^{215649}40^{159348}41^{36015}42^{10864}.$$

11. A $[30, 8, 18]_8$ 2-QC code:

$$(100010110000000, 560656726647257).$$

The weight enumerator of this code is

$0^1 18^{2940} 19^{9030} 20^{32550} 21^{105000} 22^{307440} 23^{758100} 24^{1546965} 25^{2598120} 26^{3473400} 27^{3607030}$
$28^{2721180} 29^{1313760} 30^{301700}$.

Remark: Among these new codes, it has come to our attention that recently the codes # 3 and # 4 are also constructed independently in [25] and [2]. The codes # 1, # 2 and # 5 are one unit away from being optimal.

Definition 3.1 *The largest possible minimum distance for a linear code of length n and dimension k over the finite field of order q is denoted by $d_q[n,k]$.*

Before we conclude with the main theorem we would like to point out that by several methods such as puncturing or shortening these new codes, we obtain further improvements on minimum distances.

Theorem 3.1

$20 \leq d_8[26,4] \leq 21$, $22 \leq d_8[28,4] \leq 23$, $18 \leq d_8[27,6] \leq 20$,
$20 \leq d_8[30,6] \leq 23$, $28 \leq d_8[38,6] \leq 29$, $30 \leq d_8[42,6] \leq 32$,
$70 \leq d_8[90,6] \leq 75$, $19 \leq d_8[30,7] \leq 22$, $26 \leq d_8[38,7] \leq 28$,
$28 \leq d_8[42,7] \leq 32$, *and* $18 \leq d_8[30,8] \leq 21$.

Finally, we would like to thank the referee for his/her valuable suggestions.

References

[1] Viyaj K. Bhargava, Gerald E. Séguin, J.M. Stein, *Some (mk,k) cyclic codes in quasi-cyclic form*, IEEE Trans. on Information Theory, Vol. II-24, No 5, September 1978, p. 630-632.

[2] A.E. Brouwer, *Linear code bound (server)*, Eindhoven University of Technology, The Netherlands, http://www.win.tue.nl/ ~aeb/voorlincod.html.

[3] Zhi Chen, *Six new binary Quasi-Cyclic codes*, IEEE Trans. on Information Theory, Vol. 40, No. 5, September 1994, p. 1666-1667.

[4] Jean Conan and Gerald Seguin, *Structural Properties and Enumeration of Quasi Cyclic Codes*, AAECC 4, p.25-39, (1993).

[5] R.N. Daskalov, T. A. Gulliver and E. Metodieva, *New good quasi-cyclic ternary and quaternary linear codes*, IEEE Trans. on Information Theory, Vol. 43, p. 1647-1650, 1997.

[6] R.N. Daskalov, T. A. Gulliver and E. Metodieva, *New ternary linear codes*, IEEE Trans. Inf. Theory, Vol. 45, No.5, p. 1687-1688, July 1999.

[7] P.P. Greenough and R. Hill, *Optimal ternary quasi-cyclic codes*, Designs Codes and Cryptography, Vol. 2, p. 81-91, 1992.

[8] T. Aaron Gulliver, Vijay K. Bhargava, *Two new rate 2/p binary quasi-cyclic codes*, IEEE Trans. on Information Theory, Vol. 40, No. 5, September 1994, p. 1667-1668.

[9] T. Aaron Gulliver, Vijay K. Bhargava, *Nine good rate (m-1)/pm quasi-cyclic codes*, IEEE Trans. on Information Theory, Vol. 38, No 4, July 1992, p. 1366-1369.

[10] T. Aaron Gulliver, Vijay 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, Vol. 38, No 4, July 1992, p. 1369-1374,

[11] T. Aaron Gulliver, Patrick R.J. Östergard, *Improved bounds for ternary linear codes of dimension 7*, IEEE Trans. on Information Theory, Vol. 43, No 4, July 1997, p. 1377-1381.

[12] T. Aaron Gulliver, Vijay K. Bhargava, *New good rate (m-1)/pm ternary and quaternary quasi-cyclic codes* , Designs Codes and Cryptography, Vol. 7, p. 223-233, 1996.

[13] T. Aaron Gulliver and Patric R.J. Östergard, *New binary linear codes*, Ars Combinatoria, Vol. 56, p.105-112, July 2000.

[14] T. Aaron Gulliver, Vijay K. Bhargava, *Some best rate 1/p quasi-cyclic codes over GF(5)*, Information Theory and Applications II, Springer-Verlag Lecture Notes in Computer Science, Vol. 1133, p. 28-40, Sept. 1996.

[15] T. Aaron Gulliver, *New optimal ternary linear codes of dimension 6*, Ars Combin., Vol. 40, p. 97-108, 1995.

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

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

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

[19] V.S. Pless and W. Huffman (Editors), *Handbook Of Coding Theory*, Volume I, Bounds on the size of linear codes (A.E. Brouwer). 1998.

[20] G.E. Séguin and G. Drolet, *The Theory Of* 1*-Generator Quasi-Cyclic Codes*, preprint 1990.

[21] Irfan Siap, Nuh Aydin and Dijen K. Ray-Chaudhuri, *New Ternary Quasi-Cyclic Codes with Better Minimum Distances*, IEEE Information Theory, Vol. 46 N. 4, p. 1554-1558, July 2000.

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

[23] Koshy Thomas, *Polynomial Approach to Quasi-Cyclic Codes* , Bul. Cal. Math. Soc. 69, p.51-59, (1977).

[24] Henk van Tilborg, *On quasi-cyclic codes with rate 1/m*, IEEE Trans. on Information Theory, Vol. II-24, No 5, September 1978, p. 628-630.

[25] Chaoping Xing, and San Ling, *A Class of Linear Codes with Good Parameters*, IEEE IT, 46, p. 2184-2188, 2000.