J. Algebra Comb. Discrete Appl.
5(2) • 65–70

Received: 9 November 2016
Accepted: 22 November 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

Some new binary codes with improved minimum distances

Research Article

Eric Zhi Chen

Abstract: It has been well-known that the class of quasi-cyclic (QC) codes contain many good codes. In this paper, a method to conduct a computer search for binary 2-generator QC codes is presented, and a large number of good 2-generator QC codes have been obtained. 5 new binary QC codes that improve the lower bounds on minimum distance are presented. Furthermore, with new 2-generator QC codes and Construction X, 2 new improved binary linear codes are obtained. With the standard construction techniques, another 16 new binary linear codes that improve the lower bound on the minimum distance have also been obtained.

2010 MSC: 94B05, 94B65

Keywords: Binary linear codes, Quasi-cyclic codes, Algorithms

1. Introduction

A binary linear $[n, k, d]$ code is a k-dimensional subspace of $\mathrm{GF}(2)^n$, where n is the block length, k the dimension of the code, and d is the minimum distance between any two codewords. The minimum distance determines the error-correcting or error-detecting capability. Therefore, for a given block length n and dimension k, it is desired to have an $[n, k, d]$ code with the minimum distance as large as possible. One of the most fundamental problems in coding theory is to construct codes with the best possible minimum distances.

Grassl [13] maintains online code tables of linear codes for small block length, code dimension over small finite fields. The code tables contain both the lower bounds and upper bounds on the minimum distance. A code with a minimum distance meeting the upper bound is said to be optimal, while a code with a minimum distance meeting the lower bound is called best-known. The problem to construct codes with the best possible minimum distances is shown to be very difficult. For small code dimension and block length, it is possible to do exhaustive computer search for optimal codes. But when both the

Eric Zhi Chen; Department of Computer Science, Kristianstad University, 291 88 Kristianstad, Sweden (email: eric.chen@hkr.se).

code dimension and block length increase, it becomes intractable. The researchers turn to some promising subclasses of linear codes with rich mathematical structures to reduce the search time complexity. During the last decades, the class of quasi-cyclic (QC) codes and quasi-twisted codes has been shown to contain a large number of good codes. With the help of modern computers, a large number of record-breaking QC codes have been constructed [1, 2, 4–7, 10–12, 14–19]. The further improvements on [13] become difficult, and it is even difficult to improve the binary linear codes.

In this paper, a method to construct better binary linear codes is presented. In the next section, a new weight matrix for constructing 2-generator QC codes is presented, and the iterative computer search algorithm is then conducted. In section 3, new binary QC codes that improve the minimum distance in [13] are given, and the well-known Construction X is applied to produce 2 more binary linear codes. With the standard code constructions, 16 more codes that improve the minimum distance in [13] are obtained.

2. Quasi-cyclic codes and their computer constructions

A linear $[n, k, d]$ code C is called cyclic if whenever a codeword $(a_0, a_1, ..., a_{n-1})$ is in C, then so is $(a_{n-1}, a_0, a_1, ..., a_{n-2})$. A code is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword. Therefore, a cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = pm$.

A cyclic matrix is also called a circulant matrix. The circulant matrices are basic components in the generator matrix for a QC code. An $m \times m$ cyclic matrix is defined as

$$A = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\ c_{m-2} & c_{m-1} & c_0 & \cdots & c_{m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix} \tag{1}$$

and the algebra of $m \times m$ cyclic matrices over $GF(2)$ is isomorphic to the algebra in the ring $GF(2)[x]/(x^m - 1)$, if C is mapped onto the polynomial formed by the elements of its first row, $c(x) = c_0 + c_1 x + \cdots + c_{m-1}x^{m-1}$, with the least significant coefficient on the left. The polynomial c(x) is also called the defining polynomial of the matrix C and it is written in octal with least significant coefficients on the right in this paper. The generator matrix of a QC code can be transformed into rows of $m \times m$ circulant matrices by suitable permutation of columns. An h-generator QC code has a generator matrix of the following form:

$$G = \begin{bmatrix} G_{1,1} & G_{1,2} & G_{1,3} & \cdots & G_{1,p} \\ G_{2,1} & G_{2,2} & G_{2,3} & \cdots & G_{2,p} \\ G_{3,1} & G_{3,2} & G_{3,3} & \cdots & G_{3,p} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ G_{h,1} & G_{h,2} & G_{h,3} & \cdots & G_{h,p} \end{bmatrix} \tag{2}$$

where G_{ij} are $m \times m$ circulant matrices, for $i = 1, 2, \cdots, h$, and $j = 1, 2, \cdots, p$. Let $g_{ij}(x)$ be the defining polynomial of the matrix G_{ij}. Then the defining polynomials for the h-generator QC code with generator matrix given in (2) can be written as $(g_{11}(x), g_{12}(x), g_{13}(x), \cdots, g_{1p}(x), \cdots, g_{h1}(x), g_{h2}(x), g_{h3}(x), \cdots, g_{hp}(x))$. In Magma [3], the parameter h is called the height.

Most quasi-cyclic codes studied in the literature are 1-generator QC codes ($h = 1$). Very few studies on h-generator QC codes are found in the literature. In [17], 2 new rate $2/p$ QC codes were presented. In fact, they are 2-generator QC codes. In [6, 10], construction methods have been presented to obtain h-generator QC codes with improved minimum distances.

In the computer search algorithms presented in [7, 14, 15], a weight matrix is used in the computation of the minimum distance of a 1-generator QC code. The general $r \times s$ weight matrix has the following

form:

$$W = \begin{bmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,s-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,s-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{r-1,0} & w_{r-1,1} & \cdots & w_{r-1,s-1} \end{bmatrix} \tag{3}$$

where the entry $w_{i,j}$ is the Hamming weight of $I_i(x)g_j(x)$ mod x^m - 1, $I_i(x)$ is the i-th distinct information polynomial, and $g_j(x)$ is the j-th defining polynomial [14, 15].

As demonstrated in [6, 7, 10], it is often possible to extend the QC codes by adding one or more rows to the generator matrix of a 1-generator QC code. For example, with $m = 57$, a new binary 1-generator QC [228, 18, 96] code was constructed [7], with the defining polynomials $g_1(x)$= 4524727255730403632, $g_2(x)$= 5052140564035060426, $g_3(x)$= 3041362270077724243, and $g_4(x)$= 6624210767535636614. By extending one row, a 2-generator QC [228, 19, 95] code with the following generator matrix

$$\begin{bmatrix} G_1 & G_2 & G_3 & G_4 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

was obtained, where **1** is a vector of 57 1's, and **0** is a vector of 57 0's, and G_i are the circulant matrix defined by the polynomial $g_i(x)$, i = 1, 2, 3, 4. With this motivation, the known good QC codes in [9, 13] have been investigated to obtain good augmented h-generator QC codes, and many good h-generator QC codes have constructed in [10].

The interesting questions to investigate in this paper are: how to do computer search for 2-generator QC codes and will new improved codes be constructed? The general 2-generator QC codes are quite complicated. So in this paper, we study a special form of 2-generator QC codes, as motivated in the last example:

$$\begin{bmatrix} G_{11} & G_{12} & G_{13} & \cdots & G_{1p} \\ G_{21} & G_{22} & G_{23} & \cdots & G_{2p} \end{bmatrix} \tag{4}$$

where the first row of the defining polynomials are for 1-generator QC code, while the second row of defining polynomials are very special, $G_{2j} = 0$ or $1(x) = 1 + x + x^2 + \cdots + x^{m-1}$, for $i = 1, 2, 3, \cdots, p$. We start with derivation of distinct information polynomial $I_i(x)(i = 1, 2, 3, \cdots, r)$, and distinct defining polynomials $g_j(x)(j = 1, 2, 3, \cdots, s)$ as did in [14, 15] for finding 1-generator QC codes. Then we try to extend the code with another row of defining polynomials. So for each possible defining polynomial $g_j(x)$, we have 2 possible combination in constructing 2-generator QC code:

$$\begin{bmatrix} g_j(x) \\ 0 \end{bmatrix}, \begin{bmatrix} g_j(x) \\ 1(x) \end{bmatrix}$$

For the sake of convenience, we write them as $g_i(x)/0$ and $g_i(x)/1(x)$. We arrange all defining polynomials in the order of $g_0(x)/0, g_1(x)/0, g_2(x)/0, \cdots, g_{s-1}(x)/0, g_0(x)/1(x)$, $g_1(x)/1(x)$, $g_2(x)/1(x)$, $\cdots, g_{s-1}(x)/1(x)$. So we obtain the weight matrix as follows:

$$W' = \begin{bmatrix} W & W \\ 0 \cdots 0 & m \cdots m \\ W & M - W \end{bmatrix} \tag{5}$$

It has $2r + 1$ rows, and $2s$ columns, where **W** is the weight matrix calculated as in (3), $0 \cdots 0$ is a vector of all zeros of length s, $m \cdots m$ is a vector of length s and each element has a value of m (generated by all 1's vector), **M** is a $r \times s$ matrix with each entry of value m. The first row of this new weight matrix is from the r distinct information polynomials by only considering the first row in (4); the middle row $[0 \cdots 0 m \cdots m]$ corresponds to the weights generated by 0 and $1(x)$ as the defining polynomials in (4); while the third row $[WM - W]$ is obtained by the considering the combined effect of both rows in (4). With such a block structure, it is only necessary to store an $r \times s$ weight matrix W, since all other

elements of W' are 0, m, or can be calculated from W. With this weight matrix, we apply the iterative search algorithm presented in [7], and many new 2-generator QC codes have been found. Next section will present the new codes with improved minimum distances.

When the code dimension becomes large, this weight matrix becomes too large to be able to reside in a computer memory, and complete the search in reasonable time. As introduced in [8], we reduce the size of the weight matrix by selecting t distinct generator polynomials randomly and compute the $(2r+1) \times (2t)$ weight matrix for constructions of 2-generator QC codes.

3. The new binary codes

With the weight matrix (5) developed in the last section, the iterative search algorithm [7] has been used to conduct the search for good 2-generator QC codes. More than 150 good 2-generator QC codes have been obtained. They can be accessed via the on line database of quasi-twisted codes [9]. In this paper, only the codes that improve the minimum distances on [13] are presented.

Theorem 3.1. *There exist binary QC* $[219, 18, 92]$, $[225, 18, 96]$, $[210, 20, 83]$, $[81, 21, 25]$, $[210, 24, 80]$ *codes.*

Proof. The 1-generator QC $[219, 18, 92]$ code is constructed with $m = 73$, and the defining polynomials $g_1(x) = 3212271004340324237, g_2(x) = 17721056076522411474157$, and $g_3(x) = 3744160632054554\ 3443755$.

The 1-generator QC $[225, 18, 96]$ code is constructed with $m = 45$, and the defining polynomials $g_1(x) = 30426152246431, g_2(x) = 404750035361, g_3(x) = 1342223621127, g_4(x) = 1776673524175$, and $g_5(x) = 36670644573317$.

The 2-generator QC $[210, 20, 83]$ code is constructed with $m = 35$, and the defining polynomials $g_1(x) = 23477263277, g_2(x) = 17461151113, g_3(x) = 1631721217, g_4(x) = 11576655613, g_5(x) = 2267175171, g_6(x) = 14354313511, g_7(x) = g_9(x) = g_{10}(x) = g_{11}(x) = g_{12}(x) = 377777777777$, and $g_8(x) = 0$.

The 2-generator QC $[81, 21, 25]$ code is constructed with $m = 27$, and the defining polynomials $g_1(x) = 273277337, g_2(x) = 14234775, g_3(x) = 132552753, g_4(x) = 0, g_5(x) = 777777777$, and $g_6(x) = 0$.

The 3-generator QC $[210, 24, 80]$ code is constructed with $m = 105$, and the defining polynomials $g_1(x) = 633426413104323015026213710 1, g_2(x) = 437742105045157456452110240725 5, g_3(x) = g_6(x) = 777777777777777777777777777777777777$, and $g_4(x) = g_5(x) = 0$.

The weight distributions of these codes can be found in on line database of quasi-twisted codes [9]. □

The well-known Construction X is a simple and efficient method to construct new codes by combining 3 codes.

Theorem 3.2. *(Construction X) Let* $C_1 = [n, k_1, d_1]$ *and* $C_2 = [n, k_2, d_2]$ *be a pair of nested codes, where* $C_1 \subset C_2$. *Let* $C_3 = [n_3, k_2 - k_1, d_3]$ *be an auxiliary code. Then there exists a* $C = [n + n_3, k_2, d]$ *code with* $d \geq min(d_1, d_2 + d_3)$.

Theorem 3.3. *There exists binary* $[86, 18, 30]$, *and* $[107, 18, 40]$ *codes.*

Proof. Let $m = 21$. With the search method given above, a best-known 2-generator QC $[84, 18, 28]$ code was found. Its defining polynomials are $g_1(x) = 54211, g_2(x) = 26515, g_3(x) = 321125, g_4(x) = 244147, g_5(x) = g_8(x) = 7777777$, and $g_6(x) = g_7(x) = 0$. Let C_1 be its sub-code of dimension 17. It is defined by the first row defining polynomials and is a 1-generator QC $[84, 17, 30]$ code. Let C_2 be the 2-generator QC $[84, 18, 28]$ code, and let C_3 be a binary $[2, 1, 2]$ code. By applying Construction X, we obtain a new binary $[86, 18, 30]$ code.

Let $m = 21$. With the search method given above, a best-known 2-generator QC $[105, 18, 38]$ code was found. Its defining polynomials are $g_1(x) = 77415, g_2(x) = 1525677, g_3(x) = 13427, g_4(x) = 22137, g_5(x) = 141531$, and $g_6(x) = g_7(x) = g_{10}(x) = 0$, and $g_8(x) = g_9(x) = 7777777$. Let C_1 be its sub-code of dimension 17. It is defined by the first row defining polynomials, and is a 1-generator QC $[105, 17, 40]$ code. Let C_2 be the 2-generator QC $[105, 18, 38]$ code and let C_3 be a binary $[2, 1, 2]$ code. By applying Construction X, we obtain a new binary $[107, 18, 30]$ code. □

It should be noted that all the codes given above improve the minimum distances in [13]. By applying standard construction methods, such as puncturing, shortening and extending, 16 more improvements on [13] are obtained. All the codes given in the paper have been checked with the Magma algebraic system [3].

4. Conclusion

In this paper, a construction method for binary 2-generator QC codes is presented and many good new QC codes are obtained. Although it is quite difficult to improve the binary codes, we have made a total of 23 improvements on [13]. It should also be noted that these codes (and ones given in [10]) are only special cases of h-generator QC codes. Further investigation on general h-generator QC codes is promising.

Acknowledgment: The author is grateful to the referees for their helpful comments and suggestions that improved the presentation of the results.

References

[1] N. Aydin, I. Siap, D. K. Ray–Chaudhuri, The structure of 1–generator quasi–twisted codes and new linear codes, Des. Codes Cryptogr. 24(3) (2001) 313–326.
[2] N. Aydin, I. Siap, New quasi–cyclic codes over F_5, Appl. Math. Lett. 15(7) (2002) 833–836.
[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24(3–4) (1997) 235–265.
[4] C. L. Chen, W. W. Peterson, E. J. Weldon Jr., Some results on quasi–cyclic codes, Inform. and Control 15(5) (1969) 407–423.
[5] E. Z. Chen, Six new binary quasi–cyclic codes, IEEE Trans. Inform. Theory 40(5) (1994) 1666–1667.
[6] E. Z. Chen, New quasi–cyclic codes from simplex codes, IEEE Trans. Inform. Theory 53(3) (2007) 1193–1196.
[7] E. Z. Chen, A new iterative computer search algorithm for good quasi–twisted codes, Des. Codes Cryptogr. 76(2) (2015) 307–323.
[8] E. Z. Chen, N. Aydin, A database of linear codes over F_{13} with minimum distance bounds and new quasi–twisted codes from a heuristic search algorithm, J. Algebra Comb. Discrete Appl. 2(1) (2015) 1–16.
[9] E. Z. Chen, Database of quasi–twisted codes, 2017, available at http://www.tec.hkr.se/∼chen/ research/codes
[10] E. Z. Chen, New binary h–generator quasi–cyclic codes by augmentation and new minimum distance bounds, Des. Codes Cryptogr. 80(1) (2016) 1–10.
[11] R. N. Daskalov, T. A. Gulliver, New good quasi–cyclic ternary and quaternary linear codes, IEEE Trans. Inform. Theory 43(5) (1997) 1647–1650.
[12] R. Daskalov, P. Hristov, Some new quasi–twisted ternary linear codes, J. Algebra Comb. Discrete Appl. 2(3) (2015) 211–216.

[13] M. Grassl, Bounds on the minimum distances of linear codes, available at http://www.codetables.de, accessed on November 2, 2016.
[14] T. A. Gulliver, V. K. Bhargava, Some best rate 1/p and rate (p-1)/p systematic quasi–cyclic codes, IEEE Trans. Inform. Theory 37(3) (1991) 552–555.
[15] T. A. Gulliver, V. K. Bhargava, Nine good rate (m-1)/pm quasi–cyclic codes, IEEE Trans. Inform. Theory 38(4) (1992) 1366–1369.
[16] T. A. Gulliver, V. K. Bhargava, Twelve good rate (m-r)/pm quasi–cyclic codes, IEEE Trans. Inform. Theory 39(5) (1993) 1750–1751.
[17] T. A. Gulliver, V. K. Bhargava, Two new rate 2/p binary quasi–cyclic codes, IEEE Trans. Inform. Theory 40(5) (1994) 1667–1668.
[18] I. Siap, N. Aydin, D. K. Ray–Chaudhuri, New ternary quasi–cyclic codes with better minimum distances, IEEE Trans. Inform. Theory 46(4) (2000) 1554–1558.
[19] H. van Tilborg, On quasi–cyclic codes with rate 1/m, IEEE Trans. Inform. Theory 24(5) (1978) 628–630.