Good Quasi-Cyclic Codes Derived From Irreducible Cyclic Codes

Eric Zhi Chen

Email: eric.chen@tec.hkr.se

School of Engineering
Kristianstad University
291 88 Kristianstad
Sweden

2004-06-05

Abstract – As a generalization of cyclic codes, quasi-cyclic codes contain many good linear codes. Extensive search is made and lots of good quasi-cyclic codes are obtained from irreducible cyclic codes. A new binary [95, 13, 40] code which improves the lower bound on the minimum distance, is also constructed.

Index Term — Codes and coding, linear codes, cyclic codes, idempotent, irreducible codes, quasi-cyclic codes

Good Quasi-Cyclic Codes Derived From Irreducible Cyclic Codes

Eric Zhi Chen

School of Engineering, Kristianstad University, 291 88 Kristianstad, Sweden

Abstract – As a generalization of cyclic codes, quasi-cyclic codes contain many good linear codes. Extensive search is made and lots of good quasi-cyclic codes are obtained from irreducible cyclic codes. A new binary [95, 13, 40] code which improves the lower bound on the minimum distance, is also constructed.

Index Term — Codes and coding, linear codes, cyclic codes, idempotent, irreducible codes, quasi-cyclic codes

1. INTRODUCTION

A code is said to be quasi-cyclic if every cyclic shift of a codeword by p positions results in another codeword. Therefore quasi-cyclic (QC) codes are a generalization of cyclic codes with $p = 1$. It has been shown that QC codes contain many good linear codes [1-3]. Unfortunately, there are not many construction methods for good QC codes. Lots of researchers have turned to the power of modern computers, and many good QC codes which improve lower-bounds on the minimum distance of linear codes have been found [4-11]. The author maintains a database of best-known binary QC codes [12], which is searchable via web interface. The problem is that exhaustive computer search is intractable for large code dimension, and/or for large p.

Piret presented a construction of quasi-cyclic codes using irreducible cyclic codes [13, 14] and some good block codes were obtained. In this paper, Piret's method is used to construct 1-generator QC codes [15]. Computer search is conducted and lots of good QC codes are tabulated. A new binary linear [95, 13, 40] code, which improves the lower bound on minimum distance, is also constructed.

The rest of the paper is arranged as follows. Section 2 presents basics on cyclic codes, quasi-cyclic codes. Piret's construction is discussed in Section 3 and many good QC codes are obtained and listed.

2. CYCLIC CODES AND QUASI-CYCLIC CODES

2.1 Cyclic Codes

A binary linear [n, k, d] code is a k-dimensional subspace of an n-dimensional vector space over GF(2), with minimum distance d between any two codewords. A code is said to be cyclic if every cyclic shift of a codeword is also a codeword. A cyclic is described by polynomial algebra. A cyclic [n, k, d] code has a unique generator polynomial g(x). It is a polynomial with degree of n – k. So all codewords of a cyclic are multiples of g(x) modulo $x^n - 1$. A q-ary cyclic [n, k, d] code is also an ideal in the polynomial ring $GF(q)[x]/(x^n - 1)$.

A cyclic code contains a unique idempotent. A polynomial E(x) in the ring $GF(q)[x]/(x^n - 1)$ is an idempotent if $E(x) = E(x)^2 = E(x^2)$.

A minimal ideal is the one which does not contain any smaller nonzero ideal. The corresponding cyclic code is called minimal or irreducible code, and corresponding idempotent is called a primitive idempotent. Irreducible cyclic codes are used to construct good QC codes in this paper.

2.2 Quasi-Cyclic Codes

A code is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is still a codeword. Thus a cyclic code is a QC code with p = 1. The block length n of a QC code is a multiple of p, or $n = m \times p$.

Circulants, or cyclic matrices, are basic components in the generator matrix for a QC code. An $m \times m$ cyclic or circulant matrix is defined as

$$C = \begin{bmatrix} c_0 & c_1 & \cdots & c_{m-1} \\ c_{m-1} & c_0 & \cdots & c_{m-2} \\ c_{m-2} & c_{m-1} & \cdots & c_{m-3} \\ \vdots & \vdots & \cdots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix} \qquad (1)$$

and it is uniquely specified by a polynomial formed by the elements of its first row, $c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1}$, with the least significant coefficient on the left.

Sèguin and Drolet [15] studied 1-generator QC codes. A 1-generator QC code has the following form of the generator matrix:

$$G = [\, G_0 \; G_1 \; G_2 \; \ldots \; G_{p-1} \,] \qquad (2)$$

Where G_i, i= 0,1, 2, …, p-1, are circulants of order m. Let $g_0(x)$, $g_1(x)$, …, $g_{p-1}(x)$ are the corresponding defining polynomials. It was proved [15] that The dimension of an 1-generator QC code is

$$k = m - \text{degree}(\gcd (g_0(x), g_1(x), \ldots, g_{p-1}(x), x^m - 1)) \quad (3)$$

If k = m, then generator matrix in (2) can be put into a systematic form:

$$G = [I \;\; G_1 \;\; G_2 \;\; \ldots \; G_{p-1}] \quad (4)$$

where I is the identity matrix of order m. If k < m, the code generated is called degenerate and only k rows in (2) are linear independent.

3. GOOD QUASI-CYCLIC CODES DERIVED FROM IRREDUCIBLE CYCLIC CODES

3.1 Irreducible Cyclic Codes and Finite Field

The following theorem was proved in [17]

Theorem 1 The irreducible cyclic [n, k] code is isomorphic to the field $GF(2^k)$.

Let $\theta(x)$ be the idempotent of an irreducible cyclic [n, k, d] code. Here k is the smallest integer such that n divides $2^k - 1$. Let ξ be a primitive element of $GF(2^k)$. Let β be a primitive n-th root of unity. Then for any codeword a(x), any isomorphism φ between the irreducible [n, k, d] code and the field $GF(2^k)$ is $a(x)^{\varphi} = a(\beta)$.

Example 1 Consider irreducible cyclic [7, 3, 4] code with idempotent $\theta(x) = 1 + x + x^2 + x^4$. Let ξ be a primitive element of $GF(2^k)$, with primitive polynomial $1 + \xi + \xi^3 = 0$. Let $\beta = \xi, \xi^2$, or ξ^4. We get 3 isomorphic mappings between the [7, 3, 4] code and $GF(2^3)$:

Codeword a(x)							Elements of $GF(2^3)$		
0	1	2	3	4	5	6	$a(\xi)$	$a(\xi^2)$	$a(\xi^4)$
0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	0	0	1	1	1
0	1	1	1	0	1	0	ξ	ξ^2	ξ^4
0	0	1	1	1	0	1	ξ^2	ξ^4	ξ
1	0	0	1	1	1	0	ξ^3	ξ^6	ξ^5
0	1	0	0	1	1	1	ξ^4	ξ	ξ^2
1	0	1	0	0	1	1	ξ^5	ξ^3	ξ^6
1	1	0	1	0	0	1	ξ^6	ξ^5	ξ^3

3.2 Piret's Construction

Piret [13, 14] proposed a construction technique to obtain good QC codes by combining irreducible cyclic codes. To show how it works, we use the discussion in [17].

Given $\theta(x)$, the idempotent of an irreducible cyclic [n, k, d] code, where dimension k is the smallest integer such that n divides $2^k - 1$. Let $N = (2^k - 1) / n$ and ξ be a primitive element of $GF(2^k)$, and let $\alpha = \xi^N$. Thus $\alpha^n = 1$, and the nonzeros of the code can be mapped to elements of the field $GF(2^k)$:

Codeword	↔	Element of $GF(2^k)$
$\theta(x)$	↔	1
$x\,\theta(x)$	↔	α
$\gamma(x)\theta(x)$	↔	ξ

where $\gamma(x)$ is a polynomial that defines the mapping above.

Then any nonzero codeword can be written as

$$\gamma(x)^j\theta(x) \quad \leftrightarrow \quad \xi^j$$

for $0 \le j \le 2^k - 2$. Let $w_j = wt\,(\gamma(x)^j\theta(x))$. Then we have $w_{j+N} = w_j$, since

$$\gamma(x)^{j+N}\theta(x) \leftrightarrow \xi^{j+N} = \alpha\,\xi^j \leftrightarrow x\,\gamma(x)^j\theta(x)$$

So the following polynomials are nonzero codewords for a QC [2n, k] code:

$$|\,\gamma(x)^j\theta(x) \mid \gamma(x)^{j+b}\theta(x)\,|, \quad 0 \le j \le 2^k - 2.$$

To get the best QC [2n, k] code with largest minimum distance, we choose the integer b to maximize

$$d' = \min\,(w_j + w_{j+b}) \quad \text{for} \quad 0 \le j \le N - 1.$$

It is obvious that d' is at least as large as 2d.

3.3 Good QC Codes Obtained by Piret's Construction

vanTilborg [5] presented the exhaustive search method to find best QC codes with k = 7 and 8. The method was modified and used by many other researchers [6-11]. The storage required is in $O((2^k/n)^2)$. It should be noted that the exhaustive search is intractable with the increases in the code dimension and p. The non- exhaustive search is shown to be a time-consuming work. All these approach also requires much storage. The Piret's construction given above does not require much storage. It needs only an array of N elements to keep weights $w_0, w_1, \ldots, w_N$. Or in other word, it requires only $O(2^k/n)$. But Piret's construction may not give the best QC codes for the given parameters, since it does not check for all possible defining polynomials for the QC codes. In this paper, we limit our discussion to the QC codes derived from irreducible cyclic codes.

MacWilliams [16] presented a table of primitive binary idempotents of odd length up to 511. Given $\theta(x)$, the idempotent of an irreducible cyclic [n, k] code, where dimension k is the smallest integer such that n divides 2^k -1. Let $N = (2^k - 1) / n$. We get the polynomial $\gamma(x)$ and compute the weights $w_0, w_1, \ldots, w_N$.

To obtain a good QC [p×n, k, d´] code, we maximize the minimum distance by choosing the integers b_i, i = 1, 2, …, p – 1:

$$d' = \min (w_j + w_{j+b_1} + w_{j+b_2} + ... + w_{j+b_{p-1}}) \qquad \text{for} \quad 0 \le j \le N - 1.$$

The nonzero codewords of the QC [p×n, k, d´] code are

$$| \gamma(x)^j \theta(x) | \gamma(x)^{j+b_1} \theta(x) | ... | \gamma(x)^{j+b_{p-1}} \theta(x) |, \quad 0 \le j \le 2^k - 2.$$

Tables 1-3 list the resulting QC codes and their parameters. In the tables, $\theta(x)$ and $\gamma(x)$ are the idempotent and polynomial defining the mapping used in Piret's construction. They are given in octal. b_i gives the optimal integers that maximize minimum distance of the resulting QC code. The code marked with $^{-t}$ denotes that the minimum distance of the code is t from the best-known or optimal linear binary codes. Weight distributions of these codes can be found in the database of best-known binary QC codes [12].

3.3.1 Irreducible binary [9, 6, 2] code and derived QC codes

Given the irreducible cyclic [9, 6, 2] code with idempotent $\theta(x) = x^3 + x^6$. We have N = 7, $\alpha = \xi^7$, $\gamma(x) = x^3 + x^4 + x^6 + x^8$, and $(w_0, w_1, \ldots, w_6) = (2, 6, 6, 4, 6, 4, 4)$. The best choice for b is 1, and d´ = 6. So a QC [18, 6, 6] code is obtained. Other good QC codes constructed are given in the Table 1. Most of QC codes derived from the cyclic [9, 6, 2] code are optimal.

3.3.2 Irreducible binary [21, 6, 8] code and derived QC codes

Given the irreducible cyclic [21, 6, 8] code with idempotent $\theta(x) = 6462240$ in octal. We have N = 3, and $\gamma(x) = 1 + x$. $(w_0, w_1, w_2) = (8, 12, 12)$. It is simple to construct good QC codes listed in the Table 2, by repeating shorter QC codes, adding one or deleting one defining polynomial.

3.3.3 Other codes

For other irreducible cyclic codes, N is larger and it is not possible to optimize b_i by hand. So a computer program is used to find the best choices for b_i. Good QC codes constructed are listed in the Table 3.

Table 1 Good Binary QC Codes Derived From Irreducible Cyclic [9, 6, 2] Code With θ(x) = 110 and γ(x) = 530

QC Code[n, k, d]	p	b_i
[27, 6, 12]	3	1, 3
[36, 6, 16]	4	1, 2, 3
[54, 6, 26]	6	1, 2, 3, 4, 5
[63, 6, 32]	7	1, 2, 3, 4, 5, 6
[72, 6, 34] $^{-1}$	8	0, 1, 1, 2, 3, 3, 4
[81, 6, 40]	9	0, 1, 1, 2, 3, 3, 4, 5
[90, 6, 44]	10	0, 1, 1, 2, 3, 3,4, 5, 6
[99, 6, 48]	11	0, 0, 1,1, 2, 2, 3, 3, 4, 6
[117, 6, 58]	13	0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6
[126, 6, 64]	14	0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, 6
[135, 6, 66]	15	1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0
[144, 6, 72]	16	0, 0, 1, 1, 1, 2, 2, 3, 3, 3, 4, 4, 5, 5 , 6
[153, 6, 76]	17	0, 1, 1, 1, 2, 2, 3, 3, 4, 4, 5, 0, 3, 5, 6, 6
[162, 6, 80]	18	0, 1, 1, 1, 2, 2, 3, 3, 4, 4, 5, 0, 0, 1, 3, 3, 5
[180, 6, 90]	20	1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5
[189, 6, 96]	21	1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6
[198, 6, 98] $^{-1}$	22	1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0
[207, 6, 104]	23	0, 0, 1, 1, 1, 2, 2, 3, 3, 4, 0, 1, 2, 3, 3, 4, 4, 5, 5, 5, 6, 6
[216, 6, 108]	24	0, 0, 1, 1, 1, 2, 2, 3, 3, 4, 0, 1, 2, 3, 3, 4, 4, 5, 5, 5, 6, 6, 6
[225, 6, 112]	25	0, 1, 1, 1, 2, 2, 3, 3, 3, 4, 4, 5, 0, 0, 0, 1, 1, 2, 3, 3, 4, 5, 5, 6
[243, 6, 122]	27	1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 1, 2, 2, 0, 3, 3, 4, 4, 5, 5, 6
[255, 6, 128]	28	1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6

Table 2 Good Binary QC Codes Derived From Irreducible Cyclic [21, 6,] Code With θ(x) = 6462240 and γ(x) = 3

QC Code [n, k, d]	p	b_i
[42, 6, 20]	2	1
[63, 6, 32]	3	1, 2
[84, 6, 40] $^{-1}$	4	1, 2, 0
[105, 6, 52]	5	1, 2, 0, 1
[126, 6, 64]	6	1, 2, 0, 1, 2
[147, 6, 72] $^{-1}$	7	1, 2, 0, 1, 2, 0
[168, 6, 84]	8	1, 2, 0, 1, 2, 0, 1
[189, 6, 96]	9	1, 2, 0, 1, 2, 0, 1, 2
[210, 6, 104] $^{-1}$	10	1, 2, 0, 1, 2, 0, 1, 2, 0
[231, 6, 116]	11	0, 0, 0, 1, 1, 1, 1, 2, 2, 2
[252, 6, 128]	12	1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2

Table 3 Good Binary QC Codes Derived From Irreducible Cyclic Codes

Code [n, k, d]	QC Code [n, k, d]	p	θ(x)	γ(x)	b_i
[17, 8, 6]	[34, 8, 14]	2	56350	3	5
	[51, 8, 24]	3			5, 10
	[68, 8, 32]	4			1, 3, 7
	[85, 8, 40]	5			0, 5, 7, 13
	[102, 8, 48]	6			0, 5, 5, 10, 10
	[119, 8, 56] $^{-1}$	7			0, 1, 3, 5, 7, 10
	[170, 8, 82] $^{-1}$	10			1, 2, 3, 4, 5, 7, 10, 12, 13
[23, 11, 8]	[69, 11, 28]	3	1231537	3	1, 7
	[92, 11, 40]	4			1, 4, 60
	[161, 11, 72] $^{-1}$	7			1, 20, 43, 48, 66
[39, 12, 12]	[78, 12, 32]	2	7737153551310	40201	15
	[195, 12, 88] $^{-1}$	5			1, 2, 8, 79
[41, 20, 10]	[82, 20, 26]	2	33160255203466	13	253
[51, 8, 24]	[102, 8, 48]	2		3	0
	[255, 8, 128]	5			1, 2, 3, 4
[55, 20, 16]	[110, 20, 40]	2	1516556105172014110	13	1271
	[165, 20, 64]	3			7, 8342
[65, 12, 26]	[130, 12, 56]	2	3312261030550604322466	3	9
	[195, 12, 88] $^{-1}$	3			9, 45
[85, 8, 40]	[255, 8, 128]	3	32343661365571233271666272220	13	1, 2

3.4 A New Binary Linear [95, 13, 40] Code

In many cases, it is possible to add parity-check digits and information digits to a QC code. For binary irreducible cyclic [23, 11, 8] code, θ(x) = 1231537 and γ(x) = 3. A QC [92, 11, 40] code is constructed. A new binary [95, 13, 40] code which improves the lower bound on the minimum distance [18], is constructed. The generator matrix is given below in octal

```
 1231537   3652741  25403257  20725435
 2463276   7525702  13006537   1653073
 5146574  17253604  26015276   3526166
12315370  36527410  14032575   7254354
24632760  35257021  30065372  16530730
11465741  32536043  20152765  35261660
23153702  25274107    325753  32543541
 6327605  12570217    653726  25307303
14657412  25360436   1527654  12616607
31537024  12741075   3257530  25435416
23276051  25702172   6537260  13073035
77777777  77777777  00000000  00000000
77777777  00000000  77777777  00000000
```

The weight distribution of the code is given below:

0__1, 40__1748, 48__5224, 56__1196, 64__23

4. CONCLUSION

As a generalization of cyclic codes, quasi-cyclic codes contain many good linear codes. In this paper, Piret's construction of QC codes by combining irreducible cyclic codes is used to obtain lots of good QC codes. Computer search is made and lots of good quasi-cyclic codes are listed. A new binary [95, 13, 40] code which improves the lower bound on the minimum distance, is also constructed.

REFERENCES

[1] C. L. Chen and W.W. Peterson, "Some results on quasi-cyclic codes", Infom. Contr., vol. 15, pp.407-423, 1969

[2] E. J. Weldon, Jr., "Long quasi-cyclic codes are good", IEEE Trans. Inform. Theory, vol.13,no.1, p.130, Jan. 1970

[3] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2", IEEE Trans. Inform. Theory, vol. IT-20, p.679, 1974

[4] S.E. Tavares, V.K. Bhargava, and S.G.S. Shiva,"Some rate p/(p+1) quasi-cyclic codes", IEEE Trans. Inform.Theory, vol.IT-20, no.1, pp.133-135, Jan. 1974

[5] H.C.A. van Tilborg, "on quasi-cyclic codes with rate 1/m", IEEE Trans. Inform. Theory, vol.IT-24, no.5, pp.628-629, Sept. 1978

[6] T.A. Gulliver and V.K. Bhargava, "Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes", IEEE Trans. Inform.Theory, vol.IT-37, no.3, pp.552-555, May 1991

[7] T.A. Gulliver and V.K. Bhargava, "Nine good (m-1)/pm quasi-cyclic codes", IEEE Trans. Inform.Theory, vol.IT-38, no.4, pp.1366-1369, July 1992

[8] T.A. Gulliver and V.K. Bhargava, "Twelve good rate (m-r)/pm binary quasi-cyclic codes", IEEE IT-39,no.5,pp.1750-1751, 1993

[9] Eric Zhi Chen, "Six new binary quasi-cyclic codes", IEEE Trans. Inform. Theory, vol.IT-40, no.5, pp.1666-1667, Sept. 1994

[10] Eric Zhi Chen, " New Results on Binary Quasi-Cyclic Codes", Proceeding IEEE Intern. Symp. on Information Theory, ISIT2000, Sorrento, Italy, 2000

[11] Petra Heijnen, Henk van Tilborg, Tom Verhoeff, and Sander Weijs, "Some new binary quasi-cyclic codes", IEEE Trans. Inform. Theory, vol. 44, 1994-1996, Sept. 1998

[12] Eric Zhi Chen, Web database of binary QC codes, http://rimula.hkr.se/~chen/research/codes/searchqc2.htm

[13] P. Priet, "Good block codes derived from cyclic codes", Electronics Letters, vol 10, no.18, pp. 391—392, Sept. 1974

[14] P. Priet, "Structure and constructions of cyclic convolutional codes", IEEE Trans. Inform. Theory, vol. IT-22, no. 2, pp.147—155, March 1976

[15] G. E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes", manuscript, Dept of Electr. and Comp. Eng., Royal Military College of Canada, Kingston, Ontario, June 1990

[16] F. J. MacWilliams, "A table of primitive binary idempotents of odd length n, 7=n=511", IEEE Trans. Inform. Theory, vol. IT-25, no. 1, pp. 118—121, Jan. 1979

[17] F. J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, North Holand, Amsterdam, 1977
[18] A. E. Brouwer, “Bounds on the minimum distance of linear codes (http://www.win.tue.nl/~aeb/voorlincod.html)”, Eindhoven Univ. Technol., Eindhoven, The Netherlands