Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 59-64*

On the binary quasi-cyclic codes

Stefka Bouyuklieva stefka@uni-vt.bg
Faculty of Mathematics and Informatics, Veliko Tarnovo University,
and Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
5000 Veliko Tarnovo, Bulgaria
Iliya Bouyukliev[1] iliya@moi.math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. In this paper we present a description of quasi-cyclic codes which relies on matrices and gives an efficient algorithm for their construction.

1 Introduction

A code is said to be quasi-cyclic if every cyclic shift of a codeword by s positions results in another codeword ($s \geq 1$). If $s = 1$ the code is cyclic and therefore quasi-cyclic (QC) codes actually are a generalization of cyclic codes. Many such codes have been discovered with minimum distance exceeding that previously known for any linear code of the same length and dimension, or, indeed, taking the maximum possible value. Eric Chen maintains a database of best-known binary QC codes [5].

There are many construction methods for good QC codes. Generally, a QC code of length lm and index l may be represented as the row space of a block matrix, each row of which has the form $(G_1, \ldots, G_l)$, where G_i is an $m \times m$ circulant. These rows, or the equivalent polynomial vectors, are conventionally called "generators". A method for constructing 1-generator quasi-cyclic codes was given by van Tilborg in [10], as well as the results of an exhaustive computer search for such codes over the binary alphabet, for $m = 7, 8$ and length up to 120. Some 1, 2 and 3-generator QC codes are constructed by Chen [2, 3].

QC codes have rich algebraic structure and therefore there are very interesting theoretical results. A trace description of QC codes using modules has been given by Séguin and Drolet in [9]. Another approach employs Gröbner bases [6]. Ling and Solé have introduced another algebraic approach [7].

In this paper we present a description of quasi-cyclic codes which is close to the Piret construction [8], because it uses irreducible cyclic codes, but relies on matrices and gives an efficient algorithm for their construction.

[1] The research of this author is partially supported by the Bulgarian NSF under Contract I01/0003/2012

2 Irreducible cyclic codes

We begin with the usual definition of irreducible cyclic codes, and then switch to an alternative which is more useful for our investigations.

Definition 1. *Let $f(x)$ be an irreducible divisor of x^n-1 over $\mathbb{F}_q$ where $(q,n)=1$. The cyclic code of length n over $\mathbb{F}_q$ generated by $(x^n-1)/f(x)$ is called an irreducible (or minimal) cyclic code.*

Definition 2. *Let n be a divisor of q^s-1 and let γ be a primitive n-th root of unity in $K=\mathbb{F}_{q^s}$. Then*

$$C(q,s,r)=C_\gamma=\{(Tr(\xi),Tr(\xi\gamma),\ldots,Tr(\xi\gamma^{n-1}))\mid \xi\in K\}$$

is called an irreducible cyclic code over $\mathbb{F}_q$ $(r=(q^s-1)/n)$.

Remark 1: The dimension of C_γ is $k=ord_n(q)$. Moreover, every irreducible cyclic $[n,k]$ code is isomorphic to the field $GF(q^k)$.
Remark 2: These two definitions are equivalent even when γ is a nonprimitive n-th root of unity, but in that case the codewords of C_γ are periodic with period $ord(\gamma)$. Such codes are called degenerate in [1].

We use a different representation of the irreducible cyclic codes. Let $K=\mathbb{F}_{q^s}$ be a finite field and α be its primitive element. Let $q^s-1=m\cdot r$ and $\beta=\alpha^r$. If $G=\langle\beta\rangle<K^*$ then G is a cyclic group of order m and $G,\alpha G,\alpha^2G,\ldots,\alpha^{r-1}G$ are all different cosets of G in K^*.

For $a\in\mathbb{Z}_r$ we define two circulant $m\times m$ matrices with i,j-th entry:

$$D_a[i,j]=Tr(\alpha^a\beta^{j-i})\quad\text{and}\quad C_a[i,j]=Tr(\alpha^{r(i+j)+ma})=Tr(\alpha^{ma}\beta^{i+j}).$$

When m and r are coprime, the matrices C_a correspond to the different cosets of G in K^*. In the next statements we will consider the matrices C_a.

Lemma 1. *If m and r are coprime, the code $C(0)$ whose nonzero codewords are the rows of the matrix*

$$\begin{pmatrix} C_0\\ C_1\\ \vdots\\ C_{r-1}\end{pmatrix}$$

is an irreducible cyclic code of length m and dimension $ord_m(q)$.

Proof. We take $\gamma=\beta=\alpha^r$. The i-th row of the circulant C_a is

$$(Tr(\alpha^{ma}\beta^i),Tr(\alpha^{ma}\beta^{i+1}),\ldots,Tr(\alpha^{ma}\beta^{i+m-1}))$$

$$=(Tr(\alpha^{ma}\beta^i),Tr(\alpha^{ma}\beta^i\beta),\ldots,Tr(\alpha^{ma}\beta^i\beta^{m-1}))$$

$$= (Tr(\xi), Tr(\xi\beta), \dots, Tr(\xi\beta^{m-1}))$$

where $\xi = \alpha^{ma}\beta^i = \alpha^{ma+ir}$. Hence $C(0) \subseteq C_\beta = C(q,s,r)$.

In the other hand, if $\xi \in K^*$ then $\xi = \alpha^b$ for some $b \in \{0, 1, \dots, q^s - 2\}$. Now, because of the Chinese remainder theorem, and because m and r are coprime, b can be written uniquely as $b = ri + ma$ for some $0 \le a \le r-1$ and $0 \le i \le m-1$. Thus

$$(Tr(\xi), Tr(\xi\beta), \dots, Tr(\xi\beta^{m-1})) = (Tr(\alpha^{ma}\beta^i), Tr(\alpha^{ma}\beta^{i+1}), \dots, Tr(\alpha^{ma}\beta^{i+m-1}))$$

is the i-th row of the matrix C_a. It follows that $C(0) = C_\beta$ and so $C(0)$ is an irreducible cyclic code. □

In [2] Eric Chen uses simplex codes to construct 2-generator and 3-generator QC codes, and in [3] he obtains good quai-cyclic codes from irreducible cyclic codes. We also use irreducible cyclic codes and the simplex code but in a different way.

From now on we consider only the binary case, so $K = \mathbb{F}_{2^s}$, $2^s - 1 = mr$ where m and r are coprime.

Lemma 2. *The code whose nonzero weights are the rows of the matrix*

$$M = \begin{pmatrix} C_0 & C_1 & \dots & C_{r-1} \\ C_1 & C_2 & \dots & C_0 \\ & & \vdots & \\ C_{r-1} & C_0 & \dots & C_{r-2} \end{pmatrix} \tag{1}$$

is the simplex $[2^s - 1 = mr, s, 2^{s-1}]$ *code.*

Proof. Let see how the element $M[i,j]$ looks like. If $i = mi_1 + i_2$, $j = mj_1 + j_2$, $0 \le i_1, j_1 \le r-1$, $0 \le i_2, j_2 \le m-1$,

$$M[i,j] = C_{i_1+j_1}[i_2, j_2] = Tr(\alpha^{r(i_2+j_2)+m(i_1+j_1)}) = Tr(\alpha^{(mi_1+ri_2)+(mj_1+rj_2)}).$$

Since m and r are coprime, for a fixed i the exponents $(mi_1 + ri_2) + (mj_1' + rj_2')$ and $(mi_1 + ri_2) + (mj_1'' + rj_2'')$ are different for $j' = mj_1' + j_2' \neq j'' = mj_1'' + j_2''$, where $j', j'' \in \{0, 1, \dots, mr-1\}$. Hence the i-th row consists of the traces of all nonzero elements of the field, and this holds for all $i = 0, 1, \dots, mr-1$. The same is true for the columns of this matrix. Therefore we can reorder the rows and the columns of M and obtain the matrix $M' = (Tr(\alpha^{i+j}))_{i=0,\dots,mr-1; j=0,\dots,mr-1}$. It is easy to see that the rows of M' are the different codewords of a linear constant weight code, which is essentially the simplex $[2^s - 1 = mr, s, 2^{s-1}]$ code. □

3 QC codes - a cyclotomic description

A code is quasi-cyclic if every cyclic shift of a codeword by s positions results in another codeword. We can define this in the following way.

Definition 3. *Let T be the cyclic shift operator on $\mathbb{F}_q^n$. A quasi-cyclic (QC) code is a linear subspace of $\mathbb{F}_q^n$ invariant under T^r for some integer r. The smallest such positive integer r is called the index of the code.*

A trace description of QC codes using modules has been given by Séguin and Drolet in [9]. Moreover, they have introduced the notion of an irreducible quasi-cyclic code. Our approach is different because we don't use modules but only matrices.

Let $0 \leq a_1 < a_2 < \cdots < a_t \leq r-1$. We investigate the code $C(a_1, a_2, \dots, a_t)$ whose nonzero weights are the rows of the matrix

$$\begin{pmatrix} C_{a_1} & C_{a_2} & \dots & C_{a_t} \\ C_{a_1+1} & C_{a_2+1} & \dots & C_{a_t+1} \\ & & \vdots & \\ C_{a_1+r-1} & C_{a_2+r-1} & \dots & C_{a_t+r-1} \end{pmatrix},$$

where $a_i + l$ is taken modulo r. It is easy to see that $C(a_1, \dots, a_t)$ can be obtained by selecting the columns $a_1, \dots, a_t$ from the block matrix M given in (1), and therefore it is linear (after adding the zero vector). Since the matrices C_{a_i+l} are circulants, it is a quasi-cyclic code of length mt.

The following theorem gives some equivalences between the codes of the defined type.

Theorem 1. *The following transformations send the code $C(a_1, a_2, \dots, a_t)$ to an equivalent one:*

(i) a permutation of the column-circulants: $C(a_1, \dots, a_t) \approx C(a_{1\sigma}, \dots, a_{t\sigma})$, $\sigma \in S_t$;

(ii) a cyclic shift with l positions to each circulant: $C(a_1, a_2, \dots, a_t) = C(a_1 + l, a_2 + l, \dots, a_t + l)$, $0 \leq l \leq r-1$;

(iii) a substitution $x \to x^2$ (Frobenius isomorphism): $C(2a_1, 2a_2, \dots, 2a_t) \approx C(a_1, a_2, \dots, a_t)$.

From the second condition in the theorem we have

$$C(a_1, a_2, \dots, a_t) = C(0, a_2 - a_1, \dots, a_t - a_1).$$

We have realized this construction method and have obtained many results but here we give only two examples.

Example 1. Let $k = 6$. Since $2^6 - 1 = 63 = 7 \cdot 9$, we take $m = 9$, $r = 7$. Using Theorem 1, we have $C(a_1, a_2) \approx C(0, a_2 - a_1)$ and

$$C(0,1) \approx C(0,2) \approx C(0,4) \approx C(0,3) \approx C(0,6) \approx C(0,5).$$

Hence there is a unique code for $t = 2$, and this is the binary [18,6,6] code.

For $t = 3$ we have $C(0,1,3) \approx C(0,2,6) \approx C(0,4,5)$, $C(0,1,5) \approx C(0,4,6) \approx C(0,2,3)$, and $C(0,1,2) \approx C(0,2,4) \approx C(0,1,4) \approx \cdots$

These codes have length $n = 27$ and dimension $k = 6$. The codes $C(0,1,3)$, $C(0,1,5)$ and $C(0,1,2)$ are inequivalent. We list their weight enumerators and the order of their automorphism groups.

$1 + 9y^{10} + 9y^{12} + 27y^{14} + 18y^{16}, |Aut(C)| = 18$

$1 + 36y^{12} + 27y^{16}, |Aut(C)| = 51840$

$1 + 27y^{12} + 27y^{14} + 9y^{18}, |Aut(C)| = 1296$

Example 2. Let $k = 8$. Since $2^8 - 1 = 255 = 15 \cdot 17$ we can take $m = 17$, $r = 15$. The number of the constructed codes is written in the following table. In the third row we present the number of the obtained optimal codes, and in the next row we give the minimum distances of the optimal codes of corresponding length and dimension 8.

t	2	3	4	5	6	7
inequivalent codes	3	10	27	56	91	115
optimal codes	1	1	1	1	3	-
d	14	24	32	40	48	57
two-wight codes	-	1	1	1	2	1

We see in the table, that there are two-weight quasi-cyclic codes in almost all cases. There are constructions especially for two-weight quasi-cyclic codes (see for example [4]). So it is an interesting question when a quasi-cyclic code constructed with the proposed method, is also a two-weight code.

QC codes - open problems

Nevertheless we started this project three years ago, we didn't work on it some time. Recently we decided to continue our research on quasi-cyclic codes because there are many open problems regarding our approach and the quasi-cyclic codes in general. We list some of these problems.

- A sequence of the transformations from Theorem 1 is a sufficient condition for equivalence of two binary QC codes. When the products of these three transformations give a necessary condition for equivalence?

- What is going on when $m < k$?

- Is the theory for $q > 2$ the same?
- Are there Balanced weight distribution quasi-cyclic codes?
- What about two-weight irreducible quasi-cyclic codes?

Acknowledgments. The authors would like to thank Cris Coolsaet for the useful discussions on the subject during their visit to the University of Ghent.

References

[1] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[2] E. Z. Chen, New quasi-cyclic codes from simplex codes, *IEEE Trans. Inform. Theory,* **53**, 1193–1196, 2007.

[3] E. Z. Chen, Good quasi-cyclic codes derived from irreducible cyclic codes, *Proc. of Optimal Codes and Related Topics (OC2005)*, Pamporovo, Bulgaria, June 17-23, 2005, 74–81.

[4] E. Z. Chen, Constructions of quasi-cyclic two-weight codes, *Proc. of the tenth International Workshop on Algebraic and Combinatorial Coding Theory*, Zvenigorod, Russia, Septemper, 2006, 56–59.

[5] E. Z. Chen, Web Database of Binary QC Codes [Online]. Available: http://www.tec.hkr.se/ chen/research/codes/searchqc2.htm

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

[7] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: Finite fields, *IEEE Trans. Inform. Theory*, **47**, 2751–2760, 2001.

[8] P. Piret, Structure and constructions of cyclic convolutional codes, *IEEE Trans. Inform. Theory*, **22**, 147–155, 1976.

[9] G. E. Séguin, G. Drolet, The Trace Description of Irreducible Quasi-Cyclic Codes, *IEEE Trans. Inform. Theory,* **36**, 1463–1466, 1990.

[10] H. C. A. van Tilborg, On quasi-cyclic codes with rate $1/m$, *IEEE Trans. Inform. Theory,* **24**, 628–630, 1978.