http://fbe.trakya.edu.tr/tujs
Trakya Univ J Sci, 9(2):87-96, 2008
ISSN 1305–6468
DIC: 250YÇET1560812080109

Derleme/ Review

SOME QUASI-CYCLIC CODES OVER $GF(3)$ AND $GF(7)$

Yasemin ÇENGELLENMİŞ, Hülya İŞCAN, Figen ÖKE

Trakya University, Department of Mathematics, Edirne TURKEY
E-mail: ycengellenmis@yahoo.com, hiscan@trakya.edu.tr, figenoke@gmail.com

Alınış: 25 Mart 2008
Kabul Ediliş: 15 Haziran 2008

Abstract : *Any cyclic code with n=pm length can be put into quasi-cyclic form ,where* $p\neq 1$, $p,m\in Z_+$.
In this paper, some parameters of the Quasi-Cyclic codes over ***GF(3)*** *and* ***GF(7)*** *are obtained by using the best known cyclic codes.*
Keywords: *Cyclic codes, GF(q), Quasi-cyclic codes.*

GF(3) ve GF(7) üzerindeki yarı-devirli kodlar

Özet: p, m *pozitif tamsayılar ve* $p\neq 1$ *olmak üzere* $n = pm$ *uzunluğundaki devirli kodlar yarı-devirli formuna dönüştürülebilir. Bu makalede iyi bilinen devirli kodlar kullanılarak* ***GF(3)*** *ve* ***GF(7)*** *üzerinde yarı-devirli kodların bazı parametreleri elde edildi.*
Anahtar kelimeler: *Devirli kodlar, Yarı-devirli kodlar.*

Introduction

Quasi-Cyclic (QC) codes contain many good linear codes. But unfortunately, there aren't many construction methods for good QC codes. Some researchers used computers to get good QC codes $[3,4]$. Some researchers used the relation between the codes over $IF_p[x]/\langle x^2-1\rangle$ and IF_p where p is a prime, they obtained the new codes over IF_p which improve the best known minimum distance bounds of some linear codes $[6]$. In [2], there is another method to obtain good Quasi-cyclic codes.

It was shown that any cyclic code of composite length can be put into quasi cyclic form and obtained many new good QC codes over IF_2. More general, t-generator QC codes were discussed in $[2]$.

In this paper, we obtained some parameters of the QC codes over $GF(3)$ and $GF(7)$, by using the method in $[2]$.

Through this paper n, p, m are positive integers where $p\neq 1$.

Let A be a $n\times n$ circulant matrix where $n = pm$. Let us denote the polynomial corresponding to the first row of A by $a(x) = a_o + a_1x............+ a_{pm-1}x^{pm-1}$. Then

$$A=\begin{bmatrix} a_0 \quad a_1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots a_{pm-1} \\ a_{pm-1}a_0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots a_{pm-2} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_1 \quad a_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots a_0 \end{bmatrix}$$

If a_i corresponds to the element $a_{(q,r)}$, where $q = \left\lfloor \frac{i}{p} \right\rfloor$, $r \equiv i(\bmod p)$, for each $i \equiv 0,1,......pm-1$,

then $a(x)$ can be written as:

$$a(x) = a_{(0,0)} + a_{(0,1)}x + ... + a_{(0,p-1)}x^{p-1} + a_{(1,0)}x^{p} + ... + a_{(1,p-1)}x^{p-1} + \\ ... + a_{(m-1,0)}x^{(m-1)p} + ...a_{(m-1,p-1)}x^{pm-1}$$

If the rows and columns of A are reordered, then the matrix C is obtained and it can be written as follows;

$$C=\begin{bmatrix} c_0(x) & c_1(x) \text{ .... } c_{p-1}(x) \\ xc_{p-1}(x) & c_0(x) \text{ .... } c_{p-2}(x) \\ xc_{p-2}(x) & xc_{p-1}(x) \text{ .... } c_{p-3}(x) \\ xc_1(x) & xc_2(x) \text{ .... } c_0(x) \end{bmatrix}$$

where $c_i(x) = a_{(0,i)} + a_{(1,i)}x + a_{(2,i)}x^2 + ...a_{(m-1,i)}x^{m-1}$ for $i = 0,1,..., p-1$.

The polynomials $c_0(x), c_1(x),......., c_{p-1}(x)$ are derived from the defining polynomial $a(x)$ and these p polynomials specify the matrix C. In this way, a circulant matrix can be decomposed into a matrix of smaller circulant matrices. This method was given in [2].
It can be given an example to this decomposition as follows.

Example 1: The polynomial $a(x) = 1 + 2x + 2x^3 + 2x^4 \in GF(3)[x]$ uniquely specifies the circulant matrix A of order 8 :

$$A = \begin{bmatrix} 1&2&0&2&2&0&0&0 \\ 0&1&2&0&2&2&0&0 \\ 0&0&1&2&0&2&2&0 \\ 0&0&0&1&2&0&2&2 \\ 2&0&0&0&1&2&0&2 \\ 2&2&0&0&0&1&2&0 \\ 0&2&2&0&0&0&1&2 \\ 2&0&2&2&0&0&0&1 \end{bmatrix}$$

Reordering the rows and columns of A, following matrices of circulants of order 4 and 2 respectively are obtained.
$c_0(x) = 1 + 2x^2$, $c_1(x) = 2 + 2x$ for $p = 2,\ m = 4$.

$$A_1 = \begin{bmatrix} 1\,0\,2\,0 & 2\,2\,0\,0 \\ 0\,1\,0\,2 & 0\,2\,2\,0 \\ 2\,0\,1\,0 & 0\,0\,2\,2 \\ 0\,2\,0\,1 & 2\,0\,0\,2 \\ & \\ 0\,2\,2\,0 & 1\,0\,2\,0 \\ 0\,0\,2\,2 & 0\,1\,0\,2 \\ 2\,0\,0\,2 & 2\,0\,1\,0 \\ 2\,2\,0\,0 & 0\,2\,0\,1 \end{bmatrix}$$

$c_0(x) = 1 + 2x$, $c_1(x) = 2$, $c_2(x) = 0$, $c_3(x) = 2$ for $p = 4$, $m = 2$.

$$A_2 = \begin{bmatrix} 1\,2 & 2\,0 & 0\,0 & 2\,0 \\ 2\,1 & 0\,2 & 0\,0 & 0\,2 \\ 0\,2 & 1\,2 & 2\,0 & 0\,0 \\ 2\,0 & 2\,1 & 0\,2 & 0\,0 \\ 0\,0 & 0\,2 & 1\,2 & 2\,0 \\ 0\,0 & 2\,0 & 2\,1 & 0\,2 \\ 0\,2 & 0\,0 & 0\,2 & 1\,2 \\ 2\,0 & 0\,0 & 2\,0 & 2\,1 \end{bmatrix}$$

These matrices can be specified by matrices of polynomials:

$$A_1(x) = \begin{bmatrix} 1 + 2x^2 & 2 + 2x \\ x(2 + 2x) & 1 + 2x^2 \end{bmatrix}$$

$$A_2(x) = \begin{bmatrix} 1 + 2x & 2 & 0 & 2 \\ 2x & 1 + 2x & 2 & 0 \\ 0 & 2x & 1 + 2x & 2 \\ 2x & 0 & 2x & 1 + 2x \end{bmatrix}$$

An $[mp, k]$ code is said to be QC with basic block length p if every cyclic shift of a codeword by p positions is also a codeword. A general form of generator matrix for a t-generator QC code is given as follows;

$$G = \begin{bmatrix} G_{11}\ G_{12}\ \dots\dots\dots\ G_{1p} \\ G_{21}\ G_{22}\ \dots\dots\dots .G_{2p} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ G_{t1}\ G_{t2}\ \dots\dots\dots\ G_{tp} \end{bmatrix}$$

where G_{ij} is a circulant matrix of order m. Let $K=(k_1,k_2,...k_t)$ be the dimension vector. Then the dimension of t-generator QC $[mp,k]$ code is $k=k_1+k_2+....k_t$. The $k\times n$ generator matrix is formed by k_i rows from the i-th row of the circulants spans the t-generator QC code, $i=1,2,...,t$.

The two theorems in $[2]$ will be given about finding the dimension vector and getting the 1-generator Quasi-Cyclic codes.

Theorem 1: Let C be a $[n,k]$ cyclic code of composite length $n.$ A p-generator QC $[n,k]$ code of dimension vector $K=((k_0+1)\times r_1, r_2\times k_0)$ where $k_0=\left\lfloor \frac{k}{p} \right\rfloor,\ r_1=k-pk_0\ \ and\ \ r_2=p-r_1$ $[2]$.

Example 2: It is known that $a(x)=1+2x+2x^3+2x^4$ is the a generator polynomial of the cyclic $[8,4]$ code over $GF(3)$. So the dimension vector of 4-generator QC $[8,4]$ code is $(4\times 1)=(1,1,1,1)$, since $k_0=\left\lfloor \frac{4}{4} \right\rfloor=1,\ r_1=0,\ r_2=4$ and the dimension vector of 2-generator QC $[8,4]$ code is $(2\times 2)=(2,2)$, since $k_0=\left\lfloor \frac{4}{2} \right\rfloor=2,\ r_1=0,\ r_2=2$.

Theorem 2: Given a cyclic $[n,k]$ code C of composite length n. A 1-generator QC $[n,k]$ code can be obtained if

$$k=m-\deg(\gcd(g_0(x),g_1(x),.........g_{p-1}(x),x^m-1))=m-\deg(h(x))$$

where $g_i(x)$ are p generator polynomials derived from the generator polynomial $g(x)$ of C $[2]$.

When $k>m-\deg(\gcd(g_0(x),g_1(x),.........,g_{p-1}(x),x^m-1))$, then obtaining a 1-generator QC code is not possible. It is obtained t-generator QC codes with the procedure which is dealt with in $[2]$. •

By using the computer, we have determined the generator polynomials $g(x)$ of cyclic codes over $GF(3)$ and $GF(7)$ of composite length. Then, using the method in [2], t-generator QC codes are obtained from best-known cyclic codes over $GF(3)$ and $GF(7)$. t-generator QC codes that are not in www.codetables.de/ are given in the Table 1-2-3-4-5-6.

1– generator QC codes over GF(3)

QC code	m	$g(x)$	$g_i(x)$	$h(x)$
[8,2,6]	4	$1+2x+2x^2+2x^4+x^5+x^6$	$1+2x+2x^2+x^3,2+x^2$	x^2+2
[8,3,5]	4	$1+x+x^2+2x^3+x^5$	$1+x,1+2x+x^2$	$1+x$
[16,2,12]	8	$2+x+x^2+x^4+2x^5+2x^6$ $+2x^8+x^9+x^{10}+x^{12}$ $+2x^{13}+2x^{14}$	$2+x+x^2+2x^3+2x^4+x^5$ $+x^6+2x^7,1+2x^2+x^4$ $2x^6$	$2x^6+x^4$ $+2x^2+1$
[20,4,12]	5	$2+x+2x^2+2x^4+2x^5$ $+2x^6+x^{10}+2x^{11}+x^{12}$ $+x^{14}+x^{15}+x^{16}$	$2+2x+x^3+x^4,1+2x,2+2x$ $+x^2+x^3,2x^2+x^3$	$x-1$
[22,10,9]	11	$2+x+x^3+2x^4+x^6+2x^8$ $+2x^9+2x^{11}+2x^{12}$	$2+2x^2+x^3+2x^4+2x^6,1+x$ $+2x^4+2x^5$	$x-1$

TABLE 1

2-generator QC codes over $GF(3)$

$QC\,code$	m	$g(x)$	$g_i(x)$	$h(x)$	K
$[8,3,5]$	2	$1+x+x^2+2x^3+x^5$	$1,1+x,1,2$	1	(2,1)
$[8,4,4]$	2	$1+2x+2x^3+2x^4$	$1+2x,2,0,2$	1	(2,2)
$[16,3,10]$	2	$2+2x+2x^2+x^3+2x^5$ $+2x^6+2x^8+2x^9+2x^{10}$ $+x^{11}+2x^{13}$	$2+2x,2+2x,2+2x,$ $1+x,0,2+2x,2,0$	1	(2,1)
$[16,7,6]$	4	$1+x+x^3+x^4+x^5$ $+2x^6+2x^9$	$1+x,1+x+2x^2,2x,1$	1	(4,3)
$[20,4,12]$	4	$2+x+2x^2+2x^4+2x^5$ $+2x^6+x^{10}+2x^{11}+x^{12}$ $+x^{14}+x^{15}+x^{16}$	$2+2x+x^2+x^3,1+2x$ $+2x^2+x^3,2+x^2,0,2+x^2$	$2+x^2$	(2,2)
$[20,6,10]$	5	$1+2x+2x^2+x^3+x^6+x^8$ $+x^{11}+2x^{12}+x^{13}+x^{14}$	$1+x^2+2x^3,2+x^3,2$ $+x+x^3,1+x^2$	1	(5,1)

TABLE 2

t- generator QC codes over $GF(3)$ ($t \geq 3$)

$QC\,code$	m	$g(x)$	$g_i(x)$	$h(x)$	K
[8,4,4]	4	$1+2x+2x^3+2x^4$	$1+2x^2, 2+2x$	1	(1,1,1,1)
[8,5,3]	2	$1+x+x^3$	1,1,0,1	1	(2,2,1)
[20,4,12]	2	$2+x+2x^2+2x^4+2x^5+2x^6+$ [illegible] $+2x^{11}+x^{12}+x^{14}+x^{15}+x^{16}$	$2+x,1+2x,2+x,0,2+$ [illegible] $2+x,2+x,0,0,0$	$x+2$	(1,1,1,1)
[20,6,10]	2	$1+2x+2x^2+x^3+x^6+x^8$ $+x^{11}+2x^{12}+x^{13}+x^{14}$	$1, x+2, 2+2x, 1+x, x, 0$ [illegible] 1,0,1,0	1	(2,2,2)
[22,5,12]	2	$1+x^2+x^3+2x^4+x^5+x^6+2x^{1}$ [illegible] $+2x^{13}+2x^{14}+x^{15}+2x^{16}+2x^{17}$	$1+2x,0,1+2x,1+2x,$ $2+x,1+2x,1+2x,0,0,$ [illegible]	$x+2$	(1,1,1,1,1)
[22,6,12]	2	$1+x+x^2+x^3+x^6+2x^7$ $+x^8+2x^9+x^{10}+2x^{12}$ $+2x^{14}+2x^{15}+x^{16}$	$1,1+2x,1,1+2x,2x,$ $x,1,2,1,2,1$	1	(2,2,2)

TABLE 3

1-generator QC codes over $GF(7)$

$QC\ code$	m	$g(x)$	$g_i(x)$	$h(x)$
$[8,3,6]$	4	$2+6x+3x^2+4x^3+x^4+5x^5$	$2+3x+x^2, 6+4x+5x^2$	$x-6$
$[16,2,14]$	4	$3+5x+2x^2+6x^3+5x^4$ $+5x^5+4x^6+4x^8+2x^9$ $+5x^{10}+x^{11}+2x^{12}+2x^{13}+3x^{14}$	$6+x^2, 3+5x+4x^2+2x^3,$ $5+5x+2x^2+2x^3, 2+4x$ $+5x^2+3x^3$	x^2+6
$[16,2,14]$	8	$3+5x+2x^2+6x^3+5x^4$ $+5x^5+4x^6+4x^8+2x^9+5x^{10}$ $+x^{11}+2x^{12}+2x^{13}+3x^{14}$	$3+2x+5x^2+4x^3+4x^4$ $+5x^5+2x^6+3x^7, 5+6x$ $+5x^2+2x^4+x^5+2x^6$	$5+6x+5x^2$ $+2x^4+x^5$ $+2x^6$
$[16,7,8]$	8	$6+6x+6x^2+4x^4+6x^5+2x^6$ $+6x^7+5x^8+x^9$	$6+6x+4x^2+2x^3+5x^4, 6$ $+6x^2+6x^3+x^4$	$x-6$
$[18,2,15]$	2	$1+2x+5x^2+5x^3+x^4+x^6$ $+2x^7+5x^8+5x^9+x^{10}+x^{12}$ $+2x^{13}+5x^{14}+5x^{15}+x^{16}$	$1+5x, 2+x, 5, 5+x, 1+2x, 5x$ $1+5x, 2+x, 5$	1

TABLE 4

2-generator QC codes over $GF(7)$

$QC\ code$	m	$g(x)$	$g_i(x)$	$h(x)$	K
$[8,3,6]$	2	$2+6x+3x^2+4x^3+x^4+$	$2+x,6+5x,3,4$	1	(2,1)
$[8,5,4]$	4	$2+6x+x^2+5x^3$	$2+x,6+5x$	1	(4,1)
$[12,8,4]$	6	$3+4x+2x^2+5x^3+6x^4+$	$3+2x+6x^2,4+5x+x^2$	x^2+5x+4	(4,4)
$[12,8,4]$	4	$3+4x+2x^2+5x^3+6x^4+$	$3+5x,4+6x,2+x$	1	(4,4)
$[12,9,3]$	6	$3+4x+6x^2+x^3$	$3+6x,4+x$	$x-3$	(5,4)
$[16,2,14]$	2	$3+5x+2x^2+6x^3+5x^4+$ $+4x^6+4x^8+2x^9+5x^{10}$ $+x^{11}+2x^{12}+2x^{13}+3x^{14}$	$3+4x,5+2x,2+5x,6+x,5+2x$ $4+3x$	x-1	(1,1)
$[16,3,12]$	2	$3+2x+6x^3+6x^4+6x^5$ $+5x^6+2x^7+2x^8+5x^{10}$ $+3x^{11}+6x^{12}+3x^{13}$	$3+2x$, 2 , $5x,6+3x,6$ $+6x,6+3x,5,2$	1	(2,1)
$[16,5,10]$	4	$2+5x^2+3x^3+4x^4+3x^5$ $+2x^6+4x^7+6x^8+6x^9$ $+5x^{10}+2x^{11}$	$2+4x+6x^2,3x+6x^2,5+2x$ $+5x^2,3+4x+2x^2$	1	(4,1)
$[16,7,8]$	4	$6+6x+6x^2+4x^4+6x^5$ $+2x^6+6x^7+5x^8+x^9$	$6+4x+5x^2,6+6x+x^2,6+2x,$ $6x$	1	(4,3)
$[16,9,6]$	8	$6+6x+x^3+4x^4+5x^5$ $+5x^6+x^7$	$6+4x^2+5x^3,6+x+5x^2+x^3$	1	(8,1)

TABLE 5

t-generator QC codes over $GF(7)$ ($t \geq 3$)

QC code	m	$g(x)$	$g_i(x)$	$h(x)$	K
$[8,5,4]$	2	$2+6x+x^2+5x^3$	2,6,1,5	1	(2,2,1)
$[12,8,4]$	3	$3+4x+2x^2+5x^3+6x^4+x^5$	$3+6x,4+x,2,5$	1	(3,3,2)
$[12,9,3]$	2	$3+4x+6x^2+x^3$	3,4,6,1,0,0	1	(2,2,2,2,1)
$[12,9,3]$	3	$3+4x+6x^2+x^3$	3,4,6,1	1	(3,3,3)
$[16,5,10$	2	$2+5x^2+3x^3+4x^4+3x^5+2x^6+4x^7+6x^8+6x^9+5x^{10}+2x^{11}$	$2+6x,6x,5+5x,3+2x,4,3,2,4$	1	(2,2,1)
$[16,7,8]$	2	$6+6x+6x^2+4x^4+6x^5+2x^6+6x^7+5x^8+x^9$	$6+5x,6+x,6,0,4,6,2,6$	1	(2,2,2,1)
$[16,9,6]$	2	$6+6x+x^3+4x^4+5x^5+5x^6+$	6,6,0,1,4,5,5,1	1	(2,2,2,2,1)

TABLE 6

References

1. Code Tables, Bounds on the parameters of various types of codes, (www.codetables.de)
2. CHEN E.Z ,Quasi-Cyclic form of Cyclic codes of Composite Length, Int. Symp. on Information Theory and its Applications, ISITA 2004, Parma, Italy, October, 10-13, pp 162-165, 2004.
3. DASKALOV R , HRISTOV P ,New One-Generator Quasi-Cyclic Codes over GF(7), Problems of Information Transmission, Vol 38, No;1 , pp 50-54, 2002.
4. GULLIVER T.A , New Optimal Ternary Linear Codes of Dimension 6, Ars Combin, 40, pp 97-108, 1995.
5. MAC WILLIAMS F.J, SLOANE N.J.A, The Theory of Error Correcting codes, North-Holland Publishing Company,1977.
6. SIAP I, RAY-CHAUDHURI D.K, New Linear Codes over IF_3 and IF_5 and Improvements on Bounds, Designs Codes and Cryptography, 21, pp 223-233 , 2000.