МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2003
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2003
Proceedings of the Thirty Second Spring Conference of the Union of Bulgarian Mathematicians
Sunny Beach, April 5–8, 2003

NEW QUASI-CYCLIC CODES OVER GF(5)*

Plamen Hristov

Let $[n,k,d]_q$-codes be linear codes of length n, dimension k and minimum Hamming distance d over $GF(q)$. In this paper, fourteen new codes over $GF(5)$ are constructed, which improve the known lower bounds on minimum distance.

1. Introduction. Let $GF(q)$ denote the Galois field of q elements. A linear code C over $GF(q)$ of length n, dimension k and minimum Hamming distance d is called an $[n,k,d]_q$-code.

A code is called p-quasi-cyclic (p-QC for short) if every cyclic shift of a codeword by p places is again a codeword. A quasi-cyclic (QC) code is just a code of length n which is p-QC for some divisor p of n with $p < n$ [5]. A cyclic code is just a 1-QC code. Suppose C is a p-QC $[pm,k]$-code. It is convenient to take the coordinate places of C in the order

$$1, p+1, 2p+1, \ldots, (m-1)p+1, 2, p+2, \ldots, (m-1)p+2, \ldots, p, 2p, \ldots, mp.$$

Then C will be generated by a matrix of the form

$$[G_1, G_2, \ldots, G_p],$$

where each G_i is a circulant matrix, i.e. a matrix of the form

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \cdots & b_{m-3} & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \cdots & b_{m-4} & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ b_1 & b_2 & b_3 & \cdots & b_{m-1} & b_0 \end{bmatrix}, \tag{1}$$

in which each row is a cyclic shift of its predecessor.

If the row vector $(b_0 b_1 \cdots b_{m-1})$ is identified with the polinomial $g(x) = b_0 + b_1 x + \cdots + b_{m-1}x^{m-1}$, then we may write

$$B = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{m-1} g(x) \end{bmatrix}, \tag{2}$$

where each polynomial is reduced modulo $x^m - 1$.

*2000 Math. Subject Classification: 94B15, 94B65. This work was partially supported by the Bulgarian Ministry of Education and Science under Contract in TU of Gabrovo.

If C is the QC code generated by

$$(3) \qquad G = \begin{bmatrix} g_1(x) & g_2(x) & \cdots & g_p(x) \\ xg_1(x) & xg_2(x) & \cdots & xg_p(x) \\ \vdots & \vdots & \vdots & \vdots \\ x^{m-1}g_1(x) & x^{m-1}g_2(x) & \cdots & x^{m-1}g_p(x) \end{bmatrix},$$

then the $g_i(x)$'s are called the *defining polynomials* of C [5]. The code C will usually be a code of dimension m, but if the defining polynomials all happen to be a multiple of some polynomial $h(x)$, where $h(x)|x^m - 1$, then C will actually have dimension $m - r$, where r is the degree of $h(x)$. Such a QC code is called *r-degenerate* [5].

Similarly to the case of cyclic codes, a p-QC code over $GF(q)$ of length $n = pm$ can be viewed as an $GF(q)[x]/(x^m - 1)$ submodule of $(GF(q)[x]/(x^m - 1))^p$ [10], [7]. Then an r-generator QC code is spanned by r elements of $(GF(q)[x]/(x^m - 1))^p$. In this paper we consider one-generator QC codes.

Definition. *Let α be a root of a primitive polynomial of degree n over $GF(q)$. Then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ form the multiplicative group of the field $GF(q^n)$. A polynomial $g(x) \in GF(q)[x]$ is said to have consecutive roots if α^i and α^{i+1} are roots of $g(x)$.*

A well-known results regarding the one-generator QC codes are as follows.

Theorem 1 [10], [7]**.** *Let C be a one-generator QC code over $GF(q)$ of length $n = pm$. Then, a generator $\mathbf{g(x)} \in (GF(q)[x]/(x^m - 1))^p$ of C has the following form*

$$\mathbf{g(x)} = (f_1(x)g_1(x), f_2(x)g_2(x), \cdots, f_p(x)g_p(x)),$$

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

Theorem 2 [7]**.** *Let C be a one-generator QC code over $GF(q)$ of length $n = pm$ with a generator as in Theorem 1. Then*

$$p.((\#\ \textit{of consecutive roots of}\ g(x)) + 1) \leq d_{\min}(C)$$

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

Quasi-cyclic codes form an important class of linear codes which contains the well-known class of cyclic codes. The investigation of QC codes is motivated by the following facts: QC codes meet a modified version of Gilbert-Varshamov bound [6]; some of the best quadratic residue codes and Pless symmetry codes are QC codes [8]; a large number of record breaking (and optimal codes) are QC codes [1]; there is a link between QC codes and convolutional codes [11], [4].

In this paper, new one-generator QC codes ($p = 2$) are constructed using a nonexhaustive algebraic-combinatorial computer search, similar to that in [9] and [3]. The codes presented here improve the corresponding lower bounds on the minimum distance in [1] and [2].

2. The New QC Codes. Our search method is the same as that presented in [9]. We illustrate this method in the following example. Let $m = 62$ and $q = 5$. Then the $\gcd(m, q) = 1$ and the splitting field of $x^m - 1$ is $GF(q^l)$ where l is the smallest integer such that $m|(q^l - 1)$. Let α be a primitive mth root of unity. Then

$$x^m - 1 = \prod_{j=0}^{m-1} (x - \alpha^j).$$

In our case $l = 3$ and $p(x) = x^3 + 4x^2 + 4x + 2$ is a primitive polynomial of degree 3 over $GF(5)$. Let η be a root of $p(x)$, such that η is a primitive $(5^3 - 1)$th root of unity and $\alpha = \eta^{124}$ is a primitive 62th root of unity. To obtain a "good" polynomial $g(x)$ we look at the cyclotomic cosets of 5 mod 62. The cyclotomic cosets are:

$cl(0) = \{0\}$	$cl(1) = \{1, 5, 25\}$	$cl(2) = \{2, 10, 50\}$	$cl(3) = \{3, 13, 15\}$
$cl(4) = \{4, 20, 38\}$	$cl(6) = \{6, 26, 30\}$	$cl(7) = \{7, 35, 51\}$	$cl(8) = \{8, 14, 40\}$
$cl(9) = \{9, 39, 45\}$	$cl(11) = \{11, 27, 55\}$	$cl(12) = \{12, 52, 60\}$	$cl(16) = \{16, 18, 28\}$
$cl(17) = \{17, 23, 53\}$	$cl(19) = \{19, 33, 41\}$	$cl(21) = \{21, 29, 43\}$	$cl(22) = \{22, 48, 54\}$
$cl(24) = \{24, 42, 58\}$	$cl(31) = \{31\}$	$cl(32) = \{32, 36, 56\}$	$cl(34) = \{34, 44, 46\}$
$cl(37) = \{37, 57, 61\}$	$cl(47) = \{47, 49, 59\}$.		

The corresponding minimal polynomials are

$h_0(x) = x + 4$	$h_1(x) = x^3 + 2x^2 + 1$	$h_2(x) = x^3 + x^2 + x + 4$
$h_3(x) = x^3 + x^2 + 3x + 1$	$h_4(x) = x^3 + x^2 + 3x + 4$	$h_5(x) = x^3 + 2x + 4$
$h_6(x) = x^3 + 4x^2 + 3x + 1$	$h_7(x) = x^3 + x + 4$	$h_8(x) = x^4 + x + 1$
$h_9(x) = x^3 + 3x^2 + 4x + 1$	$h_{10}(x) = x^3 + 4x^2 + 4x + 4$	$h_{11}(x) = x^3 + 2x^2 + x + 4$
$h_{12}(x) = x^3 + x^2 + 1$	$h_{13}(x) = x^3 + 4x^2 + x + 1$	$h_{14}(x) = x^3 + x^2 + 4x + 1$
$h_{15}(x) = x^3 + 4x^2 + 4$	$h_{16}(x) = x^3 + 2x^2 + 4x + 4$	$h_{17}(x) = x + 1$
$h_{18}(x) = x^3 + 3x^2 + 4$	$h_{19}(x) = x^3 + 4x^2 + 3x + 4$	$h_{20}(x) = x^3 + 2x + 1$
$h_{21}(x) = x^3 + 3x^2 + x + 1$.		

Let $T = \bigcup_{i \in M} cl(i)$, $\quad M = \{2, 4, 6, 7, 8, 9, 11, 12, 17, 19, 21, 22, 24, 31, 32, 34, 37, 47\}$ and $g(x) = \prod_{i \in M} (x - \alpha^i)$. Then the polynomial $g(x)$ has 33 consecutive roots. According to Theorem 2 we expect to obtain a cyclic code with minimum distance at least 34. Taking

$$g(x) = \prod_{i \in M} (x - \alpha^i) = h_2 \prod_{i=4}^{10} h_i(x) \prod_{i=12}^{21} h_i(x),$$

we obtain a new $[62, 10, 38]_5$-cyclic code. We take $f(x) = 1$ and make search for $f_2(x)$. With

$$f_2(x) = x^7 + 3x^5 + 3x^4 + 4x^3 + 3x^2 + 3$$

we find a new $[124, 10, 84]_5$-QC code.

Now, we present the new QC codes. Their parameters are given in Table 1. The minimum distances, d_{br} [1] of the previously best known codes are given for comparison.

The coefficients of the defining polynomials of the new codes are as follows:

1. A $[42, 13, 19]_5$**-code:** 123333321000000000000, 440400412121121000000;

2. A $[44, 12, 22]_5$**-code:** 4203134302100000000000, 2412004120213102100000;

3. A $[48, 14, 22]_5$**-code:** 430201431110000000000000, 212141033120121100000000;

4. A $[52, 16, 21]_5$**-code:** 40303020201000000000000000, 12033132011243211000000000;

5. A $[62, 10, 38]_5$**-code:** (C) 43220230434200310421413113323222134240443434412201431000000000;

6. A $[66, 16, 31]_5$**-code:** 421021210404141241000000000000000, 240040314211012130330100000000000;

7. A $[78, 12, 46]_5$**-code:** 432214244322014422340311321100000000000, 114341240314120222144031103214332100000;

8. A $[78, 13, 44]_5$**-code:** 110013433412424244233022001000000000000, 320243043102001314302222040411000000000;

9. An $[88, 12, 52]_5$**-code:** 12102421024443120141421403332044100000000000, 40011332311130444022341201144310021301000000;

10. An $[88, 16, 46]_5$**-code:** 11212103300430023310321411341000000000000000, 11011401200312221442021112033441100000000000;

11. A $[104, 11, 65]_5$**-code:** 13033241342221340114110034212434403302130100000000000, 34111002420101334101213123044441233320042042201000000;

12. A $[104, 14, 61]_5$**-code:** 22334320103124331124240033010211041132100000000000000, 34014001422304342240003244032341102124241001100000000;

13. A $[124, 9, 85]_5$**-code:** 11242220124042234311403304044242022440141412434000040400000000, 20421032341230303120100402014414122312401001032214032113400000;

14. A $[124, 10, 84]_5$**-code:** 43220230434200310421413113323222134240443434412201431000000000, 31312124320412313112002234432224021423132420334231140244203100;

Table 1. Minimum distances of the new linear codes over GF(5).

code	d	d_{br}	code	d	d_{br}
[42,13]	19	18	[78,13]	44	43
[44,12]	22	21	[88,12]	52	51
[48,14]	22	21	[88,16]	46	45
[52,16]	21	20	[104,11]	65	64
[62,10]	38	37	[104,14]	61	60
[66,16]	31	30	[124,9]	85	84
[78,12]	46	44	[124,10]	84	83

REFERENCES

[1] A. E. Brouwer. Linear code bound [electronic table; online], `http://www.win.tue.nl/~aeb/voorlincod.html`.

[2] R. N. Daskalov, T. A. Gulliver. Minimum distance bounds for linear codes over GF(5). *AAECC*, **9**, No 6 (1999), 547–558.

[3] R. N. Daskalov, P. Hristov. New one-generator quasi-cyclic codes over GF(7). *Probl. Pered. Inform.*, **38**, No 1 (2002), 59–63.

[4] M. Esmaeili, T. A. Gulliver, N. P. Secord and S.A. Mahmoud. A link between quasi-cyclic codes and convolutional codes. *IEEE Trans. Inform. Theory*, **44** (1998), 431–435.

[5] P. P. Greenough and R. Hill. Optimal ternary quasi-cyclic codes. *Designs, Codes and Cryptography*, **2** (1992), 81–91.

[6] T. Kasami. A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2. *IEEE Trans. Inform. Theory*, **IT-20** (1974), 679–680.
[7] K. Lally and P. Fitzpatrick. Construction and classification of quasi-cyclic codes. In: Proc. Int. Workshop on Coding and Cryptography, WCC'99, Paris, France, 1999, 11–20.
[8] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. New York, NY, North-Holland Publishing Co., 1977.
[8] I. Siap, N. Aydin, D. Ray-Chaudhury. New ternary quasi-cyclic codes with better minimum distances. *IEEE Trans. Inform. Theory*, **46**, No 4 (2000), 1554–1558.
[9] G. E. Séguin, G. Drolet. The theory of 1-generator quasi-cyclic codes. Technical Report, Royal Military College of Canada, Kingston, ON, 1991.
[10] G. Solomon, H. C. A. van Tilborg. A connection between block and convolutional codes. *SIAM J. of Applied Mathematics*, **37**, No 2 (1979), 358–369.

Plamen Hristov
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria
e-mail: plhristov@tugab.bg

НОВИ КВАЗИ-ЦИКЛИЧНИ КОДОВЕ НАД GF(5)

Пламен Христов

Нека $[n,k,d]_q$-код е линеен код с дължина n, размерност k и минимално Хемингово разстояние d над $GF(q)$. Конструирани са четиринадесет нови кода над $GF(5)$, които подобряват познатите в момента долни граници за минималното разстояние.