МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2002
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2002
Proceedings of Thirty First Spring Conference of the Union of Bulgarian Mathematicians
Borovets, April 3–6, 2002

NEW QUASI-CYCLIC CODES OVER GF(7)*

Plamen Hristov Vasilev

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, seventeen new codes over $GF(7)$ are constructed, which improve the known lower bounds on minimum distance.

Key words: linear codes over GF(7), quasi-cyclic codes.

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 an p-QC $[pm, k]$-code. It is convenient to take the co-ordinate places of C in the order

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

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

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

*This work was partially supported by the Bulgarian Ministry of Education and Science under Contract in TU of Gabrovo.

where each polynomial is reduced modulo $x^m - 1$.
If C is the QC code generated by

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

then the $g_i(x)'s$ are called the *defining polynomials* of C [5].

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, an p-QC code over $GF(q)$ of length $n = pm$ can be considered 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. 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 $1 \le i \le p$.

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

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

where $g(x)|(x^m - 1), g(x), f_i(x) \in GF(q)[x]/(x^m - 1)$ and $(f_i(x), (x^m - 1)/g(x)) = 1$ for all $1 \le i \le p$. Then

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

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. These codes are a natural generalization of the well-known 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 ($p = 1$ or $p = 2$) are constructed using a nonexhaustive algebraic-combinatorial computers search, similar to that in [9]. The codes presented here improve the respective lower bounds on the minimum distance in [1] and [2].

2. The New QC Codes.

Our search method is the same as those presented in [9]. We illustrate this method in the following example. Let $m = 43$ and $q = 7$. Then the $\gcd(m, q) = 1$ and the splitting field of $x^m - a$ 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 $l = 6$ and $p(x) = x^6 + x^5 + 6x^4 + 6x^3 + x^2 + 5$ is a primitive polynomial of degree 6 over GF(7). Let η be a root of $p(x)$, so that is a primitive $(7^6 - 1)$th root of unity and $\alpha = \eta^{2736}$ be a primitive 43th root of unity. To obtain a "good" polynomial $g(x)$ we look at the cyclotomic cosets of 7 mod 43. The cyclotomic cosets are:

$$\begin{aligned} cl(0) &= \{0\}, \\ cl(1) &= \{1, 6, 7, 36, 37, 42\}, \\ cl(2) &= \{2, 12, 14, 29, 31, 41\}, \\ cl(3) &= \{3, 18, 21, 22, 25, 40\}, \\ cl(4) &= \{4, 15, 19, 24, 28, 39\}, \\ cl(5) &= \{5, 8, 13, 30, 35, 38\}, \\ cl(9) &= \{9, 11, 20, 23, 32, 34\}, \\ cl(10) &= \{10, 16, 17, 26, 27, 33\}. \end{aligned}$$

Let $T = cl(2) \cup cl(3) \cup cl(4) \cup cl(5) \cup cl(9) \cup cl(10)$ (So that the cyclic code generated by $g(x)$ has 28 consecutive roots. According to Theorem 2 we expect to receive cyclic code with minimum distance at leat 29).

Taken

$$g(x) = \prod_{i \in T} (x - \alpha^i) = x^{36} + 5x^{34} + 5x^{33} + 6x^{32} + 3x^{31} + 2x^{30} + 3x^{29} + 5x^{28} + 6x^{27} + 6x^{26}$$

$$+x^{25} + 2x^{24} + 3x^{23} + 2x^{21} + 6x^{20} + 5x^{19} + 5x^{18} + 5x^{17} + 6x^{16} + 2x^{15} + 3x^{13}$$

$$+2x^{12} + x^{11} + 6x^{10} + 6x^9 + 5x^8 + 3x^2 + x^6 + 3x^5 + 6x^4 + 5x^3 + 5x^2 + 1,$$

we obtain a new $[43, 7, 30]_7$-cyclic code [3]. After that we make search for $f_2(x)$. With

$$f_2(x) = x^2 + 2x + 3$$

we find a new $[86, 7, 64]_7$-QC code.

Now, we present the new QC codes. The parameters of these codes are given in Table 1. The minimum distances, d_{br} [1] and [2] of the previously best known codes are given for comparison.

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

A $[43, 12, 24]_7$**-code:**
1222146300423410063453004136555600000000000;

A $[57, 7, 41]_7$**-code:**
011355630135422311614412611045066603113515020360205400000;

A $[57, 8, 39]_7$**-code:**
126314530230052640121210331104622366455335230154360000000;

A $[57, 9, 38]_7$**-code:**
122525333656143361062433056222225133324364540210100000000;

A $[57, 10, 37]_7$**-code:**
122225222545245154024124453443652610362304462355000000000;

A $[57, 11, 36]_7$**-code:**
110014064234636111235121645125422413443131326240000000000;

A $[58, 7, 41]_7$**-code:**
15654650113645430324011000000, 33155216035504451215622321000;

A $[58, 8, 39]_7$**-code:**
16530644562153033615560000000, 36044035642656451642553600000;

A $[74, 9, 50]_7$**-code:**
1146522550015030552263126560100000000, 3402436513532603462613530214211000000;

A $[74, 10, 48]_7$**-code:**
1265350533342255313540132066000000000, 3003116253602123024105503625556000000;

A $[75, 8, 52]_7$**-code:**
115216550421363311506656046205405002155413410441403233604506212364030000000;

A $[75, 9, 51]_7$**-code:**
120232055245103601665421154664116661205236344156336140663110235104400000000;

A $[75, 10, 48]_7$**-code:**
141443634334244001110430104062540642651440333052035453520136034245000000000;

A $[76, 6, 58]_7$**-code:**
16303413012420166316255316050566100000, 12125226051435044014340463150351210100;

A $[76, 7, 56]_7$**-code:**
11443344000044660000220022553300111111, 00445544111144221111661166335511000000;

A $[76, 8, 54]_7$**-code:**
15313253556535020545152322414560000000, 50213606454253540224426642316112246000;

A $[76, 9, 52]_7$**-code:**
14222532523004064256230130646100000000, 46630241562066513425166464115254210000;

A $[76, 10, 50]_7$**-code:**
12025433023623106201003311246000000000, 21036555643164430126660446326156000000;

A $[76, 11, 48]_7$**-code:**
14365416612125246645616222160000000000, 45506445601422063311412663251660000000;

Table 1. Minimum distances of the new linear codes over GF(7).

code	d	d_{dg}	code	d	d_{dg}
[43,12]	24	23_{br}	[76, 6]	58	57
[57,7]	41	40	[76, 7]	56	55
[57,8]	39	–	[76, 8]	54	–
[57,9]	38	–	[76,9]	52	–
[57,10]	37	–	[76,10]	50	–
[57,11]	36	–	[76,11]	48	–
[58,7]	41	39	[80,6]	60	59
[58,8]	39	–	[80,7]	58	57
[74,9]	50	–	[80,8]	56	–
[74,10]	48	–	[80,9]	55	–
[75,8]	52	–	[80,10]	52	–
[75,9]	51	–	[86, 6]	66	64
[75,10]	48	–	[86,7]	64	62

A $[80, 6, 60]_7$**-code:**
1424056442152303146300461606425561600000, 2220603545163652553223125504002316506000;

A $[80, 7, 58]_7$**-code:**
1013536001014441254115354251244051000000, 4443454133440453242160556650015430451000;

A $[80, 8, 56]_7$**-code:**
1135533513423062316666223211053560000000, 2310420235545513002533253205244464600000;

A $[80, 9, 55]_7$**-code:**
1302210520560121534416265041352100000000, 2146644300550241515654306516565032100000;

A $[80, 10, 52]_7$**-code:**
1146225063356550110066114354521000000000, 5024563506661061303120262305330410000000;

A $[86, 6, 66]_7$**-code:**
1262443053544460223455013332420433515600000, 4262316023034343032061326240006425555246000;

A $[86, 7, 64]_7$**-code:**
1055632356612302655562032166532365501000000, 3224554223000012113252345313543252311210000;

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(7). *Journal of Combinatorial Mathematics and Combinatorial Computing*, **36** (2001), 175–191.
[3] R. N. Daskalov, P. Hristov. New One-Generator Quasi-Cyclic Codes over GF(7). *Probl. Pered. Inform.*, to appear.
[4] M. Esmaeili, T. A. Gulliver, N. P. Secord, 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*, **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, North-Holland Publishing Co., 1977.
[9] 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.
[10] G. E. Séguin and G. Drolet. The theory of 1-generator quasi-cyclic codes. Technical Report, Royal Military College of Canada, Kingston, ON, (1991).
[11] 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 Vasilev
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria

НОВИ КВАЗИ-ЦИКЛИЧНИ КОДОВЕ НАД GF(7)

Пламен Христов Василев

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