МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2004
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2004
Proceedings of the Thirty Third Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 1–4, 2004

SIX NEW QUASI-CYCLIC LINEAR CODES OVER GF(7)*

Elena Metodieva

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, six new linear codes over $GF(7)$ are constructed. The parameters of these codes are: $[35, 7, 23]_7$, $[27, 9, 14]_7$, $[33, 10, 17]_7$, $[50, 10, 30]_7$, $[36, 12, 18]_7$, $[39, 13, 19]_7$. The obtained results improve the corresponding known lower bounds on the minimum distance in Brouwer's table [1].

Introduction. Let $GF(q)$ denote the Galois field of q elements, and let $V(n, q)$ denote the vector space of all ordered n-tuples over $GF(q)$. The number of nonzero positions in a vector $\mathbf{x} \in V(n, q)$ is called the *Hamming weight* $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x}$. The *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}, \mathbf{y} \in V(n, q)$ is defined by $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$. A linear code C of length n and dimension k over $GF(q)$ is a k-dimensional subspace of $V(n, q)$. The *minimum distance* of a linear code C is $d(C) = \min \{d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$. Such a code is called $[n, k, d]_q$ code if its minimum Hamming distance is d. For a linear code, the minimum distance is equal to the smallest of the weights of the nonzero codewords.

A $k \times n$ matrix G having as rows the vectors of a basis of a linear code C is called a *generator matrix* for C.

Given an $[n, k, d]_q$ code C, we denote by A_i the number of codewords of weight i in C. The ordered $(n + 1)$-tuple of integers $\{A_i\}_{i=0}^{n}$ is called the *weight distribution* or *weight enumerator* of C.

Well known fact in coding theory is that if there is likelihood of transmitting each vector of C over a q-ary symmetric channel, the code C can correct up to $\lfloor (d - 1)/2 \rfloor$ errors, where $\lfloor x \rfloor$ denotes the greatest integer $\leq x$. Hence in order to obtain a q-ary linear code which is capable of correcting most errors for given values of n, k, and q, it is sufficient to obtain an $[n, k, d]_q$ code C with maximum minimum distance d among all such codes or for given values of k, d, and q, to obtain an $[n, k, d]_q$ code C whose length n is a smallest one. So a central problem in coding theory is that of optimizing one of the parameters n, k and d for given values of the other two and q-fixed.

Two versions are:

Problem 1. *Find $d_q(n, k)$, the largest value of d for which there exists an $[n, k, d]_q$ code.*

Problem 2. *Find $n_q(k, d)$, the smallest value of n for which there exists an $[n, k, d]_q$ code.*

---

*This work was partially supported by the Ministry of Education and Science under contract with TU-Gabrovo.

2000 Mathematics Subject Classification: 94B05, 94B65.

A code which achieves one of these two values is called *optimal*.

For the case of linear codes over $GF(7)$, Problem 2 has been solved for $k \leq 3$ [7]. Fifty eight new linear codes over $GF(7)$ are constructed and a table of $d_7(n,k)$, $k \leq 7$, $n \leq 100$, is presented in [2]. Thirty three linear codes over $GF(7)$ are constructed in [8]. New linear codes ($n \leq 50$) over $GF(7)$ are constructed in [4,12]. All these and other results are included in the Brouwer's table over $GF(7)$.

Our aim in this paper is to improve some lower bounds in the Brouwer's table. Using a nonexhaustive combinatorial computers search we constructed six new quasi-cyclic (QC) codes, by method similar to that in [2,3,11].

Quasi-Cyclic Codes. Let $n = pm$, where p, m are positive integers. Let $(c_1, c_2, \ldots, c_n) \in C$ and

$\mu_p : C \to V(n,q)$

$\mu_p\ ((c_1, c_2, \ldots, c_n)) = (c_{n-(p-1)}, c_{n-(p-2)}, \ldots, c_{n-1}, c_n, c_1, c_2, \ldots, c_{n-p})$.

Definition 1. *A linear code C is called p-quasi-cyclic (p-QC or QC) if and only if C is invariant under μ_p, i.e. $\mu_p(C) = C$.*

A matrix B of the form

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

is called a *circulant matrix*. With a suitable permutation of coordinates [15] a class of QC codes can be constructed from $m \times m$ circulant matrices. In this case, the generator matrix G can be represented as

$$G = [B_1,\ B_2,\ \ldots,\ B_p], \tag{2}$$

where B_i is a circulant matrix.

The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - 1)$ if B is mapped onto the polynomial $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1}$ formed from the entries in the first row of B. The $b_i(x)$ associated with a QC code are called the *defining polynomials* [6].

If the defining polynomials $b_i(x)$ contain a common factor which is also a factor of $x^m - 1$, then the QC code is called *degenerate* [6]. The dimension k of the QC code is equal to the degree of $h(x)$, where [13]

$$h(x) = \frac{x^m - 1}{\gcd\ (x^m - 1, b_0(x), b_1(x), \cdots, b_{p-1}(x))}. \tag{3}$$

If the polynomial $h(x)$ has degree m, the dimension of the code is m, and (2) is a generator matrix. If $\deg(h(x)) = k < m$, a generator matrix for the code can be constructed by deleting $m - k$ rows of (2).

Quasi-cyclic codes form an important class of linear codes. Some of the reasons for the investigation of these codes are:

- QC codes meet a modified version of Gilbert-Varshamov bound [8]; some of the best quadratic residue codes and Pless symmetry codes are QC codes [10];
- a large number of optimal and record breaking codes are QC codes [1];

- there is a link between QC codes and convolutional codes [14,5].

The new codes. Now, we present the new codes. The parameters of these codes are given in Table I. The minimum distances d_{br} [1] of the previously best known codes are given for comparison. The defining polynomials are separated by comma.

Table I: The new linear codes over GF(7).

N:	code	d	d_{br}
1	[35,7]	23	22
2	[27,9]	14	13
3	[33,10]	17	16
4	[50,10]	30	29
5	[36,12]	18	17
6	[39,13]	19	18

Theorem 1. *There exist QC codes with parameters:*

$$[35,7,23]_7, [27,9,14]_7, [33,10,17]_7, [50,10,30]_7, [36,12,18]_7, [39,13,19]_7.$$

Proof. The coefficients of the defining polynomials and the weight distributions of the new codes are as follows:

1. A $[35,7,23]_7$ **code:**
1245635, 0125114, 0122512, 0111324, 0014262;
$0^{1}23^{2226}24^{4158}25^{11676}26^{27510}27^{49686}28^{90642}29^{127470}30^{160440}31^{150150}32^{110964}33^{63252}34^{21882}35^{3486}$

2. A $[27,9,14]_7$ **code:**
000112123, 001113413, 000000001;
$0^{1}14^{810}15^{5778}16^{23058}17^{88398}18^{285672}19^{836784}20^{1995786}21^{3985920}$
$22^{6522660}23^{8509158}24^{8514756}25^{6132348}26^{2821878}27^{630600}$

3. A $[33,10,17]_7$ **code:**
00011111414, 00111111125, 00012162144;
$0^{1}17^{594}18^{4422}19^{19074}20^{74184}21^{288222}22^{927894}23^{2663166}24^{6676296}$
$25^{14434728}26^{26678058}27^{41332566}28^{53264640}29^{55076670}30^{44159610}$
$31^{25525434}32^{9598710}33^{1750980}$

4. A $[50,10,30]_7$ **code:**
0011132425, 0001112541, 0001125313, 0010215314, 0000000001;
$0^{1}30^{1410}31^{7200}32^{22500}33^{74700}34^{219900}35^{615072}36^{1525710}37^{3419880}$
$38^{7092750}39^{13042800}40^{21618396}41^{31562700}42^{40569780}43^{45277080}44^{43263600}45^{34566192}$
$46^{22552590}47^{11546040}48^{4315770}49^{1055100}50^{126078}$

5. A $[36,12,18]_7$ **code:**
000113335163, 001152463501, 000000000001;
$0^{1}18^{4572}19^{27504}20^{142560}21^{639384}22^{2618460}23^{9509832}24^{30974850}25^{89053128}$
$26^{226348812}27^{503110416}28^{970257402}29^{1604459016}30^{2248472244}31^{2609968392}32^{2447012214}33^{1779605424}$
$34^{942239520}35^{322998480}36^{53844990}$

6. A $[39,13,19]_7$ **code:**
0011112564164, 0011111203502, 0000000000001;
$0^{1}19^{4446}20^{26676}21^{151476}22^{706446}23^{3207828}24^{12657528}25^{45635382}26^{147615780}$
$27^{426459384}28^{1096070586}29^{2496007410}30^{4990437582}31^{8693212320}32^{13037793834}33^{16599153090}$
$34^{17571682674}35^{15061843056}36^{10041143112}37^{4885112388}38^{1542865194}39^{237224214}$

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, T. A. Gulliver. "New Minimum Distance Bounds for Linear Codes over Small Fields", *Problemi Peredachi Informatsii* , **37**, No 3, (2001), 24–33.

[4] R. N. Daskalov, P. Hristov. " New One-Generator Quasi-Cyclic Codes over GF(7)", *Problemi Peredachi Informatsii*, **38**, No 1 , (2002), 59–63. (English translation: *Problems of Information Transmission*, **38**, No 1, (2002), 50–54.)

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

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

[7] R. Hill. "Optimal Linear Codes", *Cryptography and Coding II*, C. Mitchel, Ed. Oxford, UK: Oxford Univ. Press, pp. 75–104, 1992.

[8] T. Kasami. "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2", *IEEE Trans. Inform. Theory*, vol. IT-20, (1974), 679–680.

[9] K. Lally, P. Fitzpatrick. "Construction and classification of quasi-cyclic codes", Proc. *Int. Workshop on Coding and Cryptography, WCC'99*, Paris, France, (1999), 11–20.

[10] F. J. MacWilliams, N. J. A. Sloane. *The Theory of Error-Correcting Codes*, New York, NY: North-Holland Publishing Co., 1977.

[11] E. Metodieva. "New good quasi-cyclic ternary linear codes and some self-orthogonal codes", *Mathematics and Education in Mathematics*, Sofia, (1997), 161–166.

[12] T. Rehfinger, N. S. Babu, K. Zimmermann. "New Good Codes via CQuest – A System for the Silicon Search of Linear Codes", In Algebraic Combinatorics and Applications, A. Betten et al., eds, Springer, (2001), 294-306.

[13] G. E. Séguin, G. Drolet. "The theory of 1-generator quasi-cyclic codes," Technical Report, Royal Military College of Canada, Kingston, ON, 1991.

[14] 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.

[15] K. Thomas, "Polynomial approach to quasi-cyclic codes", *Bul. Cal. Math. Soc.*, **69**, (1977), 51–59.

Elena Metodieva
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria

ШЕСТ НОВИ КВАЗИ-ЦИКЛИЧНИ ЛИНЕЙНИ КОДА НАД GF(7)

Елена Методиева

Нека $[n, k, d]_q$-код е линеен код с дължина n, размерност k и минимално Хемингово разстояние d над $GF(q)$. В тази статия са конструирани шест нови линейни кода със следните параметри: $[35, 7, 23]_7$, $[27, 9, 14]_7$, $[33, 10, 17]_7$, $[50, 10, 30]_7$, $[36, 12, 18]_7$, $[39, 13, 19]_7$. Получените резултати подобряват съответните познати до момента долни граници за минималните разстояния в таблиците на Брауер [1].