M a t h e m a t i c a
B a l k a n i c a

New Series Vol. 18, 2004, Fasc. 1-2

One-Generator Quasi-Cyclic Quaternary Linear Codes and Construction X [1]

Rumen Daskalov, Plamen Hristov

One of the main problems in coding theory is to construct codes with best possible minimum distances. In this paper, thirty-two new quaternary codes are constructed, which improve the best known lower bounds on minimum distance.

AMS Subj. Classification: 94B15, 94B65
Key words: linear quaternary codes, quasi-cyclic codes, construction X.

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 an $[n,k,d]_q$ 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 $m \times m$ matrix B each row of which is a cyclic shift of the previous one is called a *circulant matrix*. 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 $p < n$ [4]. 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

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

[1] This work was partially supported by the Ministry of Education and Science under contract in TU-Gabrovo.

Then C is generated by a matrix of the form $[G_1, G_2, ..., G_p]$ where each G_i is a circulant matrix.
Let the firs row of the matrix B is $(b_0, b_1, \cdots, b_{m-1})$. With this row we associate the polynomial $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1}$. The $b_i(x)$ $(1 \leq i \leq p)$, associated in this manner with a QC code, are called the *defining polynomials* [4]. The code C usually has 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 has dimension $m - r$, where r is the degree of $h(x)$. Such a QC code is called *r-degenerate* [4].

Let the defining polynomials of the code C be in the form

$$d_1(x) = g(x),\ d_2(x) = f_2(x)g(x),\ \cdots,\ d_p(x) = f_p(x)g(x), \tag{1}$$

where $g(x)|(x^m - 1), g(x), f_i(x) \in GF(q)[x]/(x^m - 1)$, $(f_i(x), (x^m - 1)/g(x)) = 1$ and $\deg f_i(x) < m - \deg g(x)$ for all $1 \leq i \leq p$. Then C is a degenerate QC code, which is one-generator QC code and for this code $n = mp$ and $k = m - \deg g(x)$. For the structural properties of one-generator codes see [5,6].

Definition. Let α be a root of primitive polynomial of degree n over $GF(q)$. Then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ form the multiplicative group of the field $GF(q^n)$. Now consider a polynomial $g(x)$ with coefficients from $GF(q)$. The polynomial $g(x)$ has consecutive roots if α^i and α^{i+1} are roots.

In this paper, new one-generator QC codes ($p = 1$ or $p = 2$) over $GF(4)$ are constructed using a nonexhaustive algebraic-combinatorial computer search, similar to that in [6,3]. For convenience, the elements of $GF(4)$ are given as integers: $2 = \beta$, $3 = \beta^2$, where β is a root of the binary primitive polynomial $y^2 + y + 1$. The codes presented here improve the respective lower bounds on the minimum distance in [1].

2. The new QC codes

Our method is an improvement (full version) of the search method, presented in [6]. We will illustrate the search method by the following example. Let $m = 51$ and $q = 4$. 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 $m|(q^l - 1)$. In our case $l = 4$ and so our splitting field is $GF(4^4)$. One of the generating polynomials for $GF(4^4)$ is $p(x) = x^4 + x^3 + 2x^2 + x + 3$ and let α be a root of $p(x)$. Then

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

For obtaining a good polynomial $g(x)$ we look at the cyclotomic cosets of 4 *mod* 51. The cyclotomic cosets are:

$$\begin{array}{ll} cl(0) = \{0\} & cl(11) = \{11, 23, 41, 44\} \\ cl(1) = \{1, 4, 13, 16\} & cl(17) = \{17\} \\ cl(2) = \{2, 8, 26, 32\} & cl(18) = \{18, 21, 30, 33\} \\ cl(3) = \{3, 12, 39, 48\} & cl(19) = \{19, 25, 43, 49\} \\ cl(5) = \{5, 14, 20, 29\} & cl(22) = \{22, 31, 37, 46\} \\ cl(6) = \{6, 24, 27, 45\} & cl(34) = \{34\} \\ cl(7) = \{7, 10, 28, 40\} & cl(35) = \{35, 38, 47, 50\} \\ cl(9) = \{9, 15, 36, 42\} & \end{array}$$

To each cyclotomic coset corresponds irreducible factor of $x^{51}-1$. Hence we have 12 factors of degree four and 3 factors of degree one. One of the possible degrees of the polynomial $g(x)$ is $s = 41$. So we can consider codes with parameters $[51p, 51 - s]_4$, where $p = 1, 2, 3, \ldots$. All cases ($p = 1, 2$) have been investigated and for $p = 2$ a new code was obtained. There are $\binom{12}{10}.3 = 198$ possibilities to obtain $g(x)$ of degree 41. We checked all of these possibilities and when $T = \bigcup_{i \in M} cl(i)$, where $M = \{1, 5, 6, 7, 9, 11, 17, 18, 19, 22, 35\}$, has been taken a new code was constructed.

The respective minimal polynomials are as follows:

$$\begin{array}{ll} h_0(x) = x + 1 & h_1(x) = x^4 + x^3 + 2x^2 + 2x + 3 \\ h_2(x) = x^4 + x^3 + 3x^2 + 3x + 2 & h_3(x) = x^4 + x^3 + 3x^2 + x + 1 \\ h_4(x) = x^4 + 2x^3 + 2x^2 + x + 2 & h_5(x) = x^4 + x^3 + 2x^2 + x + 1 \\ h_6(x) = x^4 + 3x^3 + 3x^2 + x + 3 & h_7(x) = x^4 + 3x^3 + x^2 + 3x + 1 \\ h_8(x) = x^4 + 2x^3 + x^2 + x + 2 & h_9(x) = x + 2 \\ h_{10}(x) = x^4 + 2x^3 + x^2 + 2x + 1 & h_{11}(x) = x^4 + 2x^3 + 2x^2 + 3x + 3 \\ h_{12}(x) = x^4 + 3x^3 + x^2 + x + 3 & h_{13}(x) = x + 3 \\ h_{14}(x) = x^4 + 3x^3 + 3x^2 + 2x + 2. & \end{array}$$

Let $g(x) = \prod_{i \in T}(x - \alpha^i)$. The polynomial $g(x)$ has 15 consecutive roots. According to BCH bound we expect to obtain by $g(x)$ cyclic code with minimum distance at least 16.

Taking

$$g(x) = \prod_{i \in T}(x - \alpha^i) = h_1(x)h_{14}(x) \prod_{i=4}^{12} h_i(x),$$

we obtain cyclic $[51, 10, 27]_4$ code. After that we make search for $f_2(x)$. With $f_2(x) = x^6 + 3x^5 + x^4 + 2x^3 + x + 2$ we find a new $[102, 10, 64]_4$ code.

Remark : There exist three other polynomials g(x) that have 21 consecutive roots. With these polynomials we obtain also $[51, 10, 27]_4$ cyclic codes, but we can not construct quasi-cyclic $[102, 10, 64]_4$ codes.

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

By reasons of space in the next two theorems we will present the coefficients of the defining polynomials and the weight enumerators of the first code only. The coefficients of the defining polynomials and the weight enumerators of all remaining codes are available upon request.

Theorem 2.1 *There exist cyclic codes with parameters:*

$$[51, 18, 19]_4, \quad [63, 18, 28]_4, \quad [85, 17, 43]_4, \quad [85, 18, 42]_4, \quad [85, 19, 40]_4,$$

$$[91, 15, 48]_4, \quad [91, 19, 42]_4, \quad [195, 14, 120]_4, \quad [195, 15, 119]_4, \quad [195, 16, 116]_4.$$

Proof. **A $[51, 18, 19]_4$-code:**
111030231033203101033310333300201200000000000000000;
$0^{1}19^{8415}20^{9792}21^{58752}22^{57528}23^{506736}24^{850068}25^{3625488}26^{7922952}27^{22493244}28^{66450960}29^{121739040}$
$30^{377354712}31^{501090912}32^{1519252821}33^{1568793456}34^{4225657896}35^{3585659346}36^{8183287008}37^{5844932928}$
$38^{10879750440}39^{6593646384}40^{9724854420}41^{4841926128}42^{5604249240}43^{2123867052}44^{1951577424}45^{501081120}$
$46^{374192712}47^{57792384}48^{33305346}49^{2548368}50^{899640}51^{34023}$. ∎

Theorem 2.2 *There exist quasi-cyclic codes with parameters:*
$[46, 11, 24]_4$, $[102, 10, 64]_4$, $[102, 18, 50]_4$, $[126, 16, 69]_4$, $[126, 18, 66]_4$,
$[130, 15, 74]_4$, $[130, 16, 71]_4$, $[170, 17, 98]_4$, $[170, 18, 94]_4$, $[182, 9, 120]_4$.

Proof. **A $[46, 11, 24]_4$-code:** 11111001001010000000000, 20312111313002131021000;
$0^{1}24^{4140}26^{25530}28^{109434}30^{341136}32^{755619}34^{1102068}36^{1033068}38^{600576}40^{188784}42^{32706}44^{1242}$. ∎

Theorem 2.3 *[2] (construction X) Let $C_2 = [n, k-l, d+s]_q$ code be a subcode of the code $C_1 = [n, k, d]_q$ and let $C_3 = [a, l, s]_q$ be a third code. Then there exists an $C = [n+a, k, d+s]_q$ code.*

The main prerequisite of applying construction X is to find a code C_1 and a subcode $C_2 \subset C_1$ with high minimum distance. We will demonstrate this construction in the following example.

A linear code $C_1 = [51, 10, 27]_4$ is generated by the polynomial

$$g_1(x) = h_1(x) \prod_{i=4}^{8} h_i(x) \prod_{i=10}^{14} h_i(x)$$

and a linear code $C_2 = [51, 9, 31]_4$ by the polynomial

$$g_2(x) = (x+2)g_1(x) = h_1(x) \prod_{i=4}^{14} h_i(x).$$

The code C_2 is a subcode of the code C_1. Taking a third $C_3 = [4, 1, 4]_4$ code and applying construction X we obtain new linear code $C = [55, 10, 31]_4$*code.*

The codes presented in the next Theorem 2.4 are obtained by construction X. The parameters of the component codes C_1, C_2 and C_3 are given in Table 1.

Theorem 2.4 *There exist linear codes with parameters:*

$$[52, 9, 32]_4, \quad [52, 17, 22]_4, \quad [55, 10, 31]_4, \quad [58, 10, 32]_4,$$
$$[64, 16, 30]_4, \quad [67, 18, 30]_4, \quad [69, 13, 36]_4, \quad [87, 19, 41]_4,$$
$$[90, 18, 44]_4, \quad [93, 18, 46]_4, \quad [202, 14, 122]_4, \quad [207, 14, 126]_4 .$$

Table 1: Parameters of the component codes C_1, C_2 and C_3, used to obtain the code C by construction X.

code C	code C_1	subcode C_2	code C_3
[52,9,32]	[51,9,31]	[51,8,32]	[1,1,1]
[52,17,22]	[51,17,21]	[51,16,22]	[1,1,1]
[55,10,31]	[51,10,27]	[51,9,31]	[4,1,4]
[58,10,32]	[51,10,27]	[51,8,32]	[7,2,5]
[64,16,30]	[63,16,29]	[63,15,30]	[1,1,1]
[67,18,30]	[63,18,28]	[63,15,30]	[4,3,2]
[69,13,36]	[63,13,32]	[63,10,36]	[6,3,4]
[87,19,41]	[85,19,40]	[85,17,41]	[2,2,1]
[90,18,44]	[85,18,42]	[85,14,46]	[5,4,2]
[93,18,46]	[85,18,42]	[85,14,46]	[8,4,4]
[202,14,122]	[195,14,120]	[195,8,132]	[7,6,2]
[207,14,126]	[195,14,120]	[195,8,132]	[12,6,6]

Table 2: Minimum distances of the new quaternary linear codes.

code	d	d_{br}	code	d	d_{br}	code	d	d_{br}
[46,11]	24	22	[85,18]	42	40	[130,15]	74	73
[51,18]	19	18	[85,19]	40	36	[130,16]	71	70
[52,9]	32	31	[87,19]	41	40	[170,17]	98	96
[52,17]	22	21	[90,18]	44	43	[170,18]	94	92
[55,10]	31	30	[91,15]	48	46	[182,9]	120	118
[58,10]	32	30	[91,19]	42	41	[195,14]	120	116
[63,18]	28	27	[93,18]	46	44	[195,15]	119	116
[64,16]	30	29	[102,10]	64	61	[195,16]	116	112
[67,18]	30	28	[102,18]	50	48	[202,14]	122	121
[69,13]	36	35	[126,16]	69	68	[207,14]	126	125
[85,17]	43	41	[126,18]	66	64			

References

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

[2] A. E. Brouwer, Bound on the size of linear codes, *Handbook of coding theory*, Edited by V.S. Pless and W.C. Huffman, Elsevier Science, 1998.

[3] R. Daskalov, P. Hristov, New quasi-twisted degenerate ternary linear codes, *IEEE Trans. Inform. Theory*, **49** (2003), no. 9, 2259–2263.

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

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

[6] I. Siap, N. Aydin and D. Ray-Chaudhury, New ternary quasi-cyclic codes with better minimum distances, *IEEE Trans. Inform. Theory*, **46** (2000), no. 4, 1554–1558.

Department of Mathematics,
Technical University of Gabrovo,
5300 Gabrovo, BULGARIA,
e-mail: daskalov@tugab.bg, plhristov@tugab.bg

Received 30.09.2003