Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 51–56*

New 5-ary and 7-ary linear codes [1]

Rumen Daskalov daskalov@tugab.bg
Elena Metodieva metodieva@tugab.bg
Department of Mathematics, Technical University of Gabrovo,
5300 Gabrovo, BULGARIA

Abstract. Let $[n, k, d]_q$ code be a linear code of length n, dimension k and Hamming minimum distance d over GF(q). In this paper record-breaking codes with parameters $[30, 10, 15]_5$, $[33, 11, 16]_5$, $[41, 10, 22]_5$, $[24, 14, 8]_7$, $[40, 11, 22]_7$, $[60, 10, 38]_7$, $[60, 13, 34]_7$, $[88, 8, 63]_7$, $[96, 11, 64]_7$, $[96, 13, 61]_7$ and $[96, 15, 58]_7$ are constructed.

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 Hamming weight of a vector x, denoted by $wt(x)$, is the number of nonzero entries in x. A linear code C of length n and dimension k over GF(q) is a k-dimensional subspace of V(n,q). Such a code is called $[n, k, d]_q$ code if its minimum Hamming weight is d. For linear codes, the minimum distance is equal to the minimum weight of the nonzero codewords. The orthogonal code $C^{\perp}$ of C is the set of words of length n that are orthogonal to all codewords in C, w.r.t. the ordinary inner product.

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

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. The codes with such parameters are called optimal.

Let A_i denote the number of codewords of C with weight i. The weight distribution of C is the list of numbers A_i. The weight distribution $A_0 = 1$, $A_d = \alpha, \ldots, A_n = \gamma$ is expressed as $0^1 d^{\alpha} \ldots n^{\gamma}$ also.

In the last years many good linear codes over GF(5) and GF(7) were constructed. In [2] Daskalov and Gulliver constructed 44 good codes and presented a table with lower and bounds on the minimum distances for $1 \leq k \leq 8, 1 \leq n \leq 100$. In [3] Daskalov, Hristov and Metodieva constructed 32 QC and QT codes. Grassl and White presented 28 new codes in [4] and 55 in [5]. Maruta

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

et al. constructed in [6], [7] and [8] eighteen, twenty four and twenty six new codes respectively. Six new codes were constructed in [9]. Fifty eight new linear codes over $GF(7)$ are constructed and a table for the minimum distances ($k \leq 7$, $n \leq 100$) is presented in [10]. Thirty tree linear codes over $GF(7)$ are constructed in [11]. New linear codes ($n \leq 50$) over $GF(7)$ are constructed in [12], [13], [14]. Good linear codes, including and some high-rate codes, are presented also in [15] and [16].

In the presented paper we continue our investigation from [15] and [16]. In the time of construction the codes presented in this paper improved the respective lower bounds on the minimum distances in Grassl's tables [17] and now are the best-known such codes.

2 Quasi-cyclic codes

The basic object in our considerations is the class of quasi-cyclic codes. A code C is said to be quasi-cyclic (QC or p-QC) if a cyclic shift of a codeword by p positions results in another codeword. The length, n, of a p-QC code is a multiple of p, so hat $n = pm$ [18]. With a suitable permutation of coordinates [19] a class of QC codes can be constructed from $m \times m$ circulant matrices. In this case, C has a generator matrix of the following form

$$G = [B_1,\ B_2,\ \dots,\ B_p], \qquad (1)$$

where B_i are circulant matrices.

The algebra of $m \times m$ circulant matrices over $\mathrm{GF}(q)$ is isomorphic to the algebra of polynomials in the ring $\mathrm{GF}(q)[x]/(x^m - 1)$ if B is mapped onto the polynomial, $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-1}x^{m-1}$, formed from the entries in the first row of B [1]. The polynomials $b_i(x)$, associated with a QC code are called the *defining polynomials* [18].

The dimension k of the QC code is equal to the degree of $h(x)$ [20], where

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

If $\deg h(x) = m$, then the dimension of the code is m, and (1) is a generator matrix. If $\deg h(x) = k < m$, then the matrices B_i in (1) are near circulant matrices i.e. circulant matrix with $m - k$ rows deleted. In this case the QC code is called *degenerate* [18].

3 The new codes over GF(5) and GF(7)

Theorem 3.1 *There exist QC codes with parameters* $[30, 10, 15]_5$, $[33, 11, 16]_5$.

Proof: The coefficients of the defining polynomials and the weight distributions of the codes are:

A $[30,10,15]_5$ **code**:

0000000001, 1124204402, 1121400003;

0^{1} 15^{2080} 16^{7020} 17^{22520} 18^{65280} 19^{149880} 20^{346292} 21^{660040} $22^{1083800}$ $23^{1508400}$ $24^{1746660}$ $25^{1679120}$ $26^{1291840}$ 27^{772280} 28^{329420} 29^{88360} 30^{12632}

A $[33,11,16]_5$ **code**:

01222012441, 10100324344, 00000000001;

0^{1} 16^{2420} 17^{9460} 18^{30844} 19^{93764} 20^{261800} 21^{651068} $22^{1439108}$ $23^{2717748}$ $24^{4568872}$ $25^{6545924}$ $26^{8075364}$ $27^{8360044}$ $28^{7185992}$ $29^{4938164}$ $30^{2636700}$ $31^{1025948}$ 32^{254188} 33^{30716}

Theorem 3.2 *There exist a code with parameters* $[41,10,22]_5$.

Proof: The generator matrix and the weight distribution of a code are:

$$G = \begin{pmatrix} 10000000001124204402112140000311231314300 \\ 01000000002112420440311214000001123131434 \\ 00100000000211242044031121400030112313140 \\ 00010000004021124204003112140043011231314 \\ 00001000004402112420000311214014301123134 \\ 00000100000440211242000031121431430112311 \\ 00000010002044021124400003112113143011234 \\ 00000001004204402112140000311231314301120 \\ 00000000102420440211214000031123131430113 \\ 00000000011242044021121400003112313143011 \end{pmatrix}$$

0^{1} 22^{744} 23^{3464} 24^{9868} 25^{25452} 26^{61344} 27^{134916} 28^{273636} 29^{486300} 30^{782716} $31^{1110920}$ $32^{1388616}$ $33^{1515936}$ $34^{1423136}$ $35^{1140784}$ 36^{758828} 37^{410424} 38^{173964} 39^{52796} 40^{10672} 41^{1108}

Theorem 3.3 *There exist high rate code with parameters* $[24,14,8]_7$.

Proof: The generator matrix and the weight distribution of a code are:

$$G = \begin{pmatrix} 423610423610000000000000 \\ 465201465201000000000000 \\ 026330435400100000000000 \\ 564363535200010000000000 \\ 610616214000001000000000 \\ 061061621400000100000000 \\ 561536654500000010000000 \\ 125603034200000001000000 \\ 643040234600000000100000 \\ 410214446300000000010000 \\ 256361652200000000001000 \\ 656116026400000000000100 \\ 550341464300000000000010 \\ 263304354000000000000001 \end{pmatrix}$$

0^{1} 8^{3654} 9^{50832} 10^{425052} $1^{3186288}$ $12^{20822340}$ $13^{115439688}$ $14^{544238244}$ $15^{2176066200}$ $16^{7345453896}$ $17^{20738832048}$ $18^{48394140564}$ $19^{91686811104}$ $20^{137538690156}$ $21^{157181317512}$ $22^{128605224636}$ $23^{67097856600}$ $24^{16774514034}$

Theorem 3.4 *There exist QC codes with parameters* $[40, 11, 22]_7$*,* $[60, 10, 38]_7$*,* $[60, 13, 34]_7$*,* $[88, 8, 63]_7$*,* $[96, 11, 64]_7$*,* $[96, 13, 61]_7$ *and* $[96, 15, 58]_7$*.*

Proof: The coefficients of the defining polynomials and the weight distributions of the codes are:

A $[40, 11, 22]_7$ **code**: 1556440061000000000, 35414452362321136401;
0^{1} 22^{4560} 23^{21600} 24^{96180} 25^{364080} $26^{1217880}$ $27^{3810000}$ $28^{10696560}$ $29^{26406360}$ $30^{58171548}$
$31^{112771200}$ $32^{189940560}$ $33^{276569400}$ $34^{341670240}$ $35^{351016728}$ $36^{292879380}$ $37^{189980400}$ $38^{89863260}$
$39^{27694680}$ $40^{4152126}$

A $[60, 10, 38]_7$ **code**: 331000000000, 250210261351, 403105264111, 514042322401, 560440523051;
0^{1} 38^{2376} 39^{9912} 40^{30276} 41^{96336} 42^{249240} 43^{623880} $44^{1450476}$ $45^{3045432}$ $46^{6031620}$ $47^{10754712}$
$48^{17446698}$ $49^{25622640}$ $50^{33956676}$ $51^{39919032}$ $52^{41353470}$ $53^{37437768}$ $54^{29186076}$ $55^{19092096}$
$56^{10229562}$ $57^{4301448}$ $58^{1338948}$ 59^{267696} 60^{28878}

A $[60, 13, 34]_7$ **code**: 12344321000000000000, 42613561501564230031, 05661452241504230031;
0^{1} 34^{3720} 35^{15600} 36^{74280} 37^{274920} $38^{1017480}$ $39^{3373200}$ $40^{10644720}$ $41^{31248600}$ $42^{85083120}$
$43^{213281760}$ $44^{494367840}$ $45^{1054182360}$ $46^{2063203560}$ $47^{3687216960}$ $48^{5992297590}$ $49^{8804553960}$
$50^{11624292600}$ $51^{13672393920}$ $52^{14198102910}$ $53^{12859026600}$ $54^{10002538320}$ $55^{6547491720}$ $56^{3507203700}$
$57^{1476258960}$ $58^{458310840}$ $59^{93175320}$ $60^{9375846}$

A $[88, 8, 63]_7$ **code**: 12306036, 14510603, 00012525, 00106412, 00001432, 13513142, 15511022, 11123235, 12025240,
11011353, 00000001;
0^{1} 63^{1632} 64^{4512} 65^{8256} 66^{16656} 67^{34128} 68^{65160} 69^{106704} 70^{174480} 71^{268656} 72^{381294} 73^{503328}
74^{604464} 75^{672144} 76^{701844} 77^{654720} 78^{550776} 79^{427056} 80^{281670} 81^{165792} 82^{86736} 83^{37248} 84^{12576}
85^{4128} 86^{840}

A $[96, 11, 64]_7$ **code**: 2525154106310614001460550153061126054100000000000, 360041143201301113525200615232245635252211622261;
0^{1} 64^{2754} 65^{6912} 66^{18576} 67^{67392} 68^{153216} 69^{387456} 70^{916560} $71^{1975968}$ $72^{4000140}$ $73^{8071200}$
$74^{15012432}$ $75^{26381184}$ $76^{43720848}$ $77^{68309856}$ $78^{99434448}$ $79^{136235232}$ $80^{173901780}$ $81^{205788480}$
$82^{225847152}$ $83^{228783744}$ $84^{212396592}$ $85^{179650368}$ $86^{138030048}$ $87^{95439168}$ $88^{58289796}$ $89^{31515552}$
$90^{14662464}$ $91^{5829408}$ $92^{1894032}$ 93^{497376} 94^{92592} 95^{12960} 96^{1056}

A $[96, 13, 61]_7$ **code**: 2410322246135661361664335366362534510000000000000, 024624513023516233062555644066503435351451450361;
0^{1} 61^{6048} 62^{15552} 63^{45792} 64^{147348} 65^{443232} $66^{1188480}$ $67^{3094560}$ $68^{7801200}$ $69^{18779040}$
$70^{43454160}$ $71^{95385600}$ $72^{198956064}$ $73^{393827040}$ $74^{734367600}$ $75^{1294196352}$ $76^{2144382192}$
$78^{590103968}$ $81^{1491214240}$ $84^{1816395520}$ $85^{228415168}$ $87^{367422368}$ $89^{1542674592}$ $90^{719256960}$
$91^{285332256}$ $92^{93211056}$ $93^{24076704}$ $94^{4692384}$ 95^{611136} 96^{42486}

A $[96, 15, 58]_7$ **code**: 6031440652342601354532153023400241000000000000000, 640313561105404512343502661561165326411261424651;
0^{1} 58^{4320} 59^{11808} 60^{57744} 61^{203328} 62^{656928} $63^{2152320}$ $64^{6641874}$ $65^{19658304}$ $66^{55177152}$
$67^{148230720}$ $68^{379245744}$ $69^{923984160}$ $70^{2137170528}$ $71^{+403042496}$ $72^{1194511828}$ $73^{2125657280}$

$74^{1643946448}$ $76^{1965003456}$ $77^{496025632}$ $79^{680604032}$ $80^{424402100}$ $81^{367055072}$ $82^{1333042272}$ $86^{703990672}$ $87^{929886976}$ $90^{937797808}$ $91^{1080566592}$ $92^{260736944}$ $93^{1174700736}$ $94^{224626032}$ $95^{28479744}$ $96^{1770216}$

References

[1] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[2] R. Daskalov, T. Gulliver, Bounds on minimum distance for linear codes over GF(5), *AAECC* 9, 1999, 521-546.

[3] R. Daskalov, P. Hristov, E. Metodieva, New minimum distance bounds for linear codes over GF(5), *Discr. Math.* 275, 2004, 97-110.

[4] M. Grassl, G. White, New goog linear codes by special puncturings, *Proc. ISIT2004*, Chicago, USA, 2004, 454.

[5] M. Grassl, G. White, New codes from chains of quasi-cyclic codes, *Proc. ISIT2005*, Adelaide, Australia, 2005, 2095-2099.

[6] T. Maruta, M. Takenaka, M. Shinohara, Y. Shobara, Constructing new linear codes from pseudo-cyclic codes, *Proc. Ninth Intern. Workshop ACCT*, Kranevo, Bulgaria, 2004, 292-298.

[7] T. Maruta, M. Shinohara, F. Yamane, K. Tsuji, E. Takanaka, H. Miki, R. Fujiwara, New linear codes from cyclic and generalized cyclic codes by puncturing, *Proc. Tenth Intern. Workshop ACCT*, Zvenigorod, Rissia, 2006, 194-197.

[8] T. Maruta, M. Shinohara, M. Takenaka, Constructing linear codes from some orbits of projectivities, *Discr. Math.*, to appear.

[9] M. Braun, A. Kohnert, A. Wassermann, Optimal linear codes from matrix groups, *IEEE Trans. Inform. Theory* 51, 2005, 4247-4251.

[10] R. N. Daskalov, T. A. Gulliver, Minimum distance bounds for linear codes over GF(7), *JCMCC* 36, 2001, 175-191.

[11] R. N. Daskalov, T. A. Gulliver, New minimum distance bounds for linear codes over small fields, *Probl. Pered. Inform.* 37, 3, 2001, 24-33.

[12] R. N. Daskalov, P. Hristov, New one-generator quasi-cyclic codes over GF(7), *Probl. Pered. Inform.* 38, 1 , 2002, 59-63.

[13] T. Rehfinger, N. S. Babu, K. Zimmermann, New good codes via CQuest – a system for the silicon search of linear codes, *Algebr. Combin. Appl.*, A. Betten et al., eds, Springer, 2001, 294-306.

[14] E. Metodieva, Six new linear codes over GF(7), *Math. Educ. Math.*, Sofia, 2004, 158-161.

[15] R. Daskalov, Some high-rate linear codes over GF(5) and GF(7), *Probl. Pered. Inform.* 43, 2, 2007, 65-73.

[16] R. Daskalov, E. Metodieva, Minimum distance bounds for 7-ary linear codes, *Proc. Fifth Intern. Workshop OCRT*, White Lagoon, Bulgaria, 2007, 62-67.

[17] M. Grassl, Bounds on the minimum distance of linear codes [electronic table; online], `http://www.codetables.de`.

[18] P. P. Greenough, R. Hill, Optimal ternary quasi-cyclic codes, *Des., Codes Crypt.* 2, 1992, 81-91.

[19] T. Koshy, Polynomial approach to quasi-cyclic codes, *Bul. Cal. Math. Soc.* 69, 1977, 51-59.

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