МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2001
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2001
Proceedings of Thirtieth Spring Conference of the Union of Bulgarian Mathematicians
Borovets, April 8–11, 2001

NEW SYSTEMATIC QUASI-CYCLIC CODES OVER $GF(9)$ IN DIMENSIONS 7 AND 8

Rumen N. Daskalov, Stoyan N. Kapralov

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, the existence of the next record-breaking codes $[35,7,23]_9$, $[42,7,29]_9$, $[49,7,34]_9$, $[56,7,40]_9$, $[63,7,46]_9$, $[98,7,75]_9$, $[105,7,81]_9$, $[112,7,87]_9$, $[119,7,93]_9$, $[126,7,99]_9$, $[133,7,105]_9$, $[48,8,32]_9$, $[56,8,39]_9$, $[104,8,78]_9$, $[112,8,85]_9$, $[120,8,91]_9$, $[128,8,98]_9$ and $[136,8,105]_9$ is proved.

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 $GF(q)$. 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 distance is d.

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. 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.

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

For the case of linear codes over $GF(9)$, Problem 2 has been solved for $k \leq 3$ (see [6]). In addition Bierbrauer and Gulliver [1] constructed many new codes in dimensions $k = 4$, 5. Daskalov and Gulliver [3] obtained new codes in dimension $k = 6$. In this paper we consider the next two dimensions. Eleven new 7-dimensional and seven new 8-dimensional quasi-cyclic (QC) linear codes are constructed, which improve the respective lower bounds in Brouwer's tables [2].

2. Preliminary results. Quasi-cyclic codes form an important class of linear codes which contains the well-known class of cyclic codes. These codes are a very natural generalization of cyclic codes and some of the next facts motivated many researches for their investigation:

- QC codes meet a modified version of Gilbert-Varshamov bound [8];

This work was partially supported by the UNESCO UVO-ROSTE Grant No. 875.695.0.

- Some of the best quadratic residue codes and Pless symmetry codes are QC codes [9];
- QC codes consist a large number of record breaking codes and many of them are optimal codes;
- There is a link between QC codes and convolutional codes [4].

The Structure of Quasi-Cyclic Codes. A code C is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword in C. A cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = mp$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $(m \times m)$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0; R_1; R_2; \ldots; R_{p-1}]\,, \tag{1}$$

where R_i, $i = 0, 1, \ldots, p-1$ is a circulant matrix of the form

$$R = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & a_1 & \cdots & a_{m-2} \\ a_{m-2} & a_{m-1} & a_0 & \cdots & a_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}. \tag{2}$$

If one of the matrices R_i, $i = 0, 1, \ldots, p-1$ is the identity matrix, then the QC code is called *systematic.*

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 R is mapped onto the polynomial, $r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1}$, formed from the entries in the first row of R [9]. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [5].

If the defining polynomials $r_i(x)$ contain a common factor which is also a factor of $x^m - 1$, then the QC code is called *degenerate* [5]. Define the *order* of this QC code as [10]

$$h(x) = \frac{x^m - 1}{\gcd\{x^m - 1, r_0(x), r_1(x), \ldots, r_{p-1}(x)\}}. \tag{3}$$

The dimension k of the QC code is equal to the degree of $h(x)$. If the polynomial $h(x)$ is of degree m, the dimension of the code is m, and (1) 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 (1).

For convenience, the coefficients of the defining polynomials are given as integers. For GF(9), $\alpha = 3$, $\alpha^2 = 7$, $\alpha^3 = 8$, $\alpha^4 = 2$, $\alpha^5 = 6$, $\alpha^6 = 5$, $\alpha^7 = 4$, where α is a root of the ternary primitive polynomial $x^2 + x + 2$. The defining polynomials are listed with the lowest degree coefficient on the left, i.e., 17352 corresponds to the polynomial $1 + 7x + 3x^2 + 5x^3 + 2x^4$.

3. The New Codes.

Theorem 1. *There exist quasi-cyclic codes with parameters:*

$$[35,7,23]_9,\ [42,7,29]_9,\ [49,7,34]_9,\ [56,7,40]_9,\ [63,7,46]_9,$$

$$[98,7,75]_9,\ [105,7,81]_9,\ [112,7,87]_9,\ [119,7,93]_9,\ [126,7,99]_9,\ [133,7,105]_9$$

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

A $[35,7,23]_9$**-code:**
1000000, 5100011, 1126467, 6330121, 3011338;
$0^{1}23^{616}24^{4536}25^{12880}26^{42560}27^{108416}28^{247128}29^{479136}30^{765408}31^{996240}32^{988064}33^{723576}34^{335888}35^{78520}$

A $[42,7,29]_9$**-code:**
1000000, 0113383, 1132204, 6711264, 0015663, 0121633;
$0^{1}29^{1176}30^{6160}31^{18536}32^{48104}33^{110600}34^{236264}35^{439552}36^{677600}37^{884744}38^{930160}39^{760760}40^{455616}$
$41^{180488}42^{33208}$

A $[49,7,34]_9$**-code:**
1000000, 3301216, 1111160, 1205357, 0015663, 4671126, 0113383;
$0^{1}34^{224}35^{1400}36^{8568}37^{21392}38^{53536}39^{113848}40^{219800}41^{397152}42^{618528}43^{803488}44^{857920}45^{762608}$
$46^{546448}47^{273056}48^{90608}49^{14392}$

A $[56,7,40]_9$**-code:**
1000000, 1126467, 0121633, 1112316, 3383011, 1111706, 1205357, 5663001;
$0^{1}40^{504}41^{3192}42^{9416}43^{23744}44^{52248}45^{113400}46^{216384}47^{369936}48^{553168}49^{719600}50^{806064}51^{765128}$
$52^{589512}53^{350112}54^{159096}55^{45416}56^{6048}$

A $[63,7,46]_9$**-code:**
1000000, 0010257, 1112804, 0611117, 7120535, 0113383, 0015663, 1126467, 0121633;
$0^{1}46^{952}47^{3864}48^{10472}49^{25992}50^{55216}51^{113008}52^{204624}53^{336616}54^{500192}55^{659792}56^{766136}57^{740600}$
$58^{620256}59^{410200}60^{222096}61^{86352}62^{23128}63^{3472}$

A $[98,7,75]_9$**-code:**
1000000, 1120127, 1120316, 1112364, 0010408, 1117034, 0101356, 1112804, 1111706, 1205357, 5663001, 1264671, 0121633, 1338301;
$0^{1}75^{392}76^{3472}77^{6888}78^{14840}79^{28392}80^{53984}81^{95872}82^{155120}83^{234416}84^{346416}85^{450296}86^{556360}$
$87^{604576}88^{606704}89^{541576}90^{437864}91^{304592}92^{182672}93^{100520}94^{40936}95^{13104}9^{2968}97^{896}98^{112}$

A $[105,7,81]_9$**-code:**
1000000, 1205357, 0015663, 1126467, 0113383, 0121633, 1120415, 2711201, 0010408, 3411170, 0101356, 0411128, 1120316, 1112364, 1111706;
$0^{1}81^{1008}82^{3864}83^{7616}84^{13720}85^{27440}86^{54208}87^{92400}88^{142408}89^{225960}90^{326144}91^{419328}92^{518056}$
$93^{581056}94^{591864}95^{547120}96^{455224}97^{334656}98^{222216}99^{123536}100^{63112}101^{22512}102^{7224}103^{1904}104^{280}105^{112}$

A $[112,7,87]_9$**-code:**
1000000, 1120412, 1121476, 2711201, 1120316, 1112364, 0800104, 3411170, 0101356, 1112804, 1111706, 1205357, 3001566, 7112646, 0121633, 0113383;
$0^{1}87^{1624}88^{3416}89^{7112}90^{15344}91^{29568}92^{49784}93^{85960}94^{137928}95^{213192}96^{300552}97^{403984}98^{486976}$
$99^{552384}100^{567392}101^{547064}102^{473816}103^{363832}104^{249200}105^{157032}106^{81816}107^{36680}108^{13384}109^{4144}$
$110^{616}111^{112}112^{56}$

A $[119,7,93]_9$**-code:**
1000000, 1123705, 1130128, 1121476, 0121633, 0113383, 1120127, 1120316, 1236411, 0010408, 1117034, 0101356, 7061111, 1205357, 0015663, 1126467, 1112804;

$0^{1} 93^{1512} 94^{2688} 95^{7784} 96^{16744} 97^{28392} 98^{50736} 99^{83272} 100^{130928} 101^{197848} 102^{281960} 103^{378112} 104^{456288}$
$105^{530768} 106^{551432} 107^{544712} 108^{479192} 109^{389032} 110^{279272} 111^{184520} 112^{10288} 113^{53368} 114^{20608} 115^{8400}$
$116^{2128} 117^{336} 118^{56}$

A $[126, 7, 99]_9$**-code:**
1000000, 1117034, 0101356, 1112804, 1111706, 1205357, 1120415, 1124345, 1130128, 1121476, 1120127, 3161120, 1112364, 0800104, 0015663, 0113383, 1126467, 0121633;
$0^{1} 99^{1680} 100^{3248} 101^{9016} 102^{15400} 103^{27216} 104^{50120} 105^{78680} 106^{123816} 107^{189448} 108^{265328} 109^{350168}$
$110^{435512} 111^{502320} 112^{540960} 113^{532560} 114^{487480} 115^{407120} 116^{305144} 117^{208656} 118^{128296} 119^{69280} 120^{32144}$
$121^{14168} 122^{3752} 123^{1176} 124^{168} 125^{112}$

A $[133, 7, 105]_9$**-code:**
1000000, 0112863, 1121760, 1124345, 1130128, 1111706, 1205357, 0015663, 1126467, 1121476, 1120127, 1120316, 6411123, 4080010, 1117034, 0101356, 1112804, 0121633, 0113383;
$0^{1} 105^{1288} 106^{4032} 107^{9016} 108^{15232} 109^{27608} 110^{48888} 111^{75040} 112^{118552} 113^{174552} 114^{250936} 115^{335832}$
$116^{407120} 117^{478688} 118^{517104} 119^{533064} 120^{485576} 121^{423416} 122^{326312} 123^{236824} 124^{151424} 125^{86464} 126^{43856}$
$127^{21000} 128^{8176} 129^{2184} 130^{728} 131^{56}$

Table 1. New 7-dimensional QC codes over GF(9)

N:	code	d	d_{br}	N:	code	d	d_{br}
1	[35,7]	23	22	7	[105,7]	81	79
2	[42,7]	29	27	8	[112,7]	87	84
3	[49,7]	34	33	9	[119,7]	93	91
4	[56,7]	40	39	10	[126,7]	99	96
5	[63,7]	46	45	11	[133,7]	105	
6	[98,7]	75	74				

Theorem 2. *There exist quasi-cyclic codes with parameters:*

$$[48, 8, 32]_9,\ [56, 8, 39]_9,\ [104, 8, 78]_9,$$

$$[112, 8, 85]_9,\ [120, 8, 91]_9,\ [128, 8, 98]_9,\ [136, 8, 105]_9.$$

Proof. The coefficients of the defining polynomials end the wieght distributions of these codes are as follows:
A $[48, 8, 32]_9$**-code:**
10000000, 11112468, 11165047, 11128523, 11360420, 01134665;
$0^{1} 32^{544} 33^{4800} 34^{17472} 35^{53952} 36^{153824} 37^{393984} 38^{927200} 39^{1881536} 40^{3387696} 41^{5293184} 42^{7057152} 43^{7890240}$
$44^{7185792} 45^{5092800} 46^{2650848} 47^{899008} 48^{156688}$

A $[56, 8, 39]_9$**-code:**
10000000, 12607811, 20211140, 28523111, 13604201, 65047111, 34665011;
$0^{1} 39^{2176} 40^{8800} 41^{27712} 42^{77760} 43^{207552} 44^{478208} 45^{1023360} 46^{1941152} 47^{3320256} 48^{4952192} 49^{6515648} 50^{7292384}$
$51^{6880320} 52^{5258784} 53^{3173056} 54^{1412288} 55^{414784} 56^{60288}$

A $[104, 8, 78]_9$**-code:**
10000000, 00101415, 00010281, 11206364, 11121340, 11242285, 11572132, 11136525, 11140202, 11128523, 11360420, 11165047, 01134665;
$0^{1} 78^{1440} 79^{3840} 80^{9968} 81^{26304} 82^{53952} 83^{117824} 84^{228160} 85^{424960} 86^{755776} 87^{1266752} 88^{1936432} 89^{2782272}$

$90^{3744576}\,91^{4579456}\,92^{5175152}\,93^{5360832}\,94^{5035008}\,95^{4200448}\,96^{3164264}\,97^{2076480}\,98^{1190144}\,99^{586944}\,100^{235872}$
$101^{69696}\,102^{16992}\,103^{2880}\,104^{296}$

A $[112, 8, 85]_9$**-code:**
10000000, 00128631, 00101828, 00010281, 11206364, 11121340, 11242285, 11572132, 11136525, 11140202, 11128523, 11360420, 11165047, 01134665;
$0^{1}\,85^{1728}\,86^{5056}\,87^{13824}\,88^{27200}\,89^{64512}\,90^{133216}\,91^{254848}\,92^{462272}\,93^{773248}\,94^{1255104}\,95^{1906304}\,96^{2722696}$
$97^{3579520}\,98^{4382592}\,99^{4980992}\,100^{5149296}\,101^{4935808}\,102^{4244832}\,103^{3268544}\,104^{260400}\,105^{1382080}\,106^{742976}$
$107^{336128}\,108^{120400}\,109^{34816}\,110^{7040}\,111^{1216}\,112^{72}$

A $[120, 8, 91]_9$**-code:**
10000000, 01134665, 00010127, 00128631, 00101828, 00010281, 11206364, 11128523, 11121340, 11242285, 11360420, 13211572, 25111365, 11140202, 04711165;
$0^{1}\,91^{704}\,92^{2352}\,93^{7040}\,94^{15104}\,95^{33920}\,96^{76016}\,97^{143616}\,98^{271008}\,99^{477952}\,100^{803488}\,101^{1254784}\,102^{1885248}$
$103^{2638080}\,104^{3463280}\,105^{4204928}\,106^{4769408}\,107^{4984128}\,108^{4792576}\,109^{4253056}\,110^{3377312}\,111^{2431360}$
$112^{1563944}\,113^{890496}\,114^{443616}\,115^{181376}\,116^{62272}\,117^{16576}\,118^{2784}\,119^{256}\,120^{40}$

A $[128, 8, 98]_9$**-code:**
10000000, 00124245, 00010248, 00128631, 00101828, 00010281, 11206364, 11121340, 11242285, 11572132, 11136525, 11140202, 11128523, 11360420, 11165047, 01134665;
$0^{1}\,98^{1088}\,99^{3584}\,100^{9344}\,101^{19520}\,102^{39840}\,103^{82496}\,104^{161528}\,105^{279296}\,106^{506272}\,107^{806912}\,108^{1268992}$
$109^{1840512}\,110^{2556096}\,111^{3354944}\,112^{4033424}\,113^{4580480}\,114^{4840960}\,115^{4714880}\,116^{4225616}\,117^{3439296}$
$118^{2573280}\,119^{1717312}\,120^{1036280}\,121^{555840}\,122^{260352}\,123^{96832}\,124^{31408}\,125^{8896}\,126^{1248}\,127^{128}\,128^{64}$

A $[136, 8, 105]_9$**-code:**
10000000, 01127243, 00128242, 00010248, 00128631, 82800101, 00010281, 36411206, 11121340, 85112422, 21321157, 65251113, 11140202, 28523111, 11360420, 11165047, 34665011;
$0^{1}\,105^{1344}\,106^{4064}\,107^{11392}\,108^{24000}\,109^{46272}\,110^{92160}\,111^{170752}\,112^{299832}\,113^{511552}\,114^{821120}\,115^{1259200}$
$116^{1828400}\,117^{2504384}\,118^{3222656}\,119^{3888256}\,120^{4405296}\,121^{4667712}\,122^{4600864}\,123^{4224192}\,124^{3510912}$
$125^{2674752}\,126^{1883168}\,127^{1180160}\,128^{662360}\,129^{329984}\,130^{146400}\,131^{56512}\,132^{14896}\,133^{3648}\,134^{384}\,135^{64}\,136^{32}$

Table 2. New 8-dimensional QC codes over GF(9)

N:	code	d	d_{br}	N:	code	d	d_{br}
1	[48,8]	32	31	5	[120,8]	91	87
2	[56,8]	39	38	6	[128,8]	98	94
3	[104,8]	78	77	7	[136,8]	105	
4	[112,8]	85	82				

REFERENCES

[1] J. Bierbrauer, T. A. Gulliver. New linear codes over $GF(9)$. *Austral. J. Comb.*, **21** (2000), 131–140.

[2] A. E. Brouwer. Linear code bounds [electronic table; online], www.win.tue.nl/math/dw/personalpages/aeb/voorlincod.html.

[3] R. N. Daskalov, T. A. Gulliver. New 6-Dimensional Linear Codes over $GF(8)$ and $GF(9)$. *J. Combinatorial Math. & Combinatorial Compt.* (submitted for publication, Oct. 2000).

[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), No 1, 431–435.

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

[6] R. Hill. Optimal linear codes. In: Cryptography and Coding II (Ed. C. Mitchel). Oxford, UK, Oxford Univ. Press, 1992, 75–104.
[7] R. Hill, D. E. Newton. Optimal ternary linear codes. *Designs, Codes & Crypt.*, **2** (1992), 137–157.
[8] T. Kassami. A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2. *IEEE Trans. Inform. Theory*, **IT-20** (1974), 679–680.
[9] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. New York, North-Holland Publishing Co., 1977.
[10] G. E. Séguin, G. Drolet. The theory of 1-generator quasi-cyclic codes. Techncial Report, Royal Military College of Canada, Kingston, ON, 1991.

Rumen Nikolov Daskalov, Stoyan Nedkov Kapralov
Department of Mathematics
Technical University of Gabrovo
5300 Gabrovo, Bulgaria
e-mail: `daskalov@tugab.bg, kapralov@tugab.bg`

НОВИ СИСТЕМАТИЧНИ КВАЗИ-ЦИКЛИЧНИ КОДОВЕ НАД $GF(9)$ В РАЗМЕРНОСТИ 7 И 8

Румен Н. Даскалов, Стоян Н. Капралов

Нека $[n,k,d]_q$-код е линеен код с дължина n, размерност k и минимално хемингово разстояние d над $GF(q)$. В този доклад са конструирани следните нови кодове $[35,7,23]_9$, $[42,7,29]_9$, $[49,7,34]_9$, $[56,7,40]_9$, $[63,7,46]_9$, $[98,7,75]_9$, $[105,7,81]_9$, $[112,7,87]_9$, $[119,7,93]_9$, $[126,7,99]_9$, $[133,7,105]_9$, $[48,8,32]_9$, $[56,8,39]_9$, $[104,8,78]_9$, $[112,8,85]_9$, $[120,8,91]_9$, $[128,8,98]_9$, $[136,8,105]_9$, които подобряват известните в момента долни граници за минималното разстояние в таблиците на Брауер.