New linear codes over $\mathbb{F}_9$

Jürgen Bierbrauer

Department of Mathematical Sciences
Michigan Technological University, Houghton, Michigan, USA
jbierbra@mtu.edu

T. Aaron Gulliver*

Department of Electrical and Electronic Engineering
University of Canterbury, Christchurch, New Zealand

Abstract

Let $d_9(n,k)$ be the maximum possible minimum Hamming distance of a linear $[n,k]$ code over $\mathbb{F}_9$. In this paper, twenty-four new linear codes over $\mathbb{F}_9$ are constructed which improve the table of $d_9(n,k)$ by Brouwer. Four of these codes meet the upper bound on $d_9(n,k)$ and so are optimal. A geometric interpretation of the small dimensional codes is also given.

1 Introduction

Let $\mathbb{F}_q$ denote the Galois field of q elements, and let $V(n,q)$ denote the vector space of all ordered n-tuples over $\mathbb{F}_q$. A linear $[n,k]$ code C of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of $V(n,q)$. Define an inner product on $\mathbb{F}_q^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n$ where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$. The $[n, n-k]$ dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. An $[n,k,d]$ code is an $[n,k]$ code with minimum (Hamming) distance d. Let A_i be the number of codewords of (Hamming) weight (or distance) i in C. Then the numbers $A_0, A_1, \ldots, A_n$ are called the weight distribution of C.

A central problem in coding theory is that of optimising one of the parameters n, k and d for given values of the other two. One version is to find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d]$ code over $\mathbb{F}_q$. Another is to find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d]$ code over $\mathbb{F}_q$. A code which achieves either of these values is called *optimal*.

* Current address: University of Victoria, P.O. Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6, agullive@ece.uvic.ca

The Griesmer bound is a well-known lower bound on $n_q(k,d)$

$$n_q(k,d) \geq g_q(k,d) = \sum_{j=0}^{k-1} \lceil \frac{d}{q^j} \rceil, \tag{1}$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$. For $k \leq 2$, the Griesmer bound is met for all q and d. In addition, most values of $n_9(3,d)$ (and thus $d_9(n,3)$) have been determined [4]. For larger dimensions, far less is known. In this paper we consider codes for dimensions $k = 3 - 5$. Twenty-four codes are found which improve the lower bounds on minimum distance. Four of these codes meet the Griesmer bound and so are optimal.

A *punctured code* of C is a code obtained by deleting a coordinate from every codeword of C. A *shortened code* of C is a code obtained by taking only those codewords of C having a zero in a given coordinate position and then deleting that coordinate. The following bounds can be established based on these constructions

1) $d_q(n+1,k) \leq d_q(n,k) + 1$,

and

2) $d_q(n+1,k+1) \leq d_q(n,k)$.

Using the codes given in this paper, they provide many additional bound improvements.

The next section presents the class of linear codes considered in this paper, and the construction results.

2 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

$$G = [R_0;\ R_1;\ R_2;\ \ldots;\ R_{p-1}], \tag{2}$$

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

$$R_i = \begin{bmatrix} r_{0,i} & r_{1,i} & r_{2,i} & \cdots & r_{m-1,i} \\ r_{m-1,i} & r_{0,i} & r_{1,i} & \cdots & r_{m-2,i} \\ r_{m-2,i} & r_{m-1,i} & r_{0,i} & \cdots & r_{m-3,i} \\ \vdots & \vdots & \vdots & & \vdots \\ r_{1,i} & r_{2,i} & r_{3,i} & \cdots & r_{0,i} \end{bmatrix}. \tag{3}$$

The algebra of $m \times m$ circulant matrices over $\mathbb{F}_q$ is isomorphic to the algebra of polynomials in the ring $\mathbb{F}_q[x]/(x^m - 1)$ if R_i is mapped onto the polynomial, $r_i(x) =$

$r_{0,i}+r_{1,i}x+r_{2,i}x^2+\cdots+r_{m-1,i}x^{m-1}$, formed from the entries in the first row of R [11]. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [6]. The set $\{r_0(x), r_1(x), \cdots, r_{p-1}(x)\}$ defines an $[mp, k]$ QC code where $k = m - \deg(h(x))$ and

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

is the *order* of the code [13]. Codes for which $k < m$ are called *degenerate* [6].

The QC codes presented here are constructed from a set of defining polynomials. These are the equivalence class representatives of a partition of the set of polynomials of degree less than m into *cyclic classes*. Two polynomials, $r_j(x)$ and $r_i(x)$ are said to be *equivalent* if they belong to the same class, i.e.

$$r_j(x) = \alpha x^l r_i(x) \bmod (x^m - 1),$$

for some integer $l > 0$ and scalar $\alpha \in \mathbb{F}_9 \backslash \{0\}$. The number of representative defining polynomials $N(m)$, for $m \leq 6$, is given below

m	$N(m)$
2	7
3	32
4	213
5	1478

The QC codes presented here were constructed using a nonexhaustive heuristic combinatorial search, similar to that in [5],[7],[9]. The search for a $[pm, k]$ code was initialized with a randomly selected subset of p defining polynomials, or in some cases, with defining polynomials from a power residue code [10]. Since every subset of these polynomials gives a QC code, the object is to find a subset which gives a high minimum distance. To achieve this goal, polynomials were substituted into this subset using a greedy algorithm until either a distance bound or an iteration limit was reached.

The codes which improve the lower bounds on minimum distance are given in Table 1. The defining polynomials are listed with the lowest degree coefficient on the left, i.e., 4321 corresponds to the polynomial $x^3 + 2x^2 + 3x + 4$. The correspondence between these coefficients and the elements of $\mathbb{F}_9$ is

Coeff.	$\mathbb{F}_9$
0	0
1	1
2	2
3	α
4	$\alpha+1$
5	$\alpha+2$
6	2α
7	$2\alpha+1$
8	$2\alpha+2$

Table 1: QC Codes Over $\mathbb{F}_9$ Which Improve the Lower Bounds on Minimum Distance

code	d	$d^{\perp}$	m	$r_i(x)$
[55,3]	48	3	5	15351, 14837, 14241, 14413, 14726, 15775, 18481, 15188, 14365 1551, 14678
[24,4]	19	4	4	1168, 1, 1236, 113, 1175, 176
[32,4]	26	4	4	1114, 1468, 18, 1187, 1535, 1184, 164, 1142
[40,4]	33	4	5	2535, 246, 26187, 22788, 21222, 2625, 2562, 2112
[45,4]	37	3	5	2715, 2361, 2163, 2157, 21246, 21516, 2343, 2517, 27438
[55,4]	46	3	5	22878, 2247, 21534, 2328, 2265, 22353, 21222, 264, 21786, 246, 2157
[105,4]	90	3	7	2874281, 2835277, 232521, 255583, 281318, 2871114, 2868385 2864176, 241263, 277457, 288661, 2753824, 285824, 254154, 224723
[119,4]	102	3	7	2755485, 226431, 2856372, 247126, 210403, 2868385, 287532 233706, 2866724, 21357, 2881228, 2741165, 2613761, 2867253 251077, 282747, 23065
[126,4]	108	3	7	272633, 2881228, 248558, 282747, 241263, 22786, 235367, 2864176 263137, 232521, 2837825, 2753824, 2713472, 2761322, 288661 221646, 2888571, 27571
[130,4]	111	3	5	21555, 2112, 21183, 21615, 21444, 22416, 21327, 21318, 21285 26547, 2184, 22776, 21624, 2472, 27654, 2427, 2037, 21174, 21888 22434, 27267, 222, 27465, 21264, 2046, 2481
[32,5]	24	4	8	686667, 68541, 62321121, 6755406
[40,5]	31	4	8	615012, 681255, 65772366, 6676464, 62772768
[48,5]	38	4	8	664626, 68541, 6425838, 6238356, 68448537, 6471474
[55,5]	44	4	11	1175761245, 12785132328, 1572374127, 1128283458, 11135413524
[66,5]	53	4	11	12127183437, 1308705183, 11175862134, 11214136785, 1027064358 12685252416
[77,5]	63	4	11	1206264438, 115056864, 1563501762, 157430286, 1224157773 1745764878, 12546262815
[80,5]	65	3	8	6814203, 6615411, 6576018, 608478, 62153721, 62334186, 6632241 68268882, 6733527, 6718362
[88,5]	72	3	11	1282733361, 1775131518, 12783141516, 1362465126, 11512742646 1336171614, 1031486832, 1306714074
[99,5]	82	3	11	1124247864, 1774152327, 11223246774, 1226175558, 1173770133 1487547534, 11875142316, 11684132517, 1047542178
[110,5]	91	3	11	1427814264, 1583412882, 1881124743, 1862225844, 1636711341 156451068, 1621361385, 12537182823, 1126265346, 1274662233
[121,5]	101	3	11	1182853482, 1310830857, 1724517237, 11226273447, 1131366741 1153505313, 11318625285, 1204246683, 1206264438, 1774152327 155415414
[132,5]	110	3	11	11177826816, 146332188, 104258763, 12764242317, 1053325404 11542118376, 1153505313, 11155324314, 1147452087, 1881124743 1663141317, 1050388731

with α a root of the primitive polynomial $x^2 + x + 2$. The minimum distance and the dual distance of the codes are also given in Table 1.

As an example, consider a [36,3] code with $m = 3, p = 12$, and the following generator matrix

$$G = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c} 176 & 116 & 011 & 117 & 018 & 112 & 127 & 017 & 016 & 158 & 015 & 125 \\ 617 & 611 & 101 & 711 & 801 & 211 & 712 & 701 & 601 & 815 & 501 & 512 \\ 761 & 161 & 110 & 171 & 180 & 121 & 271 & 170 & 160 & 581 & 150 & 251 \end{array}\right].$$

The corresponding weight distribution is

i	A_i
0	1
31	288
32	360
36	80

This code is optimal since it meets the Griesmer bound (1). Now consider a degenerate [48,3] code with $m = 4, p = 12$, and the following generator matrix

$$G = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c} 0156 & 1185 & 1158 & 1545 & 0174 & 0183 & 1173 & 1263 & 1518 & \cdots & 1353 & 1257 & 1236 \\ 6015 & 5118 & 8115 & 5154 & 4017 & 3018 & 3117 & 3126 & 8151 & & 3135 & 7125 & 6123 \\ 5601 & 8511 & 5811 & 4515 & 7401 & 8301 & 7311 & 6312 & 1815 & & 5313 & 7512 & 3612 \end{array}\right].$$

This code has the following three-weight distribution

i	A_i
0	1
42	576
45	128
48	24

and also meets the Griesmer bound.

Two codes listed in Table 1 also meet (1). The [55,3,48] code establishes that $d_9(55, 3) = 48$. This code has weight distribution

i	A_i
0	1
48	360
49	240
50	48
51	40
54	40

The [24,4,19] code establishes that $d_9(24, 4) = 19$. This code has weight distribution

Table 2: Weight Distributions of the New QC Codes

Code	Weight Distribution
$[32,4]$	$0^1 26^{896} 27^{1792} 28^{640} 29^{1280} 30^{640} 31^{1280} 32^{32}$
$[40,4]$	$0^1 33^{960} 34^{1280} 35^{1600} 36^{800} 37^{640} 38^{320} 39^{960}$
$[45,4]$	$0^1 37^{840} 38^{880} 39^{1240} 40^{1040} 41^{960} 42^{600} 43^{640} 44^{320} 45^{40}$
$[55,4]$	$0^1 46^{880} 47^{1360} 48^{1240} 49^{720} 50^{680} 51^{520} 52^{680} 53^{240} 54^{240}$
$[105,4]$	$0^1 90^{2184} 93^{2128} 96^{1624} 99^{560} 102^{56} 105^{8}$
$[119,4]$	$0^1 102^{1008} 103^{1008} 104^{616} 105^{1072} 106^{392} 107^{448} 108^{896} 109^{280} 110^{168} 111^{280} 112^{112} 113^{112} 114^{112} 115^{56}$
$[126,4]$	$0^1 108^{1008} 109^{784} 110^{840} 111^{616} 112^{672} 113^{616} 114^{504} 115^{504} 116^{392} 117^{224} 118^{168} 119^{64} 120^{56} 121^{56} 122^{56}$
$[130,4]$	$0^1 111^{680} 112^{720} 113^{720} 114^{720} 115^{720} 116^{680} 117^{400} 118^{360} 119^{680} 120^{240} 121^{360} 122^{80} 123^{200}$
$[32,5]$	$0^1 24^{1112} 25^{2944} 26^{4736} 27^{7808} 28^{11408} 29^{13056} 30^{11392} 31^{5376} 32^{1216}$
$[40,5]$	$0^1 31^{1792} 32^{3208} 33^{4352} 34^{7424} 35^{10048} 36^{12208} 37^{10112} 38^{6688} 39^{2816} 40^{400}$
$[48,5]$	$0^1 38^{2240} 39^{3072} 40^{5392} 41^{6592} 42^{8512} 43^{10688} 44^{9824} 45^{7744} 46^{3648} 47^{1216} 48^{120}$
$[55,5]$	$0^1 44^{1672} 45^{3872} 46^{5104} 47^{6072} 48^{8184} 49^{8624} 50^{9328} 51^{8008} 52^{5280} 53^{2728} 54^{176}$
$[66,5]$	$0^1 53^{1408} 54^{2024} 55^{3872} 56^{4664} 57^{6512} 58^{9416} 59^{8624} 60^{7304} 61^{7304} 62^{4048} 63^{2816} 64^{792} 65^{264}$
$[77,5]$	$0^1 63^{2200} 64^{2904} 65^{4576} 66^{5984} 67^{6160} 68^{6512} 69^{8888} 70^{7920} 71^{5456} 72^{4488} 73^{2640} 74^{880} 75^{264} 76^{176}$
$[80,5]$	$0^1 65^{960} 66^{2368} 67^{3456} 68^{4832} 69^{5696} 70^{6784} 71^{7168} 72^{8600} 73^{6848} 74^{5312} 75^{4096} 76^{1936} 77^{704} 78^{128} 79^{128} 80^{32}$
$[88,5]$	$0^1 72^{1496} 73^{2552} 74^{2816} 75^{4136} 76^{5632} 77^{7040} 78^{7392} 79^{7568} 80^{6512} 81^{5984} 82^{3608} 83^{2552} 84^{1232} 85^{440} 86^{88}$
$[99,5]$	$0^1 82^{1936} 83^{2992} 84^{3608} 85^{5984} 86^{5016} 87^{6072} 88^{7568} 89^{5808} 90^{6248} 91^{5720} 92^{3960} 93^{2288} 94^{968} 95^{440} 96^{440}$
$[110,5]$	$0^1 91^{1320} 92^{2464} 93^{2992} 94^{2904} 95^{4136} 96^{6864} 97^{7568} 98^{6248} 99^{7040} 100^{5192} 101^{4576} 102^{2728} 103^{2464} 104^{1496} 105^{616} 106^{352} 107^{88}$
$[121,5]$	$0^1 101^{1584} 102^{3696} 103^{3256} 104^{4488} 105^{3960} 106^{5368} 107^{6072} 108^{6072} 109^{7392} 110^{5368} 111^{3696} 112^{3520} 113^{2112} 114^{1232} 115^{1056} 116^{176}$
$[132,5]$	$0^1 110^{1320} 111^{1848} 112^{3520} 113^{3080} 114^{3784} 115^{4664} 116^{5808} 117^{5984} 118^{5896} 119^{6248} 120^{5456} 121^{4048} 122^{2992} 123^{1496} 124^{1672} 125^{1144} 126^{88}$

i	A_i
0	1
19	1088
20	1056
21	1088
22	1600
23	1344
24	384

The weight distributions of the remaining codes from Table 1 are given in Table 2.

The next two sections of this paper present a geometrical interpretation of the small dimensional codes found during the search for good QC codes.

3 A geometric description of linear codes

Let a linear code $[n,k,d]_q$ be described by a generator matrix G. The columns of G can be seen as points in projective space $PG(k-1,q)$. For every point $P \in PG(k-1,q)$ (=1-dimensional subspace of $\mathbb{F}_q^k$) denote by $w(P)$ the number of times P appears as a column of G. It follows that G may be described as a weight function

$$w : PG(k-1,q) \longrightarrow \{0,1,2,\ldots\}.$$

Conversely any such weight function will give a generator matrix G of a q-ary code $\mathcal{C}$ of dimension $\leq k$ and length $n = \sum_P w(P)$. The dimension of $\mathcal{C}$ will be $= k$ if and only if the points P with nonzero weight are not contained in a hyperplane. If all weights are 0 or 1, the code is called **projective.** Denote the rows of G by $v_1, v_2, \ldots, v_k$. A typical nonzero element of $\mathcal{C}$ is a linear combination $v = \sum_{i=1}^{k} \lambda_i v_i$, where the coefficients are not all 0. Word v vanishes at a certain coordinate if and only if the dot product of $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ and the point describing that column of G is 0, equivalently if this point of $PG(k-1,q)$ is contained in the hyperplane $(\lambda_1, \lambda_2, \ldots, \lambda_k)^{\perp}$. We see that $wt(v) = n - \sum_P w(P)$, where P varies over the hyperplane $(\lambda_1, \lambda_2, \ldots, \lambda_k)^{\perp}$. This motivates the following:

Definition 1 *Let*

$$w : PG(k-1,q) \longrightarrow \{0, 1, 2, \ldots\}$$

be a weight function. Define the **mass** *of w as the sum $\sum w(P)$, where the sum is over all $P \in PG(k-1,q)$. For every hyperplane $H \subset PG(k-1,q)$ define*

$$w(H) = \sum_{P \in H} w(P).$$

We have seen the following:

Lemma 1 *Let*

$$w : PG(k-1,q) \longrightarrow \{0, 1, 2, \ldots, n\}$$

be a weight function such that $w(H) < mass(w)$ for every hyperplane H of $PG(k-1,q)$. Then the construction discussed above yields a code $[n,k,d]_q$, where $n = mass(w)$ and $d = n - max_H w(H)$.

It is clear that every q-ary code may be described in this way. We may also describe the weight distribution of the code in this geometrical language. In fact, $A_i/(q-1)$ is the number of hyperplanes H satisfying $n - w(H) = i$, for every $i > 0$. This geometrical language is particularly profitable in the description of low-dimensional codes.

4 Codes related to conic sections

We work in the projective plane $PG(2,q)$ for odd q and use homogeneous coordinates. Points are therefore written as $(x : y : z)$, lines as $[a : b : c]$, and point $(x : y : z)$ is on line $[a : b : c]$ if and only if the dot product $xa + yb + zc = 0$. Our conic section will be $\mathcal{Q} = V(Y^2 - XZ)$, that is the set of all points $(x : y : z)$ satisfying $y^2 = xz$. It is clear that there are $q+1$ such points, more precisely

$$\mathcal{Q} = V(Y^2 - XZ) = \{(0 : 0 : 1)\} \cup \{(1 : y : y^2) \mid y \in \mathbb{F}_q\}.$$

Put $P_\infty = (0 : 0 : 1), P_y = (1 : y : y^2)$. As matrices

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & y_1 & y_2 \\ 1 & y_1^2 & y_2^2 \end{pmatrix},$$

and

$$\begin{pmatrix} 1 & 1 & 1 \\ y_1 & y_2 & y_3 \\ y_1^2 & y_2^2 & y_3^2 \end{pmatrix},$$

have nonzero determinants when the y_i are pairwise different, we have that no three points of $\mathcal{Q}$ are collinear. In particular there are at most three types of lines, relative to their behaviour concerning $\mathcal{Q}$: **secants** (two points in common with $\mathcal{Q}$), **tangents** (containing one point from $\mathcal{Q}$) and **exterior lines.** Clearly the number of secants is $\binom{q+1}{2}$. As every point of $PG(2,q)$ is on precisely $q+1$ lines and every point of $\mathcal{Q}$ is on q secants, we see that every point of $\mathcal{Q}$ is on precisely one tangent. The number of tangents is therefore $q+1$. It follows that the number of exterior lines is $\binom{q}{2}$. Let t_P be the tangent through $P \in \mathcal{Q}$. We have

$$t_\infty = [1:0:0] \text{ and } t_y = [y^2 : -2y : 1].$$

It is simple to determine the intersections of the tangents:

$$t_\infty \cap t_y = (0:1:2y), t_y \cap t_{y'} = (1:(y+y')/2 : yy').$$

Assume three tangents meet in a common point. This would mean that $(1 : (y + y')/2 : yy') \in t_{y''}$, or

$$0 = y''^2 - y''(y+y') + yy' = (y''-y)(y''-y'),$$

which is impossible since y, y', y'' were chosen as different. We conclude that there are three types of points in $PG(2,q)$ with respect to their position relative to $\mathcal{Q}$: points of $\mathcal{Q}$, **exterior points** (on precisely 2 tangents) and **interior points** (on no tangent at all). In fact, we have seen that no point off $\mathcal{Q}$ is on more than 2 tangents. That such a point cannot be on precisely one tangent follows from a trivial parity argument. As we have $q+1$ tangents and each contains q exterior points we see that there are precisely $(q+1)q/2$ exterior points. It follows that the number of interior points must be $\binom{q}{2}$. Let us determine the exterior points explicitly: these are the points $(0:1:2y)$ with arbitrary y, and the points which can be written $(1:(y+y')/2 : yy')$, where $y \neq y'$. The point $(1:v:w)$ is exterior if and only if we can find $y \neq y'$ such that $y+y' = 2v, yy' = w$. Eliminating y' from the first equation we arrive at a quadratic equation for y, which after completing the square becomes $(y-v)^2 = v^2 - w$. It follows that $v^2 - w$ must be a square. $v^2 - w = 0$ is not possible as this would lead to $y = y' = v$, violating the condition $y \neq y'$. Each square $v^2 - w$ gives 2 solutions. This provides a complete description.

Lemma 2 *A point $(x:y:z)$ is an exterior point of $\mathcal{Q}$ if and only if $y^2 - xz$ is a nonzero square. It is interior if $y^2 - xz$ is a non-square.*

It is now a trivial counting problem to find the distribution of types of points on types of lines:

Lemma 3 *Every secant has $(q-1)/2$ exterior points and $(q-1)/2$ interior points. Each tangent has q exterior points and no interior points. Each exterior line has $(q+1)/2$ exterior points and equally many interior points.*

This suffices to allow the construction of some good 3-dimensional codes. Take all interior points and one point of $\mathcal{Q}$ as columns of a generator matrix. We obtain a code of length $\binom{q}{2}+1$. Every line (=hyperplane) intersects our point set in $\leq (q+1)/2$ points (see Lemma 3). It follows that $d = \binom{q}{2} + 1 - (q+1)/2 = (q-1)^2/2$.

Theorem 1 *Let $\mathcal{Q}$ be a quadric (conic section) in $PG(2,q), q$ odd. The set of interior points together with one point of $\mathcal{Q}$ defines a code*

$$[\binom{q}{2} + 1, 3, (q-1)^2/2]_q.$$

For $q = 9$ we obtain a $[37, 3, 32]_9$ code, which corresponds to an extension of the first 3-dimensional code in Section 2. If we use all interior points and all points of $\mathcal{Q}$ the following is obtained:

Theorem 2 *Let $\mathcal{Q}$ be a quadric (conic section) in $PG(2,q), q$ odd. The set of interior points together with the points of $\mathcal{Q}$ define a code*

$$[\binom{q+1}{2} + 1, 3, (q^2-1)/2]_q.$$

The constructions of Theorems 1 and 2 are not new. In geometrical language they can be found in unpublished work by Barlotti [2]. If $q = p$ is an odd prime, then the constructions of these theorems are optimal. This was proved by Ball [1]. This statement is not true for odd prime-powers in general. In fact, a code $[48, 3, 42]_9$ was constructed by Mason [12]. An advantage of our explicit construction is that we obtain generic generator matrices. In the case of the first family the columns of a generator matrix can be chosen as $(0,0,1)^t$ and all $(1,y,z)^t$, where $y^2 - z$ is a non-square. Other interesting codes of higher dimension can be obtained via concatenation. We concentrate on the quadratic case. Use the Q-ary code from one of our families, where $Q = q^2$, and concatenate with the code $[q+1, 2, q]_q$. This gives the following codes:

Theorem 3 *q-ary codes with the following parameters exist for all odd q :*

$$[(q+1)(\binom{q^2}{2} + 1), 6, q(q^2-1)^2/2]_q$$

and

$$[(q+1)(\binom{q^2+1}{2} + 1), 6, q(q^4-1)/2]_q.$$

In the ternary case we obtain optimal codes $[148, 6, 96]_3$ and $[184, 6, 120]_3$. Codes with these parameters were first constructed by Boukliev and Gulliver, respectively. Even in the $\mathbb{F}_5$-case this is not completely uninteresting. The first family yields a $[1806, 6, 1440]_5$ code of Griesmer defect 4.

References

[1] S. Ball: *Multiple blocking sets and arcs in finite planes, Journal of the London Mathematical Society* **54** (1996), 581–593.

[2] A. Barlotti: *Some topics in finite geometrical structures, Institute of Statistics, University of Carolina, Mimeo Series* **439** (1965).

[3] E.R. Berlekamp: *Algebraic Coding Theory*, McGraw-Hill, New York 1968.

[4] A.E. Brouwer: Minimum distance bounds for linear codes over $\mathbb{F}_9$, lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, the Netherlands.

[5] R.N. Daskalov and T.A. Gulliver: *New good quasi-cyclic ternary and quaternary linear codes, IEEE Trans. Inform. Theory* **43** (1997) 1647–1650.

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

[7] T.A. Gulliver and V.K. Bhargava: *Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4), IEEE Trans. Inform. Theory* **38** (1992) 1369–1374.

[8] T.A. Gulliver: *New optimal ternary linear codes, IEEE Trans. Inform. Theory* **41** (1995), 1182–1185.

[9] T.A. Gulliver and V.K. Bhargava: *New good rate (m-1)/pm ternary and quaternary quasi-cyclic codes, Designs, Codes and Crypt.* **7** (1996) 223–233.

[10] T.A. Gulliver and V.K. Bhargava: *Some optimal nonbinary power residue codes,* (submitted).

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

[12] J.R.M. Mason: *On the maximum sizes of certain (k, n) arcs in finite projective geometries, Math. Proc. Cam. Phil. Soc.* **91** (1982) 153–161.

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

(Received 1/4/99)